Establishment of Harmonized Policies for the ICT Market in the ACP Countries

Cybercrime directive: Explanatory notice

Economic Community of West African States (ECOWAS)

HIPSSA

Harmonization of ICT Policies in Sub-Saharan Africa

Establishment of Harmonized Policies for the ICT Market in the ACP Countries

Cybercrime directive: Explanatory notice

Economic Community of West African States (ECOWAS)

HIPSSA

Harmonization of ICT Policies in Sub-Saharan Africa

Disclaimer

This document has been produced with the financial assistance of the European Union. The views expressed herein can in no way be taken to reflect the official opinion of the European Union.

The designations employed and the presentation of material, including maps, do not imply the expression of any opinion whatsoever on the part of ITU concerning the legal status of any country, territory, city or area, or concerning the delimitations of its frontiers or boundaries. The mention of specific companies or of certain products does not imply that they are endorsed or recommended by ITU in preference to others of a similar nature that are not mentioned.

Please consider the environment before printing this report.

Foreword

Information and communication technologies (ICTs) are shaping the process of globalisation. Recognising their potential to accelerate Africa's economic integration and thereby its greater prosperity and social transformation, Ministers responsible for Communication and Information Technologies meeting under the auspices of the African Union (AU) adopted in May 2008 a reference framework for the harmonization of telecommunications/ICT policies and regulations, an initiative that had become especially necessary with the increasingly widespread adoption of policies to liberalise this sector.

Coordination across the region is essential if the policies, legislation, and practices resulting from each country's liberalization are not to be so various as to constitute an impediment to the development of competitive regional markets.

Our project to 'Support for Harmonization of the ICT Policies in Sub-Sahara Africa' (HIPSSA) has sought to address this potential impediment by bringing together and accompanying all Sub-Saharan countries in the Group of African, Caribbean and Pacific States (ACP) as they formulate and adopt harmonized ICT policies, legislation, and regulatory frameworks. Executed by the International Telecommunication Union (ITU), co-chaired by the AU, the project has been undertaken in close cooperation with the Regional Economic Communities (RECs) and regional associations of regulators which are members of the HIPSSA Steering Committee. A global steering committee composed of the representatives of the ACP Secretariat and the Development and Cooperation – EuropeAid (DEVCO, European Commission) oversees the overall implementation of the project.

This project is taking place within the framework of the ACP Information and Telecommunication Technologies (@CP-ICT) programme and is funded under the 9th European Development Fund (EDF), which is the main instrument for providing European aid for development cooperation in the ACP States, and co-financed by the ITU. The @CP-ICT aims to support ACP governments and institutions in the harmonization of their ICT policies in the sector by providing high-quality, globally-benchmarked but locally-relevant policy advice, training and related capacity building.

All projects that bring together multiple stakeholders face the dual challenge of creating a sense of shared ownership and ensuring optimum outcomes for all parties. HIPSSA has given special consideration to this issue from the very beginning of the project in December 2008. Having agreed upon shared priorities, stakeholder working groups were set up to address them. The specific needs of the regions were then identified and likewise potentially successful regional practices, which were then benchmarked against practices and standards established elsewhere.

These detailed assessments, which reflect sub-regional and country-specific particularities, served as the basis for the model policies and legislative texts that offer the prospect of a legislative landscape for which the whole region can be proud. The project is certain to become an example to follow for the stakeholders who seek to harness the catalytic force of ICTs to accelerate economic integration and social and economic development.

I take this opportunity to thank the European Commission and ACP Secretariat for their financial contribution. I also thank the Economic Community of West African States (ECOWAS), West African Economic and Monetary Union (UEMOA), Economic Community of Central African States (ECCAS), Economic and Monetary Community of Central Africa (CEMAC), East African Community (EAC), Common Market for Eastern and Southern Africa (COMESA), Common Market for Eastern and Southern Africa (COMESA), Southern African Development Community (SADC), Intergovernmental Authority on Development (IGAD), Communication Regulators' Association of Southern Africa (CRASA), Telecommunication Regulators' Association of Central Africa (ARTAC), United Nations Economic Commission for Africa (UNECA), and West Africa Telecommunications Regulators' Association (WATRA), for their contribution to this work. Without political will on the part of beneficiary countries, not much would have been achieved. For that, I express my profound thanks to all the ACP governments for their political will which has made this project a resounding success.

