Working Paper submitted by the Delegation of Egypt
To the Open-Ended Working Group on Developments in The Field of Information and Telecommunications in The Context of International Security

I. Introduction:

1. Egypt attaches great importance to this historic Open-Ended Working Group (OEWG) as the first inclusive institutional process under the auspices of the United Nations (UN) which enjoys the full participation of all Member States on this increasingly important topic.

2. The international security aspects of Information and Telecommunication Technologies (ICTs) are becoming increasingly important and represent a global challenge that requires a global response. ICTs offer both massive opportunities and challenges. There is an urgent and pressing need to identify and develop rules for State behaviour to increase stability and security in the global ICT environment.

3. It is also important to highlight how timely this historic process is in light of the exponential growth of technological advancements and the heated debates related to the far-reaching revolutionary implications of the 5th Generation technologies and the "Internet of Things", combined with rising tensions at the global and regional levels and alarming trends towards the militarization and weaponization of ICTs, including the increasing incidents involving the malicious use of ICTs by State and non-State actors in a manner that represents a real threat to international peace and security.

4. Therefore, this process provides an excellent platform for achieving meaningful progress, building on the previous recommendations on this topic in order to codify rules on responsible State behavior in cyberspace and on tangible international cooperation to minimize the threats posed to international security by the malicious uses of ICTs, thereby creating improved conditions for reaping the full benefits of their peaceful uses.

5. This OEWG is an important steppingstone that should lead to meaningful outcomes on three main fronts:

    a. Elaborating detailed rules based on the recommendations of the previous Groups of Governmental Experts (GGEs) of 2013 and 2015 which have been endorsed by the General Assembly. It is long overdue for the United Nations to adopt binding rules for responsible State behaviour in relation to the use of ICTs. Most, if not all, of the 2015 GGE recommendations could be used as the basis for such politically or legally binding rules, especially that most of these recommendations and guidelines are derived from the established rules and principles of international law and the UN Charter.

    b. Reaching an initial agreement on the establishment of an inclusive institutional platform dedicated to international cooperation on safeguarding the peaceful uses of ICTs and mitigating their associated risks. Such an institutional platform would enable an inclusive and transparent exchange of information on vulnerabilities and best-practices, foster international cooperation and capacity-building, issue recommendations on Confidence-Building Measures (CBMs), and contribute to

resolving possible international disputes in a cooperative and non-arbitrary manner in conformity with international law.

c. Issuing meaningful recommendations on capacity-building measures, especially for developing countries, and on international cooperation in this domain.

II. Existing and Potential Threats

6. There is no disagreement regarding the gravely alarming trends related to malicious uses of ICTs and the risks they pose to international peace and security. Effective cooperation among States is essential for reducing those risks.

7. A number of States are developing ICT capabilities for offensive military purposes. The possible use of ICTs in future conflicts between States is becoming a reality.

8. The most harmful attacks using ICTs are those targeted against the critical civilian infrastructure and associated information systems. The risk of harmful ICT attacks against critical civilian infrastructure is both real and serious.

9. Furthermore, the use of ICTs by terrorist and criminal organizations, including attacks against ICT-dependent infrastructures, is a rising possibility that, if left unaddressed, may threaten international peace and security, especially in light of the attribution-related challenges. States are rightfully concerned about the possibility of harm to their citizens, economy, and national security.

10. New types of extremely serious cyber-attacks have recently emerged, aimed at disrupting critical services or destroying ICT infrastructure and control systems, especially in vital facilities. Such cyber-attacks deploy several channels. In practice, critical facilities may be vulnerable to advanced cyber-attacks, even if they are not directly connected to the Internet.

11. Recently, dangerous types of cyber-attacks and cyber-crimes have spread using advanced technologies, including advanced malicious software (malware) and complex and sophisticated computer viruses, which often require advanced knowledge and non-conventional expertise, available only in technologically advanced countries, to be used in addition to, or sometimes instead of, conventional military attacks, in what is known as cyber-warfare.

12. A real threat lies in the fact that such malicious technologies that are being developed by States are being transferred, copied or reproduced by terrorists and criminals. Leading cyber-security experts are right to expect an increased proliferation of sophisticated cyber-attacks in the near future. The relevant malicious technologies are available and accessible to a very large number of State and non-State actors and their continued development makes their proliferation inevitable.

13. Practices such as the “stockpiling vulnerabilities”, as well as the lack of agreed rules addressing supply chain security and threats such as the malicious uses of “mass computing technologies” or “autonomous cyber-attacks”, severely multiply the risk factor from the international security point of view. The exportable versions of some

ICT products may contain backdoors or vulnerabilities that make them a source of additional threats. These threats can spread easily and rapidly and it is difficult, if not impossible, to trace the main origin of those threats in time to address them. Such acts can have widespread impacts that can harm a whole population.

14. Other than cyber-warfare technologies, there are evident and real threats related to Digital Identity and Private Data Theft and targeted propaganda campaigns in manners that could go beyond personal losses to harm national economies and jeopardize national security.

