Unofficial translation

Guiding Questions

1. Criminalization

i. First group of questions[1]:

1. What elements [mental/unlawful] (for example, [malicious/dishonest] intent) should be recorded when considering the offences of [illegal/unlawful/unauthorized] access and interception? Should the convention provide for putting in place legal protections for cybersecurity researchers and other professionals working in cybersecurity (including, inter alia, penetration testers)?

Acts included in the criminalization chapter of the draft convention co-sponsored by China and a number of other States are characterized by direct intent, which is related to the characteristics and way of committing crimes in the field of ICTs. In particular, unlawful interference with digital information (Article 8), creation, use and spread of malicious software (Article 10), etc. imply the intent to commit a specific crime and achieve a certain goal, acting in one's own vested or other personal interests. However, in a number of cases the awareness of a presence of such an offence can be absolutely missing when a malware-infected IT device belonging to an individual is used to conceal the illegal activity of an intruder. At the same time, there can be cyber-dependent acts when there is no direct intent contained in the activities of a perpetrator.

---

1 ***First group: questions related to the following proposed provisions:***
[Illegal] [unlawful] [unauthorized] access; [data] [digital information] interference; computer [system] [network], [telecommunication network] or [electronic device] interference; Obstruction of a computer, programme or data; Disruption of information and communications technologies networks; Attack on a site design; Unauthorized access to or interference with a critical information infrastructure; [Illegal] [unlawful] [unauthorized] interception; Unlawful use of devices or creation, use and distribution of malicious software; Dishonestly receiving stolen computer resource or communication device; Unlawful use or facilitation of unlawful use of information and communications technologies

As for the legal protection of persons conducting the so-called "lawful" breach of computer systems or their protection systems (e.g., various experts, testers, or specialists), the limits of such "bona fide" interference should be restricted by the territory or infrastructure of their own State with no possibility to carry out such activities in the territories of other States or within their information networks and space. An opportunity to carry out a "lawful" breach in the territory of another State can only be granted at the request and with the consent from the competent authorities thereof, otherwise such activities can lead to the violation of the right of States to sovereignty.

2. Do you imply that, to be considered an offence, any of the proposed conducts must result in, or be intended to result in a specific or serious harm, or material damage? How should "harm" be defined?

This issue is mostly relevant to cyber-dependent conducts. The extent of damage is defined by the domestic law. This criterion can be used to distinguish crimes and offences. At the same time, when it comes specifically to harm and not a material damage, then it can include harm to health, state interests, environment, etc.

3. Should the infringement of security measures be considered as a condition for recognizing some conducts an offence, and if so, under which circumstances?

See commentary to Question 1.

4. Could we consider the proposed provisions on "Obstruction of a computer, programme or data", "Attack on a site design" and "Disruption of information and communications technologies networks", as forms of [illegal] [unlawful] [unauthorized] interference?

The above provisions are partially covered by Articles 8 (Unlawful interference with digital information) and 9 (Disruption of information and

communications networks) of the Russian draft convention co-sponsored also by China and a number of other States.

5. How do you think the convention should deal with the question of "unauthorized access to, or interference with a critical information infrastructure"?

In this case, it is necessary to establish an intent or absence of special authorization under the domestic law. Should these elements of offence be criminalized, the list of critical information infrastructure (CII) should remain open-ended and be compiled by each country depending on its national priorities.

6. Why do some Member States choose to use the term "illegal", others choose "unlawful", and still others "unauthorized". Where, do you think, is the difference?

We believe the term "illegal" ("unlawful") to be the most definitive, explicit and comprehensible for all State Parties, since it cannot be interpreted ambivalently. The term "unauthorized" is found in most international crime-related treaties. The term "unauthorized", in our view, does not always indicate the illegality of actions.

7. Why do some State Parties choose to use the term "without right", others chose "without due authorization", and still others "unlawful"? What is the difference?

We believe that the answer to this question is contained in the answer to question 6. The term "illegal" ("unlawful"") is the most acceptable in view of certainty.

8. Is there any difference between the terms "data" and "digital information"? Which term would be preferred by you?

We believe the terms "information" and "data" to be synonymous. It appears that for the purposes of the convention being drafted one should speak exclusively about information/data to be subject to automated

processing. At the same time, the term "data", in our view, being broad in nature, covers also the forms of information unacceptable for automated processing. Therefore, the term "digital data" or "digital information" is deemed the most preferable for the purposes of the convention.

9. Was there a reason for some proposals not to include the deterioration of data, and for other proposals to prefer the term "blocking" or "suppressing"?

Further comments by the State Parties that use those terms are required to resolve that issue.

