INTERNATIONAL LAW AND CYBERSPACE

Report of the Study Group co-organised by the University of Bologna, University of Milan and University of Westminster

February 2021

Ministry of Foreign Affairs
and International Cooperation

This Report is realized with the support of the Policy Planning Unit of the Ministry of Foreign Affairs and International Cooperation pursuant to Art. 23bis of Presidential Decree 18/1967.

The options contained in this Report are solely those of the authors and do not necessarily reflect the opinions of the Ministry of Foreign Affairs and International Cooperation, the University of Bologna, the University of Milano or the University of Westminster.

MEMBERS OF THE STUDY GROUP

- Prof. Attila Tanzi (University of Bologna): Principal Investigator
- Prof. Angelica Bonfanti (University of Milan): Unit coordinator
- Prof. Chiara Ragni (University of Milan): Unit coordinator
- Prof. Marco Roscini (University of Westminster): Unit coordinator
- Prof. Federico Casolari (University of Bologna)
- Dr Ludovica Chiussi (University of Bologna)
- Dr Gian Maria Farnelli (University of Bologna)
- Dr Niccolò Lanzoni (University of Bologna)
- Dr Alessandra Sardu
- Ms Valentina Anemoni (University of Bologna)
- Mr Marco Argentini (University of Bologna)
- Mr Daniele Mandrioli (University of Milan)

TABLE OF CONTENTS

REPORT ON INTERNATIONAL LAW AND CYBERSPACE

1 The protection of sovereignty in cyberspace 1
1.1 The "sovereignty as a rule debate". 2
1.2 The application of the principle of territorial sovereignty. 2
1.3 The assets upon which sovereignty shall be exercised. 5
1.4 The identification of the actions that can amount to a violation of sovereignty 6
1.5 'Technology neutrality' and cyberspace 9
1.6 Literature 10
1.7 Review of national and international positions 10
1.7.1 Entities and States making reference to the dual nature of technology and to the need that the approach remains technology neutral 11
1.7.2 Entities and States making reference to the relationship between cyber war and the law of neutrality .. 13

2 The application of the Law of States Responsibility to activities in the cyberspace 15
2.1 Attribution 15
2.1.1 The Three Types of Attribution of Cyber-attacks 15
2.1.2 Evidentiary Issues 17
2.1.3 Review of National Positions 17
2.2 Due diligence 27
2.2.1 Issues not debated 28
2.2.2 Issues still under debate 28
2.2.3 Review of national positions 30
2.3 Countermeasures 36
2.3.1 Issues not debated 37
2.3.2 Issues still under debate 38
2.3.3 Review of national positions 40

3 The application of International Humanitarian Law to activities in the Cyberspace 46
3.1 Cyber operations and Article 2(4) of the UN Charter 46
3.1.1 Review of national positions 46
3.2 Cyber operations and the exercise of self-defence by states 50
3.2.1 Review of national positions 51
3.3 Cyber operations and the principle of non-intervention in the internal affairs of other states 58
3.3.1 Review of national positions 59
3.4 Cyber operations and the application of the law of armed conflict 64
3.4.1 Review of national positions 65
3.5 Cyber operations and the definition of 'attack' under Article 49(1) of the 1977 Protocol I additional to the 1949 Geneva Convention on the Protection of Victims of War 68
3.5.1 Review of national positions 69
3.6 Cyber operations and the law of neutrality 71
3.6.1 Review of national positions 71

4 The application of International Disaster Law to activities in the cyberspace 72
4.1 Normative aspects concerning IDL in cyber space 73
4.2 Relevant examples of regional efforts in reducing the risks of cyber disasters (European Union) 75

5 The role of private stakeholders in cyberspace 77
5.1 Review of National Positions 77
5.2 Comments to the initial OEWG Pre-Draft Report (April 2020) 80
5.2.1 OEWG Initial Pre-Draft Report and Italian comments thereto 80
5.2.2 Comments by EU and EU Member States 81
5.2.3 Comments by other States 83
5.2.4 OEWG Second Pre-Draft Report 86

6 International cooperation in the cybersecurity domain 87
6.1 Issues not debated 87
6.2 Issues still under debate 88
6.2.1 Preference for regional or global cooperation 88
6.2.2 New institutional framework 88
6.3 Review of National Positions 89

6.4 Comments to the initial OEWG Pre-Draft Report (April 2020) *92*
6.4.1 OEWG Initial Pre-Draft Report and Italian comments thereto 92
6.4.2 Comments by EU and EU Member States 101
6.4.3 Comments by other States 110
6.4.4 OEWG Second Pre-Draft Report 115

PROPOSAL FOR THE ITALIAN POSITION

1 Introduction 119
1.1 The protection of sovereignty in cyberspace and violations of the principle of non-intervention 120
1.2 'Technology neutrality' and cyberspace 122
2 The application of the Law of States Responsibility to activities in the cyberspace 122
2.1 Attribution 122
2.2 Due diligence 124
2.3 Countermeasures 126
3 Cyber Operations and the Use of Force 128
3.1 Cyber operations and Article 2(4) of the UN Charter 128
3.2 Cyber operations and the exercise of self-defence by states 128
3.3 Cyber operations and the application of International Humanitarian Law 130
3.4 Cyber operations and the definition of 'attack' under Article 49(1) of the 1977 Protocol I additional to the 1949 Geneva Convention on the Protection of Victims of War 131
3.5 Cyber operations and the law of neutrality 133
4 Human rights in cyberspace 134
4.1 The application of the international human rights law 134
5 The application of International Disaster Law to activities in the cyberspace 135
6 The role of private stakeholders in cyberspace 135
7 International cooperation in the cybersecurity domain 136

REPORT ON INTERNATIONAL LAW AND CYBERSPACE

1 The protection of sovereignty in cyberspace

1. States have agreed that international law, including the principle of sovereignty, applies to cyberspace (GGE Report 2013, UN Doc A/68/98; GGE Report, A/70/174). More precisely, in the GGE Report A/70/174 it is stated that "The international norms and principles that flow from State sovereignty apply to the use of ICT by States and to their territorial jurisdiction over ICT infrastructure" (GGE Report, A/70/174, 22 July 2015, §§ 27-28).

2. In their national positions, States have basically reaffirmed what was previously stated on the application of the principle of sovereignty to cyberspace in the aforementioned Report. Some of them have also provided definitions of the principle of sovereignty. For instance, The Netherlands considers that both the internal and external aspects of sovereignty apply in cyberspace (The Kingdom of Netherlands, "Appendix: International law in cyberspace", p. 2, hereinafter "Netherlands' National Position"). The same approach is endorsed also in the Tallinn Manual, which defines internal sovereignty in Rule 2 ("A State enjoys sovereign authority with regard to the cyber infrastructure, persons, and cyber activities located within its territory, subject to its international legal obligations"), and external sovereignty in Rule 3 ("A State is free to conduct cyber activities in its international relations, subject to any contrary rule of international law binding on it"). Finland considers sovereignty as "a foundational principle of the international legal order", which "confers each State the exclusive right to exercise the functions of a State within a certain territory, and protects its territorial integrity and political independence from interference by other States" (Finland, "International law and cyberspace", p. 1, hereinafter "Finland's National Position"). In more general terms, New Zealand defines the principle of sovereignty as that prohibiting "the interference by one state in the inherently governmental functions of another and prohibits the exercise of state power or authority on the territory of another state" (New Zealand, "The Application of International Law to State Activity in Cyberspace", §14, hereinafter "New Zealand's National Position").

3. These definitions use partially different terms to identify the notion of sovereignty, but they converge on the essential contents of this notion. On the contrary, there is disagreement on two main issues, i.e. the so called "sovereignty as a rule debate", and the application of the principle of territorial sovereignty in cyberspace.

1.1 *The "sovereignty as a rule debate".*

4. With regard to the first issue, i.e. the so called "sovereignty as a rule debate", the controversial point is whether sovereignty should be considered only as a principle, from which legal rules are derived, or as a discreet binding rule of international law. The United Kingdom has favored the former approach. More specifically, during his speech "Cyber and International Law in the 21st Century", the Attorney General Jeremy Wright claimed that, despite the fact that sovereignty is fundamental to the international rules-based system, it is not possible to "extrapolate from that general principle a specific rule or additional prohibition for cyber activity beyond that of a prohibited intervention. The UK Government's position, therefore, is that there is no such rule as a matter of current international law". Following this reasoning, the cyber intrusions below the threshold of the non-intervention principle can only be considered unfriendly, but they will not constitute a breach of international law. Consequently, in the cyber context sovereignty cannot be considered as a standalone primary rule, but only a fundamental principle of international law that guides the relations among the States.

5. The vast majority of States have expressed a contrary position. Among them, The Netherlands considers that "the respect for sovereignty of other countries is an obligation in its own right, the violation of which may in turn constitute an internationally wrongful act" (Netherlands' National Position, p. 2). Finland also observes that "[a]greeing that a hostile cyber operation below the threshold of prohibited intervention cannot amount to an internationally wrongful act would leave such operations unregulated and deprive the target State of an important opportunity to claim its rights". Consequently, a breach of sovereignty, considered as a primary rule of international law, "amounts to an internationally wrongful act and triggers State responsibility" (Finland's National Position, p. 3).

1.2 *The application of the principle of territorial sovereignty.*

6. With regard to the second issue, i.e. the application of the principle of territorial sovereignty in cyberspace, it is necessary to clarify some aspects. As The Netherlands observed, in the physical realm the principle of sovereignty "has legal effect through the prohibition on the use of force, through the rule of non-intervention and also through a standalone rule of territorial sovereignty". It is precisely the existence and the applicability in cyberspace of the principle of territorial sovereignty that has been questioned. This happens especially because cyberspace

has some peculiar features. More precisely, it contains "a virtual element which has no clear territorial link" (New Zealand's National Position, §13), and that consequently makes it difficult the application by analogy of the principle of territorial sovereignty. Indeed, in the physical realm, the actions that can constitute violations of the principle of territorial sovereignty are typically conducted through physical incursions into another state's territory and, more generally, the exercise of jurisdiction on foreign territory (Finland's National Position, p. 2). Unlike in the analogue context, in cyberspace "the concepts of territoriality and physical tangibility are often less clear" (Netherlands' National Position, p. 2).

7. However, while acknowledging the existence of relevant differences between the physical and cyber realms, the majority of States believe that the principle of territorial sovereignty is applicable to the latter. It is still unclear at present how it shall apply in cyberspace, especially because - as New Zealand pointed out - "further state practice is required for the precise boundaries of its application to crystallize" (New Zealand's National Position, §12). In the national positions until now expressed, no particular attention is given to this aspect.

8. Two main answers have been provided to the question of when a state-sponsored cyber operation is in breach of another state's sovereignty. The first takes into consideration the "physical violations", i.e. the activities executed by a state agent physically present on the territory of the victim state, the second considers the "remote violations", i.e. the operations that are carried out from outside the territory of the victim state but that produce effects in the territory of the latter. The first approach is endorsed, for instance, in the Tallinn Manual, where the experts agreed that, in the cyber context, "it is a violation of territorial sovereignty for an organ of a State, or others whose conduct may be attributed to the State, to conduct cyber operations while physically present on another State's territory against that State or entities or persons located there" (Tallinn Manual, p. 19). The second approach is endorsed by New Zealand and France. France contends that a hostile cyber operation against French cyber infrastructure or one causing effects on French territory violates French sovereignty (France, "International Law Applied to Operations in Cyberspace", p. 7). New Zealand defines territorial sovereignty as the principle that "prohibits states from using cyber means to cause significant harmful effects manifesting on the territory of another state" (New Zealand's National Position, §14). However, this would not imply that every unauthorized intrusion into a foreign ICT system or every cyber activity which has effects on the territory of another state are prohibited, since "[t]here is a range of circumstances – in addition to pure espionage activity – in which an unauthorized cyber intrusion, including one causing effects on the territory of another state,

would not be internationally wrongful. For example, New Zealand considers that the rule of territorial sovereignty as applied in the cyber context does not prohibit states from taking necessary measures, with minimally destructive effects, to defend against the harmful activity of malicious cyber actors" (New Zealand's National Position, §14).

9. Alongside the rights deriving from the principle of sovereignty, some States have also tried to explore the legal obligations deriving from it. This is the case of France, which underlines the need to respect the due diligence requirement. More precisely, it says that the territory of a State cannot be used for internationally wrongful acts using ICTs, and that "this is a customary obligation for States, which must (i) use cyberspace in compliance with international law, and in particular not use proxies to commit acts which, using ICTs, infringe the rights of other States, and (ii) ensure that their territory is not used for such purposes, including by non-state actors" (France's National Position, p. 6).

10. Italy shall restate what previously affirmed in the 2015 GGE Report, i.e. that "The international norms and principles that flow from State sovereignty apply to the use of ICT by States and to their territorial jurisdiction over ICT infrastructure"

11. It is also advisable to consider both the internal and external aspects of sovereignty, following the approach of the Tallinn Manual.

12. Furthermore, it is advisable to consider the principle of sovereignty as a primary rule of international law, whose violation amounts to an international wrongful act, and to consider it also in cyberspace as a principle distinct from the prohibition of the use of force and the principle of non-intervention. Even if it is not possible at present to analyze precisely the boundaries of this question given the absence of state practice, this approach seems to be preferable taking into account the possible consequences that could derive from the non-recognition of the principle of sovereignty as a primary rule, i.e. the impossibility for the target State to claim its rights in a wide range of situations below the threshold of prohibited intervention, including the adoption of countermeasures.

13. The principle of territorial sovereignty should also encompass both "physical violations", i.e. activities executed by a state agent unlawfully present on the territory of the victim state, and "remote violations", i.e. operations that are carried out from outside the territory of the victim state but that produce effects in the territory of the latter. Indeed, considering that both are

relevant in cyberspace, it does not make sense to limit the scope of application of the principle of territorial sovereignty exclusively to one of them.

1.3 *The assets upon which sovereignty shall be exercised*

14. Another controversial point is represented by the identification of the assets upon which sovereignty can effectively be exercised taking into account the features of cyberspace.

15. First of all, it has to be acknowledged that cyberspace is a global domain that can be assimilated to the high seas, to the international airspace or the outer space. Some scholars have suggested to include it in the category of the "global commons". This means concretely, as Finland specifies, that "cyberspace as a whole cannot be subject to appropriation by any State" (Finland's National Position, p. 1). This view is also shared in the Tallinn Manual, where it is said that "no State may claim sovereignty over cyberspace per se" (Tallinn Manual 2.0, p. 13).

16. Bearing this consideration in mind, it is nevertheless necessary to identify the assets located in the territory of each State upon which sovereignty can be exercised. From this perspective, it can be observed that each State has adopted a different approach. France, for instance, has chosen a vague definition stating that it exercises its sovereignty "over the information systems located on its territory" (France's National Position, p. 6). In a footnote, it specifies that "information system" shall include "equipment and infrastructure located on national territory, connected objects, logical components and content operated or processed via electronic communication networks which cover the national territory or from an IP address attributed to France, domains belonging to national registers" (France's National Position, p. 6). Finland has adopted a different definition, saying that "each State has jurisdiction over the cyber infrastructure and the persons engaged in cyber activities within its territory" (Finland's National Position, p. 1). It does not provide a definition of "cyber infrastructure". However, this is a frequently used word in the conspicuous literature on this topic, which means that definitions can easily be found in several texts. The Netherlands went even further by referring to the definition provided in the Tallinn Manual 2.0, which adds the "logical layer" (i.e. the connections that exist between network devices, i.e. applications, data and protocols that allow the exchange of data across the physical layer) to the "physical layer" (referring to the network components, such as hardware and other infrastructure, such as cables, routers, servers and computers) and the "social layer" (individuals and groups engaged in cyber activities) (Tallinn Manual 2.0, p. 12). More precisely, according to The Netherlands "States have exclusive

authority over the physical, human and immaterial (logical or software-related) aspects of cyberspace within their territory" (Netherlands' National Position, p. 2). In concrete terms, this would allow States within their territory "to set rules concerning the technical specifications of mobile networks, cybersecurity and resilience against cyberattacks, take measures to combat cybercrime, and enforce the law with a view to protecting the confidentiality of personal data. In addition, they may independently pursue foreign cyber policy and enter into treaty obligations in the area of cybersecurity".

17. The most complete position among those listed above seems to be that expressed by The Netherlands and the Tallinn Manual. It is advisable for Italy to adopt a similar position, especially taking into account that the element labelled as "immaterial aspect" (which corresponds to what is called "logical layer" in the Tallinn Manual) is going to have greater importance in cyberspace, and consequently cannot be neglected.

18. Another point needs to be analyzed, i.e. whether a State is entitled to exercise jurisdiction within its territory over assets that enjoy sovereign immunity. In the Tallinn Manual, it is admitted that "customary or treaty law may restrict the exercise of sovereign rights by the territorial State", such as those relating to immunity. Rule 5 of the Manual provides that "[a]ny interference by a State with cyber infrastructure aboard a platform, wherever located, that enjoys sovereign immunity constitutes a violation of sovereignty". The same position is adopted by The Netherlands, which affirms that the exclusive jurisdiction of the states over persons, property and events within their territory shall be exercised "within the limits of their obligation under international law, such as those relating to diplomatic privileges and immunity, and those arising from human rights conventions" (Netherlands' National Position, p. 2)

19. The position expressed by The Netherlands and the Tallinn Manual can be shared, and Italy should mention among the limits imposed by international law both the norms pertaining to diplomatic privileges and immunity and those arising from human rights conventions.

1.4 *The identification of the actions that can amount to a violation of sovereignty*

20. The last aspect that needs to be clarified is the identification of the actions which can amount to a violation of the sovereignty. As The Netherlands has correctly pointed out, there are several difficulties in identifying such conduct in cyberspace since the traditional concept of sovereignty has a "firmly territorial and physical connotations" and has "traditionally been

aimed at protecting a state's authority over property and persons within its own national borders".

21. In the physical realm, the exact borders of this principle have been defined by the International Court of Justice. Finland has summarized this case-law observing that "[t]he International Court of Justice has consistently confirmed that it is a duty of every State to respect the territorial sovereignty of others. This applies to unauthorized intrusions to physical spaces such as overflight of a State's territory by an aircraft belonging to another State or under its control (ICJ, Nicaragua v. US), penetration of territorial waters by foreign warships (ICJ, Corfu Channel case), conducting of certain activities in another State's territory without its consent (ICJ, Costa Rica v. Nicaragua), but also to producing effects in another State's territory without physical intrusion (ICJ, Nuclear Tests)" (Finland's National Position, p. 2).

22. It is clear that a transposition tout court of this case-law to the cyber context is not possible, since "[i]n cyberspace, the concepts of territoriality and physical tangibility are often less clear" (Netherlands' National Position, p. 2).

23. Some possible approaches to solve this issue have been suggested. This is the case of Finland, which has stated that, similarly to what happens in the physical realm, "a non-consensual intrusion in the computer networks and systems that rely on the cyber infrastructure in another State's territory may amount to a violation of the State's sovereignty". This non-consensual intrusion should cause "material harm to the cyber infrastructure", "a loss of functionality or the equipment relying on it", "modifies or deletes information belonging to the target State", or "interfere[] with data or services that are necessary for the exercise of inherently governmental functions". In an attempt to define the boundaries of sovereignty in cyberspace, The Netherlands endorses Rule 4 of the Tallinn Manual 2.0 (Netherlands' National Position, p. 3). This Rule establishes that "[a] State must not conduct cyber operations that violate the sovereignty of another State" (Tallinn Manual 2.0, p. 17 ss.). In the commentary to this Rule, the Group of Experts who drafted the Manual determined a violation of sovereignty on two bases, i.e. the degree of infringement upon the target State's territorial integrity, and the interference with or the usurpation of inherently governmental functions (Tallinn Manual 2.0, p. 20). As to the first basis, the Experts agreed that cyber operations constitute a violation of sovereignty in the event they result in "physical damage or injury", or if they cause "loss of functionality of cyber infrastructure located in another State". No consensus was achieved on whether to consider cyber operations that results in neither physical damage nor loss of functionality should be considered as violations of sovereignty. Some cases in point were

considered. Among these, there were "the altering or deleting data stored in cyber infrastructure" and the "emplacing malware into a system". As to the second basis, the Experts agreed that "a violation of sovereignty occurs … when one State's cyber operation interferes with or usurps the inherently governmental functions of another State". This is mainly due to the fact that "the target State enjoys the exclusive right to perform them, or to decide upon their performance". The Experts did not define the concept of "inherently governmental functions", but gave some examples such as the "changing and deleting data such that it interferes with the delivery of social services, the conduct of the elections". This, however, is problematic, as the notion of 'inherently governmental functions is a subjective one and might change from state to state.

24. In the Italian position, it could be sufficient to restate that a State must not conduct cyber operations that violate the sovereignty of another State. Italy, however, might prefer to further clarify the situations where this occur by including cyber operations resulting in physical damage to property or persons, loss of functionality of infrastructures, and any authorized intrusion into computer systems and servers located on the territory of another state.

25. Other aspects that should be investigated are the gravity of a certain breach of sovereignty should be assessed, on what elements the decision to respond should be based, and what kind of response may be adopted. In this regard, France prefers a case-by-case approach and affirms that "[t]he gravity of a breach of sovereignty will be assessed on a case-by-case basis in accordance with French cyberdefence governance arrangements in order to determine possible responses in compliance with international law" (France's National Position, p. 7). It also emphasises that "the decision whether or not to respond to such operations is a political one, taken in the light of the nature and characteristics of the intrusion" and that "the response, chosen from among the range of options offered by international law, depends, subject to an appropriateness assessment, on the gravity of the breach of sovereignty" (France's National Position, p. 7).

26. At present, the approach endorsed by France is sufficiently balanced, and a case-by-case approach seems to be the preferable option. The decision whether or not to respond is rightly qualified as a political one, and it is also correct to affirm that a possible response, to be chosen among the options allowed by international law, depends on the gravity of the breach.

1.5 *'Technology neutrality' and cyberspace*

27. The expression "technology neutrality" can be ambiguous: a number of different meanings might be identified:

    i. The neutrality (*ie*, the dual-use) of technology;

    ii. The relationship between cyber war and the law of neutrality;

    iii. The freedom of individuals and organizations to choose the most appropriate and suitable technology to their needs and requirements;

    iv. In the framework of international trade law:

    v. «a designed technical standard should focus on the result to be achieved to avoid externalities and market operators should be free to adopt the technology they deem most appropriate to achieve the defined result»;[1]

    vi. «the same principles or rules should apply to all technologies and/or should apply regardless of the technology used in a specific case»;[2]

    vii. «regulators should abstain from using their regulatory powers to push the market in a specific direction, which they may consider 'optimal'».[3]

28. For the purposes of our analysis, we refer to the meaning sub a) mainly. However, references to literature and national and international positions are also provided on the other potential meanings.

29. In particular, the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, the European Union and the Open-Ended Working Group have addressed technology neutrality and the dual-use of technology as one of the pillars of the debate on the application of rules of international responsibility in cyber space.

[1] Gabriele Gagliani, "Cybersecurity, Technological Neutrality, and International Trade Law", *Journal of International Economic Law* (2020), 23: 723-745, p. 731.
[2] *Ibid*.
[3] *Ibid*.

30. Accordingly, it is suggested that Italy, too, expresses its position of the issue, aligning itself to the position expressed by the European Union.

1.6 *Literature*

31. There are few contributions focusing on the neutrality of technology:

> Nella società civile è gradualmente aumentata la percezione che l'utilizzo irresponsabile delle tecnologie da parte degli Stati può avere degli effetti devastanti per i cittadini. Attraverso lo slogan «There is no peace without digital peace» si è esplicitata la volontà dei cittadini digitali di poter "vivere" in un Internet neutrale e demilitarizzato.[4]

32. Non-profit organizations such as the TOR-project, Anonymous or CCC, as well as thematic pressure groups such as Bits of Freedom, Privacy First or the Electronic Frontier Foundation will pursue political and/or ideological goals. Their cyber activities will be more focussed upon freedom of expression, free Internet, net neutrality, privacy, etc. Cyber may be at the heart of their strategic values, or may offer leverage as a vector or medium for their activities.[5]

33. In adding some flesh to the bones of this statement the [Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security] highlighted the 'dual use' character of cyberspace. Indeed, the notion that the Internet is 'neutral' so that the use to which it is put and the consequences of this are dependent upon the intent of its user is a recurring theme of resolutions of the UNGA.[6]

1.7 *Review of national and international positions*

34. Those States and entities which have already expressed their position on "technology neutrality" have referred to either to the meaning *sub* a) or *sub* b) (*supra*, para. 1).

---

[4] Alessandra Sardu, "L'*international cybersecurity law*: lo stato dell'arte", *La Comunità Internazionale* (2020), 1: 5-42, p. 35.
[5] Paul Ducheine, "The notion of cyber operations", in Nicholas Tsagourias and Russell Buchan (Eds.), *International Law and Cyberspace. Research Handbooks in International Law,* Elgar, Cheltenham (2015): 465-490, p. 217.
[6] Christian Henderson, "The United Nations and the regulation of cyber-security", in Nicholas Tsagourias and Russell Buchan (Eds.), *International Law and Cyberspace. Research Handbooks in International Law,* Elgar, Cheltenham (2015): 465-490, p. 476.

1.7.1 *Entities and States making reference to the dual nature of technology and to the need that the approach remains technology neutral*

35. On the one hand, the GGE, the European Union and the OEWG have made reference to the dual nature of technology and to the need that the approach remains technology neutral, as follows:

36. The Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security of 30 July 2010 (A/65/201) reads as follows (§§ 5-6):

> The global network of ICTs has become an arena for disruptive activity. The motives for disruption vary widely, from simply demonstrating technical prowess, to the theft of money or information, or as an extension of State conflict. The source of these threats includes non-State actors such as criminals and, potentially, terrorists, as well as States themselves. ICTs can be used to damage information resources and infrastructures. Because they are inherently dual-use in nature, the same ICTs that support robust e-commerce can also be used to threaten international peace and national security. Thus far, there are few indications of terrorist attempts to compromise or disable ICT infrastructure or to execute operations using ICTs, although they may intensify in the future. At the present time terrorists mostly rely on these technologies to communicate, collect information, recruit, organize, promote their ideas and actions, and solicit funding, but could eventually adopt the use of ICTs for attack.

37. The EU Lines To Take in view of UN OEWG on security & telecommunications in context of international security (31 January 2020) read as follows (§§ 8-9):

> While discussions on emerging technologies are particularly instructive, also on the subject of existing and future threats, it is important to emphasize that technological developments concern both civil and military applications and that technologies related to cyberspace can be of dual nature. As recognized by previous UN GGE reports, given the unique character of ICTs technologies, our approach must remain technology neutral. This is consistent with the concept and UN acknowledgement that existing international law applies to new areas, including the use of emerging technologies.

38. The EU Lines To Take in view of the June 2020 online meetings of the Open-Ended Working Group on developments in the field of information and telecommunications in the context of international security (OEWG) - 15, 17 and 19 June 2020 read as follows (§§ 6-7)

> Currently, the OEWG report underline the unique attributes of ICTs technologies, as well as the dual-use nature of some of them. On different occasions, the EU and its Member States have expressed their position, including under the item "Existing and potential threats", on the dual nature of some ICT technologies. Dual-use technologies, such as ICTs, are technologies that can be used for both civilian and military applications. Such characterization only applies to some ICTs technologies. This should be seen in counter-point to a definition of dual-use as the use of technology for beneficial purposes that can also be misused for harmful purposes. Such a definition is misleading and risks misinterpreting the uniqueness of ICT technologies. Both underscores the importance of maintaining a technology-neutral approach in the course of our work, as recognized by previous UN GGE reports, in order to further advance peace and stability in cyberspace. In the same vein, the EU and its Member States support the notion that measures to promote responsible State behaviour should remain technology-neutral, underscoring that it is the misuse of such technologies, not the technologies themselves, that is of concern. This is consistent with the concept and UN acknowledgement that existing international law applies to new areas, including the use of emerging technologies. The rise of malicious cyber activities, regardless of the emerging or novel nature of malicious activities, is also of concern. Such behaviour undermines and threatens the integrity, security, economic growth, and can lead to destabilising and cascading effects with enhanced risks of conflict.

39. The Second "Pre-draft" of the report of the OEWG on developments in the field of information and telecommunications in the context of international security reads as follows (§ 21):

> States confirmed that measures to promote responsible State behaviour should remain technology-neutral, underscoring that it is the misuse of such technologies, not the technologies themselves, that is of concern. Nonetheless, it was recognized that technological advances and new applications may expand attack surfaces, amplify vulnerabilities in the ICT environment or be leveraged for novel malicious activities. Particular technological trends were highlighted in this regard, including progress in machine learning and quantum computing; the ubiquity of connected

devices (”Internet of Things“); new ways to store and access data through distributed ledgers and cloud computing; and the expansion of big data and digitized personal data.