Brahima Sanou

BDT Director

Acknowledgements

The present document represents an achievement of a global activity carried out under the HIPSSA project ("Support to the Harmonization of ICT Policies in Sub-Sahara Africa") officially launched in Addis Ababa in December 2008.

In response to both the challenges and the opportunities of information and communication technologies' (ICTs) contribution to political, social, economic and environmental development, the International Telecommunication Union (ITU) and the European Commission (EC) joined forces and signed an agreement aimed at providing "Support for the Establishment of Harmonized Policies for the ICT market in the ACP", as a component of the Programme "ACP-Information and Communication Technologies (@CP-ICT)" within the framework of the 9th European Development Fund (EDF). i.e., ITU-EC-ACP Project.

This global ITU-EC-ACP project is being implemented through three separate sub-projects customized to the specific needs of each region: Sub-Saharan Africa (HIPSSA), the Caribbean (HIPCAR), and the Pacific Island Countries (ICB4PAC).

As members of the HIPSSA Steering Committee co-chaired by the African Union's Commission (AUC) and the ITU, all the Regional economic communities (RECs) especially Economic Community of West African Countries (ECOWAS), Southern African Development Community (SADC), and Economic Community of Central African States (ECCAS) provided guidance and support to the consultants.

ITU would like to thank all the Regional Regulatory associations in Africa and telecommunications ministries, regulators, academia, civil society and operators for their hard work and commitment in producing the contents of the final report.

Without the active involvement of all of these stakeholders, it would have been impossible to produce a document such as this, reflecting the overall requirements and conditions of the Sub-Sahara West Africa while also representing international best practice.

The activities have been implemented by Mr. Jean-François Le Bihan, responsible for the coordination of the activities in Sub-Saharan Africa (HIPSSA Senior Project Coordinator), and Mr. Sandro Bazzanella, responsible for the management of the whole project covering Sub-Saharan Africa, Caribbean and the Pacific (ITU-EC-ACP Project Manager) with the overall support of Ms. Hiwot Mulugeta, HIPSSA Project Assistant, and of Ms. Silvia Villar, ITU-EC-ACP Project Assistant. The work was carried out under the overall direction of Mr. Cosmas Zavazava, Chief, Project Support and Knowledge Management (PKM) Department. The team at ITU's Publication Composition Service was responsible for its publication.

Table of Contents

Table of contents

Page

Part 1 :
INTRODUCTION

Part 1

Introduction

I. Introduction

1 The aim of the report

This report was put together to respond to the "Request for Collaboration on ICT Legal Texts" addressed to the ITU by Jean de Dieu Somda, Vice President, ECOWAS Commission (Dated 11 August 2009). ITU hopes that these comments can assist the ECOWAS Commission in its work to increase understanding on how countries in the region can go about criminalizing the misuse of ICTs in their national legislation and as a result help countries in the region hestablish a sound legal foundation. The comments are based on the recently released ITU Toolkit for Cybercrime Legislation and ITU publication on Understanding Cybercrime: A Guide for Developing Countries, and other relevant resources.

2 General Aspects

2.1 As the request did not call for specific input on certain aspects of the Draft Directive, the analysis focuses on general comments related to the content by comparing it to international standards as well as instruments provided by ITU[1] (especially the ITU Toolkit for Cybercrime Legislation[2] and the ITU publication Understanding Cybercrime: A Guide for Developing Countries). The analysis will – wherever possible – refer to the publication and other relevant background information on issues that can not be further discussed within the context of this analysis.

