Kingdom of Norway

1. The Government of the Kingdom of Norway is pleased to respond to the invitation to the Member States to submit their views on the scope, objectives and structure of the new convention on the countering of the use of information and communications technologies for criminal purposes, with regard to implementation of UN General Assembly resolutions 74/247 and 75/272. International cooperation is key to tackle the continuously developing threats of cybercrime, and the Government of Norway looks forward to participate in the negotiations for a comprehensive convention on the matter.

Scope

2. In resolution 74/247, the UN General Assembly decided to establish an open-ended intergovernmental committee of experts, representative of all regions, to elaborate a comprehensive international convention *on countering the use of information and communication technologies for criminal purposes*. As the resolution clearly targets criminal behavior, criminalization of core cybercrime offences should be a central part of the convention.
3. Questions regarding cybersecurity and cyber-governance fall outside the mandate given by the General Assembly, and should not be the topic of the convention. These matters are subjected to other UN fora and processes. Attempts to include provisions on cybersecurity and cyber-governance will make it harder to create an instrument that will attract broad support.
4. Cybercrime has already been a challenge for decades, and it is a persistent problem that criminal perpetrators often are one step ahead of the national law enforcement agencies. Cybercrime tomorrow is not the same as cybercrime today, and the ongoing digital revolution creates an immense task for the international community of states. In that regard, it is of utmost importance to strive for the inclusion of an updated and modern catalogue of offences, which can stand the test of time.

5. Even though cybercrime develops every day, national and international agencies have managed to identify central reoccurring types of conduct. These offences are already criminalized in many Member States today. In that regard, the Government of the Kingdom of Norway would like to recommend at least the following cyber-dependent and cyber-enabled offences to be considered:
    - Illegal access, i.e. accessing a computer or computer system without authorization,
    - Illegal interception, i.e. real-time unlawful interception of the content of communications or traffic data related to communications,
    - Data or system interference, i.e. malware, denial of service attacks, ransomware, data deletion or modification,
    - Misuse of devices, i.e. trafficking or using credit data, passwords and personal information which permit access to resources,
    - Offenses related to child sexual abuse materials,
    - Offences related to computer-facilitated fraud, i.e. manipulation of computer systems or data for fraudulent purposes such as phishing, business email compromises, and auction fraud, and
    - Offences related to infringement of copyright and related rights.
6. The convention should also include provisions on attempt, aiding and abetting and conspiracy, the laundering of the proceeds of cybercrime, and the liability of corporations and other legal persons.
7. Since cybercrime is developing continuously, it is important for the Ad hoc Committee to focus on updated reports from national law enforcement agencies, and equivalent reports from regional and international organizations. The UNODC Comprehensive study on cybercrime is important. The Government of the Kingdom of Norway would also like to call attention to the annual Internet Organised Crime Threat Assessment (IOCTA) from Europol, as a significant source of information regarding dominating types og cybercrime.
8. In addition to provisions on criminalization, the convention should also include provisions on procedural authorities, in particular provisions on the collection

and sharing og electronic evidence. It is important that these provisions are consistent with due process and the protection of human rights and fundamental freedoms.

9. Dealing with the challenge of modern cybercrime, the convention should require the Member States to include domestic provisions specifically aimed at electronic evidence, such as rules on expedited preservation of stored computer data, search and seizure of stored computer data and real-time collection of computer traffic data and content data in cases of serious crime. Furthermore, the convention should allow cooperation to collect and obtain electronic evidence for any type of crime, not only cybercrime.
10. In particular, the Ad hoc Committee should consider provisions on obtaining electronic evidence in the so called cloud. In the last decade, storage of computer data in the cloud has reoccurred as a challenge for national law enforcement agencies, especially due to jurisdiction related issues, and the dependency on other states. A modern and updated convention on cybercrime should therefore reflect how Member States can cooperate to secure evidence stored through the cloud in other states.
11. It is also necessary for the convention to include provisions on international cooperation. In this regard, the Ad hoc committee should draw experiences from existing treaties, especially UNTOC and UNCAC. Provisions on extradition and mutual assistance should be taken into account.
12. It is also important for the convention to reflect the different abilities of the Member States to comply with the suggested provisions, especially regarding technical infrastructure and capabilities. Therefore, the convention should establish instruments for capacity building, and provide avenues to Member States to seek such assistance.
13. Finally, the convention should address how citizens, businesses, organizations and other stakeholders can work together with the governments to protect themselves and the community from cybercrime. Even though cybersecurity

falls outside the scope of the convention, prevention of cybercrime is naturally relevant, and should be considered.

Objectives

14. The Ad hoc Committee should take aim at creating a robust convention that requires the Member States to adopt national legislation that improves the prevention and handling of cybercrime globally. Domestic provisions on criminalization of certain types of cybercrime, as well as provisions on procedural authorities and international cooperation, will be especially important.
15. It should be an objective for the upcoming drafting process to create an instrument that can stand the test of time, updated on all modern forms of cybercrime, as well as the most likely trends to come. Furthermore, it should be an objective to draft an ambitious instrument, that can adequately address the central cybercrime challenges. At the same time, a consensus-based approach is vital.
16. The Government of the Kingdom of Norway would also like to reiterate the importance of maintaining an open, inclusive, transparent and multi-stakeholder process that will allow all Member States to negotiate in good faith toward well-informed, practical solutions, which we believe is key to ensure widespread accession for the new convention.

Structure

17. Taking into account the proposed scope and objectives for the convention, main parts of the convention is given. However, it will be fruitful for the Ad hoc committee and the Member States to have an open mind regarding the structure of the convention. Even though provisions on criminalization, procedural authorities and international cooperation should make up central parts of the convention, other matters may also influence the final structure. The Government of the Kingdom of Norway recommends an open approach to the structure of the convention.

Human rights

18. International human rights law applies to cyber activities just as it does to any other activity. States must comply with their human rights obligations also in cyberspace, as they must in the physical world. States must both respect and protect human rights, including the right to freedom of expression and the right to privacy and other relevant data protection principles.
19. It is self-explanatory that human rights standards as enshrined in the International Covenant on Civil and Political Rights (ICCPR) entail an important framework for any new provisions on cybercrime. Regardless, the Government of the Kingdom of Norway would like to reiterate the importance of human rights in the upcoming negotiations, especially regarding provisions requiring national legislation on procedural authorities.