40. The Comments from Italy on the initial “pre-draft” report of the Open-Ended Working Group on developments in the field of information and telecommunication in the context of international security read as follows (p. 2):

> Without prejudice of the specific mentions of new threats that the section contains, Italy recalls that several interventions have mentioned that technological advances can have a dual-use application and that is one of the main reasons why our approach should focus on States behaviour and remain technological neutral. The report should reflect those interventions that have supported a tech neutral approach also because innovation happens so fast that listing every single potential threat stemming from new advances increases the risk of uncertainty and incompleteness.

1.7.2 *Entities and States making reference to the relationship between cyber war and the law of neutrality*

41. On the other hand, a number of States have made reference to the relationship between cyber war and the law of neutrality, as follows:

42. The Netherlands national position reads as follows (p. 5):

> A key component of IHL is international law on neutrality. Neutrality requires that states which are not party to an armed conflict refrain from any act from which involvement in the conflict may be inferred or acts that could be deemed in favour of a party to the conflict. In its relations with parties to the armed conflict the neutral state is required to treat all parties equally in order to maintain its neutrality. A state may not, for example, deny access to its IT systems to one party to the conflict but not to the other. In its response to the above-mentioned advisory report by the AIV/CAVV, the government noted that, ‘In an armed conflict involving other parties, the Netherlands can protect its neutrality by impeding the use by such parties of infrastructure and systems (e.g. botnets) on Dutch territory. Constant vigilance, as well as sound intelligence and a permanent scanning capability, are required here.’[13]

[13 'Cyber Warfare', Advisory report no 77, AIV/no. 22, CAVV December 2011, p. 26].

43. The France national position reads as follows (p. 16):

> Cyberoperations carried out in the context of an international armed conflict, or which trigger such a conflict, are subject to the law of neutrality[83]. As such, the States party to an IAC may neither carry out cyberoperations linked to the conflict from installations situated on the territory of a neutral State or under the exclusive control of a neutral State, nor take control of computer systems of the neutral State in order to carry out such operations[84]. The neutral State must prevent any use by belligerent States of ICT infrastructure situated on its territory or under its exclusive control. However, it is not required to prevent belligerent States from using its ICT networks for communication purposes[85]. Routing a cyberattack via the systems of a neutral State without any effect on that State does not breach the law of neutrality, which prohibits only the physical transit of troops or convoys. The law of neutrality applies to cyberoperations. Belligerents must refrain from causing harmful effects to digital infrastructure situated on the territory of a neutral State or from launching a cyberattack from such infrastructure.
>
> [83 [A]s in the case of the principles of humanitarian law applicable in armed conflict, international law leaves no doubt that the principle of neutrality, whatever its content, which is of a fundamental character similar to that of the humanitarian principles and rules, is applicable (subject to the relevant provisions of the United Nations Charter) to all international armed conflict, whatever type of weapons might be used", Advisory opinion on the Legality of the Threat or Use of Nuclear Weapons, ICJ Reports 1996, p. 39, § 89 | 84 Article 1 of Convention V respecting the Rights and Duties of Neutral Powers and Persons in Case of War on Land, and of Convention XIII respecting the Rights and Duties of Neutral Powers in Naval War, The Hague, 18 October 1907 | 85 Article 8 of Convention V respecting the Rights and Duties of Neutral Powers and Persons in Case of War on Land, The Hague, 18 October 1907.]

2 The application of the Law of States Responsibility to activities in the cyberspace

2.1 *Attribution*

44. Many Italian partners have addressed attribution as one of the issues to be tackled with regard to application of rules of international responsibility in cyber space.

45. Accordingly, it is suggested that Italy, too, expresses its position on this issue.

46. The attribution of unlawful acts is one of the two elements that make up States' international responsibility regime. The concept of 'attribution of acts' means the possibility of attributing the conduct materially put in place by a subject to a State. In particular, the subject in question can be, formally, an organ of that State; a subject (natural, such as an individual, or legal, such as a company) that, although not formally an organ of the State, actually behaves as such (so-called *de facto* organ); or a subject that, although not a de jure or de facto organ, acts on the basis of some relationship (normally, 'direction and control') with that State.

2.1.1 *The Three Types of Attribution of Cyber-attacks*

47. The attribution of cyber-attacks to States is a complex endeavor, both from a practical and a legal perspective. In particular, the attribution of cyber-attacks can be of three types: a technical attribution, a political attribution and a legal attribution.

48. Technical attribution consists in tracing back cyber-attacks to their source. This attribution is ideally divided into three steps, subsequent and of increasing difficulty: the 'where', that is, the identification of the place(s) (namely, the territory of the State(s)) from which the cyber-attack started; the 'how', that is, the identification of the hardware(s) used in order to launch the cyber-attack; and the 'who', that is, the identification of the subject (individual, company or State's organ) that launched the cyber-attack.

49. Political attribution consists in the self-assessment carried out by the attacked State(s)/ third States(s) on the 'responsible' (in an a-technical and a-legal sense) of cyber-attacks. Political attribution translates into an almost discretionary exercise, free from technical/ legal rules. It may or may not be public. On the one hand, political attribution is claimed by States as a sovereign prerogative; on the other hand, there is general consensus regarding the need that

political attribution should be reasonably supported by factual elements. In this vein, technical attribution can corroborate political attribution.

50. Legal attribution consists in the attribution of cyber-attacks from one State to another in accordance with international law. The great majority of the international Community supports the application of already existing rules on the attribution of acts, instead of the elaboration of *ad hoc* rules to the cyber-space realm. Consequently, the International Law Commission *Draft Articles on the Responsibility of States for Internationally Wrongful Acts* of 2001 (DARSIWAs) apply. The DARSIWAs are a set of provisions which, by themselves, being a soft-law act, have no binding value, but which reflect customary international law on the topic of attribution of conducts to States (see also Rules 15, 16, 17 and 18 of the Tallinn Manual (2nd ed., 2017 and, extensively, Finland, pp. 6-7).

51. In particular, according to the DARSIWAs, different rules will apply depending on the relationship between the State and the subject carrying out the cyber-attack. The rules that shall be taken into account are: Article 4 (*Conduct of organs of a State*), Article 5 (*Conduct of persons or entities exercising elements of governmental authorities*), Article 6 (*Conduct of organs placed at the disposal of a State by another State*), Article 8 (*Conduct directed or controlled by a State*), Article 9 (*Conduct carried out in the absence or default of the official authorities*) and Article 11 (*Conduct acknowledged and adopted by a State as its own*).

52. The most problematic scenario is that depicted by Article 8. In particular, it should be noted that the various 'direction and control' tests recognized in international law practice (the extremely exigent 'effective control' test developed by the International Court of Justice in the *Nicaragua v. United States* case; the more relaxed 'overall control' test (also known as 'Cassese test') developed by the International Criminal Tribunal for the Former Yugoslavia in the *Tadić* case; and the 'direction and control' test – a sort of middle ground between the two – specifically referred to under Article 8) hardly apply to the dynamics behind cyber-attacks. This is because, from a practical point of view, it is extremely difficult to prove the existence of 'direction and control' relationships and, from a legal point of view, none of these tests captures less-tangible relationships – such as mere induction or even financial contribution – that usually characterize States' *modus operandi* when launching cyber-attacks via proxies.

2.1.2 *Evidentiary Issues*

53. Moreover, in a hypothetical diplomatic or judicial scenario, legal attribution should/must be proven. It is important to note that the rules on attribution are different from those on evidence. In particular, the latter are not defined in the DARSIWAs, and vary according to the circumstances and judicial bodies rules on procedure. In this context, technical attribution can support legal attribution. That is, proving that the attack originated in a specific place, from a specific hardware, via a specific IP address and so forth, provides factual elements in relation to which the DARSIWAs may be invoked.

54. Given the difficulty of intertwining technical attribution with legal attribution and the evidentiary regime, four hypotheses have been proposed:

55. the elaboration of new tests and new rules on the legal attribution of conduct that better adapt to the problems raised by cyber-attacks (essentially, the introduction of 'less restrictive' rules in attributing cyber-attacks to a State);

56. the introduction of an *ad hoc* and common evidential regime based either on technical attribution or a reversal of the burden of proof, or both (essentially, once it has been technically ascertained that the attack originated from the territory of a State, it would be up to the latter to prove not to be involved);

57. a robust recourse to international cooperation, in order to better gather all the factual elements that allow already existing rules on legal attribution to apply without an inversion of the burden of proof;

58. delegate the ascertainment of the attribution of cyber-attacks to States to an international organization and, more specifically, to the United Nations.

2.1.3 *Review of National Positions*

59. Among those States which have already expressed themselves on the applicability of international law to cyber-space, some issues stand out with respect to the attribution regime of cyber-attacks to States.

2.1.3.1 *The Need to Highlight the Existence of the Three Types of Attribution*

60. Australia's position reads as follows (Australia's comments on the Initial "Pre-draft" of the report of the UN Open Ended Working Group in the field of information and telecommunications in the context of international security (OEWG) (16 April 2020), par. C4):

> The Report should make the distinction between different attribution assessments, including factual attribution assessments (which includes an assessment of technical and other contextual information) and legal attribution assessments (where there has been a breach of international law and/or domestic law), as well as the political decision to act – publicly or privately – on those attribution assessments. It may be more appropriate for this observation to be included in the section on Rules, Norms and Principles of Responsible State Behaviour (referencing norm 13(b) from the 2015 GGE report).

61. Finland's position reads as follows (*Finland's National Position* (2020) p. 5):

> The rules of attribution reflected in the UN International Law Commission's Articles on State Responsibility remain fully valid in cyberspace. If State organs, or private groups or individuals acting on behalf of the State, can be identified as the authors of a cyber operation that violates the State's international obligations, its international responsibility is engaged. It is in this regard useful to distinguish identification as a technical operation from attribution as a legal operation. Identification may be technically challenging given the often covert nature of hostile cyber activities but this is without consequence to the legal rules of attribution.

2.1.3.2 *The Need to Develop Common Rules on Technical Attribution*

62. Argentina's position reads as follows (Initial "Pre-draft" of the report of the OEWG on developments in the field of information and telecommunications in the context of international security Comments by Argentina, para. 2):

> We strongly support the notion that it is necessary to work towards developing common approaches regarding attribution at a technical level, which would contribute to transparency, accountability and responsible behaviour, enhance

deterrence and could provide grounds for legal action by victims of malicious cyber activities.

63. Brazil's position reads as follows (Comments submitted by Brazil to the Initial "Pre-draft" of the report of the OEWG on developments in the field of information and telecommunications in the context of international security (8 April 2020), p. 2):

> Brazil also strongly supports (…) the need for a common approach to the problem of attribution of cyber attacks, an issue that deserves further development. In the view of Brazil, this is one of the crucial (and, at the same time, one of the most contentious) points in the field of cybersecurity. The political and technical complexities associated with attribution of responsibility for the use of cyber weapons has no parallel in the regimes applicable to other categories of weapons, be they conventional or of mass destruction.

64. China's position reads as follows (China's Contribution to the Initial Pre-Draft of OEWG Report, p. 4):

> China takes note of "developing a common approach to attribution at the technical level" in the pre-draft. It is China's consistent position that the best approach to attribution should be a universally-accepted one under the auspices of the UN. And until the international community finds such an approach, countries should first settle their disagreements and disputes through consultation and avoid unilateral actions that may escalate the current situation.

65. Pakistan's position reads as follows (Pakistan's inputs in response to the letter dated 11 March 2020 from the Chair of the Open-ended Working Group on developments in the field of information and telecommunications in the context of international security (OEWG), para. 11, i), f):

> Member States should cooperate to address the challenges associated with attribution in the ICT environment. Developing a common approach to attribution in a universal setting under the UN auspices remains the most effective way forward in this regard.

66. The Netherlands' position (*Appendix: International law in cyberspace*, p. 5) reads as follows:

To support a claim that a state or non-state actor has acted wrongfully **requires credible attribution.** This starts with collecting and analyzing evidence, and there is both technical and procedural work that can be done now to improve the quality and timeliness of attribution. More specifically, as with other technical disciplines, having well-accepted protocols for collecting and analyzing evidence is important to improving the quality of investigations. Thus, the standardization of investigative methods is important because it may reduce concerns over the integrity of evidence, even if attribution must be decided on a case-by-case basis. In addition to improving attribution as a technical matter, there is much that can be done to shorten the bureaucratic processes associated with making attribution decisions and then, when appropriate, making them public. The often long delay between an event and a declaration of responsibility is due, in no small part, to unclear or unwieldy processes for reaching such decisions at a national level and is exacerbated when several countries are involved in making collective attribution statements. Designing and exercising processes for reaching attribution at a national level and international level, and improving information sharing between countries, can significantly improve the timeliness and effectiveness of attribution statements and facilitate any further appropriate action.

2.1.3.3 *The Relationship Among the Three Types of Attribution*

67. One of the most debated issues is the relationship among the three types of attribution. In particular, the positions of the States are divided among those which believe that political attribution is first and foremost an absolute sovereign prerogative; those which believe that, although a sovereign prerogative, political attribution should be supported, if not by evidence, at least by credible factual elements; and those who believe that, by itself, the attribution of cyber-attacks cannot constitute a discretionary/political act, otherwise leading to power politics and possible abuses.

1.1.1.i.a States supporting the view that political attribution is an absolute sovereign prerogative

68. Australia (AUSTRALIAN PAPER – OPEN ENDED WORKING GROUP ON DEVELOPMENTS IN THE FIELD OF INFORMATION AND TELECOMMUNICATIONS IN THE CONTEXT OF INTERNATIONAL SECURITY (September 2019), p. 9):

> Australia will, in its sole discretion, and based on its own judgement, attribute unlawful cyber operations to another state. In making such decisions, Australia relies on the assessments of its law enforcement and intelligence agencies, and consultations with its international partners.

69. France (International Law Applied to Operations in Cyberspace, pp. 10-11):

> The identification of a State as being responsible for a cyberattack that is an internationally unlawful act does not in any way oblige the victim State to make a public attribution. Such attribution is a discretionary choice made, inter alia, according to the nature and origin of the operation, the specific circumstances and the international context . It is a sovereign decision insofar as France reserves the right to attribute publicly, or not, a cyberattack against it and to bring that information to the attention of its population, other States or the international community. (…)
>
> This policy does not rule out close coordination with France's allies and partner States, including international or regional organisations, in particular the European Union (EU) and the North Atlantic Treaty Organisation (NATO). However, while the decision may go as far as collective attribution of a cyberattack, it lies solely with France. In addition, international law does not require States to provide the evidence on which the public attribution of a cyberattack is based, though such information helps to legitimise the validity of such attribution.

70. Germany (Initial "Pre-draft" of the report of the OEWG on developments in the field of information and telecommunications in the context of international security And Non-paper listing specific language proposals under agenda item "Rules, norms and principles" from written submissions received before 2 March 2020 COMMENTS FROM GERMANY (6 April 2020), p. 2):

> Germany is of the view that, the application of the international rules on State responsibility and hence the act of formally attributing a malicious cyber operation to a State under international law is first and foremost a national prerogative.

71. Switzerland (UN Open-ended working group on developments in the field of information and telecommunications in the context of international security, 2019/2020 Written feedback by Switzerland to the first pre-draft report of the OEWG (9 April 2020), p. 5):

it is our view that attribution is a national prerogative. We are convinced that the report would provide a significant added value by referring to attribution as a process which takes into account the technical characteristics of an attack, the wider context, the full range of information gathering and the legal criteria as set out in the ILC Draft Articles on Responsibility of States for Internationally Wrongful Acts. This process lays the basis for political decision-makers to attribute an attack to a specific actor. We would therefore welcome the explicit reference to "national prerogative" in this paragraph.

72. The United Kingdom

i) *Cyber and International Law in the 21st Century* (23 May 2018) (p. 6):

There is no legal obligation requiring a state to publicly disclose the underlying information on which its decision to attribute hostile activity is based, or to publicly attribute hostile cyber activity that it has suffered in all circumstances. However, the UK can and does attribute malicious cyber activity where we believe it is in our best interests to do so, and in furtherance of our commitment to clarity and stability in cyberspace. Sometimes we do this publicly, and sometimes we do so only to the country concerned. We consider each case on its merits.

ii) *Non-Paper on Efforts to Implement Norms of Responsible State Behaviour in Cyberspace, as Agreed in UN Group of Government Expert Reports of 2010, 2013 and 2015. United Kingdom of Great Britain and Northern Ireland* (September 2019) (pp. 5-6):

On attribution specifically, the UK Government's starting point is that attribution is a political decision and can be a powerful deterrence tool when deployed effectively. The UK will decide whether attribution – public or private – is in the UK's national interest. We consider attribution a sovereign political decision on a case by case basis. Attributing is a first step and opens up further response options, in the UK national interest and under international law. When considering attribution, the UK Government will consider, alongside a technical assessment from the National Cyber Security Centre:

a. Geopolitical and bilateral factors: our wider objectives towards the State in question, including national security objectives, regional stability, the sensitivities of our allies and the likelihood of counter-response.

b. Impact on victim: the impact of UK attribution (especially public) on the victim(s) of a cyber-incident will be reviewed.

c. Impact on law enforcement activity: the impact of UK attribution (especially public) on the law enforcement investigation of a cyber-incident; for instance the effect on our ability to arrest and prosecute.

d. UK values and ability to operate: attribution should not limit the UK's ability to carry out our own cyber operations in full adherence to domestic and international law. Attribution should be in line with our stated positions in national and international fora, where we champion a free, open, peace and secure cyberspace, and adhere to norms of state behaviour. It should enhance the UK's reputation as a competent cyber actor and weigh up the risk of misattribution.

e. Wider response options: the effect of UK attribution on other deterrence activity, which the UK government has agreed or is implementing. The timing of attribution should be calibrated to enhance the impact of other responses.

iii) *Contribution by United Kingdom to the Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the context of International Security* (February 2020) (p. 3):

The UK can and does attribute malicious cyber acts to States where we believe it is in our best interests to do so, and in furtherance of our commitment to clarity and stability in cyberspace. We continue to consider that the decision to attribute malicious cyber activity to a State, and crucially to make that attribution public, is ultimately a political decision for States based on technical evidence, legal advice and wider diplomatic and political considerations».

2.1.3.3.1 States supporting the view that political attribution is a sovereign prerogative to be corroborated by factual elements

73. European Union (para. 16):

> Attributing malicious cyber activities remains a sovereign decision by a State. The EU and its Member States recall the existing norms and mechanisms for the settlement of disputes, including the Security Council and the International Court of Justice.

74. Finland (Finland's National Position (2020), p. 6):

There is no general obligation for a State taking countermeasures to disclose the information on the basis of which the action is taken. At the same time, it is in each State's best interests to ensure that a decision to take countermeasures is based on solid evidence, given that recourse to countermeasures would otherwise constitute an internationally wrongful act. (…)

Public attribution, as a sovereign choice, is primarily a question of political consideration. Public attribution may nevertheless have legal effects to the extent it includes determinations of conduct that constitutes an internationally wrongful act.

75. The Netherlands (Annex 4: ADVANCING CYBERSTABILITY FINAL REPORT of NOVEMBER 2019):

> To support a claim that a state or non-state actor has acted wrongfully requires credible attribution. (…) Even after the evidence points to a given actor, the next step (attribution) may remain challenging. In the past, some state and non-state actors have asserted that attribution is impossible or required absolute proof. But absolute proof is not required and while attribution may be difficult, it is not as insurmountable as some have suggested. In the nation state context, attribution, whether in the cyber or physical realm, is often a political act, and while there is no particular agreed upon standard of proof, countries still have a strong incentive to not make spurious allegations, lest they lose credibility. In short, what is needed is for attribution to be convincing to other countries and to the public. Even if an aggrieved party is satisfied that a particular actor is responsible (and attribution has in fact occurred in international cases), holding actors truly accountable has also proven challenging, thus undermining the value of norms. After all, if there are no adverse consequences for those who violate accepted norms, those norms become little more than words on paper and they will be unlikely to discourage destabilizing activities.

76. New Zealand (The Application of International Law to State Activity in Cyberspace (1 December 2020), para. 20):

> States should act in good faith and take care when attributing legal responsibility to another state for malicious cyber activity. While international law prescribes no clear evidential standard for attributing legal responsibility for internationally wrongful acts, a victim state must be sufficiently confident of the identity of the

state responsible. What constitutes sufficient confidence in any case will depend on the facts and nature of the activity. While any legal attribution should be underpinned by a sound evidential basis, there is no general obligation on the attributing state to disclose that basis. However, a state may choose as a matter of policy to disclose specific information that it considered in making its attribution decision, and may be required to defend any such deci- sion as part of international legal proceedings.

2.1.3.3.2 States supporting the view that attribution of cyber-attacks cannot be merely discretionary/political

77. Iran (Open-ended working group on: Developments in the field of information and telecommunications in the context of international security Second substantive session (February 2020), point 5):

> The anonymity in ICT environment has given rise to possibility of fabricated attribution. Some states are relying their offensive doctrines, policies, measures and operations against target states on fabricated image-building and xenophobia, with an ultimate goal of hostile policies and fabricated attribution. This poses a major threat against peaceful nature of ICT environment as well as international security.

78. Russia (COMMENTARY OF THE RUSSIAN FEDERATION ON THE INITIAL "PRE-DRAFT" OF THE FINAL REPORT OF THE UNITED NATIONS OPEN-ENDED WORKING GROUP ON DEVELOPMENTS IN THE FIELD OF INFORMATION AND TELECOMMUNICATIONS IN THE CONTEXT OF INTERNATIONAL SECURITY, para. 3):

> It is unacceptable to include in the text the concept of political "attribution" of cyber attacks which runs counter to the agreements reached within the framework of the 2015 GGE which clearly indicate the need to support any accusations against States with appropriate technical evidence.

79. Venezuela (PRELIMINARY CONSIDERATIONS OF VENEZUELA TO THE INITIAL PRE-DRAFT OF THE REPORT OF THE OEWG ON DEVELOPMENTS IN THE FIELD OF INFORMATION AND TELECOMMUNICATIONS IN THE CONTEXT OF INTERNATIONAL SECURITY, para. 31):

> Venezuela does not accept the use of the term political "attribution" of cyberattacks, as it considers that, at the time being, no procedure has been yet established, neither a scientific, nor a technical or legal one, to determine and adjudicate responsibilities of cyberattacks or any other such incident to State or non-State actors.

80. Colombia's position on the delegation to the United Nations of the ascertainment of the attribution of cyber-attacks to States stands out:

> For example, discussions regarding attribution of cyber-attacks at the UN level are welcome, in order to increase accountability for malicious cyber activities, and to determine the international responsibility of the States for their internationally wrongful acts in the use of ICTs (*Colombia's comments on the initial "Pre-draft" of the report of the OEWG on developments in the field of information and telecommunications in the context of international security* (16 April 2020), p. 2).

2.1.3.3.3 States highlighting the benefit of international cooperation in assessing the attribution of cyber-attacks

81. Estonia (Estonia's comments to the "Initial "Pre-draft" of the report of the OEWG on developments in the field of information and telecommunications in the context of international security (16 April 2020), para. 14):

> The pre-draft refers to developing a common approach to attribution but fails to recognise that attribution should remain a sovereign decision of each individual state. In order to increase states' capacities to conduct attribution activities, we encourage states to share their best practices regarding attribution.

82. France (International Law Applied to Operations in Cyberspace, p. 11):

> It is a sovereign decision insofar as France reserves the right to attribute publicly, or not, a cyberattack against it and to bring that information to the attention of its population, other States or the international community. This policy does not rule out close coordination with France's allies and partner States, including international or regional organisations, in particular the European Union (EU) and the North Atlantic Treaty Organisation (NATO).

83. The Netherlands (Annex 4: ADVANCING CYBERSTABILITY FINAL REPORT of NOVEMBER 2019):

> Designing and exercising processes for reaching attribution at a national level and international level, and improving information sharing between countries, can significantly improve the timeliness and effectiveness of attribution statements and facilitate any further appropriate action.

84. The United Kingdom (Cyber and International Law in the 21st Century (23 May 2018), p. 6):

> If more states become involved in the work of attribution, then we can be more certain of the assessment.

2.2 *Due diligence*

85. Many Italian partners have addressed due diligence as one of the issues to be tackled with regard to application of rules of international responsibility in cyber space.

86. Accordingly, it is suggested that Italy, too, expresses its position of the issue.

87. "Due diligence" is as a general principle in the field of international responsibility which has been detailed through specific rules developed within many fields of international law, most prominently the field of diplomatic immunities, protection of the environment and human rights.

88. Under a due diligence perspective, a State which negligently does not prevent the occurrence of a specific harm stemming from potentially dangerous activities caused by private actors, rather than its officials, may be held liable. This, irrespective of the lawful or unlawful nature of the activity causing the harm.

89. In other word, due diligence would impose States to establish legal and technical control mechanisms aimed at preventing the occurrence of a harm, even if that harm is caused by private actors.

90. Due diligence obligations are thus obligations of conduct, rather than obligations of result. This means that a due diligence obligation is breached any time a State fails to take steps towards a given end. Failure to achieve the desired result is not relevant for due diligence obligations in so far as the State demonstrates that it acted diligently.

91. It is suggested that Italy expresses its favour for framing States' obligation in the cyber domain as due diligence one.

2.2.1 *Issues not debated*

92. Among those States supporting the application of due diligence in the cyber domain (*infra*, Section 2.2.3.i), some issues are not debated, namely:

i. Due diligence encompasses activities of which a State is aware or should have reasonably been aware.

ii. Due diligence requires prevention of harms caused also by private actors.

iii. Due diligence requires States to take all "reasonable", rather than "necessary", measures for preventing the harm.

iv. Due diligence requires States to prevent physical and non-physical harms.

93. Accordingly, it is suggested that Italy aligns with these positions.

2.2.2 *Issues still under debate*

94. Conversely, the main issues still under debate are:

i. Whether due diligence is an obligation per se, or a standard which, in the words of the ILC, "var[ies] from one context to another for reasons which essentially relate to the object and purpose of the treaty provision or other rule giving rise to the primary obligation";[7]

ii. Whether due diligence should be aimed at protecting only international peace and security or also other international values.

2.2.2.1 *Due diligence as an obligation per se or as a standard*

95. Issue *i*), that is the nature of due diligence as an obligation *per se*, as purported by The Netherlands (*infra*, para 110), or a standard, as maintained by Finland (*infra*, para 108) is of preliminary relevance.

[7] ILC, "Draft articles on Responsibility of States for Internationally Wrongful Acts, with commentaries", *Yearbook of the International Law Commission*, 2001, vol. II, Part Two, at 34, para 3.

96. The former option – due diligence as an obligation *per se* – would require States to take all *necessary* measures to prevent, eliminate or mitigate the occurrence of a harm. The very occurrence of the harm would constitute an internationally wrongful act attributable to the State who was under the due diligence obligation, unless that State is able to demonstrate the existence of a circumstance precluding wrongfulness, such as *force majeur*.

97. On the contrary, the latter option – due diligence as a standard – would not require State to achieve an absolute result concerning prevention, elimination or mitigation of a harm. It would only require States to act diligently, that is take all *reasonable* measures, to prevent the occurrence of a harm.

98. A similar construction of due diligence allows a differentiated approach to the implementation of obligations according to the technical and/or financial capacities of the States involved. This means that the standard of diligence required to States with limited capacities will be lower than the one required to States with higher capacities, to the effect of adding elements of distributive justice to the assessment of liability.

99. On this count, it is therefore suggested that Italy supports the construction of due diligence as a standard, rather than an obligation. This, with a view to making a "due diligence legal regime for the cyberspace" highly flexible, sensitive to technological development and capable of being "tailored" on the specific capacities of any given State.

2.2.2.2 *Interests to be protected via due diligence*

100. Issue *ii*), that is the interest to protect by means of due diligence, is one of content. In that regard, it is to be noted that Australia implies that only international peace and security is to be protected (*infra*, para 107), whilst Finland implies that due diligence in cyber space should encompass other values (*infra*, para 108).

101. This issue appears strongly connected to the role that the territory of a State may play with regard to the generation of malicious cyber activities.

102. The higher the possibility that malicious cyber activities are generated from the territory of a State, the higher would be its benefit from restricting the scope of the interests to be protected *via* due diligence.

103. Conversely, the higher the risk that a State is targeted by malicious cyber activities generated abroad, the higher would be its benefit in widen the scope of interests to be protected from harms *via* due diligence. This latter situation appears to be the one applicable to Italy.

104. Accordingly, it is suggested that Italy uses a language which widens the scope of due diligence.

2.2.3 *Review of national positions*

105. Amongst those States which have already expressed their position on the applicability of international law to cyber space, two different approaches to due diligence may be found.