2.2 The analysis is based on the provided English version of the ECOWAS Draft Directive.[3]

2.3 With regard to the fact that a number of issues pointed out in the analysis refer to the interpretation of special terms used in the Draft Directive, a review of these questions with the help of local experts would be necessary.

2.4 The view of this report does not necessary reflect the official position of ITU.

3 The importance of an effective fight against cybercrime for developing countries

In 2005 the number of Internet users in developing countries surpassed the industrial nations for the first time[4] and although the development of new technology mainly focuses on the demands of consumers in western countries, developing countries do benefit from the new technology[5] and thus more citizens get access to the Internet.[6] The development of cheap hardware and wireless access could enable developing countries to connect people even in difficult territories with very little technical infrastructure.[7]

---

[1] The ITU Toolkit for Cybercrime Legislation and the publication Understanding Cybercrime: A Guide for Developing Countries can be downloaded at: http://www.itu.int/ITU-D/cyb/cybersecurity/legislation.html.

[2] The ITU Toolkit for Cybercrime Legislation has been released in May 2009 as part of ITU's dedicated cybercrime legislation resources

[3] See Appendix 2.

[4] See Development Gateway's Special Report, Information Society – Next Steps?, 2005 – available at: http://topics.developmentgateway.org/special/informationsociety.

[5] Regarding the possibilities and technology available to access the Internet in developing countries see: *Esteve/Machin*, Devices to access Internet in Developing countries, available at: http://www2007.org/workshops/paper_106.pdf.

[6] See Understanding Cybercrime: A Guide for Developing Countries, page: 15.

[7] An example for new technology in this area is Wimax - Worldwide Interoperability for Microwave Access -a standards-based wireless technology that provides broadband connections over long distances. Each WIMAX node could enable high-speed Internet connectivity in a radius of approximately up to 50 km. For more information see: The Wimax Forum – available at www.wimaxforum.org ; *Andrews, Ghosh, Rias*, Fundamentals of WiMax: Understanding Broadband Wireless Networking; *Nuaymi*, Wimax, Technology for Broadband Wireless Access

Taking into consideration the urgent fundamental demands of developing societies makes the participation in Internet communication appear less important – but it is very likely that in the near future the participation in the economic development of a globalised society, the access to the information technology and services will be of a great importance.[8]

For societies in developing countries this development comes with great opportunities. As examples from Eastern Europe show, the unfiltered access to information can support democracy as the flow of information is taken out of the control of state authorities.[9] But even in the everyday life of society, the technical developments brought along numerous improvements. In this context it is important to highlight that the development towards an information society is going along with serious threats for industrialised nations as well as developing countries.[10] By taking a closer look at the foundation of the western information societies it turns out that they are up to a large degree depending on the availability of the information technology.[11] Without proper functioning information technology essential services such as water and electricity supply would not work as they are based on information technology. A majority of services related to critical infrastructure is depending on the functioning of the information technology and as a result attacks against the information infrastructure and Internet services can harm the society in a critical way.[12] The approach undertaken to protect the critical infrastructure by the means of criminal law is therefore an important step towards securing the transition process.

4 Role of regional approaches in harmonising cybercrime legislation

Approaches undertaken by regional organisations such as ECOWAS are seen as an important instrument for harmonisation of cybercrime legislation.[13] The recent approaches within the European Union are one example of an effective and successful regional approach. With the EU Framework Decision on Attacks against Computer Systems and the EU Data Retention Directive, the European Union has undertaken two important steps to harmonise parts of the cybercrime legislation in all 27 EU member states.[14]

Compared to national approaches, regional approaches go along with the advantage of addressing the transnational dimension of cybercrime. The harmonisation of legal standards is widely identified as an important strategy to improve international investigations and avoid the creation of safe havens. [15] Such harmonisation certainly needs to go beyond the mandate of regional organisations.[16] As a consequence, regional approaches cannot substitute international approaches but they can add to them. This is especially relevant with regard to the fact that regional organisations in general have the possibility to

[8] Regarding the transition to information societies and the related consequences see: *Masuda*, The Information Society as Post-Industrial Society; *Dutta/De Meyer/Jain/Richter*, The Information Society in an Enlarged Europe; *Maldoom/Marsden/Sidak/Singer*, Broadband in Europe: How Brussels can wire the Information Society; Salzburg Center for International Legal Studies, Legal Issues in the Global Information Society; *Hornby/Clarke*, Challenge and Change in the Information Society.

