WRITTEN SUBMISSION BY

THE REPUBLIC OF SOUTH AFRICA

7TH SESSION OF THE INTERGOVERNMENTAL EXPERT GROUP MEETING ON CYBERCRIME

AGENDA 2:

CONSIDERATION OF ALL PRELIMINARY CONCLUSIONS AND RECOMMENDATIONS RESULTING FROM THE FOURTH, FIFTH AND SIXTH MEETINGS OF THE EXPERT GROUP, HELD IN 2018, 2019 AND 2020, AND PRODUCTION OF CONCLUSIONS AND RECOMMENDATIONS FOR SUBMISSION TO THE COMMISSION ON CRIME PREVENTION AND CRIMINAL JUSTICE

Vienna

Check against delivery

WRITTEN INPUT FROM SOUTH AFRICA

Pursuant to paragraph 5 and 6 of the Chair's proposed workplan of the Expert Group for the period 2018-2021, adopted by the 4th Session of the IEG, the Rapporteur was requested to prepare a list of preliminary conclusions and recommendations for each of the Sessions in line with member states' suggestions, focusing on practical responses to cybercrime. Subsequently, these preliminary recommendations and conclusions were circulated to Member States through Conference room paper UNODC/CCPCJ/EG/.4/2021/CRP.1

We recognize that the following key themes emerged from all sessions:

- The need to ensure the widest form of international co-operation using all available tools and regional instruments;
- The need for legislation, policy and frameworks which facilitate the fight against cybercrime which includes both the use of existing crimes and the enactment of cyber specific offences
- The need for public/private partnerships, legislation, policy and frameworks which respect human rights and confidentiality;
- The need for a community of cybercrime experts to meet under the auspices of the UNODC, sharing best practices, knowledge and skills and training; and
- The need for an international legally binding instrument under the auspices of the UN.

We recognise that member states may wish to engage on the language in the report and on the substance of the recommendations.

We further recognise that as the study is a stock taking exercise and as such will encompass divergent views on the state of cybercrime under the various themes.

Consensus in these circumstances may be difficult to achieve. However, the process embarked upon requires the IEG in this sitting to prepare a report which identifies where broad consensus can be achieved and those areas which will remain contested.

We respect and accept that the work of the IEG should be concluded as its mandate is complete with the finalisation of the work plan.

A procedural report which encompasses the entire study highlighting the areas of consensus is therefore necessary. The work undertaken by the IEG and this report will no doubt feed into the necessary work being undertaken in the field of cybercrime by the CCPCJ and the Third Committee of the UN General Assembly endorsed Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communication Technologies for Criminal Purposes"

Pursuant to this, we have highlighted recommendations and conclusions from the report which support these broad themes, which we feel will assist the process going forward.

II. Meeting of the Expert Group to Conduct a Comprehensive Study on Cybercrime held in Vienna from 3 to 5 April 2018

A. Legislation and frameworks

Legislation theme is best supported by:

(a) Member States should ensure that their legislative provisions withstand the test of time with regard to future developments in technology by enacting laws with formulations that are technologically neutral and criminalize the activity deemed illegal instead of the means used. Member States should also consider establishing consistent terminology to describe cybercrime activities and facilitate, to the extent possible, accurate interpretations of relevant laws by law enforcement agencies and the judiciary;

(d) In formulating policies and legislation, Member States should consider the need to strike a balance between human rights protection on the one hand, and national security, public order and the legitimate rights of third persons on the other. National legislations that criminalize conduct associated with cybercrime and grant procedural authority to investigate, prosecute and adjudicate on cybercrime cases should be consistent with due process guarantees, privacy interests, civil liberties and human rights. National policies and legislations as well as existing and/or future international instruments should follow a multidimensional approach. On the one hand, they should include adequate cybercrime policies based on a comprehensive understanding of the broader concept of cybersecurity. On the other hand, they should not only cover illegal conduct, but also focus on crime prevention and provide help to victims of crime and assistance to the general public. In order to create a solid base for international cooperation on combating cybercrime, Member States should strive to find and promote a culture of establishing a common future for cyberspace;