2.2.3.1 *States supporting due diligence in cyber space*

106. On the one hand, some States have made explicit reference to the need to frame States' obligations in the cyberspace as due diligence ones/obligations of preventions, as follows:

107. The Australian national position reads as follows (pp. 9 & 11):

> In the Strategy, Australia recognised that the law on state responsibility, much of which is reflected in the International Law Commission's Articles on the Responsibility of states for Internationally Wrongful Acts, applies to state behaviour in cyberspace. Under the law on state responsibility, there will be an internationally wrongful act of a state when its conduct in cyberspace – whether by act or omission – is attributable to it and constitutes a breach of one of its international obligations. [...]
>
> Consistent with the purposes of the United Nations, including to maintain international peace and security, States should cooperate in developing and applying measures to increase stability and security in the use of ICTs and to prevent ICT practices that are acknowledged to be harmful or that may pose threats to international peace and security.

108. The Finland national position reads as follows (pp. 4-5):

> Another cardinal principle flowing from sovereignty, closely related to the obligation to respect the sovereignty of other States, is each State's obligation not to knowingly allow its territory to be used to cause significant harm to the rights of other States. It is widely recognized that this principle, often referred to as due diligence, is applicable to any activity which involves the risk of causing significant

transboundary harm. Due diligence is a variable standard in the sense that its content can change over time as a result of technological development or changes in risk assessment, and as such fully applicable to cyber operations.

States may thus not knowingly allow their territory, or cyber infrastructure within a territory under their control, to be used to cyber operations that produce serious adverse consequences for other States. While only States can violate sovereignty, the sovereignty-based obligation of due diligence extends to private activities taking place in a State's territory. Significant harm caused to other States by private cyber activities may give rise to a State's international responsibility but only if the State in question has breached its due diligence obligations.

Some legal obligations are inherent in the principle of due diligence and apply to cyber activities even in the absence of cyber-specific elaborations of the principle. For instance, if a State knows about a planned cyber activity in its territory likely to affect another State adversely and seriously, it must notify that other State. In addition to actual knowledge of harmful acts emanating from the territory of a State, a State's responsibility may be engaged in situations in which it should have known about the activities in question. It is nevertheless clear that "it cannot be concluded from the mere fact of the control exercised […] over its territory […] that [a] State necessarily knew, or ought to have known, of any unlawful act perpetrated therein". If harmful cyber activity takes place and causes serious harm to another State, the State of origin must take appropriate action to terminate it, as well as to investigate the incident and bring those responsible to justice. In order to be able to do this, States should have the necessary procedural and legal mechanisms in place. It should nevertheless be recalled that due diligence is an obligation of conduct, not one of result. In general, what is required of States is that they take all measures that are feasible under the circumstances. A particular question in this regard is related to the position of transit States through which a particular harmful data is routed. Much depends on whether such a State has any knowledge of the ongoing operation, or ability to take feasible measures to terminate it.

Furthermore, while States must show due diligence in the control of the national territory, doing so does not release them from the observance of other international obligations such as those related to human rights.

109. The France national position reads as follows (pp. 6 & 10):

> France exercises its sovereignty over the information systems located on its territory. In compliance with the due diligence requirement13, it ensures that its territory is not used for internationally wrongful acts using ICTs. This is a customary obligation for States, which must (i) use cyberspace in compliance with international law, and in particular not use proxies to commit acts which, using ICTs, infringe the rights of other States, and (ii) ensure that their territory is not used for such purposes, including by non-state actors. [...]
>
> In accordance with the due diligence principle, "States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs", including acts that infringe the territorial integrity or sovereignty of another State. In addition, States must ensure that non-state actors do not use their territory to carry on such activities, and not use proxies to commit internationally wrongful acts using ICTs. The fact that a State fails to comply with its due diligence obligation can justify the taking of political and diplomatic measures that may include counter-measures or a referral to the UNSC.
>
> The fact that a State does not take all reasonable measures to stop wrongful acts against other States perpetrated from its territory by non-state actors, or is incapable of preventing them, cannot constitute an exception to the prohibition of the use of force.
>
> Under these conditions, France does not recognise the extensive approach to self-defence expressed by a majority of the Tallinn Manual Group of Experts which allows a State that is victim of a large-scale cyberattack perpetrated by non-state actors from the territory of another State to use self-defence against that State, including if such a response is carried out in compliance with the principle of necessity, is the only means to counter the armed attack, and the territorial State is unwilling or unable to prevent the perpetration of such acts.
>
> Under the due diligence obligation, States should ensure that their sovereign domain in cyberspace is not used to commit internationally unlawful acts.
>
> A State's failure to comply with this obligation is not a ground for an exception to the prohibition of the use of force, contrary to the opinion of the majority of the Tallinn Manual Group of Experts.

110. The Netherlands national position reads as follows (pp. 4-5):

The due diligence principle holds that states are expected to take account of other states' rights when exercising their own sovereignty. The principle is articulated by the International Court of Justice, for example, in its judgment in the Corfu Channel Case, in which it held that states have an obligation to act if they are aware or become aware that their territory is being used for acts contrary to the rights of another state. It should be noted that not all countries agree that the due diligence principle constitutes an obligation in its own right under international law. The Netherlands, however, does regard the principle as an obligation in its own right, the violation of which may constitute an internationally wrongful act.

In the context of cyberspace, the due diligence principle requires that states take action in respect of cyber activities:

- carried out by persons in their territory or where use is made of items or networks that are in their territory or which they otherwise control;
- that violate a right of another state; and
- whose existence they are, or should be, aware of.

To this end a state must take measures which, in the given circumstances, may be expected of a state acting in a reasonable manner. It is not relevant whether the cyber activity in question is carried out by a state or non-state actor, or where this actor is located. If, for example, a cyberattack is carried out against the Netherlands using servers in another country, the Netherlands may, on the basis of the due diligence principle, ask the other country to shut down the servers, regardless of whether or not it has been established that a state is responsible for the cyberattack. It is generally accepted that the due diligence principle applies only if the state whose right or rights have been violated suffers sufficiently serious adverse consequences. The precise threshold depends on the specific circumstances of the case. It is clear, however, that such adverse consequences do not necessarily have to include physical damage.

111. Lastly, in commenting the OEWG Initial Pre-Draft Report, the Republic of Korea stated that:

The principle of due diligence is one of essential elements for responsible behavior of States in cyberspace. This principle is embodied in the paragraph 13 (c) of the 2015 UNGGE report as below:

States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs; (2015 ¶ 13(c))

The ROK believes that the international community should embark on discussions to review the legal status of due diligence to be elevated as a legal obligation. However, the ROK also recognizes that States' views on this matter may vary and it will take more time to come to an agreement. In order to effectively respond to increased cyber threats in the meantime, it is necessary to concretize and clarify what is already agreed. The ROK sees that further elaboration of the principle will serve as guidelines for voluntary implementation of responsible State behavior in cyberspace and as a safety net for the affected States. Hence, the ROK suggests following ways to implement the norm in the paragraph 13 (c).

- When an affected State notifies another State that ICT incidents has emanated from or involve the notified State's territory with qualified information, the notified State should, in accordance with international and domestic law and within their capacity, take all reasonable steps, within their territory, to cause these activities to cease, or to mitigate its consequences.
- It should be understood that said notification does not imply responsibility of the notified State for the incident.
- The minimum requirement of qualified information may include Indicator of Compromise (IoC), such as IP address, location of perpetrators and computers used for malicious ICT acts and malware information.

Additional or other requirements for qualified information can be further discussed. Ideally, it would be better that if the OEWG can come up with a universal template for notification and establish the relevant national point of contact as well.

2.2.3.2 *States not supporting due diligence in cyber space*

112. Other States have excluded either explicitly, or implicitly, the possibility to frame States obligation in cyberspace as due diligence ones:

113. The New Zealand national position reads as follows (paras. 16-17):

An agreed norm of responsible state behaviour provides that states should not knowingly allow their territory to be used for internationally wrongful acts using ICTs. Whether this norm also reflects a binding legal obligation is not settled. Some states consider that, subject to certain knowledge and capacity requirements,

customary international law requires states to take reasonable measures to put an end to malicious cyber activity which is conducted from, or routed through, their territory, if the activity is contrary to the rights of another state.

New Zealand is not yet convinced that a cyber-specific "due diligence" obligation has crystallised in international law. It is clear that states are not obliged to monitor all cyber activities on their territories or to prevent all malicious use of cyber infrastructure within their borders. If a legally binding due diligence obligation were to apply to cyber activities, New Zealand considers it should apply only where states have actual, rather than constructive, knowledge of the malicious activity, and should only require states to take reasonable steps within their capacity to bring the activity to an end.

114. The "Cyber and International Law in the 21st Century" speech by UK Attorney General Jeremy Wright QC (23 May 2018) reads as follows:

> The international law rules on the attribution of conduct to a state are clear, set out in the International Law Commissions Articles on State Responsibility, and require a state to bear responsibility in international law for its internationally wrongful acts, and also for the acts of individuals acting under its instruction, direction or control.
>
> These principles must be adapted and applied to a densely technical world of electronic signatures, hard to trace networks and the dark web. They must be applied to situations in which the actions of states are masked, often deliberately, by the involvement of non-state actors. And international law is clear – states cannot escape accountability under the law simply by the involvement of such proxy actors acting under their direction and control.
>
> But the challenge, as ever, is not simply about the law. As with other forms of hostile activity, there are technical, political and diplomatic considerations in publicly attributing hostile cyber activity to a state, in addition to whether the legal test is met.

2.2.3.3 *EU and OEWG position*

115. The EU apparently supports a due diligence approach to States obligations in the cyber domain. Indeed, the "EU Lines To Take in view of the June 2020 online meetings of the Open-Ended Working Group on developments in the field of information and telecommunications in the

context of international security (OEWG) (15, 17 and 19 June 2020)" reads as follows (para. 9):

> We reaffirm that global cyber resilience reduces the ability of potential perpetrators to misuse ICTs for malicious purpose. Nonetheless, during the current global health crisis, we also observe cyber threats and malicious cyber activities targeting essential operators globally, including in the healthcare sector. Since the beginning of the pandemic, significant phishing and malware distribution campaigns, scanning activities and distributed denial-of-service (DDoS) attacks have been detected, some affecting critical infrastructures that are essential to managing the crisis. Every country is called upon to exercise due diligence and take appropriate actions against actors conducting such activities from its territory, consistent with international law and the 2010, 2013 and 2015 consensus reports of the United Nations Groups of Governmental Experts (UNGGEs) in the field of Information and Telecommunications in the Context of International Security.

116. It is further to be noted that a discourse on due diligence in cyberspace appears particularly relevant, given the stress put on capacity-building by the OEWG. Indeed, the Second Pre-Draft Reports reads as follows (p. 10):

> Capacity-building helps to develop the skills, define the policies and build the institutions that increase the resilience and security of States so they can fully enjoy the benefits of digital technologies and sustainable development. The international community's ability to prevent or mitigate the impact of malicious ICT activity depends on the capacity of each State to prepare and respond. Capacity-building can also support adherence to binding or voluntary commitments. In a digitally interdependent world, the benefits of capacity-building "spill over" national borders and thereby contribute to a more secure and stable ICT environment for all.

2.3 *Countermeasures*

117. Some Italian partners address the question whether states may resort to countermeasures in the case where they are victims of cyberattacks.

118. National positions that tackle the topic suggest that international customary rules as codified in ILC Draft Articles on State Responsibility for wrongful acts (ARSIWA) should apply to the matter.

119. They also agree that the application customary rules should adapt to the peculiarity of cyberspace.

120. Accordingly, it is suggested that Italy, too, takes a position on the matter.

121. Under customary international law a state, which is the victim of a breach of its rights or of an unlawful act (the 'injured State') may adopt unilateral measures (countermeasures) against the perpetrator (the 'wrongdoing' or 'target' State) under certain circumstances.

122. Countermeasures are aimed at ensuring cessation of the wrongful act and reparation for its consequences.

123. Countermeasure which complies with certain conditions preclude the wrongfulness of an act which would otherwise be contrary to international law.

124. It is generally agreed that the – both substantive and procedural - conditions that a countermeasure is required to meet are set out in the ILC Articles on State Responsibility (notably Articles 22 and 49–53).

125. The same conditions should apply to the cyberspace, even if with some adaptations due to the peculiar characteristics of the considered context.

126. It is suggested that Italy expresses its favour for the application of countermeasures in cyber space subject to the conditions set out by international customary rules on state responsibility.

2.3.1 *Issues not debated*

127. All those States supporting the application of countermeasures in cyberspace agree on the substantive conditions that they should meet in order to be consistent with customary international law, namely:

128. a state which is victim of cyber activity is entitled to take countermeasures against the perpetrator.

129. Countermeasures that amount to a threat or use of force are not permissible. In the case where the attack reaches the gravity threshold to be equated to an armed attack the recourse to self-defence may be considered.

130. The response to a cyberoperation may involve digital means as well as other means (such as the infringement of treaty obligations due to the perpetrator).

131. Countermeasures in any case shall not violate fundamental human rights, humanitarian obligations prohibiting reprisals, or peremptory international legal norms.

132. Countermeasures shall be proportionated i) to the injury suffered by the victim state and ii) to what it is necessary to ensure compliance with international legal obligations and the termination of the ongoing unlawful conduct.

2.3.2 *Issues still under debate*

2.3.2.1.1 Target sate

133. The application of customary rules on countermeasures to cyberspace is problematic to some extent. One of the most controversial issue regards the identification of the state target. The question is strongly linked to the problem of attribution: according to Article 49 of Articles on State Responsibility "injured State may only take countermeasures against a State which is responsible for an internationally wrongful act in order to induce that State to comply with its obligations".

134. Identifying the originator of a cyber operation is a very difficult exercise because of the anonymity, the speed, and the multistage character of such operations.

135. In this regard Finland suggests that "A State that responds to a hostile cyber operation must have adequate proof of the source of the operation and convincing evidence of the responsibility of a particular State".

2.3.2.2 *Procedural requirements*

136. Under Article 52 ARSIWA, before taking countermeasures an injured State is required to call on the responsible State in accordance with article 43 to comply with its obligations. The injured State is also required to notify the responsible State that it intends to take countermeasures and to offer to negotiate with that State.

137. According to the position expressed by Finland "Some of the procedural requirements concerning countermeasures may nevertheless require adjustment. For instance, it may be possible to attribute a hostile cyber operation only afterwards whereas countermeasures normally should be taken while the wrongful act is ongoing." In addition, France suggests that "the victim State may, in certain circumstances, derogate from the obligation to inform the State responsible for the cyberoperation beforehand, where there is a need to protect its rights. The possibility of taking urgent counter-measures is particularly relevant in cyberspace, given the widespread use of concealment procedures and the difficulties of traceability." According to The Netherlands: "the injured state must in principle notify the other state of its intention to take countermeasures. However, if immediate action is required in order to enforce the rights of the injured state and prevent further damage, such notification may be dispensed with".

2.3.2.3 *Collective countermeasures*

138. In principle, according to customary international law, third States cannot take countermeasures against the responsible State. However the ILC has recognised the situation where third States can react to illegality. According to Article 48 ARSIWA any State other than the injured State can invoke the responsibility of another State if the obligation breached is owned to a group of States including that State and is established for the protection of a collective interest.

139. As regards cyberspace States expressed different opinions on the possibility to make resort to collective countermeasures. France argues that: "Collective counter-measures are not authorised, which rules out the possibility of taking such measures in response to an infringement of another State's rights".

140. Quite different the position of New Zealand, which reads: "Given the collective interest in the observance of international law in cyberspace, and the potential asymmetry between malicious and victim states, New Zealand is open to the proposition that victim states, in limited circumstances, may request assistance from other states in applying proportionate countermeasures to induce compliance by the state acting in breach of international law. In those circumstances, collective countermeasures would be subject to the same limitations set out above."

141. Both France and New Zealand moreover agree that in most serios cases a State may bring the situation to UN bodies. In this regard the position of France reads as it follows: "In the most serious cases constituting a threat to international peace and security, France may also bring the

matter before the UNSC under Chapter VI of the United Nations Charter, or even Chapter VII if there is a threat to peace or breach of peace"; a similar opinion has been expressed by New Zealand, according to which: "Where malicious cyber activity gives rise to a situation leading to international friction or a dispute endangering the maintenance of peace and security, any UN Member State may bring the situation or dispute to the attention of the UN Security Council and/or General Assembly".

2.3.3 *Review of national positions*

142. Australian paper – Open ended working group on developments in the field of information and telecommunications in the context of international security, September 2019 (p. 6 f.)

> If a state is a victim of malicious cyber activity which is attributable to a perpetrator state, the victim state may be able to take countermeasures against the perpetrator state, under certain circumstances. However, countermeasures that amount to a use of force are not permissible. Any use of countermeasures involving cyberspace must be proportionate. It is acknowledged that this raises challenges in identifying and assessing direct and indirect effects of malicious cyber activity, in order to gauge a proportionate response. The purpose of countermeasures is to compel the other party to desist in the ongoing unlawful conduct.
>
> Australia does not conduct or knowingly support activity to harm the information systems of the authorized emergency response teams (sometimes known as computer emergency response teams (CERT) or cybersecurity incident response teams (CSIRT)) of another State. Australia does not use its national CERT to engage in malicious international activity.

143. Australian case studies on application of international law in cyberspace

> Scenario 1 – Cyber operation by State B against government websites of State A
>
> The application of international law presents five key advantages to State A: as regards the consequences of the wrongful act, it would entitle State A to take countermeasures – acts which would ordinarily be unlawful – in response to State B's wrongdoing. Countermeasures could be cyber in nature or taken through alternative means – such as reneging on certain bilateral treaty obligations with State B. However, State A would need to ensure that such countermeasures: • were directed against State B • did not constitute a threat or use of force, violate

fundamental human rights, humanitarian obligations prohibiting reprisals, or peremptory international legal norms • were reversible (as far as possible) • were proportionate to the injury suffered by State A, and • were intended to induce State B to comply with its international legal obligations.

Scenario 2 – State A's territory/infrastructure used by State B to conduct malicious cyber activities against State C Servers located on State A's territory are used, without its knowledge, by State B's defence intelligence agency to conduct malicious cyber activities against State C. The activities are contrary to the rights of State C (although they do not constitute an unlawful use of force). State A's relationship with State C could be damaged.

Third, as State A is not directly rseesponsible for any unlawful act committed by State B against State C, State C could not take any countermeasures – acts that would ordinarily be unlawful – against State A in response to State B's conduct. Were it to do so, State A would itself be entitled to respond through countermeasures and seek remedies.

Scenario 3 – State B conducts a major offensive cyber operation that constitutes a serious threat to State A's national security

Fifth, it would entitle State A to take countermeasures – acts which would ordinarily be unlawful – in response to State B's wrongdoing. Countermeasures could be cyber in nature or taken through alternative means – such as implementing otherwise unlawful tariffs on trade in important goods/services from State B. However, State A would need to ensure that such countermeasures: • were directed against State B • did not constitute a threat or use of force, violate fundamental human rights, humanitarian obligations prohibiting reprisals, or peremptory international legal norms • were reversible (as far as possible) • were proportionate to the injury suffered by State A, and • were intended to induce State B to comply with its international legal obligations.

144. FINLAND - International law and cyberspace. Finland's national positions (2020), p. 5 f.

An internationally wrongful act may justify recourse to countermeasures by the injured State if the State responsible for an internationally wrongful act declines to cease the wrongful conduct or pay reparation. Countermeasures may only be taken with the purpose of ensuring compliance, not for retaliation. Countermeasures may furthermore not breach the prohibition of the threat or use of force, or other

peremptory norms of general international law, and must be consistent with other customary law requirements and limitations concerning countermeasures, most of which are reflected in the International Law Commission's Articles on State Responsibility.[8] Some of the procedural requirements concerning countermeasures may nevertheless require adjustment. For instance, it may be possible to attribute a hostile cyber operation only afterwards whereas countermeasures normally should be taken while the wrongful act is ongoing.

There is no general obligation for a State taking countermeasures to disclose the information on the basis of which the action is taken. At the same time, it is in each State's best interests to ensure that a decision to take countermeasures is based on solid evidence, given that recourse to countermeasures would otherwise constitute an internationally wrongful act. A State that responds to a hostile cyber operation must therefore have adequate proof of the source of the operation and convincing evidence of the responsibility of a particular State.

Public attribution, as a sovereign choice, is primarily a question of political consideration. Public attribution may nevertheless have legal effects to the extent it includes determinations of conduct that constitutes an internationally wrongful act.

In addition to countermeasures, other circumstances precluding wrongfulness may justify taking of cyber measures that would otherwise constitute an internationally wrongful act.[9] This may be the case, for instance, if deviating from an international obligation is the only way for the State to safeguard an essential interest against a grave and imminent peril. Facing such an exceptional situation, a State may deviate from its international obligations within the limits specified in the law of State responsibility.[10]

145. FRANCE - International law applied to operations in cyberspace (p. 3 f.)

In response to a cyberattack, France may consider diplomatic responses to certain incidents, countermeasures, or even coercive action by the armed forces if an attack constitutes armed aggression.

1.1.3.International law authorises several responses to a cyberattack that constitutes a breach of French sovereignty or a use of force Facing adversaries who make

[8] *Ibid*., arts. 49–54.

[9] ARSIWA, Chapter V, Circumstances precluding wrongfulness.

[10] Ibid., art. 25. See also Tallinn Manual 2.0, Rule 26.

increasing use of cyberattacks, France is taking a number of measures to prevent, anticipate, protect against, detect and respond to them, including by neutralising their effects. For that purpose, the State agencies designated by the Prime Minister are implementing cyberdefence operations designed to anticipate, detect and respond to cyberattacks in coordination with their national and international partners. In general, France can respond to cyberattacks by taking counter-measures.

In response to a cyberattack that infringes international law (including use of force), France may take counter-measures designed to (i) protect its interests and ensure they are respected and (ii) induce the State responsible to comply with its obligations. Under international law, such counter-measures must be taken by France in its capacity as victim. Collective counter-measures are not authorised, which rules out the possibility of France taking such measures in response to an infringement of another State's rights.

Counter-measures must also be taken in compliance with international law, in particular the prohibition of the threat or use of force. Consequently, they form part of a peaceful response, their sole purpose being to end the initial violation, including in reaction to a cyberoperation that constitutes a use of armed force within the meaning of Article 2, para. 4 of the United Nations Charter. The response to a cyberoperation may involve digital means or not, provided that it is commensurate with the injury suffered, taking into account the gravity of the initial violation and the rights in question. Lastly, the use of counter-measures requires the State responsible for the cyberattack to comply with its obligations. The victim State may, in certain circumstances, derogate from the obligation to inform the State responsible for the cyberoperation beforehand, where there is a need to protect its rights. The possibility of taking urgent counter-measures is particularly relevant in cyberspace, given the widespread use of concealment procedures and the difficulties of traceability. In the most serious cases constituting a threat to international peace and security, France may also bring the matter before the UNSC under Chapter VI of the United Nations Charter, or even Chapter VII if there is a threat to peace or breach of peace.

In accordance with the due diligence principle, "States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs", including acts that infringe the territorial integrity or sovereignty of another State. In addition,

States must ensure that non-state actors do not use their territory to carry on such activities, and not use proxies to commit internationally wrongful acts using ICTs. The fact that a State fails to comply with its due diligence obligation can justify the taking of political and diplomatic measures that may include counter-measures or a referral to the UNSC. The fact that a State does not take all reasonable measures to stop wrongful acts against other States perpetrated from its territory by non-state actors, or is incapable of preventing them, cannot constitute an exception to the prohibition of the use of force.

146. NETHERLANDS. Appendix of the document sent by the Government of the Kingdom of the Netherlands to Parliament (p. 7).

Countermeasures. If a state is the victim of a violation by another state of an obligation under international law (i.e. an internationally wrongful act), it may under certain circumstances take countermeasures in response. Countermeasures are acts (or omissions) that would normally constitute a violation of an obligation under international law but which are permitted because they are a response to a previous violation by another state. In cyberspace, for example, a cyber operation could be launched to shut down networks or systems that another state is using for a cyberattack. A countermeasure is different to the practice of retorsion in that it would normally be contrary to international law. For this reason, countermeasures are subject to strict conditions, including the requirement that the injured state invoke the other state's responsibility. This involves the injured state establishing a violation of an obligation under international law that applies between the injured state and the responsible state and requires that the cyber operation can be attributed to the responsible state. In addition, the injured state must in principle notify the other state of its intention to take countermeasures. However, if immediate action is required in order to enforce the rights of the injured state and prevent further damage, such notification may be dispensed with. Furthermore, countermeasures must be temporary and proportionate, they may not violate any fundamental human rights, and they may not amount to the threat or use of force.

147. NEW ZEALAND - The Application of International Law to State Activity in Cyberspace (1st December 2020), p. 3 f.

If State A attributes internationally wrongful cyber activity to State B, State A may demand reparation and guarantees of non-repetition and/or utilise peaceful dispute resolution mechanisms, including the International Court of Justice where available. State A may also respond with countermeasures against State B. Countermeasures are otherwise internationally wrongful acts that are permitted when undertaken to induce another state to comply with its obligations under international law. They may include, but are not limited to, cyber activities that would otherwise be prohibited by international law. Any countermeasure must: a. be undertaken to induce compliance by the state in breach of international law; b. be directed at the state responsible for the internationally wrongful act; c. not rise to the level of use of force or breach peremptory norms of international law; and d. be necessary and proportionate. Given the collective interest in the observance of international law in cyberspace, and the potential asymmetry between malicious and victim states, New Zealand is open to the proposition that victim states, in limited circumstances, may request assistance from other states in applying proportionate countermeasures to induce compliance by the state acting in breach of international law. In those circumstances, collective countermeasures would be subject to the same limitations set out above. Where malicious cyber activity gives rise to a situation leading to international friction or a dispute endangering the maintenance of peace and security, any UN Member State may bring the situation or dispute to the attention of the UN Security Council and/or General Assembly. A state subjected to malicious cyber activity amounting to an armed attack has further recourse to the inherent right of individual and/or collective self-defence in accordance with Article 51 of the UN Charter. The right to self-defence also arises when an armed attack is imminent, including by cyber means. Any exercise of that right: a. may include, but is not limited to, cyber activities; and b. must be consistent with relevant UN Charter and customary international law obligations, including notification to the United Nations, necessity, and proportionality.

3 The application of International Humanitarian Law to activities in the Cyberspace

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

148. To identify cyber operations which cross the threshold of the use of force, many States focus on the effects of the cyberoperation. A cyber operation carried out by one State against another State violates the prohibition of the use of force if its effects are similar to those resulting from the use of conventional weapons (Australia, *infra* para 150; Finland, *infra* para 151; France, *infra* para 152; New Zealand, *infra* para 153; The Netherlands, *infra* para 154).

149. However, *France* does not rule out the possibility that a cyberoperation without physical effects may also be characterised as a use of force. In the absence of physical damage, a cyber operation may be deemed a use of force against the yardstick of several criteria, including the circumstances prevailing at the time of the operation, such as the origin of the operation and the nature of the instigator (military or not), the extent of the intrusion, the actual or intended effects of the operation or the nature of the intended target (France, *infra* para 152). For the Government of *The Netherlands*, it cannot be ruled out that a cyber operation with a very serious financial or economic impact may qualify as a use of force (The Netherlands, *infra* para 154).

3.1.1 *Review of national positions*

150. Australia's national position reads as follows (p. 5, Annex A, para 1):

> The Charter of the United Nations requires states to seek peaceful settlements of disputes. This obligation extends to cyberspace and requires states to resolve cyber incidents peacefully without escalation or resort to the threat or use of force. This requirement does not impinge upon a state's inherent right to act in individual or collective self-defence in response to an armed attack, which applies equally in the cyber domain as it does in the physical realm.
>
> In determining whether a cyber attack, or any other cyber activity, constitutes a use of force, states should consider whether the activity's scale and effects are comparable to traditional kinetic operations that rise to the level of use of force under international law. This involves a consideration of the intended or reasonably expected direct and indirect consequences of the cyber attack, including for example whether the cyber activity could reasonably be expected to cause serious

or extensive ('scale') damage or destruction ('effects') to life, or injury or death to persons, or result in damage to the victim state's objects, critical infrastructure and/or functioning.

151. Finland's national position reads as follows (pp. 6-7):

> While there is currently no established definition of a cyber attack that would pass the threshold of "use of force" in the sense of article 2(4) of the UN Charter, or "armed attack" in the sense of article 51, it is widely recognized that such a qualification depends on the consequences of a cyberattack. For a cyberattack to be comparable to use of force, it must be sufficiently serious and have impacts in the territory of the target State, or in areas within its jurisdiction, that are similar to those of the use of force. A threat of such a cyberattack could also violate Article 2(4) of the Charter, if the threat is sufficiently precise and directed against another State.
>
> Similarly, most commentators agree that when the scale and effects of a cyberattack correspond to those of an armed attack responding to the cyberattack is justifiable as self-defence. It is obvious that the attack must have caused death, injury or substantial material damage, but it is impossible to set a precise quantitative threshold for the effects, and other circumstantial factors must be taken into account in the analysis, as well. A widely discussed question is, to what extent the definition of a cyberattack comparable to an armed attack should take account of the indirect and long-term impacts of the attack. In any case, this would require that the impacts can be assessed with sufficient precision. A question has also been raised, whether a cyberattack producing significant economic effects such as the collapse of a State's financial system or parts of its economy should be equated to an armed attack. This question merits further consideration.
>
> Any interpretation of the use of force in cyberspace should respect the UN Charter and not just the letter of the Charter but also its object and purpose, which is to prevent the escalation of armed activities. This would mean, for instance, that the distinction between armed attack as a particularly serious violation of the Charter, on the one hand, and any lesser uses of force, on the other, is preserved. Similarly, the conditions for the exercise of the right of self-defence apply in cyberspace as they do with regard to the use of armed force. The right of self-defence arises if a cyberattack comparable to an armed attack occurs and can be attributed to a

particular State. It is reasonable to think that a State victim to such an attack can respond with either cyber means or armed action. At the same time, the use of force must not be disproportionate or excessive.