[9] Regarding the impact of ICT on the development of the society see: *Barney*, Prometheus Wired;: The Hope for Democracy in the Age of Network Technology, 2001; *Yang*, Between Democracy and Development: The impact of new information technologies on civil societies in China, available at: http://programs.ssrc.org/itic/publications/civsocandgov/yangpolicyrevised.pdf; *White*, Citizen Electronic: Marx and Gilder on Information Technology and Democracy, Journal of Information Technology impact, 1999, Vol. 1, page 20, available at: http://www.jiti.com/v1n1/white.pdf.

[10] See *Sieber*, The Threat of Cybercrime, Organised crime in Europe: the threat of Cybercrime, page 212.

[11] See *Gercke*, Computer Law Review International, 2006, page 141 et seq..

[12] See *Wigert*, Varying policy responses to critical information infrastructure protection (CIIP) in selected countries, Cybercrime and Security, IIB-1, page 1.

[13] Regarding the relation between national, regional and international approaches see: *Gercke*, Computer Law Review International, 2008, page 7 et seq.

[14] *Gercke*, Europe's approaches to cybercrime, ERA-Forum 2009; Understanding Cybercrime: A Guide for Developing Countries, page 95 et seq.

[15] This issue was addressed by a number of international organisations. The UN General Assembly Resolution 55/63 points out: "States should ensure that their laws and practice eliminate safe havens for those who criminally misuse information technologies". The full text of the Resolution is available at: http://www.unodc.org/pdf/crime/a_res_55/res5563e.pdf. The G8 10 Point Action plan highlights: "There must be no safe havens for those who abuse information technologies". See below: Chapter 5.2.

[16] *Gercke*, Computer Law Review International, 2008, page 8.

pick up topics where an agreement can be reached within a region but not necessary globally.[17] An example is Art. 21 of the ECOWAS Draft Directive that criminalises the act of denying acts of genocide.18 A global approach to criminalise such acts is currently impossible as in some countries the denial of acts of genocide is covered by principles of freedom of speech.19 A harmonisation of legislation within a region cannot prevent that offenders are acting from safe heavens outside the jurisdiction of the regional organisations but at least ensure a consistent approach within the region.

[17] Understanding Cybercrime: A Guide for Developing Countries: page 111.

18 Article 21 (Intentionally denying, approving or justifying acts or crimes against humanity by means of a computer system) Any intentional act to deny, approve or justify acts of genocide or crimes against humanity by means of a computer system.

19 Regarding the principle of freedom of speech see: Understanding Cybercrime: A Guide for Developing Countries, page 29; Tedford/HerbeckHaiman, Freedom of Speech in the United States, 2005; Barendt, Freedom of Speech, 2007; Baker; Human Liberty and Freedom of Speech; Emord, Freedom, Technology and the First Amendment, 1991; Regarding the importance of the principle with regard to electronic surveillance see: Woo/So, The case for Magic Lantern: September 11 Highlights the need for increasing surveillance, Harvard Journal of Law & Technology, Vol 15, No. 2, 2002, page 530 et seqq; Vhesterman, Freedom of Speech in Australian Law; A Delicate Plant, 2000; Volokh, Freedom of Speech, Religious Harassment Law, and Religious Accommodation Law, Loyola University Chicago Law Journal, Vol. 33, 2001, page 57 et. seq., available at: http://www.law.ucla.edu/volokh/harass/religion.pdf; Cohen, Freedom of Speech and Press: Exceptions to the First Amendment, CRS Report for Congress 95-815, 2007, available at: http://www.fas.org/sgp/crs/misc/95-815.pdf.