10. Is the act of "copying" considered a part of data interference?

We believe that if the copying of digital data is carried out intentionally for the purpose of its subsequent unlawful use or as a result of unlawful access to it, then such actions constitute data interference. The intentional unlawful interference with digital information/data is possible by damaging, deleting, altering, blocking, modifying it or copying the information in the digital form.

11. Regarding the punishable acts related to system/network interference, what are in your view the devices (and an array thereof) to which this article applies: computer system, computer network, telecommunication network, electronic device, or ICT device?

This article may apply to punishable acts against information systems, information and telecommunications networks and ICT devices.

12. Would there be a need for the interception to be considered an act carried out fraudulently?

If we understand the question correctly, its essence is the following: is it always so that the interception is carried out fraudulently?

It is not always that the interception is carried out fraudulently. At the same time, an interception can be viewed as an act committed in a fraudulent way, for example, if the intention is to steal the property by

destroying, blocking, modifying or copying digital information or otherwise interfering with ICT operation.

i. Second group[2] of questions:

1. Do you think a fraud committed fully or partly over the Internet is sufficient to cover other conducts such as theft, scam, financial offences, and electronic payment tools offences?

A fraud is a form of theft in the same manner as robbery. Theft should be understood as an unlawful gratuitous withdrawal and/or obtaining of another person's property for the benefit of the guilty or other persons that inflicted damage on the owner or another proprietor of that property committed for mercenary purpose.

The Russian draft, co-sponsored by China and a number of other States, reflects the general category of such offences – "ICT-related theft - i.e. the theft of property or the illegal acquisition of rights over it, including by means of fraud, through destruction, blocking, modification or copying of digital information or other interference with ICT operations." In Russian criminal law, the universal language "using information and telecommunication networks, including the Internet network" is applied to such crimes, while the crime of theft through the use of electronic payment instruments is also identified separately.

The language "using information and telecommunication networks, including the Internet network" is of universal character. Thefts committed using electronic payment instruments are identified separately.

2. Regarding computer/ICT-related forgery, what kinds of [mental/fault] elements (for example [malicious/dishonest] intent) should be included in the criminalization of such act? Should the convention

---

2 ***Second group: questions related to the following proposed provisions:***
[Computer] [ICT]-based forgery; Creation and use of digital information to mislead the user; Information and communications technologies-related theft; Computer- [ICT-] related fraud; Illicit use of electronic payment tools; Identity-related crimes; Infringement of copyright and related rights by means of information and communications technologies

consider putting in place legal protections for cybersecurity researchers and other professionals working in cybersecurity (including, inter alia, penetration testers)?

See comments to Question 1 from the first group of questions.

3. Could we consider the proposed provisions on "creation and use of digital information to mislead the user", as a form of [computer] [ICT]-related forgery?

We can answer this question positively, taking into account the provisions contained in the Russian draft, which cover the forgery. However, such qualification will depend on the circumstances of the commission of the crime related to misleading the user.

4. How do you think the convention should deal with identity-related offences?

Criminalization of relevant acts is important given a large-scale character of unlawful acts in relation to such data. Data can thus be directly an object of offence or used also to commit other crimes through sending malicious software to corporate or personal e-mails, social engineering to obtain bank details or mislead a victim. Personal data can also be further used to commit a number of criminal acts, including, for instance, "identity-related offences." Apart from the criminalization of actions related to unlawful data processing, we also consider it necessary to criminalize actions related to creation, use and distribution of information resources deliberately designed for such unlawful data processing.

5. What would be the justification for the inclusion of offences related to the infringement of copyright in the scope of the convention, since this issue is already covered by other international instruments?

The inclusion of some or other unlawful acts in the scope of the convention should be justified by their social danger. The use of ICTs when committing them predetermines their large-scale expansion, frequency and

pace of commitment as well as anonymity of perpetrators and access to a broad scope of objects of offences and information. Therefore, in essence, a corresponding generally accepted international instrument will be a response to those challenges and threats that are set against the rights and legitimate interests of the citizens by perpetrators when they commit acts criminalized by the convention.

i. **Third group[3] of questions:**

1. How can offences relating to online child sexual abuse be defined so as to provide children with the greatest protection from harm? What should be considered in the choice of terminology?

This issue deserves special attention. Opinions and proposals from other States on this topic are of interest.

A general language on the criminalization of crimes associated with fabrication and distribution of materials or objects with pornographic pictures of minors using the ICTs may allow in the widest possible way to provide at the national level for an appropriate format of liability for the acts of such category.

2. Should the access or viewing of child sexual abuse material be criminalized; if yes, should a condition be made for the obligation of the criminalization of these acts such as "consistent with a State party's legal principles" or "without prejudice to a State party's domestic law"?

The issue of the criminalization of such type of crimes should be examined at the domestic level.