152. France's national position reads as follows (Section 1.1.2):

> The most serious violations of sovereignty, especially those that infringe France's territorial integrity or political independence, may violate the prohibition of the threat or use of force[14], which applies to any use of force, regardless of the weapons employed[15].
>
> In digital space, crossing the threshold of the use of force depends not on the digital means employed but on the effects of the cyberoperation.
>
> A cyberoperation carried out by one State against another State violates the prohibition of the use of force if its effects are similar to those that result from the use of conventional weapons.
>
> However, France does not rule out the possibility that a cyberoperation without physical effects may also be characterised as a use of force. In the absence of physical damage, a cyberoperation may be deemed a use of force against the yardstick of several criteria, including the circumstances prevailing at the time of the operation, such as the origin of the operation and the nature of the instigator (military or not), the extent of intrusion, the actual or intended effects of the operation or the nature of the intended target. This is of course not an exhaustive list. For example, penetrating military systems in order to compromise French defence capabilities, or financing or even training individuals to carry out cyberattacks against France, could also be deemed uses of force.
>
> However, not every use of force is an armed attack within the meaning of Article 51 of the United Nations Charter16, especially if its effects are limited or reversible or do not attain a certain level of gravity.

153. New Zealand's position reads as follows (para 7):

> 7. State cyber activity can amount to a use of force for the purposes of international law. Whether it does in any given context depends on an assessment of the scale and effects of the activity. State cyber activity will amount to a use of force if it results in effects of a scale and nature equivalent to those caused by kinetic activity which constitutes a use of force at international law. Such effects may include death,

serious injury to persons, or significant damage to the victim state's objects and/or state functioning. In assessing the scale and effects of malicious state cyber activity, states may take into account both the immediate impacts and the intended or reasonably expected consequential impacts.

154. The Netherlands' national position reads as follows (pp. 3-4)

> Article 2(4) of the UN Charter lays down a prohibition on the threat or use of force. It reads as follows: 'All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state.' This prohibition applies to the use of force in any form, regardless of the weapons or means employed.6
>
> The prohibition of the use of force is virtually absolute. There are only three situations in which the threat or use of force does not contravene international law. One is in the case of self-defence against an armed attack (article 51 of the UN Charter). Another concerns certain actions implementing a UN Security Council resolution under Chapter 7 of the Charter.7 The final exception is when the use of force takes place with the agreement of the state in whose territory that force will be used.
>
> When applying this prohibition in the context of cyberspace, the question arises: when can cyber operations be considered 'use of force', given that no use is made of 'weapons' in the usual (physical) sense of the word? The government believes that cyber operations can fall within the scope of the prohibition of the use of force, particularly when the effects of the operation are comparable to those of a conventional act of violence covered by the prohibition. In other words, the effects of the operation determine whether the prohibition applies, not the manner in which those effects are achieved. This position is supported by the case law of the International Court of Justice, which has ruled that the scale and effects of an operation must be considered when assessing whether an armed attack in the context of the right of self-defence has taken place (see below). There is no reason not to take the same approach when assessing whether an act may be deemed a use of force within the meaning of article 2 (4) of the UN Charter. A cyber operation would therefore in any case

3.2 *Cyber operations and the exercise of self-defence by states*

155. A cyber attack that causes damage of a significant scale or severity may constitute an armed attack giving entitlement to the use of self-defence (Australia, *infra* para 159; Finland, *infra* para 160; France, *infra* para 161; New Zealand, *infra* para 162; The Netherlands, *infra* para 163; United Kingdom, *infra* para 164). The victim State may respond in individual or collective self-defence (Australia, *infra* para 159; France, *infra* para 161; New Zealand, *infra* para 162). In accordance with ICJ case law, however, *France* does not recognise the extension of the right to self-defence to acts perpetrated by non-State actors whose actions are not attributable, directly or indirectly, to a State (France, *infra* para 161). Nonetheless, for *France* it cannot be ruled out that general practice may shift towards an interpretation of the law of self-defence as being authorised in response to an armed attack by non-State actors whose acts are not attributable to a State (France, *infra* para 161). *The Netherlands* argues that States may use force in self-defence against both States and non-State actors, but only if the origin of the attack and the identity of those responsible are sufficiently certain (The Netherlands, *infra* para 163).

156. In exceptional circumstances, *France* allows itself to use pre-emptive self-defence in response to a cyber attack that 'has not yet been triggered but is about to be, in an imminent and certain manner, provided that the potential impact of such an attack is sufficiently serious'. However, it does not recognise the legality of the use of force on the grounds of preventive self-defence (France, *infra* para 161). For the Government of *Australia* a State may react in anticipatory self-defence against an armed attack when the attacker is clearly committed to launching an armed attack, in circumstances where the victim will lose its last opportunity to effectively defend itself unless it acts (Australia, *infra* para 159).

157. A cyber attack could be qualified as an armed attack if it causes substantial loss of life or considerable physical or economic damage (Australia, *infra* para 159; Finland, *infra* para 160; France, *infra* para 161; New Zealand, *infra* para 162; The Netherlands, *infra* para 163; United Kingdom, *infra* para 164). To be categorised as an armed attack, a cyberattack must also have been perpetrated, directly or indirectly, by a State. A State is responsible for acts perpetrated by non-State actors only if they act on its instructions or orders or under its control in accordance with the rules on State responsibility for internationally wrongful acts and ICJ case-law (France, *infra* para 161).

158. Cyber attacks which do not reach the threshold of an armed attack when taken in isolation could be categorised as such if the accumulation of their effects reaches a sufficient threshold of

gravity, or if they are carried out concurrently with operations in the physical sphere which constitute an armed attack, where such attacks are coordinated and stem from the same entity or from different entities acting in concert (France, *infra* para 161). A question raised by *Finland* is whether a cyber attack producing significant economic effects such as the collapse of a State's financial system or parts of its economy should be equated to an armed attack (Finland, *infra* para 160). *The Netherlands* affirms that at present there is no international consensus on qualifying a cyber attack as an armed attack if it does not cause fatalities, physical damage or destruction yet has very serious non-material consequences (The Netherlands, *infra* para 163). Another question raised by *Finland* is to what extent the definition of a cyber attack comparable to an armed attack should take account of the indirect and long-term impacts of the attack (Finland, *infra* para 160). Another condition that Government of *The Netherlands* underlines is that an armed attack must have a cross-border character (The Netherlands, *infra* para 163).

3.2.1 *Review of national positions*

159. Australia's national position reads as follows (p. 5, Annex A, para 1, and p. 8):

> The Charter of the United Nations requires states to seek peaceful settlements of disputes. This obligation extends to cyberspace and requires states to resolve cyber incidents peacefully without escalation or resort to the threat or use of force. This requirement does not impinge upon a state's inherent right to act in individual or collective self-defence in response to an armed attack, which applies equally in the cyber domain as it does in the physical realm.
>
> In determining whether a cyber attack, or any other cyber activity, constitutes a use of force, states should consider whether the activity's scale and effects are comparable to traditional kinetic operations that rise to the level of use of force under international law. This involves a consideration of the intended or reasonably expected direct and indirect consequences of the cyber attack, including for example whether the cyber activity could reasonably be expected to cause serious or extensive ('scale') damage or destruction ('effects') to life, or injury or death to persons, or result in damage to the victim state's objects, critical infrastructure and/or functioning […].
>
> The United Nations Charter (Charter) and associated rules of customary international law apply to activities conducted in cyberspace. Article 2(3) of the

Charter requires states to seek the peaceful settlement of disputes and Article 2(4) prohibits the threat or use of force by a state against the territorial integrity or political independence of another state, or in any manner inconsistent with the purposes of the UN. In the Strategy, Australia made clear that these obligations – and the UN Charter in its entirety, including those obligations, apply in cyberspace as they do in the physical realm.

A use of force will be lawful when the territorial state consents, it is authorised by the Security Council under Chapter VII of the UN Charter or when it is taken pursuant to a state's inherent right of individual or collective self-defence in response to an armed attack, as recognised in Article 51 of the Charter. Australia considers that the thresholds and limitations governing the exercise of self-defence under Article 51 apply in respect of cyber operations that constitute an armed attack and in respect of acts of self- defence that are carried out by cyber means. Thus if a cyber operation – alone or in combination with a physical operation – results in, or presents an imminent threat of, damage equivalent to a traditional armed attack, then the inherent right to self-defence is engaged. The rapidity of cyber attacks, as well as their potentially concealed and/or indiscriminate character, raises new challenges for the application of established principles. These challenges have been raised by Australia in explaining its position on the concept of imminence and the right of self-defence in the context of national security threats that have evolved as a result of technological advances.

160. Finland's national position reads as follows (pp. 6-7):

While there is currently no established definition of a cyber attack that would pass the threshold of "use of force" in the sense of article 2(4) of the UN Charter, or "armed attack" in the sense of article 51, it is widely recognized that such a qualification depends on the consequences of a cyberattack. For a cyberattack to be comparable to use of force, it must be sufficiently serious and have impacts in the territory of the target State, or in areas within its jurisdiction, that are similar to those of the use of force. A threat of such a cyberattack could also violate Article 2(4) of the Charter, if the threat is sufficiently precise and directed against another State.

Similarly, most commentators agree that when the scale and effects of a cyberattack correspond to those of an armed attack responding to the cyberattack is justifiable

as self-defence. It is obvious that the attack must have caused death, injury or substantial material damage, but it is impossible to set a precise quantitative threshold for the effects, and other circumstantial factors must be taken into account in the analysis, as well. A widely discussed question is, to what extent the definition of a cyberattack comparable to an armed attack should take account of the indirect and long-term impacts of the attack. In any case, this would require that the impacts can be assessed with sufficient precision. A question has also been raised, whether a cyberattack producing significant economic effects such as the collapse of a State's financial system or parts of its economy should be equated to an armed attack. This question merits further consideration.

Any interpretation of the use of force in cyberspace should respect the UN Charter and not just the letter of the Charter but also its object and purpose, which is to prevent the escalation of armed activities. This would mean, for instance, that the distinction between armed attack as a particularly serious violation of the Charter, on the one hand, and any lesser uses of force, on the other, is preserved. Similarly, the conditions for the exercise of the right of self-defence apply in cyberspace as they do with regard to the use of armed force. The right of self-defence arises if a cyberattack comparable to an armed attack occurs and can be attributed to a particular State. It is reasonable to think that a State victim to such an attack can respond with either cyber means or armed action. At the same time, the use of force must not be disproportionate or excessive.

161. France's national position reads as follows (pp. 8-9):

1.2. A cyberattack that causes damage of a significant scale or severity may constitute an armed attack giving entitlement to the use of self-defence

In accordance with the case law of the International Court of Justice (ICJ), France distinguishes the gravest forms of the use of force, which constitute an armed attack to which the victim State may respond by individual or collective self-defence, from other less grave forms. Cyberattacks may constitute a grave form of the use of force to which France could respond by self-defence.

1.2.1. Categorisation of a cyberattack as an armed attack

France reaffirms that a cyberattack may constitute an armed attack within the meaning of Article 51 of the United Nations Charter, if it is of a scale and severity

comparable to those resulting from the use of physical force. In the light of these criteria, the question of whether a cyberattack constitutes armed aggression will be examined on a case-by-case basis having regard to the specific circumstances.

A cyberattack could be categorised as an armed attack if it caused substantial loss of life or considerable physical or economic damage. That would be the case of an operation in cyberspace that caused a failure of critical infrastructure with significant consequences or consequences liable to paralyse whole swathes of the country's activity, trigger technological or ecological disasters and claim numerous victims. In such an event, the effects of the operation would be similar to those that would result from the use of conventional weapons.

To be categorised as an armed attack, a cyberattack must also have been perpetrated, directly or indirectly, by a State. Leaving aside acts perpetrated by persons belonging to State organs or exercising elements of governmental authority, a State is responsible for acts perpetrated by non-state actors only if they act de facto on its instructions or orders or under its control in accordance with the rules on State responsibility for internationally wrongful acts and ICJ case law. To date, no State has categorised a cyberattack against it as an armed attack.

In accordance with ICJ case law, France does not recognise the extension of the right to self-defence to acts perpetrated by non-state actors whose actions are not attributable, directly or indirectly, to a State.

France has, in exceptional cases, invoked self-defence against an armed attack perpetrated by an actor having the characteristics of a "quasi-State", as with its intervention in Syria against the terrorist group Daesh (ISIS/ISIL). However, this exceptional case cannot constitute the definitive expression of recognition of the extension of the concept of self-defence to acts perpetrated by non-state actors acting without the direct or indirect support of a State.

Nonetheless, it cannot be ruled out that general practice may shift towards an interpretation of the law of self-defence as being authorised in response to an armed attack by non-state actors whose acts are not attributable to a State. However, any such development will have to be made bearing in mind the Rome Statute of the International Criminal Court (ICC) as amended in 2010 to add the crime of aggression, and the case law of the ICC that may emerge in this sphere.

1.2.2. Use of the right of self-defence against a digital armed attack

Under Article 51 of the United Nations Charter, a State that suffers an armed attack is entitled to use individual or collective self-defence. Self-defence in response to an armed attack carried out in cyberspace may involve digital or conventional means in compliance with the principles of necessity and proportionality. On a decision by the President of the Republic to commit the French armed forces, the Armed Forces Ministry may carry out cyberoperations for military purposes in cyberspace.

Cyberattacks which do not reach the threshold of an armed attack when taken in isolation could be categorised as such if the accumulation of their effects reaches a sufficient threshold of gravity, or if they are carried out concurrently with operations in the physical sphere which constitute an armed attack, where such attacks are coordinated and stem from the same entity or from different entities acting in concert.

In exceptional circumstances, France allows itself to use pre-emptive self-defence in response to a cyberattack that "has not yet been triggered but is about to be, in an imminent and certain manner, provided that the potential impact of such an attack is sufficiently serious". However, it does not recognise the legality of the use of force on the grounds of preventive self-defence.

States which, in the conduct of a cyberoperation or in their response to a cyberattack, decide to use non-state actors, such as companies providing offensive cyber services or groups of hackers, are responsible for those actors' actions. In view of the risk of systemic instability arising from the private-sector use of offensive capabilities, France, following on from the Paris Call, is in favour of regulating them strictly and prohibiting such non-state actors from carrying out offensive activities in cyberspace for themselves or on behalf of other non-state actors.

Lastly, any response on the grounds of self-defence remains provisional and subordinate. It must be promptly reported to the UNSC and suspended as soon as the Security Council takes the matter in hand, replacing unilateral action with collective measures or, failing that, as soon as it has achieved its purpose, namely to repel or end the armed attack. Other measures, such as counter-measures or referral to the UNSC, may be preferred if they are deemed more appropriate.

162. New Zealand's position reads as follows (paras 8 & 24):

8. Cyber activity that amounts to a use of force will also constitute an armed attack for the purposes of Article 51 of the UN Charter if it results in effects of a scale and nature equivalent to those caused by a kinetic armed attack. As an example, cyber activity that disables the cooling process in a nuclear reactor, resulting in serious damage and loss of life, would constitute an armed attack […]

24. A state subjected to malicious cyber activity amounting to an armed attack has further recourse to the inherent right of individual and/or collective self-defence in accordance with Article 51 of the UN Charter. The right to self-defence also arises when an armed attack is imminent, including by cyber means. Any exercise of that right: (*a*) may include, but is not limited to, cyber activities; and (*b*) must be consistent with relevant UN Charter and customary international law obligations, including notification to the United Nations, necessity, and proportionality.

163. The Netherlands' national position reads as follows (pp. 8-9)

A state targeted by a cyber operation that can be qualified as an armed attack may invoke its inherent right of self-defence and use force to defend itself.20 This right is laid down in article 51 of the UN Charter. This therefore amounts to a justification for the use of force that would normally be prohibited under article 2(4) of the UN Charter.21 For this reason strict conditions are attached to the exercise of the right of self-defence.

An armed attack is not the same as the use of force within the meaning of article 2(4) of the UN Charter (see above). In the Nicaragua case, the International Court of Justice defined an armed attack as the most serious form of the use of force. This implies that not every use of force constitutes an armed attack.

To determine whether an operation constitutes an armed attack, the scale and effects of the operation must be considered. International law is ambiguous on the precise scale and effects an operation must have in order to qualify as an armed attack. It is clear, however, that an armed attack does not necessarily have to be carried out by kinetic means. This view is in line with the Nuclear Weapons Advisory Opinion of the International Court of Justice, in which the Court concluded that the means by which an attack is carried out is not the decisive factor in determining whether it constitutes an armed attack. The government therefore endorses the finding of the CAVV and the AIV that 'a cyber attack that has comparable consequences to an armed attack (fatalities, damage and destruction) can justify a response with cyber

weapons or conventional weapons (...)'. There is therefore no reason not to qualify a cyberattack against a computer or information system as an armed attack if the consequences are comparable to those of an attack with conventional or non-conventional weapons.

At present there is no international consensus on qualifying a cyberattack as an armed attack if it does not cause fatalities, physical damage or destruction yet nevertheless has very serious non-material consequences.

The government endorses the position of the International Court of Justice, which has observed that an armed attack must have a cross-border character. It should be noted that not all border incidents involving weapons constitute armed attacks within the meaning of article 51 of the UN Charter. This depends on the scale and effects of the incident in question.

The burden of proof for justifiable self-defence against an armed attack is a heavy one. The government shares the conclusion of the CAVV and the AIV that 'No form of self-defence whatever may be exercised without adequate proof of the origin or source of the attack and without convincing proof that a particular state or states or organised group is responsible for conducting or controlling the attack.' States may therefore use force in self-defence only if the origin of the attack and the identity of those responsible are sufficiently certain. This applies to both state and non-state actors.

When exercising their right of self-defence, states must also meet the conditions of necessity and proportionality. In this regard the government shares the view of the CAVV and the AIV that invoking the right of self-defence is justifiable only 'provided the intention is to end the attack, the measures do not exceed that objective and there are no viable alternatives. The proportionality requirement rules out measures that harbour the risk of escalation and that are not strictly necessary to end the attack or prevent attacks in the near future.'

164. The "Cyber and International Law in the 21st Century" speech by UK Attorney General Jeremy Wright QC (23 May 2018) reads as follows (p. 4):

> The next relevant provision of the UN Charter is in Article 2(4) which prohibits the threat or use of force against the territorial independence or political integrity of any state. Any activity above this threshold would only be lawful under the usual exceptions – when taken in response to an armed attack in self-defence or as a

Chapter VII action authorised by the Security Council. In addition, the UK remains of the view that it is permitted under international law, in exceptional circumstances, to use force on the grounds of humanitarian intervention to avert an overwhelming humanitarian catastrophe.

Thirdly, the UK considers it is clear that cyber operations that result in, or present an imminent threat of, death and destruction on an equivalent scale to an armed attack will give rise to an inherent right to take action in self- defence, as recognised in Article 51 of the UN Charter.

If a hostile state interferes with the operation of one of our nuclear reactors, resulting in widespread loss of life, the fact that the act is carried out by way of a cyber operation does not prevent it from being viewed as an unlawful use of force or an armed attack against us. If it would be a breach of international law to bomb an air traffic control tower with the effect of downing civilian aircraft, then it will be a breach of international law to use a hostile cyber operation to disable air traffic control systems which results in the same, ultimately lethal, effects.

Acts like the targeting of essential medical services are no less prohibited interventions, or even armed attacks, when they are committed by cyber means.

3.3 *Cyber operations and the principle of non-intervention in the internal affairs of other states*

165. A malicious State cyber activity will violate the principle of non-intervention if it:

i. has significant effects on a matter which falls within the target State's inherently sovereign functions / domaine réservé (e.g. the right freely to choose its political, economic, social and cultural system, or matters such as taxation, national security, policing, border control, and the formulation of foreign policy); and

ii. is coercive (i.e. there is an intention to deprive the target State of control over matters falling within the scope of its inherently sovereign functions). Coercion can be direct or indirect and may range from dictatorial threats to more subtle means of control. While the coercive intention of the State actor is a critical element of the rule, intention may in some circumstances be inferred from the effects of cyber activity (New Zealand, infra para 172).

166. For a cyber operation to amount to a prohibited intervention, both above-mentioned elements must be present (Australia, *infra* para 169; Finland, *infra* para 170; New Zealand, *infra* para 172; The Netherlands, *infra* para 173; United Kingdom, *infra* para 174). *France* is the only State that defines 'interference' without mentioning 'coercion' in the definition: 'Interference by digital means in the internal or external affairs of France, i.e. interference which causes or may cause harm to France's political, economic, social and cultural system, may constitute a violation of the principle of non-intervention' (France, *infra* para 171).

167. In addition, the Government of *The Netherlands* specifies that 'the goal of the intervention must be to effect change in the behaviour of the target State. Although there is no clear definition of the element of coercion, it should be noted that the use of force will always meet the definition of coercion. Use of force against another State is always a form of intervention' (The Netherlands, *infra* para 173).

168. Some examples of intervention: the practical application of the principle in this context would be the use by a hostile State of cyber operations to manipulate the electoral system to alter the results of an election in another State, intervention in the fundamental operation of Parliament, or in the stability of our financial system (United Kingdom, *infra* para 174), a prolonged and coordinated cyber disinformation operation that significantly undermines a State's public health efforts during a pandemic; and cyber activity deliberately causing significant damage to, or loss of functionality in, a State's critical infrastructure, including – for example – its healthcare system, financial system, or its electricity or telecommunications network (New Zealand, *infra* para 172).

3.3.1 *Review of national positions*

169. Australia's national position reads as follows (p. 5, Annex A, para 1, and p. 8):

> The Charter of the United Nations requires states to seek peaceful settlements of disputes. This obligation extends to cyberspace and requires states to resolve cyber incidents peacefully without escalation or resort to the threat or use of force. This requirement does not impinge upon a state's inherent right to act in individual or collective self-defence in response to an armed attack, which applies equally in the cyber domain as it does in the physical realm.
>
> In determining whether a cyber attack, or any other cyber activity, constitutes a use of force, states should consider whether the activity's scale and effects are

comparable to traditional kinetic operations that rise to the level of use of force under international law. This involves a consideration of the intended or reasonably expected direct and indirect consequences of the cyber attack, including for example whether the cyber activity could reasonably be expected to cause serious or extensive ('scale') damage or destruction ('effects') to life, or injury or death to persons, or result in damage to the victim state's objects, critical infrastructure and/or functioning […].

The United Nations Charter (Charter) and associated rules of customary international law apply to activities conducted in cyberspace. Article 2(3) of the Charter requires states to seek the peaceful settlement of disputes and Article 2(4) prohibits the threat or use of force by a state against the territorial integrity or political independence of another state, or in any manner inconsistent with the purposes of the UN. In the Strategy, Australia made clear that these obligations – and the UN Charter in its entirety, including those obligations, apply in cyberspace as they do in the physical realm.

A use of force will be lawful when the territorial state consents, it is authorised by the Security Council under Chapter VII of the UN Charter or when it is taken pursuant to a state's inherent right of individual or collective self-defence in response to an armed attack, as recognised in Article 51 of the Charter. Australia considers that the thresholds and limitations governing the exercise of self-defence under Article 51 apply in respect of cyber operations that constitute an armed attack and in respect of acts of self- defence that are carried out by cyber means. Thus if a cyber operation – alone or in combination with a physical operation – results in, or presents an imminent threat of, damage equivalent to a traditional armed attack, then the inherent right to self-defence is engaged. The rapidity of cyber attacks, as well as their potentially concealed and/or indiscriminate character, raises new challenges for the application of established principles. These challenges have been raised by Australia in explaining its position on the concept of imminence and the right of self-defence in the context of national security threats that have evolved as a result of technological advances.

170. Finland's national position reads as follows (pp. 3-4):

A hostile interference by cyber means may also breach the customary prohibition of intervention in the internal affairs of another State, provided that it is done with

the purpose of compelling or coercing that State in relation to affairs regarding which it has free choice (so-called domaine réservé). The requirement of coercion leaves out lesser forms of influence and persuasion that are commonplace in international relations. The limitation to sovereign affairs – such as a State's political, economic or cultural system or the direction of its foreign policy – further distinguishes prohibited intervention from measures, the purpose of which is to compel another State to comply with its international obligations.

For a cyber operation to amount to a prohibited intervention, both above-mentioned elements must be present. Most open questions relate to the element of coercion and to how it manifests itself in cyber operations. For instance, while the conduct of elections belongs undisputedly to the internal affairs of each State, all methods of electoral interference do not display the element of coercion. Hacking of voter databases or manipulation of vote counts in order to alter the election results has nevertheless been recognized as a fairly clear case. To be comparable to a real world intervention, cyber interference must also be of a serious nature.

According to the International Court of Justice, the element of coercion is particularly clear if force is used through means of military action, threats of such action, or through support to armed groups in another State. Military or economic pressure may also qualify as coercion. Hostile cyber interference done with the purpose of promoting or supporting armed action in another State could constitute an example of prohibited intervention, provided that it seeks to force a certain policy change.

Compared to a violation of sovereignty, the requirement of coercive nature and that of domaine réservé make the threshold of prohibited intervention considerably higher. This underlines the importance of continued understanding of sovereignty as not only a principle but also an independent primary rule of international law.

171. France's national position reads as follows (pp. 6-7):

1.1.1. Cyberattacks may constitute a violation of sovereignty

The international norms and principles that flow from State sovereignty apply to the use of ICT by States and to their territorial jurisdiction over ICT infrastructure. France exercises its sovereignty over the information systems located on its territory. In compliance with the due diligence requirement, it ensures that its

territory is not used for internationally wrongful acts using ICTs. This is a customary obligation for States, which must (i) use cyberspace in compliance with international law, and in particular not use proxies to commit acts which, using ICTs, infringe the rights of other States, and (ii) ensure that their territory is not used for such purposes, including by non-state actors.

Any cyberattack against French digital systems or any effects produced on French territory by digital means by a State organ, a person or an entity exercising elements of governmental authority or by a person or persons acting on the instructions of or under the direction or control of a State constitutes a breach of sovereignty.

Interference by digital means in the internal or external affairs of France, i.e. interference which causes or may cause harm to France's political, economic, social and cultural system, may constitute a violation of the principle of non-intervention.

A cyberattack which penetrates State digital systems, affects the military or economic power, security or survival capacity of the Nation, or constitutes interference in France's internal or external affairs, will entail defensive cyber warfare operations that may include neutralisation of the effect.

The decision whether or not to respond to such operations is a political one, taken in light of the nature and characteristics of the intrusion. The response, chosen from among the range of options offered by international law, depends, subject to an appropriateness assessment, on the gravity of the breach of sovereignty.

172. New Zealand's position reads as follows (paras 9-10):

9. Malicious state cyber activity may be inconsistent with the rule of non-intervention. Such activity will violate the rule of non-intervention if it:

a. has significant effects on a matter which falls within the target state's inherently sovereign functions / domaine réservé (e.g. the right freely to choose its political, economic, social and cultural system, or matters such as taxation, national security, policing, border control, and the formulation of foreign policy); and
b. is coercive (i.e. there is an intention to deprive the target state of control over matters falling within the scope of its inherently sovereign functions). Coercion can be direct or indirect and may range from dictatorial threats to more subtle means of control. While the coercive intention of the state actor is a critical element of the rule, intention may in some circumstances be inferred from the effects of cyber activity.

10. Examples of malicious cyber activity that might violate the non-intervention rule include: a cyber operation that deliberately manipulates the vote tally in an election or deprives a significant part of the electorate of the ability to vote; a prolonged and coordinated cyber disinformation operation that significantly undermines a state's public health efforts during a pandemic; and cyber activity deliberately causing significant damage to, or loss of functionality in, a state's critical infrastructure, including – for example – its healthcare system, financial system, or its electricity or telecommunications network.