Part 2 :
Summary and general remarks

II. Summary and general remarks

5 Executive summary

5.1 The Draft Directive is an important step in the fight against cybercrime within ECOWAS. It clearly shows that ECOWAS is well aware of the challenge of cybercrime.[20] In addition, the fact that the provisions are drafted with a clear focus on international standards[21] – as highlighted in the preamble[22] - demonstrates that the importance of international harmonisation has been recognised. In this context ECOWAS did not limit its approach to an improvement of the cooperation within ECOWAS. Instead, by aiming to bring its legislation in line with international standards it also went further with regard to the development of a foundation for international cooperation.[23] Taking into account the international dimension of cybercrime[24] the approach reflects the trend towards global harmonisation.

5.2 The Draft Directive contains three main areas of regulation: substantive criminal law, procedural law and judicial cooperation. With regard to the number of provisions the focus is on substantive criminal law. Experience shows that the harmonisation of substantive criminal law provisions is in general easier than the harmonisation of procedural law and international cooperation. As a consequence a number of recent approaches focus on substantive criminal law.

5.3 Despite the fact that the Draft Directive contains more than double as many provisions compared to the Budapest Convention, which is mentioned in the preamble, and the ITU Toolkit for Cybercrime Legislation, the areas of crime covered are those widely recognised as criminal offences, such as illegal access to a computer system and child pornography. The criminalisation of new phenomena, such as Identity Theft[25], which is currently intensively discussed[26] and was for example recommended by the Ad Hoc Forum Working Group on Legal Foundation and Enforcement during the ITU Regional Cybersecurity Forum for Eastern and Southern Africa, held in Zambia in 2008 were not included in the Draft Directive.[27]

The higher number of provisions in the Draft Directive is a result of a strategy to split up offences into different provisions. In other legal instruments, such as the Budapest Convention, many of these are combined in one provision. An example is Art. 9 Budapest Convention and Art. 14-17 Draft Directive which both deal with child pornography offences. Covering an area of crime by a set of provisions instead of a single one is a strategy that is similar to the one developed by the ITU Toolkit for Cybercrime Legislation.

5.4 The procedural instrument provided by the Draft Directive is solely related to search and seizure.[28] Widely recognised instruments such as expedited preservation of computer data[29], lawful real-time interception of content data[30] and real-time collection of traffic-data[31] that are contained in both the

[20] Regarding the challenges of fighting Cybercrime see: Understanding Cybercrime: A Guide for Developing Countries, page 63 et seq.

[21] See for example Art. 1 of the Draft Directive that refers to the relevant UN Convention.

[22] "RECALLING international initiatives relating to issues on repression of offences resulting from cyber criminality notably the Budapest Convention."

[23] Regarding the importance and practical application of international cooperation see: Understanding Cybercrime: A Guide for Developing Countries, page 208 et seq.

[24] Regarding the transnational dimension of cybercrime see: *Sofaer/Goodman*, "Cyber Crime and Security – The Transnational Dimension" in *Sofaer/Goodman*, "The Transnational Dimension of Cyber Crime and Terrorism", 2001, page 7, available at: http://media.hoover.org/documents/0817999825_1.pdf.

[25] Regarding the phenomenon of ID-Theft see: Understanding Cybercrime: A Guide for Developing Countries, page 48 et seq. and page 160 et seq.

[26] *Gercke*, Legal Approaches to Criminalize Idenity Theft, Commission on Crime Prevention and Criminal Justice, 18th session, 2009, E/CN.15/2009/CRP.13.

[27] Regarding the recommendation see: Document RFL/2008/WG02-E.

[28] See Art. 33 Draft Directive.

[29] See: Sec. 14 ITU Toolkit for Cybercrime Legislation; Regarding the importance of the instrument in Cybercrime investigations see: : Understanding Cybercrime: A Guide for Developing Countries, page 177 et seq.