Once the provisions are introduced to criminalize such acts, consideration should be given to the possibility for the States to make a reservation to such provisions.

---

3 ***Third group: questions related to the following proposed provisions:***
Online Child Sexual Abuse; Sexual extortion; Non-consensual dissemination of intimate images ("revenge porn"); Offences related to pornography; Encouragement of or coercion to suicide; Involvement of minors in the commission of illegal acts; Sending offensive messages through communication service; Threat and blackmail; Violation of privacy.

3. What would be the justification (lack of harmonization, new forms of online sexual abuse emerging due to new means of technology, insufficiency of current international instruments…) for the inclusion of the proposed provisions on: "sexual extortion, non-consensual dissemination of intimate images and other offences related to pornography"?

This issue deserves attention and should be examined at the domestic level.

4. Will there generally be an agreement on the age limit for the definition of a child to be under the age of 18 year for the purposes of Articles (that would be in line with the Convention on the Rights of the Child)?

We have no objections. We believe that the application of the provisions of the Convention on the Rights of the Child is acceptable when formulating the norms being drafted.

5. What would be the justification for the inclusion of the proposed provisions on: "encouragement of or coercion to suicide and involvement of minors in the commission of illegal acts"?

There are different games disseminated in the Internet network, the final part of which leads or can lead to the commission of suicidal acts, and the abusers make money by selling them. There are also other suicide-related applications and various materials that contain information on the ways of suicide or self-harm, which are distributed.

Besides, it should be taken into account that the use of ICTs in such cases not only facilitates committing a crime (as regards its anonymity, pace, large-scale character, etc.) but also creates necessary conditions for a large-scale mental influence on the whole groups of children in various parts of the world.

6. What would be the justification for the inclusion of the proposed provisions on: "sending offensive messages through communication service; threat and blackmail; violation of privacy"?

We would like to know the opinions of other States that propose the inclusion of such provisions in the draft convention; the Russian draft, which was co-sponsored by China and a number of other States, has no such provisions.

i. **Fourth group[4] of questions:**

1. What would be the justification for the inclusion of the following proposed provisions:

- "Offences related to discrimination, racism or xenophobia";
- "Offences related to the distribution of narcotic drugs and psychotropic substances, arms trafficking, illegal distribution of counterfeit medicines and medical products; arms manufacturing, trafficking in persons, criminal association"?

The use of ICTs not only facilitates committing a crime (in terms of anonymity, the creation of shadow trading platforms, transnational communication channels, the legalization of illicit proceeds, including with the use of cryptocurrencies, etc.), but also creates the necessary conditions for cross-border and massive crime attempts, allowing the creation of broad networks of criminal organizations with complete "isolation" of specific organizers of such crimes. At the same time, at present, in fact, almost all acts in the areas under consideration are committed with the use of ICT tools.

---

4 ***Fourth group: questions related to the following proposed provisions:***
Incitement to subversive or armed activity; Terrorism-related offences; Extremism-related offences; Offences related to discrimination, racism or xenophobia; Offences related to the distribution of narcotic drugs and psychotropic substances; Offences related to arms trafficking; Rehabilitation of nazism, justification of genocide or crimes against peace and humanity; Illegal distribution of counterfeit medicines and medical products; Use of information and communications technologies to commit acts established as offences under international law.

The inclusion of such provisions is predetermined by the danger of such acts, as well as by the coverage of the general public, both as perpetrators and as victims of such encroachments.

In particular, counterfeit medical products are sold through social networks and individual websites. During the pandemic, criminals skilfully built into the news agenda and exploited the COVID-19 vaccine to its fullest extent.

The UNTOC and its protocols, the universally adopted Anti-Drug Conventions and other international treaties do not provide for the use of ICTs to commit these crimes. Given the increased social danger of such acts, in our opinion, it is necessary to separately criminalize the use of ICTs to commit them.

The apparent duplication in this case should not be a reason to leave such types of crimes out of the convention in question, since, on the contrary, it would provide an additional reason for States to cooperate in order to investigate them effectively.

2. What would be the justification for the inclusion of a provision on "terrorism-related offences and extremism-related offences"?

For the leaders of radical structures the Internet continues to be a tool to recruit new members, a means of communication and organizing extremist (terrorist) actions, inciting inter-ethnic hatred, and spreading racist and xenophobic ideas.

There is a continued trend to disseminate deliberately misleading messages about acts of terrorism in administrative buildings of government bodies, educational institutions, shopping centres, and transport infrastructure facilities through electronic mail services and IP telephony. This is done in order to destabilize the activities of the authorities and law enforcement agencies, to escalate tensions in society.