173. The Netherlands' national position reads as follows (p. 3)

> The development of advanced digital technologies has given states more opportunities to exert influence outside their own borders and to interfere in the affairs of other states. Attempts to influence election outcomes via social media are an example of this phenomenon. International law sets boundaries on this kind of activity by means of the non-intervention principle, which is derived from the principle of sovereignty. The non-intervention principle, like the sovereignty principle from which it stems, applies only between states.
>
> Intervention is defined as interference in the internal or external affairs of another state with a view to employing coercion against that state. Such affairs concern matters over which, in accordance with the principle of sovereignty, states themselves have exclusive authority. National elections are an example of internal affairs. The recognition of states and membership of international organisations are examples of external affairs.
>
> The precise definition of coercion, and thus of unauthorised intervention, has not yet fully crystallised in international law. In essence it means compelling a state to take a course of action (whether an act or an omission) that it would not otherwise voluntarily pursue. The goal of the intervention must be to effect change in the behaviour of the target state. Although there is no clear definition of the element of coercion, it should be noted that the use of force will always meet the definition of coercion. Use of force against another state is always a form of intervention.

174. The "Cyber and International Law in the 21st Century" speech by UK Attorney General Jeremy Wright QC (23 May 2018) reads as follows (pp. 4-5):

In certain circumstances, cyber operations which do not meet the threshold of the use of force but are undertaken by one state against the territory of another state without that state's consent will be considered a breach of international law.

The international law prohibition on intervention in the internal affairs of other states is of particular importance in modern times when technology has an increasing role to play in every facet of our lives, including political campaigns and the conduct of elections. As set out by the International Court of Justice in its judgment in the Nicaragua case, the purpose of this principle is to ensure that all states remain free from external, coercive intervention in the matters of government which are at the heart of a state's sovereignty, such as the freedom to choose its own political, social, economic and cultural system.

The precise boundaries of this principle are the subject of ongoing debate between states, and not just in the context of cyber space. But the practical application of the principle in this context would be the use by a hostile state of cyber operations to manipulate the electoral system to alter the results of an election in another state, intervention in the fundamental operation of Parliament, or in the stability of our financial system. Such acts must surely be a breach of the prohibition on intervention in the domestic affairs of states.

Furthermore, a breach of this principle of non-intervention provides victim states with the ability to take action in response that would otherwise be considered unlawful, but which is permissible if it is aimed at returning relations between the hostile state and the victim state to one of lawfulness, and bringing an end to the prior unlawful act. Such action is permissible under the international law doctrine of countermeasures. Put simply, if a hostile state breaches international law as a result of its coercive actions against the target state's sovereign freedoms, then the victim state can take action to compel that hostile state to stop.

3.4 *Cyber operations and the application of the law of armed conflict*

175. Cyber operations dedicated to the engagement of armed forces in an armed conflict are governed by the law of armed conflict (Australia, *infra* para 176; Finland, *infra* para 177; France, *infra* para 178; New Zealand, *infra* para 179; The Netherlands, *infra* para 180; United Kingdom, *infra* para 181). The existence of an armed conflict (international or non-international) is thus a requirement for the application of this area of law (he Netherlands, *infra*

para 180). Cyber operations that constitute hostilities between two or more States may determine the existence of international armed conflict (IAC). Likewise, prolonged cyber operations by government armed forces against one or more armed groups or by several armed groups between themselves may constitute a non-international armed conflict (NIAC), where such groups show a minimum level of organisation and the effects of such operations reach a sufficient threshold of violence (France, *infra* para 178). *China* rejects the application of the law of armed conflict to cyberspace, as it fears that this might lead to its militarisation.

3.4.1 *Review of national positions*

176. Australia's national position reads as follows (pp. 8-9):

> The Strategy and the 2015 Report of the UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (A/70/174), discussed the applicability of international humanitarian law (IHL) to cyber operations in armed conflict, including the principles of humanity, military necessity, proportionality and distinction. Australia considers that, if a cyber operation rises to the same threshold as that of a kinetic 'attack' (or act of violence) under IHL, the rules governing such attacks during armed conflict will apply to those kinds of cyber operations. Applicable IHL rules will also apply to cyber operations in an armed conflict that do not constitute or rise to the level of an 'attack', including the principle of military necessity and the general protections afforded to the civilian population and individual civilians with respect to military operations.
>
> International human rights law (IHRL) also applies to the use of cyberspace […]. States have obligations to protect relevant human rights of individuals under their jurisdiction, including the right to privacy, where those rights are exercised or realised through or in cyberspace. Subject to lawful derogations and limitations, states must ensure without distinction individuals' rights to privacy, freedom of expression and freedom of association online.

177. Finland's national position reads as follows (p. 7):

> International humanitarian law only applies to cyber operations when such operations are part of, or amount to, an armed conflict. Most so far known cyberattacks have not been launched in the context of an armed conflict, and none

has met the threshold of armed conflict. At the same time, when cyber means are used in the context of a pre-existing armed conflict, as has been done in many current conflicts, there is no reason to deny the need for the protections that international humanitarian law provides.

This includes that cyber means and methods of warfare must be used consistently with the principles of distinction, proportionality and precautions, as well as the specific rules flowing from these principles. When assessing the capacity of cyber means and methods to cause prohibited harm, their foreseeable direct and indirect effects should be taken into account. Particular care should be taken to ensure the protection of civilians, including essential civilian infrastructure, civilian services and civilian data.

The unique characteristics of cyberspace, such as interconnectedness and anonymity, may affect how international humanitarian law is interpreted and applied with regard to certain cyber means and methods warfare. The related problems can nevertheless mostly be solved on the basis of existing rules. New technologies do not render the existing rules of international humanitarian law meaningless or necessarily require new legal regulation. Furthermore, while international humanitarian law is *lex specialis* in an armed conflict, it does not override other areas of international law, such as human rights law, which may continue to apply throughout the conflict.

178. France's national position reads as follows (p. 12):

2.1. Cyberoperations may characterise the existence of armed conflict

Cyberoperations that constitute hostilities between two or more States may characterise the existence of international armed conflict (IAC). Likewise, prolonged cyberoperations by government armed forces against one or more armed groups or by several armed groups between themselves may constitute a non-international armed conflict (NIAC), where such groups show a minimum level of organisation and the effects of such operations reach a sufficient threshold of violence.

They are generally military operations concurrent with conventional military operations: that is why it is not difficult to categorise an armed conflict situation. While an armed conflict consisting exclusively of digital activities cannot be ruled

out in principle, it is based on the capacity of autonomous cyberoperations to reach the threshold of violence required to be categorised as such.
Although virtual, cyberoperations still fall within the geographical scope of IHL, insofar as their effects must arise on the territory of the States party to the IAC and on the territory where the NIAC hostilities occur.

179. New Zealand's position reads as follows (para 25):

> In situations of armed conflict, international humanitarian law applies to cyber activities. A cyber activity may constitute an "attack" for the purposes of international humanitarian law where it results in death, injury, or physical damage, including loss of functionality, equivalent to that caused by a kinetic attack. All cyber "attacks" must comply with the principles of military necessity, humanity, proportionality and distinction.

180. The Netherlands' national position reads as follows (p. 5)

> International humanitarian law (IHL) applies to actions in the context of armed conflict. This includes cyber operations carried out as part of an armed conflict. The existence of an armed conflict (international or non-international) is thus a requirement for the application of this specialised area of law. As early as 2011, the government observed that applying the rules of international humanitarian law (jus in bello) to hostilities in cyberspace is 'technically feasible and legally necessary'.
> A key component of IHL is international law on neutrality. Neutrality requires that states which are not party to an armed conflict refrain from any act from which involvement in the conflict may be inferred or acts that could be deemed in favour of a party to the conflict. In its relations with parties to the armed conflict the neutral state is required to treat all parties equally in order to maintain its neutrality. A state may not, for example, deny access to its IT systems to one party to the conflict but not to the other. In its response to the above-mentioned advisory report by the AIV/CAVV, the government noted that, 'In an armed conflict involving other parties, the Netherlands can protect its neutrality by impeding the use by such parties of infrastructure and systems (e.g. botnets) on Dutch territory. Constant vigilance, as well as sound intelligence and a permanent scanning capability, are required here.'

> IHL also lays down specific rules regarding attacks aimed at persons or objects, which apply equally to cyber operations carried out as part of an armed conflict. When planning and carrying out such operations, states must act in accordance with, for example, the principles of distinction and proportionality, as well as the obligation to take precautionary measures.

181. The "Cyber and International Law in the 21st Century" speech by UK Attorney General Jeremy Wright QC (23 May 2018) reads as follows (p. 3):

> In 2013, the UN Group of Governmental Experts on the use of cyber technologies, affirmed the application of existing international law to states' cyber activities. On 26 June 2015, the UN Expert Group, including not just the UK and the US but also Russia and China recognised that the UN Charter applies in its entirety to cyberspace. The Group affirmed the relevance of a state's inherent right to act in self-defence in response to a cyber operation meeting the threshold of an armed attack. In addition, the 2015 Report confirmed that the fundamental protections

3.5 *Cyber operations and the definition of 'attack' under Article 49(1) of the 1977 Protocol I additional to the 1949 Geneva Convention on the Protection of Victims of War*

182. A cyber weapon is first and foremost a force multiplier, given its capacity to support weapons used in other environments. In this regard, it produces the same intelligence, neutralisation and deception effects as conventional means which are subject to targeting procedures already implemented by the French armed forces in compliance with the law of armed conflict. Such operations may constitute attacks within the meaning of Article 49 of Additional Protocol I where they cause physical damage or disable a system (France, *infra* para 183). Any cyber operation which is carried out in, and in connection with, an armed conflict situation, and constitutes an act of violence, whether offensive or defensive, against another party to the conflict, is an attack within the meaning of Article 49 of Additional Protocol I. Contrary to the *Tallinn Manual*, France considers that an attack within the meaning of Article 49 of Additional Protocol I may occur even if there is no human injury or loss of life, or physical damage to property. Thus, a cyber operation constitutes an attack if the targeted equipment or systems can no longer provide the service for which they were implemented, including temporarily or reversibly, where action by the adversary is required in order to restore the infrastructure or the system (France, *infra* para 183).

3.5.1 *Review of national positions*

183. France's national position reads as follows (pp. 12-13):

> **2.1. Cyberoperations may characterise the existence of armed conflict**
> Cyberoperations that constitute hostilities between two or more States may characterise the existence of international armed conflict (IAC)52. Likewise, prolonged cyberoperations by government armed forces against one or more armed groups or by several armed groups between themselves may constitute a non-international armed conflict (NIAC), where such groups show a minimum level of organisation and the effects of such operations reach a sufficient threshold of violence.
> They are generally military operations concurrent with conventional military operations: that is why it is not difficult to categorise an armed conflict situation. While an armed conflict consisting exclusively of digital activities cannot be ruled out in principle, it is based on the capacity of autonomous cyberoperations to reach the threshold of violence required to be categorised as such.
> Although virtual, cyberoperations still fall within the geographical scope of IHL, insofar as their effects must arise on the territory of the States party to the IAC and on the territory where the NIAC hostilities occur.
>
> **2.2. IHL applies to all cyberoperations carried out in, and in connection with, an armed conflict situation**
> The use of a cyber weapon in an armed conflict situation obeys the principles governing the conduct of hostilities. A cyber weapon, which is governed by IHL, may be used in combination with conventional military resources or in isolation. In support of conventional means, it produces the same intelligence, neutralisation and deception effects as those conventional means, which have long been subject to the targeting procedures used by the French armed forces in compliance with IHL.
> The specific nature and complexity of offensive cyber warfare resources demand risk control arrangements just as robust as those applied to conventional operations, taking into account the inherent features of the conduct of operations in cyberspace. In practice, the risks linked to the use of a cyber weapon, especially the immediacy of the action, the duality of targets and the hyperconnectivity of networks, demand a specific digital targeting process spanning all phases of the cyberoperation in

order to ensure compliance with the principles of distinction, precaution and proportionality, inter alia in order to minimise potential civilian damage and loss of life. The process involves long and specific planning carried out in close coordination with the planning of operations in the physical sphere.

2.2.1. A cyberoperation may constitute an attack within the meaning of international humanitarian law

Any cyberoperation which is carried out in, and in connection with, an armed conflict situation, and constitutes an act of violence, whether offensive or defensive, against another party to the conflict, is an attack within the meaning of Article 49 of AP I to the Geneva Conventions.

In an armed conflict situation, the primary purpose of cyber weapons is to produce effects against an adversary system in order to alter the availability, integrity or confidentiality of data. Their effects may be material (e.g. neutralisation of a weapons system) or virtual (e.g. intelligence gathering), temporary, reversible or final.

For example, the destruction of adversary military offensive cyber or conventional capabilities by disruption or the creation of major damage is an attack within the meaning of IHL. The same applies to neutralisation actions which damage adversary cyber or conventional military capabilities by destroying ICT equipment or systems or altering or deleting digital data or flows such as to disable a service essential to the operation of such capabilities.

Contrary to the definition given by the Tallinn Manual Group of Experts, France does not characterise a cyberattack solely on the basis of material criteria. It considers that a cyberoperation is an attack where the targeted equipment or systems no longer provide the service for which they were implemented, whether temporarily or permanently, reversibly or not. If the effects are temporary and/or reversible, the attack is characterised where action by the adversary is necessary to restore the infrastructure or system (repair of equipment, replacement of a part, reinstallation of a network, etc.).

Most cyberoperations carried out by the French armed forces in an armed conflict situation (mainly information-gathering) do not meet the definition of an attack. For example, altering the adversary's propaganda capabilities, and in particular making an influence site unavailable by saturation or denial of service – which is not

prohibited by IHL by analogy with conventional jamming of radio communications or TV broadcasts – cannot be characterised as an attack. However, such operations, in the same way as general information-gathering with the aim of evaluating the adversary's military capabilities or hacking a system in order to gather data, are still governed by the provisions of IHL applicable to any military operation carried out in an armed conflict situation.

3.6 *Cyber operations and the law of neutrality*

184. The law of neutrality applies to cyberoperations. Belligerents must refrain from causing harmful effects to digital infrastructure situated on the territory of a neutral State or from launching a cyberattack from such infrastructure (France, *infra* para 185). A key component of IHL is the international law of neutrality. Neutrality requires that States which are not a party to an armed conflict refrain from any involvement in the conflict or act in favour of a belligerent. In its relations with the parties to the armed conflict, the neutral State is required to treat all parties equally in order to maintain its neutrality. A State may not, for example, deny access to its IT systems to one party to the conflict but not to another. In its response to the above-mentioned advisory report by the AIV/CAVV, the Dutch government noted that '[i]n an armed conflict involving other parties, the Netherlands can protect its neutrality by impeding the use by such parties of infrastructure and systems (e.g. botnets) on Dutch territory. Constant vigilance, as well as sound intelligence and a permanent scanning capability, are required here' (see also The Netherlands, *infra* para 186).

3.6.1 *Review of national positions*

185. France's national position reads as follows (p. 16):

> **2.3.The law of neutrality applies in cyberspace**
> Cyberoperations carried out in the context of an international armed conflict, or which trigger such a conflict, are subject to the law of neutrality. As such, the States party to an IAC may neither carry out cyberoperations linked to the conflict from installations situated on the territory of a neutral State or under the exclusive control of a neutral State, nor take control of computer systems of the neutral State in order to carry out such operations. The neutral State must prevent any use by belligerent States of ICT infrastructure situated on its territory or under its exclusive control.

However, it is not required to prevent belligerent States from using its ICT networks for communication purposes.
Routing a cyberattack via the systems of a neutral State without any effect on that State does not breach the law of neutrality, which prohibits only the physical transit of troops or convoys.

186. The Netherlands' national position reads as follows (p. 5):

> A key component of IHL is international law on neutrality. Neutrality requires that states which are not party to an armed conflict refrain from any act from which involvement in the conflict may be inferred or acts that could be deemed in favour of a party to the conflict. In its relations with parties to the armed conflict the neutral state is required to treat all parties equally in order to maintain its neutrality. A state may not, for example, deny access to its IT systems to one party to the conflict but not to the other. In its response to the above-mentioned advisory report by the AIV/CAVV, the government noted that, 'In an armed conflict involving other parties, the Netherlands can protect its neutrality by impeding the use by such parties of infrastructure and systems (e.g. botnets) on Dutch territory. Constant vigilance, as well as sound intelligence and a permanent scanning capability, are required here.'

4 The application of International Disaster Law to activities in the cyberspace

187. Until now, the issue concerning the relevance and applicability of International Disaster Law (hereinafter IDL) in cyber space has been limitedly addressed. As known, States are mainly focusing their attention on the analysis of how the legal regimes of Ius ad bellum, Ius in bello, Human rights law and International responsibility shall apply in the cyber scenario.

188. However, recalling the growing attention payed by the International community to IDL in recent times and remembering that the potential for disasters to be caused in cyber space is very real, it seems advisable that Italy proposes a stimulating position on the issue.

4.1 *Normative aspects concerning IDL in cyber space*

189. The importance of cyber space with regard to the management of disasters looks like a double-edged sword (cyber neutrality). From one side, disaster response is significantly improved by the recourse to network technologies. From the other side, however, it must not be underestimated the disastrous consequences which could come from cyber incidents. This explains why it cannot be excluded the possibility to include cyber incidents among the events covered by the international-law definition of disaster.

190. Indeed, it must be remembered the high level of dependence from network and information systems characterizing essential public and private services in the contemporary age. This fact imposes to highly take into account the potential sufferings which could come from "cyber disasters". As recently highlighted by the European Union: "Cybersecurity incidents, whether accidental or the deliberate action of criminals, state and other non state actors, can cause enormous damage"[11].

191. As it is well-known, in 2016, the International Law Commission (hereinafter ILC) concluded a study on the protection of persons in the event of disaster. That study led to a project of draft articles[12], which should "facilitate an effective response to disaster that meets the essential needs of the persons concerned, with full respect for their rights" (draft article 2).

192. The international community looks divided over the possibility of continuing towards the formation of a multilateral convention based on draft articles redacted by the ILC. At the state of art, some States (for example, San Salvador, Italy[13], Sudan, Argentina, Singapore) retain that a binding legal instrument would undoubtedly make a significant contribution to the harmonization of the measures and protocols necessary for the effective prevention, reduction and management of disaster risk. On the contrary, many other States (such as U.K., Austria, Czechia, Switzerland, Russian federation, United States of America, Israel, Germany, Australia) treat them as guidelines of good practice and they do not consider it necessary, at the

[11] Joint Communication to the European Parliament and the Council, The EU's Cybersecurity Strategy for the Digital Decade, 2020.
[12] UN ILC, Draft Articles on the protection of persons in the event of disasters, 2016.
[13] UN Document A/C.6/73/SR.31, verbatim records of the intervention of Mr. Stefanile (Italy): "the articles were a sound basis for negotiating a future convention. His delegation was open to any option regarding the form and content of such a convention, but one possibility was a framework convention with a clearly defined scope that established the fundamental rules and principles of international cooperation in disaster response, especially with regard to relief operations conducted by external actors in the territory of the affected State. Such an instrument could be used by States as a basis for more specific operational instruments at the bilateral or regional level. Some form of quasi-institutional mechanism – for instance a secretariat, a meeting of the parties and/or a technical body – could be established to enable the parties to develop technical instruments facilitating the work of stakeholders and relief agencies on the ground".

present stage, to elaborate a legally binding international convention on the basis of the draft articles.

193. The extent of the scope of application of the draft articles largely depends on the definition to give to the term "disaster". In ILC's view, a disaster is a "calamitous event or series of event resulting in widespread loss of life, great human suffering and distress, or large-material or environmental damage, thereby seriously disrupting the functioning of society" (draft article 3).

194. Even though the ILC draft articles do not include any limitation concerning the origin of relevant events[14], it is quite debated whether the definition of "disaster" should include certain categories of "man-made disasters". In particular, while some States explicitly agree on this view (Togo, Mauritius, Germany, USA[15]), other States usually address this discussion by limitedly referring to "natural" disasters (San Salvador, Iceland, Honduras, Brazil). Moreover, the expression "technological disaster" is recalled by some States in addition to "traditional" natural disasters.

195. Neither the ILC nor any State explicitly took a specific position with regard to the eventual inclusion of cyber disasters within the scope of the draft articles, and so leaving quite open the question at stake. Consequently, it may be (at least) not excluded that, where cyber incidents reach a level of intensity as to cause particular calamitous consequences, IDL rules apply in the cyber context[16].

196. According to ILC work, in the occurrence of a disaster, States shall cooperate among themselves and with the United Nations and other relevant assisting actors (draft article 7). Cooperation assumes many forms, which vary from humanitarian assistance to cooperation of international relief actions and communications (draft articles 8). In principle, the adoption of these conducts looks functional to respond to cyber disastrous incidents.

[14] UN ILC, Draft Articles on the protection of persons in the event of disasters, with commentaries, 2016.
[15] Cf. Memorandum of Understanding between the Government of the United States of America and the Government of the Russian Federation on cooperation in natural and man-made technological emergency prevention and response (Moscow, 16 July 1996), United Nations, Treaty Series, No. 50116, p. 1: "the Parties intend to cooperate in natural and man-made technological disaster mitigation, preparedness, response, and recovery in the areas of training, expert assistance and exchange of experiences".
[16] Pursuant to draft article 3(a), the term "disaster" "means a calamitous event or series of events resulting in widespread loss of life, great human suffering and distress, mass displacement, or large-scale material or environmental damage, thereby seriously disrupting the functioning of society".

197. Also, particularly relevant is the duty to reduce the risks of disasters. Indeed, pursuant to draft article 9(1), "Each State shall reduce the risk of disasters by taking appropriate measures, including through legislation and regulations, to prevent, mitigate, and prepare for disasters".

198. From a strict legal perspective, this is a duty of conduct, reflected in several disaster risk reduction measures and documents, requiring States to act in compliance with parameters of due diligence, a flexible standard which declines itself in many shapes and forms. Moreover, as precisely remembered by the ILC, the duty to prevent, reduce and mitigate the risks of disasters must be performed following a precautionary approach.

199. In this respect, some States (among them USA) retain that there is no need to articulate new "rights" and "duties", for customary international law expressly imposes an obligation to take the necessary and appropriate measures to prevent, mitigate, and prepare for disasters. More generally, the existence of an international-law obligation to prevent harm finds support in human right law and environmental law.

200. It must be noted, however, that the large majority of States highlight the pivotal importance of this duty (for example: Nordic countries, Germany, Australia, Czechia, Sudan, Mauritius). Precisely, comprehensive protection of people from disasters must start from prevention. This task must be reached through many different actions, among others stand for relevance:

i. Adoption of domestic laws, regulations and public policies defining roles and responsibilities and inducing the public and private sectors to address disaster risks;

ii. Regional and international cooperation;

iii. Conduction of risks assessment, collection and dissemination of risks.

4.2 *Relevant examples of regional efforts in reducing the risks of cyber disasters (European Union)*

201. Relevant illustrations of duties concerning the reduction of risks related to cyber disasters may be found in the law of the European Union. The revised Decision establishing the EU civil protection mechanism (Decision 1313/2013/EU), which is applicable to "any situation which has or may have a severe impact on people, the environment, or property, including cultural heritage" (article 4(1)), mentions specific prevention actions to be performed by the European

Commission (article 5) as well as risk management measures to be taken by Member States (article 6).

202. Moreover, the EU Directive 2016/1148 (hereinafter NIS) provides specific forms of cooperation for prevention and mitigation of the risk of cyber incidents:

    i. NIS requires EU States to be adequately equipped - in terms of both technical and organizational capabilities - to prevent, detect, respond to and mitigate network and information system incidents and risks;

    ii. NIS requires EU States to adopt cyber national strategies, with the aim to achieve and maintain a high level of security of network and information systems;

    iii. NIS requires EU States to configure detailed forms of cooperation in order to support and facilitate strategic exchange of information among them, with a view of achieving a high common level of security of network and information systems within EU;

    iv. NIS requires EU States to identify the operators of essential services with an establishment on their territory and to ensure that they take appropriate and proportionate technical and organizational measures to manage the risks posed to the security of network and information systems which they use in their operations. Member States shall also ensure that providers notify the competent authorities of any incident having a substantial impact and take measures to prevent and minimize the impact of incidents affecting the security of their network.

203. In 2019, the European Commission has adopted specific recommendations on cybersecurity in the energy sector, introducing a non-exhaustive guidance to Member States and relevant stakeholders for achieving a higher level of cybersecurity in view of specific real-time requirements identified for the energy sector, cascading effects and the combination of legacy and state-of-the-art technologies. The instrument stresses the properly assess all related risks, proposing to adopt measures to prevent and mitigate those identified risks. Also importantly, the need to build common operational capacity to prevent cyber incidents is expressly mentioned as one of principal instruments upon which the 2020 EU's Cybersecurity Strategy for the Digital Decade is based.

5 The role of private stakeholders in cyberspace

204. The issue of the protection of human rights in cyberspace, and the role of private stakeholders, is addressed in many national positions in positive terms. Accordingly, it is suggested that Italy expresses its favour on the issue in point.

205. Moreover, the "multi-stakeholders" nature of ICTs has been central in the discussion concerning the OEWG Pre-Draft Report. It has been consistently affirmed that the pacific use of ICTs is a "shared responsibility" of private and public stakeholders alike. Accordingly, it is suggested that Italy, too, expresses its favour for a "multi-stakeholders" approach.

5.1 *Review of National Positions*

206. The Australia National position reads as follows:

> Human rights apply online just as they do offline. Australia is a strong advocate of human rights online and a full overview of its activities can be found in the Human Rights Online Chapter of the 2019 Progress Report on implementation of *Australia's International Cyber Engagement Strategy*.
> Of particular note, at the 38th Session of the Human Rights Council (HRC38) in July 2018: Australia co-sponsored four resolutions promoting the protection of human rights online, including A/HRC/38/L.10/Rev.1 on the promotion, protection and enjoyment of human rights on the Internet. We also support and sponsor the work of Freedom Online Coalition and Digital Defenders. Australia joined the Freedom Online Coalition Joint Statement at HRC41 in June 2019 on free expression, peaceful assembly, and free association online.
> Australia has re-affirmed that international human rights law (IHRL) applies to the use of cyberspace. It has said that:
> States have obligations to protect relevant human rights of individuals under their jurisdiction, including the right to privacy, where those rights are exercised or realised through or in cyberspace. Subject to lawful derogations and limitations, states must ensure without distinction individuals' rights to privacy, freedom of expression and freedom of association online (see 2019 International Law Supplement).

> Australia has strong national frameworks to ensure the promotion, protection and enjoyment of human rights online, including through the work of the Australian Information Commissioner, Human Rights Commissioner, and E-Safety Commissioner. The Australian Signals Directorate (ASD) is also subject to the Rules to Protect the Privacy of Australians made by the Minister for Defence.

207. The EU Lines to Take in view of UN OEWG on security & telecommunications in context of international security of 31 January 2020 reads as follows:

> 39. The EU and its Member States value the contribution of all stakeholders and support the recommendation to engage in an open and regular dialogue, creating a wider base of awareness and shared visions, with all relevant actors, including where appropriate the private sector, academia and civil society, and through relevant existing regional and international fora, as stated in para.31 of the 2015 UN GGE report. The EU and its Member States underline that, while States have the primary responsibility for maintaining a secure and peaceful ICT environment, effective international cooperation would benefit from identifying a mechanism for the participation of all stakeholders, inter alia, the private sector, academia and the civil society, such as the Paris Call for trust and security in the cyberspace, while avoiding the creation of new and unnecessary bodies or institutions.

208. Finland National Position reads as follows (p. 2):

> [A] non-consensual intrusion in the computer networks and systems that rely on the cyber infrastructure in another State's territory may amount to a violation of that State's sovereignty. The prohibition of cyber operations violating the territorial sovereignty of another State protects, first of all, the cyber infrastructure located in the territory of that State, or otherwise under its jurisdiction, as well as computer networks and systems supported by such infrastructure, from material harm. The situation is the same irrespective of whether such infrastructure belongs to or is operated by governmental institutions, private entities or private individuals. In addition to material harm that may be caused by such an operation, other relevant considerations include whether an intrusion in the cyber infrastructure triggers a loss of functionality of the equipment relying on it, or modifies or deletes information belonging to the target State, or to private actors in its territory.

209. France national position reads as follows (pp. 9-10):

> States which, in the conduct of a cyberoperation or in their response to a cyberattack, decide to use non-state actors, such as companies providing offensive cyber services or groups of hackers, are responsible for those actors' actions. In view of the risk of systemic instability arising from the private-sector use of offensive capabilities, France, following on from the Paris Call, is in favour of regulating them strictly and prohibiting such non-state actors from carrying out offensive activities in cyberspace for themselves or on behalf of other non-state actors. […]
>
> The cyberattacks confronting States and private-sector actors are by nature difficult to characterise in cyberspace. Digital resources are used for the purposes of espionage, cyber crime, destabilisation and even sabotage. The inherent characteristics of this environment, the difficulty of tracing and controlling activities, the increasingly extensive involvement of non-state actors and the possibilities available to States of using private-sector actors as proxies to carry out malicious activities make the identification of the perpetrators and sponsors of such attacks a particularly complex affair.