[30] See: Sec. 20 ITU Toolkit for Cybercrime Legislation; Regarding the importance of the instrument in Cybercrime investigations see: : Understanding Cybercrime: A Guide for Developing Countries, page 195 et seq.

ITU Toolkit for Cybercrime Legislation and the Budapest Convention, have not been included in the Draft Directive. In addition, new instruments that are currently intensively discussed, such as data retention obligations[32] or new forensic techniques such as remote forensics and the use of keyloggers[33], have not been included in the Draft Directive. The consideration of such instruments was one of the recommendations of the Ad Hoc Forum Working Group on Legal Foundation and Enforcement during the ITU Regional Cybersecurity Forum for Eastern and Southern Africa in 2008 and have not been included in the Draft Directive.[34]

5.5 The regulation of judicial cooperation is limited to a single provision.[35] Taking into account the great challenges related to international cooperation in cybercrime cases[36] explains why both the ITU Toolkit for Cybercrime Legislation[37] as well as the Budapest Convention[38] contain a large set of provisions dealing with international cooperation. Both instruments for example contain practical advices related to carrying out international cooperation. Further regulation of judicial cooperation among the ECOWAS member states as well as international cooperation with non-members should therefore be taken into consideration.

5.6 The Draft Directive itself does not determine the sanctions. The general regulations developed by Art. 27 - 31 Draft Directive are in line with international standards.

5.7 Art. 22 contains a regulation enabling the aggravation of penalties. The fact that the ITU Toolkit for Cybercrime Legislation unlike the Budapest Convention contains several aggravation circumstances such as acts carried out with the intent to threaten pubic safety[39]. This is an indication of the growing demand by countries to enable a differentiation between minor and serious cybercrime offences. The circumstances mentioned in Art. 22 Draft Directive are less precisely described compared to the circumstances used as justification for aggravation of penalty in the ITU Toolkit for Cybercrime Legislation. Taking into account the possible consequences of an aggravation of penalty for the suspect a review of Art. 22 should be taken into consideration. Such review should include a debate if the fact that a traditional offence such as theft is committed using ICT justifies aggravated penalties.

6 General remarks

The following general remarks summarise some general observations made in the analysis and are therefore not mentioned in the analysis of each provision.

6.1 Fraudulent

Several provisions in the Draft Directive use the term “fraudulent”. In this context the approach is different from the ITU Toolkit on Cybercrime Legislation which uses the term “without authorisation” and the Budapest Convention that makes use of the term “without right[40]”. The different terminology could

[31] See: Sec. 19 ITU Toolkit for Cybercrime Legislation; Regarding the importance of the instrument in Cybercrime investigations see: : Understanding Cybercrime: A Guide for Developing Countries, page 194 et seq.

[32] Data retention describes the collection of certain data (such as traffic data) through obliged institutions e.g., Access Providers. See: Understanding Cybercrime: A Guide for Developing Countries, page 182 et seq.

[33] See: Understanding Cybercrime: A Guide for Developing Countries, page 204 et seq.

[34] Regarding the recommendation see: Document RFL/2008/WG02-E.

[35] See Art. 35 Draft Directive.

[36] See: Understanding Cybercrime: A Guide for Developing Countries, page 207 et seq.

[37] Sec. 23 – 33.

[38] Art. 23 - 35.

[39] See for example Sec. 4 c).

[40] The element “without right” is a common component in the substantive criminal law provisions of the Budapest Convention. The Explanatory Report notes that: “A specificity of the offences included is the express requirement that the conduct involved is done "without right". It reflects the insight that the conduct described is not always punishable per se, but may be legal or justified not only in cases where classical legal defences are applicable, like consent, self defence or necessity, but where other principles or interests lead to the exclusion of criminal liability. The expression ‘without right’ derives its meaning from the context in which it is used. Thus, without restricting how Parties may implement the concept in their domestic law, it may refer to conduct undertaken without authority (whether legislative, executive, administrative, judicial, contractual or consensual) or conduct that is otherwise not covered by

