CONCEPT NOTE

Countering the use of information and communications technologies for terrorist and extrimist purposes

The mandate of the UN Ad Hoc Committee to elaborate a universal convention on countering the use of information and communications technologies (ICTs) for criminal purposes is consistent with the creation of a comprehensive international document. The Russian Federation has advocated the inclusion of provisions on cooperation between UN Member States in terms of countering the use of ICTs for terrorist and extremist purposes into the future treaty. At the same time, domestic laws of those countries that have opposed to regulate the countering of terrorism and extremism in the information sphere internationally, have very detailed provisions in this regard. These issues have also been explicitly reflected in regional conventions on combating ICT-crime.

Domestic regulation

USA

The PATRIOT Act 2001 in part of enhanced surveillance procedures provides for authority to intercept wire, oral and electronic communications relating to terrorism (Sec. 201) and computer fraud and abuse offences (Sec. 202). The Act enabled investigators ot gather information when looking into the full range of terrorism-related crimes, including: chemical-weapons offences, the use of weapons of mass destruction, killing Americans abroad, and terrorism financing. The law placed electronic trespassers on the same footing as physical trespassers. The Act also provides for deterrance and prevention of cyberterrorism techniques (Sec. 814).

UK

The Terrorism Act 2006 in its Section 3 contains provisions applying to the Internet. It says that offences contained in Section 1 («encouragement of terrorisms») and 2 («dessimination of terrorist publications») include publication and dissiminstion on the Internet and other electronic services.

France

The French Criminal Code extends Article 421-1 (terrorist acts) to computer crimes, incl. attacks on automated data processing systems (Articles 323-1 to 323-8).

European Union

The Directive (EU) 2017/541 of the European Parliament and of the Council on combating terrorism was enected on 15 March, 2017. It notes that the terrorist threat has grown and rapidly evolved in recent years. These new forms of conduct sould also be punishable if committed through the Internet, including social media (6). **The offence of public provocation to commit a terrorist offence act comprises, inter alia, the glorification and justification of terrorism of the dissemination of messages or images online and offline (10)** — in order to prevent and suppress. Self-study, including through the Internet or consulting other teaching material, should also be considered to be receiving training for terrorism when resulting from active conduct and done with the intent to commit or contribute to the commission of a terrorist offence (11). To ensure the success of investigations and the prosecution of terrorist offences, offences related to a terrorist group or offences related to terrorist activities, those responsible for investigating or prosecuting such offences should have the possibility to make use of effective investigative tools such as those which are used in combating organised crime or other serious crimes. Such tools should, where appropriate, include, for example, the search of any personal property, the interception of communications, covert surveillance including electronic surveillance, the taking and the keeping of audio recordings, in private or public vehicles and places, and of visual images of persons in public vehicles and places, and financial investigations (21).

An effective means of combating terrorism on the Internet is to remove online content constituting a public provocation to commit a terrorist

offence at its source. Member States should use their best endeavours to cooperate with third countries in seeking to secure the removal of online content constituting a public provocation to commit a terrorist offence from servers within their territory (22).

Prevention of radicalisation and recruitment to terrorism, including radicalisation online (31) also provides for in this Directive.

DIRECTIVE (EU) 2017/541

TITLE III

OFFENCES RELATED TO TERRORIST ACTIVITIES

Article 5

Public provocation to commit a terrorist offence

Member States shall take the necessary measures to ensure that the distribution, or otherwise making available by any means, whether online or offline, of a message to the public, with the intent to incite the commission of one of the offences listed in points (a) to (i) of Article 3(1),

- terrorist offences causing extensive destruction to ... an infrastructure facility, including an information system;
- manufacture, possession, acquisition, transport, supply or use of explosives or weapons, including chemical, biological, radiological or nuclear weapons, as well as research into, and development of, chemical, biological, radiological or nuclear weapons;
- illegal system interference e.t.c.

where such conduct, directly or indirectly, such as by the glorification of terrorist acts, advocates the commission of terrorist offences, thereby causing a danger that one or more such offences may be committed, is punishable as a criminal offence when committed intentionally.

Australia

The Criminal Code Act 1995 in Part 5.3 -Terrorism, Article 100.4 *«Application of provisions»* (part generally applies to all terrorist acts and preliminary acts), provides for the action [terrorist act] involves, or if carried out would involve, the use of electronic communication (5 «h»); or the threat is made using an electronic communication (5 «i»).

New Zealand

Terrorism Suppression Act 2002 in its Schedule 4D contains United Nations Security Council Resolution 2178 (2014), in which UN Member States expressed concern over the increased use by terrorists and their supporters of communications technology for the purpose of radicalizing to terrorism, recruiting and inciting others to commit terrorist acts, including through the Internet. They also underlined the need to act cooperatively to prevent terrorists from exploiting technology, communications and resources to incite support for terrorist acts. They condemned violent extremism, which can be conducive to terrorism. Member States are also encouraged to act cooperatively when taking national measures to prevent terrorists from exploiting technology, communications and resources, including audio and video, to incite support for terrorist acts.

Regional documents

African Union

African Union Convention on Cyber Security and Personal Data Protection 2014 (Para 3 Article 29 - *«Offences specific to Information and Communication Technologies»*) prescribes for State Parties to make it a criminal offence **to create, disseminate or make available ideas of rasist or xenophobic nature through a computer system** (sub. para. «e»); to threaten, through a computer system, to commit a criminal offence against a person for the reason that they belong to a group distinguished by race, colour, descent, national or ethnic origin or religion (sub. para. «f»); **to deliberately deny, approve or justify acts constituting genocide or crimes against humanity through a computer system** (sub. para. «h»).

Para 1 Article 30 - *«Adapting certain offences to Information and Communication Technologies»* - provides that State Parties shall take the necessary legislative and/or regulatory measures to consider as aggravating circumstances the use of information and communication technologies to commit offences such as theft, fraud, handling of stolen property, abuse of trust, extortion of funds, **terrorism** and money laundering.

League of Arab States

Article 15 of Arab Convention on Combating Information Technology Offences provides for ***«Offences Related to Terrorism Committed by means of information technology»***. They are dissemination and advocacy of the ideas and principles of terrorist groups; financing of and training for terrorist operations, and facilitating communication between terrorist organizations; dissemination of methods to make explosives, especially for use in terrorist operations; spreading religious fanaticism and dissention and attacking religions and beliefs.

Moreover, Article 16 criminalises **illicit traffic in arms**.

Therefore, it is obvious that the countering the use of ICTs for terrorist and extremist purposes has already been worked out in detail at the regional and national levels. However, the existing fragmentation in the regulation of these issues makes it difficult for comprehensive cooperation between states to effectively combat criminals. The Russian Federation once again calls for provisions on countering terrorism and extremism to be enshrined in the text of the universal convention. This will be in the interests of the international community and will contribute to effective international cooperation in this field.

The UN GA resolution **74/247** in its **OP 2** provides that the Ad Hoc Committee «will take into full consideration existing international instruments and efforts at the national, regional and international levels on combating the use of information and communications technologies for criminal purposes».