184. The joint submission on *The future of discussions on ICTs and cyberspac*e at the UN of 12 February 2020 reads as follows

> 5/ Organize consultations with other stakeholders (private companies, NGOs, civil society…), regional organizations, representatives of other UN processes, and relevant multi-stakeholder initiatives dealing with cyber-related issues in the context of international security. During the OEWG as well as during other initiatives such as the High Level Panel Working group on "trust and security", the benefit of conversation with all stakeholders has been largely recognized – ICTs and critical communication infrastructures often being partly managed by non-State Actors. We intend to maintain regular institutional dialogue with broad participation under the auspices of the United Nations.

5.2 *Comments to the initial OEWG Pre-Draft Report (April 2020)*

5.2.1 *OEWG Initial Pre-Draft Report and Italian comments thereto*

210. The issue of the role of private stakeholders and the "multi-stakeholders" nature of ICTs was addressed in the OEWG Initial Pre-Draft Report of April 2020, as follows:

> 40. The need to encourage partnerships and joint efforts with the private sector and other stakeholders on the implementation of norms was highlighted, including with regard to ensuring sustainable capacity-building efforts. It was noted that all stakeholders had responsibilities in their use of ICTs [...].
>
> 64. The OEWG's mandate provided for the possibility of holding intersessional consultative meetings with other stakeholders, including the private sector, non-governmental organizations and academia. The three-day informal consultative meeting of the OEWG held in December 2019 produced a rich exchange between States and other stakeholders. The OEWG also heard interventions from non-governmental organizations during an informal multi-stakeholder segment at its first and second sessions. In order to further inform their engagement with the OEWG, some States noted that they have conducted domestic multi-stakeholder consultations or calls for submissions.
>
> 65. It was recalled that States hold primary responsibility for national security, public safety and rule of law. It was also noted that regular dialogue should be primarily intergovernmental in nature, and an appropriate mechanism to leverage the experience and knowledge of other stakeholder groups would need to be found. In their interventions, States acknowledged that building a more resilient and secure ICT environment necessitates multi-stakeholder cooperation and partnerships. While recognizing the unique role and responsibility of States in relation to security, there was growing appreciation that States may benefit from the expertise in non-governmental communities and that responsible behaviour of other actors makes an essential contribution to this environment.
>
> 66. The OEWG presented a historic first opportunity for all UN Member States to discuss, under the auspices of the United Nations, matters related to ICTs and international security. The OEWG's discussions, building on the foundation provided by the consensus reports of the GGEs, were guided by the principles of inclusivity and transparency, with the aim of maintaining and promoting trust, in

the fulfilment of its mandate. Its formal and informal sessions were characterized by substantive exchanges among Member States, as well as with the private sector, non-governmental organizations, civil society and academia. The strong engagement by States and other stakeholders throughout the work of the OEWG is an undeniable indication of the increasingly universal relevance of the topics under its consideration as well as the growing recognition of the urgent need to collectively address the threats posed by the malicious use of ICTs.

211. In line with the EU comments and comments by other EU Countries (below), Italy commented the above language as follows:

> Italy would like to see the role of other stakeholders more evenly reflected in the report, either by dedicating a specific section in the introduction and in the recommendations, with highlights of both contributions and need for further cooperation for each group of stakeholders (private sector, NGOs, academia and scientists) or by allowing a dedicated paragraph in each thematic section of the report, or both. With regards to private sector, several delegations have singled out the small and medium enterprises that are a source of concern as they are particularly vulnerable while representing the majority of the world's businesses. Finally, we think that the OEWG report should mention and annex the report of the Informal intersessional consultative meeting of the OEWG with industry, nongovernmental organizations and academia (2-4 December 2019).

5.2.2 *Comments by EU and EU Member States*

212. The EU comments on the language contained in the OEWG Initial Pre-Draft Report in the "Joint comments from the EU and its Member States on the initial 'pre-draft' report of the Open-Ended Working Group on developments in the field of Information and Telecommunication in the context of international security" as follows:

> 4. The EU and its Member States believe that the role of other stakeholders should be more evenly reflected in the report, either by dedicating a specific section in the introduction and in the recommendations, which highlights both the contributions and the need for further cooperation with each group of stakeholders (government, business, non-governmental organizations and academia), or by allowing a dedicated paragraph in each thematic section of the report, or both. In addition, we

recommend that the informal conclusions drafted by Mr David Koh, Chair of the intersessional multi-stakeholder meeting (2-4 December 2019), should be annexed to the OEWG final report.

213. France commented on these issues as follows:

> In accordance with the principle of due diligence, States have the obligation to not knowingly allow their territory to be used to commit acts prohibited by international law against third States through the use of cyber means. This obligation also applies to activities conducted in cyber space by non-state actors situated in the territory or under the jurisdiction of the State in question. It should be recalled that States must not commit acts prohibited by international law against third States through the use of proxies. A better understanding of how to apply these principles to cyber issues would help bolstering cooperation between States with a view to avoiding conflicts, protecting certain critical infrastructure, and putting a stop to potential major cyberattacks perpetrated via third States. Lastly, international human rights law is only considered through a simple mention of its applicability, whereas the issues of protection of personal data and the use of cyber space as a place to exercise fundamental freedom are today essential. […]
>
> Paragraph 40 notes that various stakeholders have responsibility for security in the cyberspace. States should be called on to take the necessary outreach, cooperation and, where necessary, regulatory steps so that the various stakeholders should take their responsibilities, including the public and private sectors and civil societies.
>
> France reaffirms its commitment to the proposal formulated jointly with Croatia, Finland and Slovenia. States should be encouraged to take measures to prevent non-State actors, including the private sector, from conducting ICT activities for their own purposes or those of other non-State actors to the detriment of third parties including those located on another State's. This aim could be achieved by working with the private sector to define permissible actions using a risk-based approach and to develop concrete tools such as certification processes, best-practice guides, incident response mechanisms and, as appropriate, national regulations.

214. Germany commented as follows:

> States should be encouraged to take measures to prevent non-State actors, including the private sector, from conducting ICT activities for their own purposes or those

of other nonState actors to the detriment of third parties including those located on another State's territory.

This aim could be achieved by working with the private sector to define permissible actions using a risk-based approach and to develop concrete tools - certification processes, bestpractices guides, response mechanisms to incidents and, as appropriate, national regulations.

"State and non-state actors should neither conduct nor knowingly allow activity that intentionally and substantially damages the general availability or integrity of the public core of the Internet, and therefore the stability of cyberspace" [would be] guidance for implementation of UN GGE 2015 recommendation 13(f) and therefore bringing this also under the scope of UN GGE 2015 recommendation 13(g).

5.2.3 *Comments by other States*

215. Canada commented on the issue as follows:

> Canada would like to see a stronger reference to the request, made by several States, that nongovernmental stakeholders play as much of a role as possible in the OEWG process. We respectfully ask that the report of the December multi-stakeholder session be attached as an Annex to the final OEWG report, and that stakeholders' input continue to be reflected meaningfully moving forward. We thank you for your continued leadership in this regard, and we stand by to assist you in any way possible to advance these objectives.

216. The Non-Aligned movement commented on the issue as follows:

> NAM expresses its concern regarding the potential use of ICTs in international conflicts, covert and illegal operations, and attacks on third countries by States and non-state actors through the use of computer systems of other nations, and also expresses its concern on the expressed ability of some Governments to respond to such attacks with conventional weapons and reiterates that the most effective ways to prevent and address these new threats is through the joint cooperation among all States, and preventing the cyberspace to become a theater of military operations

217. Russia dedicated scant comments to the above issues as addressed in the OEWG initial Pre-Draft report, as follows:

5) The importance of "multi-stakeholder approach" with emphasis on the contribution of non-governmental sector, business and academia to ensuring responsible behaviour in the information space is artificially exaggerated. At the same time the problem of insufficient regulation of private sector activities in the ICT sphere and increasingly urgent issue of monopolization of this area is omitted as one of the key threats to the development of peaceful and competitive ICT environment.

218. The United Kingdom commented on the issue as follows:

The crucial nature of capacity building in supporting both the international cyberspace stability framework and the Sustainable Development Goals is well captured (Chapeau, F48). We fully support the references to two-way processes (F53) and the United Nations Women, Peace and Security agenda (F56). We consider any mention of the concept of the 'development of a global capacity-building agenda' (F55) would benefit from some clarification. We suggest that additional text could be included in this section to note the richness of the discussion on this topic, as well as strengthening the reference to the need for cyber diplomats to participate in OEWG discussions (F50). We consider that this section of the pre-draft must recognise that coordination is key (F55), but should also highlight the need for all States and stakeholders to contribute to the mobilisation of funding and resource for capacity building wherever possible, as this underpins our ability to implement the framework and achieve the recommendations made in this pre-draft. The UK may be able to support inclusion of certain recommendations subject to modifications and discussion of specifics of implementation. This includes…

. • 'establish a global mechanism for enhancing coherence in capacity-building efforts…' (H68D) Our primary concern is to see as much resource as possible directed to capacity building in a coordinated manner. The establishment of additional mechanisms could increase the existing coordination challenge, whilst diverting much needed funding to its set up costs. We propose the following alternative wording: The Secretary General be requested to call on Member States and stakeholders, including traditional development organizations and industry partners, to make available funding and resource in support of international capacity building on cybersecurity. All those in a position to contribute such expertise or resources to existing global mechanisms for enhancing coherence in capacity-

building efforts in the use of ICTs, including at the regional and sub-regional levels, should do so. (H68D)

- 'to identify and protect national and transnational critical infrastructure…' (H68D) We propose the inclusion 'to cooperate, including with stakeholders' on the basis of the extensive involvement of a broad range of stakeholders in the provision, operation and maintenance of critical national infrastructure.

The UK proposes inclusion of the following recommendations:

- 'ICT-related capacity-building efforts in the field of international security should be guided by the following principles:' Inclusive partnerships and shared responsibility; Ownership; Sustainability: Trust, transparency and accountability. (H68D) These principles reflect the Busan Principles adapted to the ICT context.

219. The United States commented on the issue as follows:

"Supranational," "trans-border," and "transnational" critical infrastructure were terms used by OEWG delegates, but it is unclear to us if delegates were using those terms interchangeably or not. If delegates view those terms as synonymous, we should choose one term to describe such critical infrastructure with international implications. If the terms are not viewed as synonymous, we should explain the distinctions among the terms. We are also unsure what it means to declare "supranational critical information infrastructure" a "special category" of such infrastructure, with protection that is a "shared responsibility" of all States. Most ICT infrastructure is owned and operated by the private sector and is located within the jurisdictions of individual States.

220. Uruguay commented on the issues as follows:

The construction of an open, safe and reliable cyberspace cannot be a task only for governments. Participation in capacity building is important not only for state actors but also international organizations, civil society and the technical community. The participation of non-governmental actors within the processes should be promoted, both in the Group of Experts and the Open-Ended Working Group, in order to achieve a true democratic and participatory approach.

5.2.4 *OEWG Second Pre-Draft Report*

221. On the basis of the above comments, the OEWG amended the text of the Pre-Draft Report as follows:

> 22. States underscored that attacks on critical infrastructure (CI) and critical information infrastructure (CII) pose a threat not only to security, but also to economic development and livelihoods, and ultimately the safety and wellbeing of individuals. The potentially devastating human cost of attacks on CI and CII supporting essential services to the public such as medical facilities, energy, water and sanitation, were stressed. Attacks on CI and CII that undermine trust and confidence in political and electoral processes, public institutions, or that impact the financial system, are also a real and growing concern.
>
> 23. States observed that CI and CII are defined differently in accordance with national prerogatives and priorities. In many States such infrastructure is owned, managed or operated by the private sector. In addition, CI and CII may be shared or networked with another State or operated across different States and jurisdictions (sometimes categorized as transborder, transnational or supranational infrastructure). As a result, inter-State or public-private cooperation may be necessary to protect its integrity, functioning and availability.
>
> 24. In light of the increasingly concerning digital threat landscape, and recognizing that no State is sheltered from these threats, the OEWG underscored the urgent need for States to further develop, through multilateral forums, cooperative measures to address such threats. It was affirmed that acting together and inclusively whenever feasible would produce more effective and far-reaching results. The value of further strengthening collaboration with the private sector, civil society and academia was also emphasized in this regard. […]
>
> 52. States drew attention to the roles and responsibilities of other actors, including the private sector, academia and civil society, in contributing to building trust and confidence in the use of ICTs at national, regional and global levels. States noted the variety of multi-stakeholder initiatives that, through the development of principles and commitments, have established new networks for exchange, collaboration and cooperation. In a similar vein, sector- or domain-specific initiatives have demonstrated the growing awareness of the roles and responsibilities of other actors and the unique contributions that they can make to

ICT security through voluntary commitments, professional codes and standards. […]

59. The importance of a multi-stakeholder approach to capacity-building that addresses technical and policy gaps in all relevant sectors of society was highlighted. States noted in particular that sustainability in capacity-building can be enhanced by an approach that entails engagement and partnership with local civil society, academic institutions and private sector actors. In this regard, it was also emphasized that national approaches to ICT security could benefit from adopting a cross-sectoral, holistic and multi-disciplinary approach to capacity-building, including by establishing national coordination bodies with the participation of relevant stakeholders to assess the effectiveness of programs. Such an approach may also help address challenges posed by newly emerging technologies.

6 International cooperation in the cybersecurity domain

222. The issue of cooperation is addressed in most national positions in favourable terms. Though differences exist among these positions, States generally support the idea of cooperating with a view to ensure peaceful use of the cyber space.

223. Accordingly, it is suggested that Italy, too, expresses its position in positive terms on the issue.

6.1 *Issues not debated*

224. The only issue which does not appear currently debated is the one concerning the contents of cooperation. On this count, States endorse the widest array of cooperation measures, ranging from capacity-building to information-sharing, with confidence-building measures acting as a means to further foster cooperation.

225. Alignment with this position is suggested also against the background of Italy being a technologically developed State which might benefit from the enhancement of cyber security protocols outside its territory.

226. Accordingly, it is suggested that Italy endorses cooperation by means of confidence-building, capacity-building and information-sharing.

6.2 *Issues still under debate*

227. Divergences exist on two discrete points, namely:

v. Whether regional or global cooperation should be preferred.

vi. Whether a new body of institutional cooperation is necessary.

6.2.1 *Preference for regional or global cooperation*

228. As to issue *i*), that is the preference for regional or global cooperation, it is to be noted that Italy has already endorsed a regional level of cooperation in its comments to the OEWG First Pre-Draft Report (para 242).

229. The above Italian position is in line with the EU Lines to Take of January 2020 (para 239) and has been endorsed by other EU Countries (paras 244-246), with specific regard to confidence-building.

230. However, Italy's diplomatic connection with non-EU Mediterranean States makes it suited to foster cooperation and partnership outside the regional level. As such, reference may be added to the possibility of establishing partnership also bilaterally.

231. Accordingly, it is suggested that Italy expresses its support for cooperation both at a regional level of cooperation, and bilaterally, so as to consider the possibility of fostering cooperation with African states.

6.2.2 *New institutional framework*

232. As to issue *ii*), namely the necessity of a new body for regular institutional dialogue, it is to be noted that Italy already excluded such possibility in its comments to the First Pre-Draft Report (para 242).

233. This, again, appears in line with the EU Lines to Take (para 239). States have expressed concerns on the issue of a new institutional framework (France, *infra* para 245) and stressed the need to avoid duplication (The Netherlands, *infra* para 246).

234. However, in line with the emphasis put on confidence and capacity-building, Italy may endorse the establishment of regular cooperation mechanism within existing institutional framework as

a way to foster compliance with shared standards of cyber security. This is apparently also endorsed by the Joint submission of *The Future of Discussion on ICT* (*infra*, para 240).

235. To this effect, Italy may refer to the experience of compliance review mechanism in the field of environmental law as bodies tasked with dispute management and prevention functions, as well as a role in facilitating technical assistance to States with lower technological and financial capacities.

236. Accordingly, it is suggested that Italy stresses the role of existing institutional framework in fostering cooperation in cyber security. Italy may further express its pledge to establishing bodies of compliance review within those existing frameworks, so as to facilitate technical assistance.

6.3 *Review of National Positions*

237. Australia National Position reads as follows (pp. 23-24):

> **Cooperative Measures** promote collaboration between countries based on a mutual commitment to improve cyber resilience and reinforce a peaceful and stable online environment.
>
> a. Australia cooperates bilaterally with a wide range of states, including through a high tempo of regional and global bilateral visits and established cyber policy dialogues with ASEAN, China, India, Indonesia, Japan, and the Republic of Korea. We are also active participants in regional and multilateral cyber meetings. These visits, dialogues and meetings provide an opportunity to engage openly on national strategies and policies, best practices, decision-making processes, relevant national organisations and measures to improve international cooperation (policy, legislative, and operational).
> b. Through its Cyber Cooperation Program (Program), Australia works across the Indo-Pacific to improve cyber resilience and thereby promote international stability, while driving global economic growth and sustainable development. The Program supports Australia's commitment to deliver on the UN 2030 Agenda for Sustainable Development, which recognises the vital role of digital technologies to achieve a better and more sustainable future for all. Australia has increased its investment through the Cyber Cooperation Program from $4

million in 2016 to $34 million out to 2023. Key initiatives delivered under the Program include:

i. Supporting establishment of the Pacific Cyber Security Operational Network (PaCSON) to share best practice across the Pacific on cyber incident response and build knowledge and awareness of cyber security threat information, tools, techniques and ideas (2017- 2020);
ii. International cyber law courses for government legal advisers from ASEAN and the Pacific, jointly funded with Singapore and the Netherlands and delivered through Cyber Law International (2018-2020); and
iii. Tailored training across the ASEAN region to consider agreed norms of acceptable state behaviour in cyberspace as recommended by the 2013 and 2015 UNGGE reports, jointly funded with the UK and delivered through the Australian Strategic Policy Institute (2019- 2020).
iv. DFAT's Cyber Bootcamp Project, which provides partners across the Indo-Pacific region with an opportunity to engage directly with policy and operational specialists from across Australia's public, private and academic sectors. Bootcamps aim to build confidence in countries' capacities to understand and engage with the full spectrum of cyber-related challenges, issues and opportunities within the region.

c. Under the Australia-Papua New Guinea (PNG) Cyber Security Memorandum of Understanding signed in 2018, Australia partnered with PNG to establish the PNG National Cyber Security Centre (NCSC). Australia will continue to collaborate with PNG to ensure the NCSC is a sustainable national capability, including through delivering training in cyber security governance, technical cyber security and incident response.
d. Together with Singapore, Australia led development of the 2018 EAS Leaders Statement on Deepening Cooperation in the Security of Information and Communications Technologies and of the Digital Economy, which affirmed EAS member states commitment to cooperate on a range of cyber and digital issues.

Australia will remain a vocal supporter of, and active player in, the development of CBMs at the bilateral, regional and international levels.

238. The 2018 Commonwealth Cyber Declaration reads as follows:

> Recognising the importance of international cooperation in tackling cybercrime and promoting stability in cyberspace, we:
> 1. Commit to the establishment of effective and proportionate domestic cybercrime and cybersecurity frameworks that take into account principles in existing international instruments, acknowledging the evolving tactics of cybercriminals and the transnational nature of cybercrime. Commit to use national contact points and other practical measures to enable cross-border access to digital evidence through mutually agreed channels to improve international cooperation to tackle cybercrime.
> 2. Commit to work towards common standards, harmonised legal approaches and improved interoperability, including through the use of Commonwealth model laws; and commit to considering the potential for further Commonwealth cooperation in this regard, including the possible coordination of common positions in international fora.
> 3. Commit to promote frameworks for cyberspace, including the applicability of international law, agreed voluntary norms of responsible state behaviour, and the development and implementation of confidence building measures to encourage trust, cooperation and transparency, consistent with the 2015 Report of the United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International security (UNGGE).
> 4. Commit to move forward discussions on how existing international law, including the Charter of the United Nations, and applicable international humanitarian law, applies in cyberspace in all its aspects.

239. The EU Lines to Take in view of UN OEWG on security & telecommunications in context of international security of 31 January 2020 reads as follows:

> 24. The EU and its Member States believe that a practical way forward should encourage increased cooperation and transparency to share best practices, including on how UN GGE norms are applied, through related initiatives and frameworks, such as regional organizations and institutions, to facilitate raising awareness and to effectively implement agreed norms of responsible behaviour. […]

29. The EU and its Member States underline the importance of confidence-building measures (CBMs) as a practical means of preventing conflicts.

30. Building effective mechanisms for state interaction in cyberspace is essential to reducing the likelihood of conflict. Regional fora have proven to be a relevant platform to create space for dialogue and cooperation among actors with shared concerns but common interests in order to address effectively specific regional challenges.

31. Cross-border cyber incidents remain a major threat in cyberspace, as they can leads to escalation and conflict. Through cooperation and information sharing, regional confidence building measures have been proven to reduce the risk of misinterpretation, escalation and conflict that may stem from ICT incidents.

32. The EU and its Member States reaffirm that implementing cyber CBMs in the OSCE, ARF, OAS and other regional settings will increase the predictability of state behaviour and reduce the risks of misinterpretation, escalation and conflict that may stem from ICT incidents thereby contributing to long term stability in cyberspace. In addition, the OEWG could consult with relevant regional organizations on CBM implementation in order to share best practices in view of the development and implementation of CBMs at the global level, with an aim as a first step to increase transparency.

240. The joint submission on *The future of discussions on ICTs and cyberspace at the UN* of 12 February 2020 reads as follows:

> 3/ Step up cooperation and capacity building, building on the implementation meetings, by defining what the most urgent needs are and by fostering coordination between States when relevant. We believe that capacity building will be crucial to ensure the success of a PoA.

6.4 *Comments to the initial OEWG Pre-Draft Report (April 2020)*

6.4.1 *OEWG Initial Pre-Draft Report and Italian comments thereto*

241. The issue of cooperation was addressed in the OEWG Initial Pre-Draft Report of April 2020 as follows:

E. Confidence Building measures […]

41. In their discussions at the OEWG, States highlighted the need to translate confidence-building measures into concrete actions that are implementable by all States.
42. States noted the continuing relevance of the CBMs recommended in the consensus GGE reports. Measures highlighted for priority attention included regular dialogue and voluntary information exchanges on existing and emerging threats, national policy or doctrine, national views on how international law applies to State use of ICTs, and national approaches to defining critical infrastructure or categorizing ICT-related incidents. Other such measures included developing guidance, training for diplomats, exchanging lessons on establishing and exercising secure crisis communication channels, and operational exercises at the technical level between Computer Emergency Response Teams (CERTs) or Computer Security Incident Response Teams (CSIRTs).
43. States highlighted that the dialogue within the Open-ended Working Group was in itself a CBM, as it stimulates an open and transparent exchange of views on perceptions of threats and vulnerabilities, responsible behaviour of States and other actors and good practices, thereby ultimately supporting the collective development of the normative framework that guides the use of ICTs by States.
44. In particular, States stressed that establishing national Points of Contact (PoC) constitutes a prerequisite for the implementation of many CBMs, and is invaluable in times of crisis. States may find it useful to have PoCs for, inter alia, diplomatic, policy, legal and technical exchanges, as well as incident reporting and response. It was suggested that a global directory of Points of Contact would be useful. At the same time, it was noted that the security of such a directory as well as its operational modalities would be crucial to its success. The value of regularly conducting exercises among a network of PoCs was also emphasized, as it can help to maintain readiness and ensure that PoC directories remain updated.
45. As CBMs can be developed at the bilateral, regional or global level, States proposed the establishment of a global repository of CBMs, with the objective of sharing policy, good practice, experiences with CBM implementation and

encouraging peer learning. Such a repository could also assist States to identify additional CBMs appropriate to their national and regional contexts.

46. Drawing from the lessons and practices shared at the OEWG, States emphasized that the prior existence of national and regional mechanisms and structures, as well as adequate resources and capacities, are essential to ensuring that CBMs serve their intended purpose. In this regard, States underscored the significant efforts of regional and sub-regional bodies in developing CBMs, adapting them to their specific contexts, as well as the crucial awareness raising and information sharing role that cross-regional or inter-organizational exchanges have served. It was noted that, as not all States are members of a regional organization and not all regional organizations have CBMs in place, it is important that other fora are used to promote CBMs as well. States also proposed that some CBMs developed at the regional level could be universalized.

47. States drew attention to the roles and responsibilities of other actors, including the private sector, academia and civil society, in contributing to building trust and confidence in the use of ICTs at national, regional and global levels. States noted the variety of multi-stakeholder initiatives that have, through the development of principles and commitments, established new networks for exchange, collaboration and cooperation. In a similar vein, sector- or domain-specific initiatives have demonstrated the growing awareness of the roles and responsibilities of other actors and the unique contributions that they can make to ICT security through voluntary commitments, professional codes and standards. […]

F. Capacity-building […]

48. In their discussions at the OEWG, States reiterated the recommendations on international cooperation and capacity-building in the consensus GGE reports. They emphasized the critical function that capacity-building can play with regard to empowering all States and other relevant actors to fully participate in the global normative framework, while also contributing to shared commitments such as the 2030 Sustainable Development Agenda. In addition, capacity-building plays an important enabling function for promoting adherence to international law and the implementation of the voluntary, non-

binding norms of responsible State behaviour and the CBMs recommended by the previous GGEs, while also offering important opportunities for building understanding between and within States.

49. States noted that capacity-building helps to address the systemic and transnational risks arising from a lack of ICT security, disconnected technical and policy capacities at the national level, and the related challenges of inequalities and digital divides. Capacity-building aimed at enabling States to identify and protect national critical infrastructure and to cooperatively safeguard supranational critical information infrastructure was deemed to be of particular importance.
50. There was a general acknowledgement that in addition to technical skills, there is a pressing need for building expertise across a range of diplomatic, policy, legislative and regulatory areas.
51. Many challenges were identified that hinder or reduce the effectiveness of capacity-building. The lack of coordination at the international level was highlighted as a significant concern. Practical challenges in the design, delivery, sustainability and accessibility of capacity-building activities, and the lack of specific metrics to measure their impact, were also raised. Once capacity has been built, some countries face the challenge of talent retention in a competitive market for ICT professionals. States highlighted that lack of access to ICT security-related technologies was also an issue.
52. States underscored that ICT-related capacity-building efforts would be more effective if they were guided by widely accepted principles. 7 To this end, States stressed the importance of national ownership in the identification of capacity-building and technical assistance needs and priorities. They also noted that capacity-building should be demand-driven, tailored to specific needs and contexts, evidence-based, results-oriented, and have sustainable impacts. Capacity-building initiatives should be transparent and accountable. Additionally, it was emphasized that capacity-building should be non-discriminatory, politically neutral, gender sensitive, and focus on peaceful outcomes. In this regard, States underscored that technical capacity-building and capacity-building on the normative framework should go hand-in-hand.
53. States stressed that capacity-building is a shared responsibility as well as a reciprocal endeavour, a so- called “two-way street”, in which participants learn

from each other and where all sides benefit from the general improvement to global ICT security. The value of South–South and triangular cooperation was also recalled.

54. The importance of a multi-stakeholder approach in capacity-building was highlighted. States noted in particular that sustainability in capacity-building can be enhanced by an approach that entails engagement and partnership with local civil society, academic institutions and private sector actors.

55. States stressed that there was a need for greater coordination in capacity-building efforts. In this regard, States suggested that existing platforms within the United Nations and in the wider global community could be used to strengthen coordination. These platforms could be used to share national views on capacity-building requirements, encourage the sharing of lessons and experiences from both recipients and providers of support, and facilitate access to information on capacity- building and technical assistance programmes. These platforms could also support the mobilization of resources or assist with pairing available resources with requests for capacity-building support and technical assistance. It was suggested that the development of a global capacity-building agenda would help to ensure greater coherence in capacity-building efforts.

56. States called attention to the "gender digital divide" and urged that specific measures be taken at the national and international levels to address gender equality and the meaningful participation of women in international discussions and capacity-building programmes on ICTs and international security. States expressed appreciation for programmes that have facilitated the participation of women in multilateral ICT-security discussions. The need to strengthen linkages between this topic and the United Nations Women, Peace and Security agenda was also emphasized.

G. Regular Institutional Dialogue […]

57. In their discussions at the OEWG, States affirmed that given increasing dependency on ICTs and the scope of threats emanating from their misuse, there was an urgent need to enhance common understandings, build confidence and intensify international cooperation.