be a result of translation. If this is not the case a change of terminology could be considered. Depending on the interpretation of the term "fraudulent[41]" by national courts, the applicability of provisions in the Draft Directive could be limited compared to international standards. This due to the fact that the term "fraudulent" is in general more focused on gaining a financial benefit compared to "illegal", "without right" or "without authorisation". Based on the explanations given in the preamble – that are often focused on fraudulent activities[42] - it is uncertain if the drafters of the Directive intended to widely criminalise cybercrime offences even if they are not committed fraudulently but nevertheless "illegal" or "without authorisation". If a criminalisation similar to the ITU Toolkit for Cybercrime Legislation and the Budapest Convention is intended, a change is needed.

6.2 Mental element

Both, the ITU Toolkit for Cybercrime Legislation and the Budapest Convention only criminalise acts if the offender acted intentionally. While the requirements related to the mental element are therefore an essential element of the provisions provided by the ITU Toolkit for Cybercrime Legislation as well as the Budapest Convention most provisions in the Draft Directive do not contain requirements regarding the mental element. An exception is for example Art. 21 that criminalises the "intentional act to deny, approve or justify acts of genocide or crimes against humanity by means of a computer system". It is likely that based on general principles of criminal law within ECOWAS countries, the provisions mentioned in the Draft Directive are only applicable to intentional acts unless otherwise defined. The fact that Art. 11 includes a clarification related to negligence ("even through negligence"), supports this interpretation. Nevertheless a clarification should be considered as the mental element has an import function. It excludes unwanted criminalisation in those cases where the offender does not either know about or want to commit the crime. The need for a restriction of criminalisation by requiring an intentional acting should be taken into consideration.

6.3 Safeguards

Unlike the ITU Toolkit for Cybercrime Legislation43 and the Budapest Convention44, the Draft Directive does not contain a specific set of safeguards. Taking into account the possible impact of the application of procedural instruments, safeguards play an important role.45 Such safeguards are for example developed by Art. 13 ITU Toolkit for Cybercrime Legislation that especially contains the principle of proportionality.46 A similar approach can be found in Art. 15 Budapest Convention. The provision requires that the procedural instruments are "subject to conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties, including rights arising pursuant to obligations it has undertaken under the 1950 Council of Europe Convention for

established legal defences, excuses, justifications or relevant principles under domestic law. The Convention, therefore, leaves unaffected conduct undertaken pursuant to lawful government authority (for example, where the Party's government acts to maintain public order, protect national security or investigate criminal offences). Furthermore, legitimate and common activities inherent in the design of networks, or legitimate and common operating or commercial practices should not be criminalised". See Explanatory Report to the Council of Europe Convention on Cybercrime, No. 38.

[41] Regarding the interpretation of the term „fraudulent"in Art. 8 Budapest Convention see: Understanding Cybercrime: A Guide for Developing Countries, page 165.

[42] „OBSERVING that the use of information and communication technologies, among others the internet or cybernetics, has generated an upsurge in fraudulent acts of various types; [...] CONSCIOUS that this concrete acts of fraudulence committed by means of internet require an identification of a legal plan and a suitable repression because of the level of damage they generate;"

[43] See Sec. 13.

[44] See Art. 15

[45] Understanding Cybercrime: A Guide for Developing Countries, page 273 et seq.

[46] „The procedural provisions set forth in Title 3 of this Law shall be conducted in compliance with the principal of proportionality, which shall be abided by in all criminal investigation activities performed by competent law enforcement bodies whenever evidence is to be gathered on and/or by means of electronic tools. Such criminal investigation activities include, but are not limited to, inspections, searches, seizure, custody, urgent inquiries, and searches for evidence. The impact of these procedural powers upon the rights, responsibilities, and legitimate interests of third parties alien to the facts investigated shall be considered when conducting such investigative activities."

the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights, and other applicable international human rights instruments, and which shall incorporate the principle of proportionality". Taking into account that the drafters of the Draft Directive incorporated the principle of proportionality with regard to one single aspect of the procedural instrument in Art. 33 ("However, where seizure of the electronic medium is undesirable, the data required to understand it shall be copied on a computer data storage medium and sealed") shows that the principle was reflected. To ensure that the highest standards have been implemented, further analysis undertaken with the support of national experts could be considered.