15. The task of the OEWG is *not* to attempt to develop an exhaustive list of all types of existing and emerging technologies that could represent a threat to international peace and security. The actual challenge is to agree on a comprehensive set of binding rules on the uses of such technologies by States (i.e. State behaviour) in a manner that is consistent with the principles of international law and the UN Charter. The implementation of such rules and possible prohibitions should be carried out by utilizing a diversified set of measures at both the national level, through harmonized legislations and policies, and at the international level, through compliance with agreed rules and standards as well as the exchange of information and cooperation.

III. International Law:

16. The UNGA has already endorsed the view that international law and the Charter of the United Nations are applicable in the ICTs environment and are essential for this environment to be open, secure, stable, and peaceful.

17. The adherence by States to international law, in particular their Charter obligations, is an essential framework for their actions in their use of ICTs. The principles of sovereignty; sovereign equality; the settlement of international disputes by peaceful means; refraining from the threat or use of force against the territorial integrity or political independence of any State, or in any other manner inconsistent with the purposes of the United Nations; respect for human rights and fundamental freedoms; and non-intervention in the internal affairs of other States, are cross-cutting and must be complied with in all domains, including cyber-space.

18. It has been also agreed that States have full jurisdiction over the ICT infrastructure located within their territory and that in their use of ICTs, they must observe the agreed principles of international law and the Charter.

19. There are legitimate concerns, however, when it comes to focusing on elements such as the “right to self-defense” under article 51 and the applicability of the rules of engagement in military conflicts in the ICT context, in a manner that may intentionally or unintentionally legitimize or encourage turning the ICT environment into an arena of conflict. An exaggerated focus on these specific aspects and their associated legal controversies and attribution challenges might divert attention from addressing the right questions on how to cooperate to prevent such conflicts from occurring in the first place.

20. It might be very helpful to agree that a common understanding has already been reached on the applicability of international law to State use of ICTs. Our attention and efforts should be focused on elaborating specific rules on what States shall and shall not do in the ICT environment with a view to preventing conflict and enhancing cooperation and mutual trust.

21. The OEWG should avoid the counter-productive debate on selectively picking which specific principles of international law apply to cyber-space and which principles do not.

22. The OEWG should focus on translating the existing norms and recommendations into more elaborate, operational, and binding measures that are tailored to specific scenarios in the ICT environment, pending the conclusion of appropriate multilateral legally-binding obligations.

23. Once such rules are developed and agreed, it will be relatively easier to develop mechanisms to foster and monitor their implementation by States at the national and the international levels.

IV. Rules, Norms and Principles:

24. Voluntary, non-binding norms of responsible State use of ICTs can reduce risks to international peace and security in the short-term. Nevertheless, taking into consideration the unprecedented risks and the rapid technological developments, there is a need to step up international efforts to develop rules on ICTs security consistent with international law, in order to sustain an open, secure, stable, and peaceful ICT environment in the long-term.

25. Such rules must not limit or prohibit any action that is otherwise consistent with international law. They should set standards for responsible State behaviour and prevent conflicts in the ICT environment while avoiding any undue restrictions on the peaceful uses of ICTs or hampering international cooperation or technology transfer.

26. The elaboration of such rules would contribute to more cooperation and trust not only between governments, but also between governments and the private sector.

27. Previous GGE reports reflected consensus on norms for responsible State behaviour in the security and use of ICTs. Relevant regional endeavours also provide a wealth of possible practical measures that should be consolidated under the UN umbrella.

28. The task before this OEWG is to agree on recommendations on where the existing norms may be codified into practical binding rules that take into account the complexity and unique attributes of ICTs as well as the differentiated technical capacities of Member States.

29. The principle of common but differentiated responsibilities in the ICT environment should represent a key element in guiding the ongoing efforts in this regard.

V. Regular Institutional Dialogue:

30. The United Nations must play a central leading role in promoting dialogue on the security of ICTs in their use by States and developing norms, rules and principles for responsible State behaviour in this arena.

31. Given the strategic importance and the global cross-border nature of the related threats and of any international measures to mitigate these threats, an inclusive, multilaterally agreed, and rules-based process within the UN System is the best and most efficient way to ensure that the agreed arrangements are equitable, comprehensive, and effective.

32. States have a primary responsibility for maintaining a secure and peaceful ICT environment. However, international dialogue within this proposed UN-led process should allow for the appropriate participation of the relevant private sector entities, academic experts, and civil society organizations to express their views.

33. This process should take place within an inclusive institutional platform dedicated for that purpose. Such a platform should not duplicate ongoing work by other international organizations and forums addressing issues such as the criminal and terrorist use of ICTs, human rights and Internet governance, but should rather focus on monitoring and disseminating information on the implementation of the agreed rules and measures from the international security perspective, as well as the further development and elaboration of such agreed rules and guidelines.