58. The consensus GGE reports of 2010, 2013 and 2015 called attention to the need for regular dialogue on the international security dimension of ICTs. The 2010 report8 recommended further dialogue among States to discuss norms, reduce collective risk and protect critical infrastructure. In 2013, in recognition that the speed of ICT developments and the scope of the threat merited strengthening cooperation and finding common ground, the GGE recommended regular institutional dialogue with broad participation under the auspices of the United Nations, as well as encouraged dialogue in bilateral, regional and other international forums. 9 The 2015 GGE reiterated the need for regular dialogue at the United Nations, while cautioning against duplication of efforts.10
59. States suggested many potential purposes for regular dialogue, including awareness raising and information exchange; developing guidance to support and monitor the implementation of existing commitments and recommendations; building trust and confidence; coordinating, strengthening and monitoring effectiveness of capacity-building; identifying and exchanging good practices; encouraging further study and discussion on areas where no common understanding has yet emerged; and negotiation of further commitments of a voluntary or binding nature. It was also emphasized that any platform for regular institutional dialogue should be a process building on previous agreements, inclusive, consensus driven, sustainable, results-oriented, with specific objectives that take forward agreements in practical and tangible ways.
60. States noted that there are established venues within the UN Disarmament Machinery where ICTs and international security could be addressed within existing resources, including the General Assembly's First Committee and the United Nations Disarmament Commission. It was also recalled that a variety of external venues for regular dialogue on these topics already exist, including at the regional and sub-regional levels. Nevertheless, States emphasized that while these are complementary efforts, they are not a substitute for regular dialogue under UN auspices due to its inter-governmental nature, inclusiveness and legitimacy.
61. Noting that many parts of the UN address digital technology issues, including their development, rights and crime dimensions, States recognized the need for

a dedicated mechanism under UN auspices focusing on international security issues. It was recalled that there are established forums within the UN system focused on issues relating to ICTs and terrorism, crime, human rights and Internet governance. Greater exchange and exploration of synergies between these bodies, such as through joint meetings of committees of the General Assembly, while respecting the expert nature or specialized mandate of each, was encouraged.11

62. A variety of proposals were made to take forward regular institutional dialogue. It was noted that the GGE process since 2004 has been a form of regular dialogue. It was also suggested that the format of the OEWG, with its inclusive membership and transparent discussions, should become the standard for discussion and therefore the renewal of its mandate was called for. It was highlighted that there was value in having the sixth Group of Governmental Experts meeting in parallel to the OEWG, stressing their complementarity and the opportunity to capitalize on the unique features of each process. Looking beyond the mandates of the OEWG and sixth GGE, a further suggestion was that regular institutional dialogue could be the follow-up mechanism to a politically binding instrument.12 Another possibility raised was that an inter-governmental specialized agency could be established.

63. In addition to questions concerning the four characteristics—"regular", "institutional", "broad participation", and "under UN auspices"—noted in the OEWG mandate,13 additional queries were raised concerning the duration of such dialogue, the timing of establishing a new mechanism for dialogue prior to the conclusion of the work of the sixth GGE, potential locations, and budgetary considerations.

64. The OEWG's mandate provided for the possibility of holding intersessional consultative meetings with other stakeholders, including the private sector, non-governmental organizations and academia. The three-day informal consultative meeting of the OEWG held in December 2019 produced a rich exchange between States and other stakeholders. The OEWG also heard interventions from non- governmental organizations during an informal multi-stakeholder segment at its first and second sessions. In order to further inform their engagement with the OEWG, some States noted that they have conducted domestic multi-stakeholder consultations or calls for submissions.

65. It was recalled that States hold primary responsibility for national security, public safety and rule of law. It was also noted that regular dialogue should be primarily intergovernmental in nature, and an appropriate mechanism to leverage the experience and knowledge of other stakeholder groups would need to be found. In their interventions, States acknowledged that building a more resilient and secure ICT environment necessitates multi-stakeholder cooperation and partnerships. While recognizing the unique role and responsibility of States in relation to security, there was growing appreciation that States may benefit from the expertise in non-governmental communities and that responsible behaviour of other actors makes an essential contribution to this environment.

242. In line with the EU comments and comments by other EU Countries (below), Italy commented the above language as follows:

E. Confidence Building Measures

The chapter could open by reiterating that there is widespread acknowledgement on the importance of Confidence Building Measures (CBMs) as a means to defuse tension and prevent unintended

conflicts stemming from the use of information and communication technology.

We support the idea to move from regional to global, starting from certain CBMs, such as the one establishing National Focal Points of Contact. A network of PoC involving the entire membership of the UN could indeed better address the global challenges arising from the use of ICTs and should be considered as a CBM in itself, and not only a prerequisite for the implementation of CBMs.

In most cases, CBMs have yet to be fully operationalized even at regional level. We therefore support the proposal to share best practices on their implementation, building also on initiatives developed by regional organisations, such as the OSCE and ASEAN, to assist States in translating CBMs into practice. At the same time, we would like the report to include a reference to the need for avoiding duplication and overlapping.

Some of the existing CBMs are based on a multi-stakeholder approach. We see it as an added value, consistent with our position on the need to foster cooperation with the private sector and academia.

We would therefore like to see this element reflected in the report as well (para. 47 could be expanded with a reference to CBMs developed by States that require the involvement of the private sector to be fully operationalized).

F. Capacity building

The chapter on capacity building reflects the importance that most States, including Italy, attach to it, as well as the richness of discussions and the membership's expectations on this topic. In fact, Capacity Building can play a crucial role also for the implementation of the 2030 Sustainable Development Agenda. Moreover, the report could further highlight that, at different levels, capacity building is a work in progress for all.

We stress the need to avoid duplication of efforts and, while reckoning it is complicated, we should also consider monitoring the effectiveness of the programs.

The report makes reference to the proposal of establishing a global mechanism aimed at enhancing coherence in capacity building efforts in the use of ICTs, suggested by some States. Such a proposal requires further discussion also on the practical means to realize it. In any case, it should be conceived as a tool to increase coordination and coherence and to avoid duplication. Regional and sub-regional capacity building initiatives should be taken into account. The multi-stakeholder approach of current efforts should also be preserved.

Regarding the principles that should guide any capacity building program, we align to the list proposed by the EU.

The proposal to develop a global capacity building agenda should be further clarified as its scope and aims are not entirely clear. The reference to it as it stands now in the text should be either eliminated or further elaborated upon.

G. Regular institutional dialogue

The report captures the lengthy discussions held around the possibility to establish a regular institutional dialogue as well as the lack of consensus, at this stage, on the way forward.

While sharing the view that substantial and frequent exchanges among Member States are essential, we would like to reiterate that any reflection on the establishment of a regular institutional dialogue is premature and should be based on the achievements of both the OEWG and the GGE, whose mandate expires in

2021. This position, shared by a great number of States, should be appropriately reflected in the text.

The report makes also reference to the suggestion to establish a regular institutional dialogue as a follow up mechanism to a politically binding instrument. However, there is a lack of consensus about negotiating such an instrument and this should be reflected in the text.

6.4.2 *Comments by EU and EU Member States*

243. The EU comments on the language contained in the OEWG Initial Pre-Draft Report reads as follows:

On confidence building measures

22. With regard to confidence-building measures (CBMs), the EU and its Member States underline the importance of CBMs as a practical means of preventing conflicts.

23. The EU and its Member States welcome the initiative to establish a mechanism to share best practices on CBMs, in coordination with interested regional and sub-regional bodies, without prejudice to the further development and implementation of CBMs at different levels. Advancing the operationalisation of such a mechanism should focus on voluntary cooperation with other States, including through existing fora, on their implementation, and should not pre-empt the development and implementation of additional CBMs, notably in regional organizations.

24. As proposed, the OEWG should consult with relevant regional organizations on CBM implementation in order to share best practices in view of the development and implementation of CBMs at the global level, without duplicating any regional efforts, with an aim as a first step to increase transparency; for instance, through the establishment of a global registry of national Points of Contacts. Such coordination between the relevant part of the United Nations system and interested regional organizations should be conducted in accordance with the decision-making processes of these regional organizations.

On capacity building

25. The EU and its Member States underline the importance of capacity-building as a means to strengthen resilience globally, with particular attention to developing countries.

26. The EU and its Member States note the recommendation to establish a global pairing mechanism for enhancing coherence in capacity-building efforts in the use of ICTs and would welcome dedicated discussions on the form of a facilitation mechanism, including on the relevant issues to address, such as financial aspects, scope, etc, bearing in mind that such mechanism should contribute to existing global multi-stakeholder efforts while avoiding duplication. As a first step, the EU and its Member States stand ready to share additional information on their existing capacity-building programmes, and invite developing countries and other potential partners to further specify their needs and expectations in this area.

27. The EU and its Member States actively promote the Busan Principles, namely ownership, sustainability, inclusive partnerships and shared responsibility, trust, transparency and accountability to guide ICT-related capacity-building efforts in the field of international security.

28. In addition, the EU and its Member States believe that ICT-related capacity-building efforts in the field of international security should also be guided by the following principles:

a. the understanding that existing international law and existing norms apply in cyberspace;
b. rights-based and gender-sensitive by design, with safeguards to protect fundamental rights and freedoms;
c. in line with a democratic and efficient multi-stakeholder internet governance model;
d. supporting the principles of open access to the Internet for all without undermining the integrity of infrastructure, hardware and services;
e. supporting a shared responsibility approach that entails involvement and partnership across public authorities, the private sector and citizens and promoting international cooperation.

29. The EU and its Member States also support the recommendation to further cooperate to build capacity to identify and protect national and transnational critical infrastructure, as well as supranational critical information infrastructure – which has been a long-standing priority for the EU. This is why the EU is sponsoring, in

cooperation with Singapore, a CBM on the Protection of ICT Enabled Critical Infrastructures, within the ASEAN Regional Forum (ARF), and would encourage sharing best practices on the implementation progress of this CBM in order to support our work.

On regular institutional framework

30. The EU and its Member States emphasize that any regular institutional framework should respect a number of principles: avoiding duplication of existing work, be consensus-driven, include open-ended consultations where appropriate with interested stakeholders, and support dialogue that provides for results-oriented, expert discussions, and that takes forward work in practical and tangible manner.

31. Bearing in mind the position of the EU and its Member States that the time is not appropriate to make any recommendation on a regular institutional framework, many provisions for any regular institutional framework, including the purpose, scope, financing, participation etc. will require further discussion, and we should aim to resume our work to support both a complementary approach with the UN GGE on advancing responsible behaviour, which will finish its work in 2021, and a constructive approach to build upon the work of both groups.

244. Estonia commented as follows:

On Confidence-building Measures

21. Estonia re-affirms the notion of interlinkages between norms and confidence-building measures as the latter may often support the effective implementation of the voluntary and non-binding norms. Operationalisation of confidence-building measures – in a way that could allow a region-specific approach – could effectively increase security and stability in these regions as well as potentially address inequalities and the existing digital divide between Member States.

22. Estonia is supportive of the idea of establishing national Points of Contact as it would increase the effective implementation of CBMs regarding policy/diplomatic, legal and technical questions. Some regional organisations (e.g. the OSCE) already have started with the Estonia's comments to the OEWG pre-draft report operationalisation of PoC network that this initiative could take into account and share information about to other regional organisations (Article 44).

23. Estonia would be supportive of an idea to add to the global repository a list of confidence-building measures adopted at regional and sub-regional levels to enable the sharing or exchange of information and best-practices on confidence-building measures; e.g. a global registry of national points of contacts that could enhance the global political/diplomatic and technical network and expertise in cybersecurity (Article 45).

On Capacity-building

24. Estonia fully supports the idea that all UN Member States need to build capacities to identify and protect national critical infrastructure (Article 49).

25. Additionally, further capacity-building efforts should focus on all elements of the 2013 and 2015 GGE reports varying from international law, policy/diplomatic, technical and regulatory areas (Article 48-50).

26. The variety and volume of capacity building projects has created a requirement for better global coordination between the existing initiatives. In order to improve efficiency and avoid duplication in coordination efforts, Estonia supports using the existing global capacity-building coordination platforms, such as the Global Forum of Cyber Expertise (Article 55).

27. We support the inclusion of human rights and gender perspective to capacity building efforts, these two elements should also shape the approach to capacity-building to ensure more stable societies and economic growth (Article 56).

On Regular Institutional Dialogue

28. The dialogue in the UN First Committee should be guided by the existing consensus to implement the voluntary and non-binding norms, confidence-building measures, as well as address capacity-building, and to elaborate on how States interpret international law's applicability to cyberspace (Article 58). The format of the dialogue should support the goal to strengthen international peace and stability, and conflict prevention in cyberspace.

245. France commented on these issues as follows:

V. Confidence-building measures

Considerable work on confidence-building measures has been done within the OEWG this year. These discussions appear to be reflected in the current proposals,

particularly when it comes to the importance of regional organizations. Within the OSCE, States participate on a voluntary basis in the implementation of confidence-building measures. Engaging in this work and cooperating is also a confidence-building measure in itself. The drafting of confidence-building measures is essential to create the conditions for serene dialogue between States, to prevent conflicts and to avoid escalation in the event of crises.

Rather than producing a repository of existing confidence-building measures implemented at regional level, the OEWG would undoubtedly benefit from working with regional bodies in order to draw up guidelines to ensure the effectiveness of such arrangements. For example, it could highlight the relevance of organizing operational exercises, as mentioned in the pre-draft, as well as strategic-level exercises, in order to enable optimal information-sharing and ensure linkage with the political level.

VI. Capacity-building

As the report highlights, capacity-building should be a major aspect of international reflection on security and stability in cyber space. Through capacity-building programmes, we can hope to improve global resilience.

We need to foster programmes which, beyond awareness-raising, offer long-term approaches and help support the development of resilient national systems and human resources associated. Effective capacity-building has to be based on programmes created jointly with beneficiaries. Capacity-building programmes also need to be developed for the private sector, which operates a large number of our critical infrastructures. Work on national governance bodies could also help produce more effective and efficient national models. These points should appear in the report.

There is a real lack of resources and there are difficulties matching needs and provisions. Good cooperation and optimal use of resources are one of the major difficulties of capacity-building. It would be useful for the report to more explicitly refer to the institutions outside the UN that could play this role internationally.

VII. Regular Institutional Dialogue

The possibility of “dedicated mechanisms” or the creation of different formats, including an inter-governmental agency, is mentioned in the Regular Institutional

Dialogue section. Many States expressed the view that the form should be guided by the content if a specific format were to be created, a point which has yet to be proven. France would like the report to better reflect this concern.

The nature of multi-stakeholder consultations reflects the discussions conducted during the first two sessions. Although the decisions within a working group attached to the United Nations First Committee should be inter-governmental, consultation with the various stakeholders remains essential. Throughout the process, the group would likely have benefited from more discussions in various formats, including with stakeholders which have not traditionally had the opportunity to express themselves within the UN. France supports the inclusion of these points in the final report.

246. Germany commented as follows:

Germany is open to extending the OEWG /establishing a new OEWG for another year. In particular this would give us more time to discuss the issues in relation to a regular institutional dialogue that are mentioned in paragraph 62 and allow us to take into account the proceedings of the current GGE while deliberating on this issue.

Germany would also suggest changing the suggested draft language in Paragraph 65, which appears to present a weaker standpoint on multistakeholder participation than that previously agreed to by the UN membership. This should be replaced with language which strongly supports multistakeholder participation. The language from the 2015 report of the GGE (A/70/174), which received UN consensus adoption in 2015 via Resolution 70/237 could serve as the basis for this.

247. The Netherlands commented as follows:

Confidence-Building Measures

33. The Netherlands sees confidence building as one of the most important objectives of the OEWG. The CBMs developed by the previous UN GGEs, complimented and brought forward by regional organizations, e.g. the OSCE, are a key element in achieving this.

34. The Netherlands highlights that not all States are members of regional organizations and that not all regional organizations have CBMs in place. In our opinion, the implementation of the CBMs contained in the GGE reports should

therefore be considered as international priority. Regional organizations not yet having CBMs should be encouraged to develop those and could benefit from using existing regional CBMs as a template, e.g. from the OSCE. It should be noted that because cyberspace is borderless, CBMs should facilitate cross-regional and international confidence building. The report of the OEWG should encourage states and regional organizations to facilitate cross-regional and international confidence building.

35. The Netherlands is supportive of further exploring the establishment of a repository of national Point of Contacts and the establishment of a repository of CBMs on bilateral, (sub) regional, multilateral and multistakeholder level. Further clarification on the role of the Secretary-General and UNIDIR, and related costs, concerning the establishment of the repository of CBMs and the establishment of a global registry of national Point of Contacts, is needed in order to fully support the recommendations.

36. The Netherlands underlines that international law, complemented by the norms formulated in the UN GGE reports, provides states with a framework for responsible behaviour in cyberspace. It is up to states to closely stick to this framework and to demonstrate the requested restraint. The Netherlands suggests that the OEWG advices States to make declaratory statements to adhere to this framework, to the positive and negative obligations, and demonstrate restraint.

Capacity building

37. The Netherlands deems cyber capacity building as the vehicle that strengthens the overall security and resilience in cyberspace. The report should underline the necessity to have a cross-sectoral, holistic and multidisciplinary approach to capacity building in the context of cybersecurity. The Netherlands would like to underline that capacity should be built in multiple areas, as are listed in paragraph 50. However, we believe that capacity building should be done around the “legal” aspect as well and is missing in the current listing.

38. The Netherlands supports a stronger involvement of other stakeholders in the field of capacity building, as expertise and capacities lie in the hands of the private sector, the technical community, academia and civil society.

39. During the substantive meetings of the OEWG, a great number of delegations mentioned the interplay between capacity building and the Sustainable

Development Goals (SDGs). The Netherlands thinks that the report should clearly affirm that capacity-building efforts in the field of ICTs are a foundational element of the achievement of the SDGs. We suggest that a recommendation in that sense be added.

40. The Netherlands would like to suggest that the report becomes more specific and explains how cybersecurity capacity building and SDGS' mutually reinforce each other. In the written contribution of the Netherlands to the Chair, we specifically point out several SDGs of specific relevance to the discussion, including SDG9 on resilient infrastructure, SDG10 on reducing inequalities and SDG5 on gender equality. The Netherlands thinks these could be useful examples on how the SDGs and cybersecurity capacity building are interlinked.

41. As raised in the Netherlands submission to the Chair1, we believe that the OEWG in its recommendation should call for the endorsement of the principles of capacity building that have been recognized by the Global Forum on Cyber Expertise in the Delhi Communiqué namely:

i. Ownership: nations need to take ownership of capacity building priorities focus on sustainable developments;
ii. Sustainability: obtaining sustainable positive impact should be the driving force for cyber capacity building;
iii. Inclusive partnerships and shared responsibility: effective cyber capacity building requires cooperation among nations, through a multi-stakeholder approach;
iv. Trust, transparency and accountability: transparency and accountability play a key role in establishing trust, which is necessary for effective cooperation.

In our view, this will support a more effective capacity-building co-operation, based on mutual trust between all parties involved.

42. When referring to a global capacity-building agenda, the Netherlands would like this proposal to be further clarified. At the moment, it is unclear what is meant by such an agenda and if it is something that already exists.

43. The Netherlands sees merit in the UN playing a more distinct convening role in the area of capacity building as long as it enhances and supports the work of regional organizations and existing global multistakeholder endeavors such as the Global Forum on Cyber Expertise (GFCE). The UN could play a meaningful role in creating a venue where those organizations interact in order to ensure

complementarity and mutual reinforcement of initiatives. We would thus like to caution against duplication of the abovementioned existing widely supported regional and multistakeholder initiatives and would welcome more clarification in the text to this end. The Netherlands is ready to share additional information on the existing capacity-building programs and invites digitally developing countries and other potential partners to further specify their needs and expectations in this area.

44. Furthermore, the Netherlands would like to see a recommendation urging all member states to make capacity-building efforts in the use of ICTs a priority in their national and international capacity building efforts and to urge development organizations to incorporate these programs into their development agendas. In order to ensure sustainability of these capacity-building initiatives, attention should be paid to the cybersecurity aspect of these initiatives.

Regular Institutional Dialogue

45. The Netherlands supports an open dialogue, that avoids duplication of existing work, within and outside of the UN, includes interested stakeholders, private sector, academia and civil society, be consensus-driven, but is not endorsing any new legally binding instrument, nor the result of a "politically binding instrument". The Netherlands will consider any proposal with the aim of reinforcing existing international and multi-stakeholder dialogue on its merits, within the scope of the First Committee, thus limited to responsible State behaviour in cyberspace in the context of international peace and security.

46. The Netherlands does not recognize the current recommendations as an outcome of the previous discussions. The pre-draft gives the impression that the discussion on a regular institutional dialogue is finalized and reached a conclusion. Which in our opinion is not the case, the Netherlands, together with a large majority of states have expressed their support for the OEWG. We found the discussions to be constructive, useful and fruitful but there are several questions remaining, which have also been raised by other delegations. In particular, questions on the criteria, modalities, and costs, to be applied if such a dialogue were to be created and endorsed. This is currently not clearly stated in the pre-draft. The Netherlands considers the discussion ongoing. Therefore, the Netherlands is of the view that the recommendation to convene a new OEWG and GGE, both, at the 76th session of

the UNGA is premature. Further discussion on the topic of regular institutional dialogue is definitely needed.

47. The Netherlands reiterates that any proposal must be designed to include all stakeholders. In our opinion, the pre-draft does not reflect enough the knowledge and the input the multi-stakeholders had during the discussions. The Netherlands would like the final report to not only mention the organization of the inter-sessional consultations, but to also reaffirm the importance of multistakeholderism and recognize the expertise and knowledge that lie outside the hands of governments. The Netherlands would recommend the report of the inter-sessional consultations to be annexed to the final report.

48. The Netherlands recognizes that the current COVID-19 pandemic brings us in an unprecedented situation. It raises important practical and substantive questions related to the future work of the OEWG and its upcoming meetings. The Netherlands remains open to discussions on adapting the process to these exceptional circumstances to make sure that all member states can fully participate to further substantive discussions and negotiations.

6.4.3 *Comments by other States*

248. Canada commented the OEWG initial Pre-Draft on capacity building, as follows:

> The capacity-building section includes many interesting elements, including those in paras 52, 54 and 56. We would draw your attention to our proposed added text on gender in para 56.
>
> Canada strongly supports the language on gender in paragraph 9. We have proposed additional language highlighting the importance of gender-related data to drive an evidence-based approach to promoting international cybersecurity.
>
> We do not agree with the proposal in para 68d that the Secretary-General establish a global mechanism for enhancing coherence in capacity building efforts in the use of ICTs. We would see this as duplicative of existing mechanisms, such as the Global Forum on Cyber Expertise.

249. China commented the OEWG initial Pre-Draft Report only with regard to the "Regular institutional dialogue", as follows:

> **IV. Regular Institutional Dialogue**

China supports the establishment of an effective and permanent mechanism under the auspices of the UN and having in-depth discussion and long-term planning for future cyberspace governance. This is also the common call of most countries. We should follow the trend of history and meet the expectations of the international community to continue the work of the OEWG. There is no need to impose restrictions on ourselves because of the existence of the GGE.

In addition,the pre-draft makes several references to the role of multi-stakeholders. It is true that multi-stakeholders play an indispensable role in maintaining cybersecurity. However, given the fact that OEWG is an intergovernmental process, our discussion should focus on the role played by states and governments, not the opposite.

250. Egypt commented as follows:

Capacity Building: the principles of capacity building should include the following:

i. The provision of assistance and cooperation should be demand-driven and made upon request by the recipient State, taking into account its specific needs and particularities.
ii. All efforts should be exerted to fully protect the confidentiality of information related to the recipient State's policies and measures to protect its national infrastructures and the confidentiality of its ICT emergency response plans in order to avoid any possibility of jeopardizing such information or undermining the effectiveness of these measures and plans.
iii. The principle of shared but differentiated responsibilities should be applied with regard to the provision of capacity building.

251. The Non-Aligned movement commented the OEWG initial Pre-Draft Report on capacity-building as follows:

NAM calls upon developed countries and relevant international entities to provide to the developing countries upon their request with assistance and cooperation, including through financial resources, capacity-building and technology transfer in ICT areas while taking into account specific needs and particularities of each recipient State. 26. NAM reaffirms that in order to transform the digital divide to digital opportunities, these activities should ensure the imperative of universal, inclusive and non-discriminatory access to information and knowledge related to

> ICTs, and should result in supporting national efforts in developing countries in the area of building, improving and strengthening capacities to facilitate their genuine involvement in all aspects of the information society and knowledge economy.
> NAM calls to immediately withdraw any coercive unilateral measures that prevent universal access to the benefits of ICTs or restrict or deny, in any manner whatsoever, developing countries of the ICTs-related science, know-how, technology and services in all its aspects for peaceful purpose. NAM stresses that international cooperation for capacity building should be targeted, need-based and nationally driven.

252. Norway commented the OEWG initial Pre-Draft Report on capacity-building as follows:

> We support proposals to recognize and integrate the link between capacity building and the UN Sustainable Development Goals. We would also support the recognition of the principles laid out in the 2017 Delhi Communiqué on a GFCE Global Agenda for Cyber Capacity Building. We welcome the recognition of the "gender digital divide" and the need to strengthen the link to the Women, Peace and Security agenda. Inclusivity and diversity should be a guiding principle for the capacity-building agenda

253. Russia dedicated scant comments to the above issues as addressed in the OEWG initial Pre-Draft report, as follows:

> We, nevertheless, assume that alongside with a range of positive traits (the report highlights the special role of the OEWG in establishing regular institutional dialogue on international information security (IIS) under the UN auspices, the need to strictly observe the UN Charter, the danger of development of offensive ICT capabilities and militarization of the digital space, etc.) the document promotes many unacceptable approaches both to substantive issues of maintaining IIS and to organizational matters of the respective negotiation process under the UN auspices.

254. South Africa commented as follows:

> That even though international law does not have specific reference to ICTs it can progressively develop and UN organs such as the UN Security Council and the ICJ are useful in arbitrating ICT related incidents between States.

South Africa is happy with the articulation that regional and sub regional organizations have an important role to play in CBMs especially the exchange of national points of contact on the diplomatic, legal, technical and policy levels. The input on the need for CBMs to be implemented in other forums is also accurate and acceptable.

South Africa indicated its support for dialogue within existing resources but remains open to the establishment of an institution that can facilitate the ongoing exchanges between member states with a view to rationalising the gaps that exist in international law and the avenues to mitigate them

255. The United Kingdom commented the OEWG initial Pre-Draft Report as follows:

E. Confidence Building Measures

We welcome the focus placed on operationalisation of confidence building measures (CBMs) (E41). It could be prefaced by a reference to the fact that States reaffirmed the value of CBMs. Listing all those CBMs mentioned in discussion may be challenging (E42). It could be better to note that there was detailed discussion of many existing, agreed CBMs, as well as some new proposals. The pre-draft could then move onto specific CBMs such as the Points of Contact (E44). On this issue, we note that Points of Contact are not just a prerequisite to CBMs, but also a CBM in their own right.

We consider that the importance of national and regional structures being in place (E46) cannot be underestimated. Such structures enable States to provide credible and wellexercised responses to incidents and require effort and resource to maintain. National Computer Emergency Response Teams (CERTs) are particularly important in this regard and should be highlighted. Equally important, but different, is the work regional organisations do to develop and implement CBMs. We consider this element, including the need for inclusion and possible universalisation could merit its own paragraph.

F. Capacity Building

The crucial nature of capacity building in supporting both the international cyberspace stability framework and the Sustainable Development Goals is well captured (Chapeau, F48). We fully support the references to two-way processes (F53) and the United Nations Women, Peace and Security agenda (F56). We

consider any mention of the concept of the 'development of a global capacity-building agenda' (F55) would benefit from some clarification.

We suggest that additional text could be included in this section to note the richness of the discussion on this topic, as well as strengthening the reference to the need for cyber diplomats to participate in OEWG discussions (F50). We consider that this section of the pre-draft must recognise that coordination is key (F55), but should also highlight the need for all States and stakeholders to contribute to the mobilisation of funding and resource for capacity building wherever possible, as this underpins our ability to implement the framework and achieve the recommendations made in this pre-draft.

G. Regular Institutional Dialogue

We welcome the description of the history of the processes (G58) and the capturing of the proposal for Regular Institutional Dialogue based on the existing process (G62). Efforts to capture the proposals for Regular Institutional Dialogue based on new arrangements (G59, G60, G61) must reflect the call from several Member States that is was important to start from the purpose of any possible dialogue and how it would further international peace and security. It would be beneficial to note that there was no consensus on such a purpose. A separate paragraph regarding possible characteristics of a dialogue would be welcome (G59 and G63).

256. The United States commented the OEWG initial Pre-Draft Report as follows:

The pre-draft contains several proposals for repositories. Some of these ideas have merit, but others may duplicate existing efforts. Also, States may have limited capacity for contributing to such repositories. We should seek to prioritize those proposals that are achievable and fill urgent gaps, such as States sharing their views regarding how international law applies to States' use of information and communications technologies (ICTs) or regarding States' implementation of norms, while also acknowledging other ongoing international efforts that could be strengthened, such as the Global Forum on Cyber Expertise's (GFCE's) work on capacity building. All these new proposals must remain voluntary and State-led, and be undertaken within existing resource constraints. […]

Comments on the Confidence Building Measures (CBMs) and Capacity Building Sections

The United States has no significant concerns with the pre-draft's sections on CBMs and capacity building.

Comments on the Regular Institutional Dialogue Section

257. Our general views on possible repositories are expressed in the opening section of our comments. We believe that it is premature to decide whether the UNGA should convene a new OEWG or if the OEWG should put forward a different proposal for future institutional dialogue. Our views on this will depend, in large part, on the outcomes of the current OEWG. In general, we would also have concerns with a working group continuing indefinitely without a clear task and timeframe for concluding its work.