(g) To enable the prosecution of criminal acts, Member States should legislate on extraterritorial jurisdiction over citizens and persons ordinarily resident on their territory, irrespective of where those acts were committed and whether they constitute offences in the foreign jurisdiction;

(h) Member States may draw on different legal bases for international cooperation, including reciprocity, bilateral or multilateral treaties and other arrangements. Moreover, Member States with more advanced capacities and infrastructure in the field of cybercrime should assume responsibilities proportionate to those capacities or infrastructure in providing legal assistance to other States;

(i) To ensure that relevant issues are properly considered, Member States should consult all relevant stakeholders, including intergovernmental stakeholders, the private sector and civil society, as early as possible when the decision is made to introduce cybercrime legislation;

(l) Effective development, enactment and implementation of national legislation to counter cybercrime should be backed up by capacity-building measures and technical assistance programmes. Member States should allocate appropriate resources for domestic capacity-building. The proper implementation of cybercrime-related legislation requires the training of police and prosecutors, as well as public awareness campaigns. Such resources will also further international cooperation, as such cooperation is enhanced by a country's domestic capacity to investigate and prosecute cybercrime-related offences; and

(s) Member States should develop a new international legal instrument on cybercrime within the framework of the United Nations that takes into account the concerns and interests of all Member States;…

B. Criminalization

The theme of criminalisation is best supported by:

(c) Member States should continue to enact cyber-specific criminal legislation that takes into account new criminal conduct associated with the misuse of information and communications technology to avoid relying on generally applicable provisions of criminal law;

(h) Member States should bear in mind that the focus of international harmonization concerning criminalization of cybercrime should be on a core set of offences against the confidentiality, integrity and accessibility of information systems, while a need to harmonize criminalization concerning general offences that are committed using information and communications technology should mainly be dealt with in specialized forums concerning specific areas of crime;

(j) Member States should adopt and implement domestic legal evidence frameworks to permit the admission of electronic evidence in criminal investigations and prosecutions, including the appropriate sharing of electronic evidence with foreign law enforcement partners;

(l) Member States should explore ways to help to ensure that the exchange of information among investigators and prosecutors handling cybercrime is made in a timely and secure way, including by strengthening networks of national institutions that may be available 24/7; and

(n) In effectively addressing cybercrime, Member States should take into consideration existing human rights frameworks, in particular as regards freedom of expression and the right to privacy, and should uphold the principles of legality, necessity and proportionality in criminal proceedings relating to the fight against cybercrime;…

III. Meeting of the Expert Group to Conduct a Comprehensive Study on Cybercrime held in Vienna from 27 to 29 March 2019

A. Law enforcement and investigations

Law enforcement theme is best represented by:

(d) Member States should promote and engage in international cooperation to combat cybercrime, making use of existing instruments, concluding bilateral agreements based on the principle of reciprocity and supporting, in collaboration with UNODC, regular networking and information-sharing among judicial and law enforcement authorities;

(g) Countries should devote resources to developing expertise to investigate cybercrime and to creating partnerships that employ cooperation mechanisms to obtain vital evidence;

(h) Member States should continue their efforts to develop and support specialized cybercrime units, bodies and structures within law enforcement and prosecution authorities and the judiciary, so that they have the necessary expertise and equipment to address the challenges posed by cybercrime and for the gathering, sharing and use of electronic evidence in criminal proceedings;

(k) Domestic procedural laws must keep pace with technological advances and ensure that law enforcement authorities are adequately equipped to combat online crime. Relevant laws should be drafted taking into account applicable technical concepts and the practical needs of cybercrime investigators, consistent with due process guarantees, privacy interests, civil liberties and human rights, as well as the principles of proportionality and subsidiarity and safeguards ensuring judicial oversight. Moreover, Member States should devote resources to enacting domestic legislation that authorizes:

(n) Domestic law enforcement agencies should reach out to and engage with domestic Internet service providers and other private industry groups. This outreach supports law enforcement investigations by increasing trust and cooperation among stakeholders;

(q) Member States should foster public-private partnerships to combat cybercrime, including through the enactment of legislation and the establishment of channels for dialogue for that purpose, in order to promote cooperation between law enforcement authorities, communication service providers and academia with a view to enhancing knowledge and strengthening the effectiveness of responses to cybercrime; and

(t) States should continue to strengthen capacity-building and enhance the capability of the judicial and law enforcement authorities in investigating and prosecuting cybercrime. The increasing challenges posed by cloud computing, the darknet and other emerging technologies should be emphasized in capacity-building activities. Moreover, States are encouraged to provide capacity-building assistance to developing countries…

B. Electronic evidence and criminal justice

The following items best support the electronic evidence theme and they are:

(b) Member States should foster efforts to build the capacity of law enforcement personnel, including those working in specialized law enforcement structures, prosecutors and the judiciary, so that such personnel possess at least basic technical knowledge of electronic evidence and are able to respond effectively and expeditiously to requests for assistance in the tracing of communications and undertake other measures necessary for the investigation of cybercrime;

(g) Member States should take necessary measures to enact legislation that ensures the admissibility of electronic evidence, bearing in mind that admissibility of evidence, including electronic evidence, is an issue that each country should address according to its domestic law;

(h) Member States should enhance international cooperation among law enforcement agencies, prosecutors, judicial authorities and Internet service providers in order to bridge the gap between the speed at which cybercriminals operate and the swiftness of law enforcement responses. In doing so, Member States should utilize existing frameworks, such as 24/7 networks and cooperation through the International Criminal Police Organization (INTERPOL), as well as mutual legal assistance treaties, to foster international cooperation involving electronic evidence. Member States should further harmonize and streamline processes related to mutual legal assistance and develop a common template to expedite such processes for the timely collection and transfer of cross-border electronic evidence;

(o) Member States should pursue action to enhance cooperation in gathering electronic evidence, including the following:

(i) Sharing of information on cybercrime threats;

(ii) Sharing of information on organized cybercriminal groups, including the techniques and methodology they use;

(iii) Fostering of enhanced cooperation and coordination among law enforcement agencies, prosecutors and judicial authorities;

(iv) Sharing of national strategies and initiatives to tackle cybercrime, including national legislation and procedures to bring cybercriminals to justice;

(v) Sharing of best practices and experiences related to the cross-border investigation of cybercrime;

(vi) Development of a network of contact points between law enforcement authorities, judicial authorities and prosecutors;

(vii) Harmonization and streamlining of processes relating to mutual legal assistance and development of a common template to expedite the process for the timely collection and transfer of cross-border electronic evidence;

(viii) Holding of workshops and seminars to strengthen the capacity of law enforcement authorities and judicial authorities for drafting requests, in the context of mutual legal assistance treaties, to collect evidence in matters related to cybercrime;

(ix) Development of standards and uniformity in procedural aspects relating to the collection and transfer of digital evidence;

(x) Development of a common approach to information-sharing arrangements with service providers in relation to cybercrime investigations and the gathering of evidence;

(xi) Engagement with service providers through public-private partnerships in order to establish modalities of cooperation in law enforcement, cybercrime investigations and evidence collection;

(xii) Development of guidelines for service providers to assist law enforcement agencies in cybercrime investigations, including with regard to the format and duration of preservation of digital evidence and information;

(xiii) Strengthening of the technical and legal capacities of law enforcement agencies, judges and prosecutors through capacity-building and skill development programmes;

(xiv) Provision of assistance to developing countries in strengthening cyber forensic capabilities, including through the establishment of cyber forensic laboratories;

(xv) Holding of workshops and seminars to raise awareness of best practices in addressing cybercrime;

(xvi) Establishment of an international agency to validate and certify digital forensics tools, preparation of manuals and strengthening of the capacity of law enforcement and judicial responses to cybercrime;