34. The Secretary General's offer in his disarmament agenda to utilize his good offices in order to resolve possible conflicts related to ICT incidents is welcomed. However, developing a specialized institutional platform could represent a major contribution towards a more reliable and secure global ICT environment and strengthening the international community's capabilities in addressing ICT security incidents and gradually developing the necessary technical, legal and diplomatic measures.

VI. Confidence-Building Measures:

35. Previous GGE reports have recognized that CBMs strengthen international peace and security. They can increase interstate cooperation, transparency, predictability and stability.

36. They have also highlighted that in their work to build confidence to ensure a peaceful ICT environment, States should take into consideration the Guidelines for CBMs adopted by the Disarmament Commission in 1988 and endorsed by consensus by the General Assembly in resolution 43/78.

37. The GGEs recommendations included important references to measures such as the identification of appropriate points of contact at the policy and technical levels to address serious ICT incidents, the development of mechanisms and processes for bilateral, regional, sub-regional and multilateral consultations to enhance confidence and to reduce the potential of conflicts, and the importance of transparency to increase confidence.

38. The voluntary sharing of information on various aspects of national and transnational threats and vulnerabilities, as well as best practices for ICT security, are powerful tools that should be utilized, as appropriate, in a more systematic and harmonized manner in the context of a multilateral inclusive specialized forum.

39. The provision by States of their national views on categories of infrastructure that they consider critical and national efforts to protect them, including information on national laws and policies for the protection of data and ICT-enabled infrastructure, could represent an important step forward.

40. At the national level, the establishment of national emergency response mechanisms is an important measure. States should support and facilitate the functioning of and cooperation among such national response entities. Such cooperation should include, as appropriate, addressing requests from other States to investigate ICT-related incidents or to mitigate malicious ICT activity emanating from their territory, while taking into account the possible limitations on the technical capacities of developing countries to address such requests.

41. Nevertheless, voluntary measures at the national level may no longer be sufficient to address the rapidly widening scope of the global threats of the malicious use of ICTs.

VII. Capacity-Building:

42. In an increasingly connected world, any international regime on cyber-security will be only as strong as its weakest link.

43. While States bear primary responsibility for national security and the safety of their citizens, some States may lack sufficient capacity to protect their ICT networks, or to assist other States to do so, which may represent a global threat taking into account the possible cross-border spillovers of major ICT incidents.

44. International cooperation and assistance play an essential role in enabling States to secure ICTs and ensure their peaceful use. Providing assistance for capacity-building in the area of ICT security is also essential for international security, by improving the capacity of States for cooperation and collective action.

45. The 2010, 2013 and 2015 GGE reports rightly recommended that the international community should provide assistance to improve the security of critical ICT infrastructure; develop technical skills and appropriate legislation, strategies and regulatory frameworks to fulfil their responsibilities; and bridge the divide in the security of ICTs and their use.

46. These reports also stressed that capacity-building involves more than a transfer of knowledge and skills from developed to developing States, as all States can learn from each other about the threats that they face and effective responses to those threats.

47. The relevant General Assembly resolutions have highlighted that States should consider a variety of measures to provide technical and other assistance to build capacity in securing ICTs in developing countries requesting assistance, including training, exchange of legal and administrative best practices, and access to technologies deemed essential for ICT security.

48. The United Nations Institute for Disarmament Research (UNIDIR) has been active in developing modules that could be of relevance in assisting developing countries to identify their needs in the area of capacity-building and to facilitate donor/recipient dialogue and matchmaking. Further development and strengthening of UNIDIR's work in this area should be encouraged.

VIII. Recommendations:

49. To that end, Egypt proposes that the outcomes of the OEWG **include a recommendation to the General Assembly to adopt a Political Declaration which stresses that**:

a. Member States reaffirm their commitment to adhere to the 11 recommendations contained in paragraph 13 of the 2015 GGE Report and step up their efforts to strengthen their implementation, and shall, in particular, refrain from:

i. any act that knowingly or intentionally damages or otherwise impairs the use and operation of critical civilian infrastructure under any circumstances,

ii. limiting the access of other States to the Internet,

iii. stockpiling ICT-related vulnerabilities,

iv. harming the information systems of the authorized emergency response teams of other States,

b. Member States shall:

i. take reasonable steps to ensure the integrity of the ICT products supply chain so that end-users can have confidence in the security of such products,

ii. seek to prevent the proliferation of malicious ICT tools and techniques and the use of harmful hidden functions,

iii. take coordinated measures towards the voluntary exchange of relevant information including on best practices and possible threats and vulnerabilities,

iv. consider the establishment of an institutional platform, preferably in the form of a standing open-ended working group or subsidiary body, dedicated to (i) elaborating international rules and recommendations on responsible State behaviour and CBMs, (ii) following and monitoring the implementation of such rules and recommendations including through the exchange of information and harmonized periodical national reporting, (iii) streamlining and strengthening capacity-building endeavours and activities with a view to assisting developing countries in enhancing and bolstering their information security and emergency response capabilities, and (iv) examining possible reliable mechanisms on the attribution of unlawful ICT-related incidents at the international level.