1. Uruguay commented as follows

3. The capacity building strategy should include not only training in cyber diplomacy, but also training in diplomatic matters for technicians. It could also include, as it already exists at the regional level, joint exercise and training programs between the countries of the region, from a gender perspective, understanding training as a measure of confidencebuilding.

4. The creation of Regional Research Centers (or Centers of Excellence) that allow the exchange of information, the execution of courses, seminars, and dissemination activities would be an invaluable pillar for the transfer of knowledge and for countries to gradually build trust which is necessary to raise levels of cooperation.

6.4.4 *OEWG Second Pre-Draft Report*

258. On the basis of the above comments, the OEWG amended the text of the Pre-Draft Report as follows:

62. Since 1998, consideration of developments in ICTs and international security at the United Nations has been pursued under the purview of the First Committee, and thus focused on its international peace, stability and conflict prevention dimensions. The importance of recurrent and structured discussions under UN auspices has been noted in the consensus GGE reports of 2010, 2013 and 2015. Each of these reports has called for regular dialogue on the international security dimension of ICTs,

recognizing that the speed of ICT developments and the scope of the threat merited strengthening cooperation and finding common ground.

63. The OEWG has served as an initial response to these recommendations by offering, for the first time, a platform under United Nations auspices open to all States and focused solely on developments in ICTs in the context of international security. In addition to its objective to seek common understandings among all States through their substantive exchanges, the OEWG has permitted the strengthening of diplomatic networks and trust through its structured, in-person meetings. The broad participation of non-governmental stakeholders has demonstrated that a wider community of actors is ready to leverage its expertise to support States in their objective to ensure an open, secure, stable, accessible and peaceful ICT environment.

64. In their discussions at the OEWG, States affirmed that given increasing dependency on ICTs and the scope of threats emanating from their misuse, there was an urgent need to enhance common understandings, build confidence and intensify international cooperation. They considered whether and how further regular dialogue could support the goal of strengthening international peace, stability and prevention of conflicts in the ICT environment, as well as the most appropriate format to achieve that goal. It was suggested that the establishment of a regular institutional dialogue would be an important outcome of the OEWG.

65. States expressed a range of views as to the specific objectives of regular institutional dialogue and which format of regular dialogue could best support these objectives. One set of proposed objectives for regular dialogue comprises awareness raising and information exchange; developing guidance to support and monitor the implementation of existing commitments and recommendations; building trust and confidence; coordinating and strengthening the effectiveness of capacity-building; identifying and exchanging good practices; and encouraging further study and discussion on areas where no common understanding has yet emerged. It was suggested that a mechanism for dialogue supporting these objectives could be the establishment of annual meetings under the purview of the existing UN disarmament machinery.

66. Another set of proposed objectives for regular dialogue comprises negotiations of further commitments of a voluntary or binding nature, including regulatory, compliance and verification efforts. It was suggested that a mechanism for dialogue

supporting these objectives could consist of meetings leading to negotiation of a binding instrument and possibly institutional structures to support it.

67. A format attending to both sets of purposes was also proposed. Such a format could serve as a follow up to encourage implementation and adherence to existing commitments, while establishing a periodic opportunity to assess whether additional measures are necessary. It was suggested that a mechanism for dialogue supporting these objectives could be through follow up to a politically-binding declaration based on consensus resolution 70/237. In this proposal, regular meetings under UN auspices could focus on supporting implementation and operationalization of existing commitments, in combination with a periodic review function for consideration of the necessity for new measures or further refinement of the existing normative framework.

68. It was also suggested that the OEWG's mandate contained in resolution 73/27 could be renewed for a limited period or indefinitely. It was also noted that different formats for dialogue are not necessarily mutually exclusive. A format with broad participation may be complementary to one with more limited membership. Together they may provide the opportunity to capitalize on the unique features of each.

69. In addition to the four characteristics—"regular", "institutional", "broad participation", and "under UN auspices"—noted in the OEWG mandate,9 States also emphasized that any platform for regular institutional dialogue should be a process with specific objectives, building on previous agreements, and be inclusive, consensus driven, sustainable, practical and results-oriented. The need for further consideration of the duration of a future dialogue, its timing, potential locations, and budgetary considerations were also raised.

70. A variety of forums within the UN system focus on the digital dimensions of other issues, including terrorism, crime, development, human rights and Internet governance.10 It was highlighted that any future process of regular dialogue should remain focused on international peace and security so as not to duplicate existing efforts and activities. It was suggested that greater exchange between these forums and the international security discussion, such as through joint meetings of committees of the General Assembly, while respecting the expert nature or specialized mandate of each, could help to reinforce synergies and improve coherence.

71. It was recalled that States hold primary responsibility for national security, public safety and the rule of law. It was also noted that regular dialogue should be primarily intergovernmental in nature, and appropriate mechanisms for engagement with other stakeholder groups would need to be found. In their interventions, States acknowledged that building a more resilient and secure ICT environment necessitates multi-stakeholder cooperation and partnerships. While recognizing the unique role and responsibility of States in relation to security, there was growing appreciation that States may benefit from the expertise in non-governmental communities and that responsible behaviour of other actors makes an essential contribution to this environment.

PROPOSAL FOR THE ITALIAN POSITION

1 Introduction

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

3. Italy thus concurs with the conclusion reached by the UN Group of Governmental Experts (GGE), 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'.[17] 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.

4. 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 to activities in cyberspace gives rise to significant difficulties inherent in the technical features of information and communication technologies (ICTs). Such difficulties require responses that the international community is currently developing. Italy thus welcomes and supports the ongoing process of exchange of views and cooperation amongst States [and other stakeholders] to that end.

[17] 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.

5. In this paper, 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 application of the Law of the international responsibility of States to activities carried out in cyberspace; cyber operations and the use of force; the application of International Disaster Law to activities in cyberspace; the role of private stakeholders; and international cooperation in the cybersecurity domain.

1.1 *The protection of sovereignty in cyberspace and violations of the principle of non-intervention*

Key message

Italy:

- Endorses the principle of sovereignty as a primary rule of international law.
- Stresses that the principle of sovereignty prohibits a State from conducting cyber operations from the territory of another State without its express authorization and from conducting cyber operations which produce harmful effects on the territory of another State, irrespective of whether the author of the operations is present on the territory of such State or not.
- Deems that a cyber-operation constitutes a violation of the customary principle of non-intervention in the internal affairs of other States when it attempts to coerce/leads a State to do something it would not have done, or not do something it would have done in a matter in which the State in question is free of international obligations.
- Considers that influence operations lacking an attempted coercive element are not as such a violation of the principle of non-intervention. This is without prejudice to the wrongfulness of cyber activities that, whilst falling short of non-intervention, might infringe upon the principle of sovereignty and the ancillary right of States to internal self-determination.

6. 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.

7. 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 material location of the author of the operations. Italy finds that, according to the same principle, States must not carry out cyber-operations from the territory of another State without its express authorization.

8. 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.

9. The decision whether or not to respond to violations of sovereignty is a political one and will depend on different factors such as the seriousness of the breach and the nature of the target. This is without prejudice of the right of self-defence, when admissible.

10. Italy believes that a cyber-operation constitutes a violation of the customary principle of non-intervention in the internal affairs of other States when it coerces a State to do something it would have not done, or not do something it would have done in a matter in which the State in question is free of international obligations. An example would be ransomware operations, where a user's critical data is encrypted to prevent the user from accessing files, databases, or applications unless a ransom is provided. Altering electoral results would be another example.

11. Influence operations, for instance those aimed at spreading information (whether real or fake) in order to affect a State's public opinion, are not as such a violation of the principle of non-intervention so long as they lack the coercive element. However, they might breach the rule protecting territorial sovereignty when they consist of an unauthorised intrusion in cyber infrastructure located on the territory of another state, or in the cyberspace under the control of that State outside its territory.

1.2 *'Technology neutrality' and cyberspace*

Key message

Italy:

- Emphasises the need to focus on States behaviour and maintain a technology-neutral approach.
- Stresses that a technology-neutral approach may foster positive uses of ICTs.

12. Italy underlines the need to focus primarily on the use of ICTs, rather than on ICTs per se, thus maintaining a technology-neutral approach. As highlighted by the EU, «measures to promote responsible State behaviour should remain technology-neutral, [as] it is the misuse of such technologies, not the technologies themselves, that is of concern».[18] Since innovation within the field of ICTs happens so fast, listing every single potential threat stemming from new advances increases the risk of uncertainty and incompleteness.

13. Italy believes that a technology-neutral approach may foster positive uses of ICTs. In particular, such positive uses may be required in the pursuit of security, *inter alia*, in the water, food, health, energy and transport sectors.

2 The application of the Law of States Responsibility to activities in the cyberspace

2.1 *Attribution*

Key message

Italy:

- Reiterates that attribution of malicious cyber activities is a national sovereign prerogative. Without prejudice to this principle, international law questions related to attribution should be discussed to strengthen dialogue on international security matters.
- Acknowledges the difficulties in attributing malicious cyber activities.

[18] *EU Lines To Take in view of the June online meetings of the Open-Ended Working Group on developments in the field of information and telecommunications in the context of international security (OEWG) – 15, 17 and 19 June 2020*, para 7.

- Endorses a ‘reasonable’ use of political attribution of malicious cyber activities.
- Considers with caution the possibility of lowering of the threshold of proof required to legally attribute malicious cyber activities.
- Sees merit in possible forms of international cooperation in addressing issues of attribution of malicious cyber activities.

14. Italy reiterates that attribution is a national sovereign prerogative and so is the decision to make it public or not, on a case-by-case basis. Having said that, Italy sees merit in contributing to the international law debate on the matter.

15. Italy is aware that the attribution of cyber activities to a State may be complex, both from a factual and from a legal perspective. That is particularly the case with regard to the attribution of cyber-attacks. We concur with the prevailing view of a three-tier process of attribution: i.e. technical, political and legal attribution proper.

16. First, we see as technical attribution the process of tracing back acyber-attack to its source. We take this attribution to be in its turn ideally divided into three successive steps characterised by increasing complexity: i.e. a) the ‘where’, that is, the identification of the place(s) from which the cyber-attack originated; b) the ‘how’, that is, the identification of the hardware(s) used in order to launch the cyber-attack; and the ‘who’, that is, the identification of the subject (individual, company or State’s organ) that launched the cyber-attack.

17. Secondly, we take political attribution to consist of a self-assessment by the victim State(s), or possibly third States(s) and organisations, as the case may be. Italy considers political attribution - which may be public or not - as a sovereign prerogative. As such, we do not find it to be governed by any specific international technical or legal rules, without prejudice to the application of general principles of law, with special regard to good faith.

18. Thirdly, Italy concurs with the view that legal attribution of cyber-attacks 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)[19]. Still, Italy acknowledges the obvious difficulties of applying the ARSIWA in a peculiar environment such as cyberspace.

19. While legal attribution must be proven Italy acknowledges that the rules on attribution are different from those on evidence. In particular, the latter are not defined in the ARSIWA, and vary according to circumstances, as well as to the adjudicative context in any given case.

20. Against this background, we believe that efforts supporting technical attribution of the kind suggested above can help significantly in relation to legal attribution.

21. Italy considers that significantly lowering the general threshold of proof in relation to legal attribution of malicious cyber activities may risk producing the opposite effect of the one sought. Namely, instead of making the ascertainment of legal attribution more straightforward and transparent, it might lead to an excessive ease in attributing unlawful conducts to States, thereby introducing greater uncertainty and international tension.

22. Italy sees merit in considering the production of soft-law instruments which may provide guidance on technical attribution. Italy also believes that the reversal of the burden of proof should be confined to due diligence aspects.

23. Finally, and without prejudice to the sovereign national nature of the prerogative of attributing, Italy sees merit in possible international cooperation – both among States and within international organizations - on the question of attribution of malicious cyber activities to States. At the same time, we are aware of the difficulties around the idea of third party assessment.

2.2 *Due diligence*

Key message

Italy:

- Endorses framing the obligations of States in the cyber domain in due diligence terms.

[19] *Responsibility of States for internationally wrongful acts*, UN Doc. A/RES/56/83, 28 January 2002.

- Endorses the due diligence no harm principle as a relative obligation of means, rather than as an absolute obligation of result.

24. 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.

25. The International Court of Justice enunciated the so called no-harm principle in due diligence general terms in the *Corfu Channel* case, whereby States are under an obligation to make their best efforts in order to prevent use of their territory, and of areas on which they exercise jurisdiction, of which they are aware or should have been aware, that causes, or may cause, significant harm to another State.[20] The principle has been further developed over the years in different fields of international law, most prominently with regard to transboundary natural resources,[21] the protection of the environment[22] and human rights.[23]

26. Italy stresses that according to the due diligence nature of the harm prevention, elimination or mitigation principle, a State would not be liable automatically for not achieving the avoidance of the occurrence of harm, its elimination, or, if elimination proves impossible, its mitigation, unless it cannot prove to have acted diligently. That is to say, that the State cannot prove to have made its best efforts to take all the appropriate steps to prevent, eliminate, or mitigate significant harm.

[20] *Corfu Channel Case*, Judgment of April 9th, 1949: I.C.J. Reports 1949, p. 4, at 18.

[21] 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.

[22] *Legality of the Threat or Use of Nuclear Weapons*, Advisory Opinion, I.C.J. Reports 1996, p. 226, para. 241-242.

[23] 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.

2.3 *Countermeasures*

Key message

Italy:

- Endorses the application of countermeasures in cyber space subject to the conditions set out by international customary rules on state responsibility (eg proportionality; respect of human rights; respect of *jus cogens*).
- Supports the use of digital, as well as physical countermeasures.
- Does not support collective countermeasures, but favours enhanced cooperation on information sharing.

27. Italy is of the view that when cyber activities cause significant harm in connection with a breach of the due diligence obligation of prevention as described above (Sec. 2.2.) the victim State may take countermeasures against the State of origin. Under customary international law, as codified by the ARSIWA[24] and corroborated by the ICJ case law,[25] 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 reparation for it.

iii. The effects of a countermeasure must be commensurate with the injury suffered, taking account of the rights in question (proportionality).

28. Italy deems that countermeasures are adequate responses to cyber operations that do not reach the gravity threshold of an armed attack. This is without prejudice to the inherent right of States to self-defence.

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

[25] *Gabćikovo-Nagymaros Project (Hungary/Slovakia)*, Judgment, I.C.J. Reports 1997, p. 7, paras 83-85.

29. The adoption of countermeasures against the State that may be held responsible, directly or indirectly, for malicious cyber activities may be problematic due to the difficulties of traceability, of the assessment of breach of the threshold of the diligence due, as well as of the significance of the harm suffered. Therefore, the responding State is to justify its response based on adequate proof of the source of the operation, and reasonable evidence of the responsibility of a particular State, considering the circumstances of the case and its technological and financial capacity.

30. Italy finds that, in conformity with general international law (ARSIWA 52.2), also in the cyber context the requirement to notify the responsible State of any decision to take countermeasures may not apply if immediate action is required to enforce the rights of the injured state and prevent further damage.

31. The response to a harmful cyberoperation may involve digital means, but not necessarily, 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 should not amount to a threat, or use, of force and should be consistent with other peremptory norms, as well as with human rights and humanitarian law.

32. Italy is of the view that collective responses to internationally wrongful cyberoperations should not be considered as legal. However, this should not prevent the victim State the possibility of seeking cooperation from other States concerning the disclosure of information on the origin of the attack.

3 Cyber Operations and the Use of Force

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

Key message

Italy:

- Qualifies any activity employing cyber capabilities able to cause (a) material damage to property; (b) loss of life or injury to persons; or (c) severe loss of functionality of physical infrastructures as use of force prohibited by Article 2(4) of the UN Charter
- Deems that a cyber operation causing mere loss of functionality may qualify as use of force under Article 2(4) of the UN Charter when it causes the interruption of essential services irrespective of the occurrence of physical damage.

33. Italy considers a cyber operation conducted by a State against another State as a use of force, thus, prohibited under Article 2(4) of the UN Charter and its customary counterpart when it employs cyber capabilities able to cause (a) material damage to property; (b) loss of life or injury to persons; or (c) severe loss of functionality of physical infrastructures. Italy finds that it is not the instrument used that defines armed force, i.e. weapons, but the instrument is identified by its damaging or disrupting consequences.

3.2 *Cyber operations and the exercise of self-defence by states*

Key message

Italy:

- Deems that a cyber operation that constitutes use of force may also qualify as an 'armed attack' for the purposes of self-defence, regardless of whether a State or non-State actor is responsible for the armed attack. The decision of qualifying a cyber operation as an armed aggression is a sovereign political one and has to be examined on a case-by-case basis having regard to the specific circumstances.

- Without prejudice to the above-stated principle. Italy considers that cyber operations affecting infrastructure functionality, but not resulting in material damage, might potentially qualify as 'armed attack' only if seriously disrupting several or all national critical infrastructures of a heavily digitalized State for a prolonged time.
- Concludes that the qualification of a cyber operation as an 'armed attack' does not automatically entitle the victim State to use force in self-defence, since such use must also be necessary and proportionate to the purpose of repelling the attack.

34. Italy deems that a cyber operation that constitutes use of force may also qualify as an 'armed attack' for the purposes of self-defence, regardless of whether a State or non-State actor is responsible for the armed attack. The decision of qualifying a cyber operation as an armed aggression is a political one and has to be examined on a case-by-case basis having regard to the specific circumstances.

35. Italy considers a cyber operation which constitutes a use of force also to qualify as an 'armed attack' for the purposes of self-defence when its scale and effects are sufficiently serious, regardless of whether a State or non-State actor is responsible for the armed attack. This would be the case of a cyber operation resulting in extensive material damage and/or significant loss of life. With regard to cyber operations affecting infrastructure functionality but not resulting in material damage, only coordinated cyber operations seriously disrupting several or all national critical infrastructures of a heavily digitized State for a prolonged time could potentially meet the high scale and effects threshold of an armed attack.

36. Concluding that a cyber operation constitutes an 'armed attack' does not automatically entitle the victim State to use force in self-defence, since such use must also be necessary and proportionate to the purpose of repelling the attack. Whenever passive cyber defences or cyber operations below the level of the use of force are reasonably effective means to react, a use of force in self-defence would be unnecessary and/or disproportionate, thus unlawful, even if the cyber operation amounted to an armed attack.

3.3 *Cyber operations and the application of International Humanitarian Law*

Key message

Italy:

- Deems that International Humanitarian Law applies to cyberspace in the same way as it applies to the analogue world.
- Considers that acknowledging the application of International Humanitarian Law to cyberspace does not encourage *per se* the use of cyber operations on the battlefield.

37. Italy finds that International Humanitarian Law applies in cyberspace in the same way as it applies to the analogue world. In particular, International Humanitarian Law applies as follows:

i. If cyber operations are conducted by belligerents against each other in an already existing international or non-international armed conflict or are otherwise conducted in support of a party to the conflict to the detriment of another and cause military harm and/or physical damage to civilians and civilian property.

ii. If the exchange of cyber operations between States amounts in itself to a 'resort to armed force', *i.e*. they entail the use of cyber means or methods of warfare resulting in material damage to property, loss of life or bodily injury, or serious disruption of critical infrastructures.

iii. If an organized armed group conducts cyber operations amounting to protracted armed violence against a State or against another organized armed group.

38. The language used in numbers *ii* and *iii* is based on the definition of 'armed conflict' as consistently adopted by the International Criminal Tribunal for the former Yugoslavia[26] and the ICJ.

[26] ICTY, *Prosecutor v Tadić,* Case No IT–94–1, Decision on the Defence Motion for Interlocutory Appeals on Jurisdiction, 2 October 1995, para. 70.

39. Contrary to the view expressed by some States, we believe that recognising that International Humanitarian Law applies in cyberspace should not encourage the use of cyber operations on the battlefield. In fact, International Humanitarian Law is restrictive, in the sense that it aims at limiting the conduct of belligerents which negatively affects the victims of an armed conflict.

3.4 *Cyber operations and the definition of 'attack' under Article 49(1) of the 1977 Protocol I additional to the 1949 Geneva Convention on the Protection of Victims of War*

Key message

Italy:

- Deems that a cyber operation constitutes an 'attack' under Article 49(1) of the 1977 Protocol I additional to the 1949 Geneva Convention on the Protection of Victims of War if it employs cyber capabilities which produce, or are reasonably likely to produce, violent consequences in the form of loss of life or injury to persons, more than minimal material damage to property, or loss of functionality of physical infrastructures.
- Considers that the law of targeting codified in Additional Protocol I fully applies to cyber operations constituting an 'attack' under Article 49(1).
- Stresses that a target located on the territory of a non-belligerent State may not be subject to an attack unless the consent of that State to the operation has been previously obtained, or other justifications for the extraterritorial use of force under the *jus ad bellum* (self-defence, authorization by the UN Security Council) apply.

40. Italy considers that a cyber operation constitutes an 'attack' under Article 49(1) of the 1977 Protocol I additional to the 1949 Geneva Convention on the Protection of Victims of War if it employs cyber capabilities which produce, or are reasonably likely to produce, violent consequences in the form of loss of life or injury of persons, more than minimal material damage to property, or loss of functionality of physical infrastructures. Because of the radically increasing reliance of modern societies on information technologies, the concept of 'violence' should be expanded to include not only material damage to objects, but also incapacitation of infrastructures without destruction.

41. We find that, when a cyber operation constitutes an 'attack' under Article 49(1), the law of targeting codified in Additional Protocol I fully applies to it. Therefore, for it to be lawful, a cyber operation amounting to 'attack', whatever its purpose, will have to meet the following conditions:

i. It must not employ unlawful means or methods of cyber warfare.

ii. It must be directed against a person or object that qualifies as a military objective.

iii. It must not be indiscriminate; and, in particular, it must not be expected to cause incidental damage on civilians or civilian property, with particular reference to health care and education institutions (i.e. infrastructure that hosts vulnerable categories of persons), which is excessive with respect to the concrete and direct military advantage anticipated,

iv. It must comply with rules providing for special protection from attack, if applicable.

v. All feasible precautions must have been taken to avoid or at least minimize incidental damage on civilians and civilian objects.

vi. It must not be contrary to other applicable rules of international humanitarian law, in particular the prohibition of perfidy and the principle of unnecessary suffering.

vii. If undertaken as a belligerent reprisal, it must comply with the stringent conditions for its adoption.

viii. It must not breach international human rights law and other peacetime international law when applicable to the cyber operation.

42. Furthermore, we find that, if the target is located on the territory of a non-belligerent State, the consent of that State to the operation must be previously obtained, unless other justifications for the extraterritorial use of force under the *jus ad bellum* (self-defence, authorization by the UN Security Council) can be invoked. Finally, the law of neutrality must also be taken into account as a possible limit in international armed conflicts.

3.5 *Cyber operations and the law of neutrality*

Key message

Italy:

- Deems that the law of neutrality may apply to cyber operations.

43. Italy stresses that the law of neutrality may extend to cyber operations whenever they are conducted in the context of an international armed conflict and have a nexus with it or when they amount themselves to such a conflict, whether or not there is a declaration of war or a State has declared its neutrality.

44. In particular, Italy finds that the matter is governed *mutatis mutandis* by the international customary law as it is still reflected by its codification in the in the 1907 *Hague Convention V Respecting the Rights and Duties of Neutral Powers and Persons in Case of War on Land* and of the *Hague Convention XIII on the Rights and Duties of Neutral Powers in Naval War*, with the following consequences:

i. It is prohibited to conduct any cyber operations amounting to acts of hostilities against belligerents from cyber infrastructure situated in neutral territory or under the exclusive control of neutral States.

ii. If conducted by a belligerent or by private individuals, the neutral State from whose territory the cyber operations are conducted has an obligation to use all the means at its disposal to terminate them.

iii. Unlike cyber operations originating from neutral territory, the routing of cyber operations through neutral cyber infrastructure is not a violation of that State's neutrality, as neither would the belligerent be able to control the pathway taken by the malware, nor would the neutral State have the means to prevent the routing.

iv. Belligerents are prohibited to conduct any cyber operation against neutral territory or neutral cyber infrastructure and from conducting cyber operations against other belligerents that have more than nominal prejudicial incidental effects on neutral territory.

v. As to the use of cyber infrastructure for communications, belligerents are allowed to 'erect' a new cyber communication installation on the territory of the neutral State as long as it is exclusively for non-military communications; use an existing one established by them before the war, even for military communications, provided that it is open 'for the service of public messages'; and use an existing communication installation established by them before the war and which is not open 'for the service of public messages', provided it is for non-military communications.

vi. The neutral State is not called upon to forbid or restrict the use by the belligerents of its cyber infrastructure for communications, providing it does not discriminate between them.

vii. The neutral State may not supply a belligerent with malware that may be used in the conduct of hostilities, although it is not required to prevent its companies or private individuals from supplying it.

viii. A neutral State may not invoke the law of neutrality to justify cyber operations that are incompatible with the UN Charter or resolutions adopted by the UN Security Council under Chapter VII. Similarly, a neutral State may not invoke the law of neutrality to avoid adopting cyber sanctions decided by the Security Council against a belligerent.

4 Human rights in cyberspace

4.1 *The application of the international human rights law*

Key message

Italy:

- Deems that the international human rights law applies to cyberspace in the same way as it applies to the analogue world.

45. Italy finds that the 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 (with particular but not exclusive reference to freedom of opinion and expression, including the right to access to information, and the right to privacy), also with respect to cyber-related activities.

5 The application of International Disaster Law to activities in the cyberspace

Key message

Italy:

- Stresses the role that International Disaster Law instruments may play in enhancing the prevention, elimination or mitigation of cyber disasters.

46. As recently highlighted by in the EU Joint Communication of the European Parliament and the Council of December 2020, '[c]ybersecurity incidents, whether accidental or the deliberate action of criminals, state and other non-state actors, can cause enormous damage'.[27] Indeed, Italy wishes to flag the appropriateness for the present debate to give due consideration to the risk of occurrence of 'cyber disasters'.

47. Italy deems that disasters caused by means of ICT, or which have their effects in cyberspace, fall well within the scope of the definition of disaster under Article 3(a) of the 2016 ILC *Draft articles on the protection of persons in the event of disasters* (2016 ILC DAs),[28] when they result in 'in widespread loss of life, great human suffering and distress, or large-material or environmental damage, thereby seriously disrupting the functioning of society'.

6 The role of private stakeholders in cyberspace

Key message

Italy:

- Stresses the need to assure full compliance with human rights in relation to cyberspace.

[27] *The EU's Cybersecurity Strategy for the Digital Decade*, EU Doc. JOIN/2020/18, 16 December 2020.

[28] ILC, *Draft articles on the protection of persons in the event of disasters*, in *Yearbook of the International Law Commission*, 2016, vol. II, Part Two (forthcoming).

- Acknowledges that malicious cyber activities may affect private stakeholders, both as individuals and as partners of public-private partnership running critical infrastructures.
- Acknowledges that public-private cooperation is key to guaranteeing cybersecurity and effective capacity-building.
- Recalls that under existing international law applicable to cyberspace Sates must take all reasonable measures to prevent, eliminate or mitigate human rights violations perpetrated also by non-State actors.

48. Italy stresses the importance of ensuring full respect for international human rights law in cyberspace, in accordance with the UN Charter and the core human rights treaties.

49. Italy finds that malicious cyber activities might seriously threaten fundamental human rights, including the right to privacy, freedom of expression, the right to information and the right to health. Human rights violations in cyber space can also affect private stakeholders, both as individuals and as partners/members of public-private partnership running critical infrastructures.

50. 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.

51. Given that States are under the obligation, not only to respect human rights, but also to protect from violations of human rights, Italy recalls that under existing international law States have to take all reasonable measures to prevent, eliminate or mitigate human rights violations perpetrated also by non-State actors. Italy deems that this equally applies to cyberspace-related human rights.

7 International cooperation in the cybersecurity domain

Key message

Italy:

- Endorses cooperation in the field of cyberspace by means of confidence-building, capacity-building and information-sharing.

- Endorses cooperation at a regional and bilateral level.
- Stresses the role of existing institutional frameworks in fostering cooperation in cyber security.
- Expresses its pledge to establishing bodies of compliance review within existing frameworks, so as to facilitate technical assistance among States.

52. Italy expresses support for any appropriate form of cooperation aimed at enhancing security of cyberspace. 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.

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

54. 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.[29]

55. Whilst supporting global cooperation, Italy deems that at the current stage regional and bilateral cooperation are best suited to foster cyber-capacities. To that end existing regional forums, such as the EU, OSCE, CoE, ASEAN and OAS, have proven commendable in this field. Italy also supports the establishment of compliance and implementation bodies within those regional frameworks, with a view to preventing and managing disputes that may arise on the use of ICTs, and foster technical assistance amongst States We are aware that the establishment of a body of the kind just described on the international level may be seen as a difficult task, but we would find it commendable.

[29] OECD, *Busan Partnership for effective co-operation in support of international development*, 1 December 2011.