(t) States should enact new or strengthen existing legislation to make it possible to recognize the admissibility of electronic evidence and define and establish the scope of electronic evidence; and

(v) States are encouraged to strengthen capacity-building for the collection of electronic evidence, create professional teams equipped with both legal and technical expertise and enhance experience-sharing and training cooperation in that regard. UNODC is encouraged to play a role in those efforts;…

IV. Meeting of the Expert Group to Conduct a Comprehensive Study on Cybercrime held in Vienna from 27 to 29 July 2020

A. International cooperation

Items that best support this theme are:

(a) As regards the scope of the definition of cybercrime for the purposes of international cooperation, countries should ensure the sufficient criminalization of cybercrime acts, which cover not only cyber-dependent crimes, but also other crimes frequently committed with the use of the Internet and electronic means (cyber-enabled crimes), such as cyberfraud, cybertheft, extortion, money-laundering, trafficking in drugs and arms, child pornography1 and terrorist activities;

(e) The efficiency of international cooperation should be improved by establishing rapid response mechanisms for international cooperation, as well as channels of communication through liaison officers and information technology systems between national authorities for the cross-border collection of evidence and online transfer of electronic evidence;

(f) States should continue strengthening cooperation to protect critical infrastructure and strengthen networks of collaboration among computer emergency response teams and computer security incident response teams;

(p) Countries are encouraged to streamline cooperation with industry and enhance collaboration between the Government and private service providers, in particular for addressing the challenges posed by harmful criminal material on the Internet;

(t) Countries are called upon to join, make wider use of and strengthen authorized networks of practitioners to preserve and exchange admissible electronic evidence, including 24/7 networks, specialized networks on cybercrime and INTERPOL channels for prompt police-to-police cooperation, as well as networking with strategically aligned partners, with a view to sharing data on cybercrime matters and enabling rapid responses and minimizing loss of critical evidence. The use of police-to-police cooperation and other methods of informal cooperation before using mutual legal assistance channels was also recommended;

(ll) Beyond domestic laws, international cooperation on cybercrime relies on both formal, treaty-based cooperation and traditional police-to-police assistance.

When debating a new instrument on cybercrime, it is important that countries remember that a new instrument should not conflict with existing instruments, which

already enable real-time international cooperation for many. Thus, countries should ensure that any new instrument on cybercrime avoids conflict with existing treaties;

(oo) International cooperation is important for gathering and sharing electronic evidence in the context of cross-border investigations and for fast and effective responses to requests for mutual legal assistance related to preserving and obtaining electronic evidence. The principles of sovereignty and reciprocity should be respected in the process; and

(nnn) States should respect the sovereignty of other States when establishing their jurisdiction over cybercrime and should not exercise excessive extraterritorial jurisdiction that lacks a sufficient and genuine link with the prosecuted cybercrime. States are encouraged to enhance communication and consultation to settle jurisdictional conflicts;…

B. Prevention

Under this theme the following points are the most relevant:

(a) It should be recognized that prevention is not just the responsibility of Governments: it also requires the participation of all relevant stakeholders, including law enforcement authorities, the private sector, especially Internet service providers, non-governmental organizations, schools and academia, in addition to the public in general;

(i) Public-private partnerships, including cooperation with cybersecurity stakeholders and big technology companies on information-sharing, are needed to prevent and combat cybercrime;

(v) Member States are encouraged to continue to include effective prevention measures at the national and international levels and to focus on proactive activities, such as raising awareness about the risks of cybercrime and the likelihood of prosecution and punishment for offenders and efforts to prevent further crime, by identifying and disrupting ongoing illicit online activities;

(ii) Regular advisories on incident prevention should be issued and shared with users, organizations and other stakeholders to enable them to prevent cyberincidents that could potentially lead to criminal activities;

(ww) It was recommended that States invest in capacity-building to upgrade the skills of officers from the whole spectrum of the criminal justice system as an efficient preventive measure of deterrent effect against cybercrime;

(xx) UNODC should facilitate the sharing of best practices on effective and successful preventive measures against cybercrime.