The engagement in activities of an extremist and terrorist nature is carried out through the Internet by recruiting into terrorist groups, as well as sharing detailed instructions for the preparation of terrorist acts. Representatives of the extremist-terrorist ideology, relying on the low level of education, use special techniques of influence on people: they distort the primary sources of spiritual teachings and historical facts, replace personal meanings with an undertaking to restore social justice, promise a special position for those who have sworn in, and special honour in the other world for the dead.

In the information space, there are both video messages from the leaders of the terrorist underground, as well as staged videos, and pseudo-news stories. The content is used both for demonstrating force, intimidating and carrying out information and psychological attacks on society, as well as to promote extremist ideas, find new supporters (video materials referring to hostilities, ideological (educational) content with a religious extremist bias, materials not related directly to terrorism propaganda, but creating a positive image of a terrorist organization and its activities).

Such content is posted by users of social networks on personal pages along with other "household" information.

Terrorist use of the Internet is a transnational challenge that requires a concerted response across borders, despite some differences in the legal systems of individual States.

3. What would be the justification for the inclusion of a provision on "incitement to subversive or armed activity"?

Implementation of appropriate actions to call for a change in the state system, etc. through the use of ICTs and thus involving large masses of people in illegal activities, which poses a threat to public and national security.

4. What would be the justification for the inclusion of a provision on "rehabilitation of Nazism, justification of genocide or crimes against peace and humanity"?

Through the use of ICTs, such ideology, propaganda of Nazism, false information related to the revision of history is spread among a wide range of people, which entails, inter alia, the revival of ideologies based on racial, religious and other types of intolerance.

5. Should the convention contain a provision to criminalize "the use of ICT to commit all acts established as offences under international law"?

We believe that in this way the broadest coverage of crimes committed with the use of ICTs can be achieved, which will contribute to the effectiveness of cooperation in the provision of mutual legal assistance between States in terms of gathering evidence, as well as mechanisms for the recovery of criminal assets.

i. Fifth group[5] of questions:

1. Would Member States be supportive of the inclusion of provisions on the criminalization of obstruction of justice and the laundering of proceeds of crimes covered by the convention?

The inclusion of provisions on the laundering of the proceeds of crimes can be considered positively.

The question of the necessity of including provisions on obstruction of justice in this convention is subject to further discussion.

2. How do you think the convention should deal with participation in, attempt of, as well as aiding and abetting in a crime?

---

5 ***Fifth group: questions related to the following proposed provisions:***
Money-laundering; Obstruction of justice; Failure to protect data; Other illegal acts; Liability of legal persons; Aiding, abetting, attempt; Sanctions and other measures

The Russian draft of the convention, which was co-sponsored by China and a number of other states, (Article 28) contains detailed provisions for regulating these acts:

- **States Parties shall take measures, in accordance with their domestic law, which recognize as an offence the preparation and attempted commission of an act criminalized in accordance with the convention;**
- **States Parties shall consider taking measures to establish as an offence the manufacture or adaptation by a person of instruments or other means for the commission of an offence, the recruitment of accomplices, conspiracy to commit an offence or other intentional enabling of an offence under the convention, if the offence is not consummated through circumstances beyond the control of that person.**
- **States Parties shall take measures under their domestic law to establish liability, in addition to the direct perpetrators of an offence established in accordance with this convention, for the organizers, instigators or accomplices involved and to enhance liability for group offences, including organized groups and criminal associations.**

3. Should criminal liability be extended beyond individuals to legal persons?

4. Could the convention follow the formulation of liability of legal persons contained in article 10 of UNTOC? Would there be a need for a separate offence punishing the negligence of legal persons in maintaining required security measures?

(Answer to Questions 3-4) Yes. The convention should include a rule establishing liability for legal persons, which could be criminal, administrative or civil, depending on the legal principles of States. Should Article 10 of the UNTOC be used, it would States to reach consensus.

5. Do you think that the convention should include a provision on aggravating circumstances? If so, should this be a general provision on

aggravating circumstances, or should specific articles include a qualifying element of aggravating circumstances? What about mitigating circumstances?

We suppose that the way ICTs are used to commit crimes included in other international treaties on combating crime could be an aggravating circumstance. This makes no sense in the convention now being drafted, since the entire convention will be devoted to this very issue.

It would be interesting to know the arguments of those States that propose to introduce an aggravating circumstance provision.

6. Regarding "other illegal acts", could para. 3 of art. 34 of UNTOC ("States parties may adopt more strict or severe measures than those provided in this convention…") be a solution to cover all these offences?

It is not quite clear what the question is.

We assume that the future convention will cover both cyberdependent and traditional crimes committed through the use of ICTs, for which there will be an obligation to take appropriate measures.

At the same time, for those illegal acts that will not be included in the convention, it will be up to the States to determine what measures (more severe, probably) should be taken with respect to those acts.