6.4 Attempt

Art. 2 – 7 criminalise an attempt to commit a crime in addition to committing the crime. Depending on the legal tradition within ECOWAS countries, a single provision defining that an attempt to commit one of the crimes in Art. 2 – 7 is criminalised could be an option to including the attempt in each of the provision.[47]

[47] See in this context for example Sec. 10 ITU Toolkit for Cybercrime Legislation.

Part 3 :
Specific remarks with regard to selected provisions of the Draft Directive and general remarks

Part 3

III. Specific remarks with regard to selected provisions of the Draft Directive

7 Art. 1 – Definition

Article 1: Definitions, Objective and Scope

Definitions

For the purposes of this Supplementary Act:

Electronic communication means making available to the public or a section of the public through a process of electronic or electromagnetic communication, signs, signals, written documents, images, sounds or messages of any kind;

Computerized data: any representation of facts, information or concepts in a form suitable for processing in a computer system;

Racism and xenophobia in relation to ICTs refer to any document, image or any other depiction of ideas or theories, which advocates or encourages hatred, discrimination or violence against a person or group of persons by reason of their race, colour, ancestry or their national or ethnic origin or religion, to the extent that this reason serves as a pretext for one or the other of such elements or incites to such acts;

Minor: any person under the age of 18 as stipulated in the United Nations Convention on the Rights of the Child;

Child pornography: any data of whatever nature or form, that visually depicts a minor engaged in a sexually explicit conduct or realistic images representing a minor engaged in a sexually explicit conduct;

Computer system: any isolated or non-isolated device or group of interconnected devices that all or in part carry out automatic processing of data pursuant to a programme.

Objective and Scope

The objective of this Directive is to adapt the substantive penal law and the criminal procedure of ECOWAS Member States to the cybercrime phenomenon.

It shall be applicable to all cyber crime-related offences within the ECOWAS sub-region.

7.1 Art. 1, subparagraph 1 Draft Directive contains a set of definitions.

The terms “computerized data” and “computer system” are defined by referring to Art. 1 Budapest Convention. Section 1 c) and b). ITU Toolkit for Cybercrime Legislation contains more complex definitions for both terms. Such more complex approach could be useful to avoid misinterpretations. Solely based on the definition in Art.1 Draft Directive / Art. 1 Budapest Convention, it is for example uncertain if the term computer systems covers storage devices as those devices do not process data pursuant to a program but store them. The explanatory report to the Budapest Convention points outthat storage devices shall be included in the definition.[48] In this regard the more complex definition provided by the ITU Toolkit for Cybercrime Legislation requires less interpretation as storage functions are already mentioned in the text itself.[49]

[48] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 23.
[49] See Section 1 c) and b) ITU Toolkit for Cybercrime Legislation.

7.3 The term "racism and xenophobic material" is defined in accordance with Art. 2, paragraph 1 of the Additional Protocol to the Budapest Convention.[50] The ITU Toolkit for Cybercrime Legislation does not provide sample language for hate speech offences and therefore does not contain such definition.

7.4 The term "child pornography" is based on Art. 9, paragraph 2 a) and c) of the Budapest Convention.[51] Fictional child pornography[52] ("virtual child pornography") as defined by Art. 9, paragraph 2 b) Budapest Convention was not included in the Draft Directive. The ITU Toolkit for Cybercrime Legislation intentionally does not provide sample language for child pornography offences and therefore does not contain such definition.[53]

7.5 As pointed out by the Draft Directive the term minor was defined in accordance with Art.1 UN Convention on the Rights of the Child.[54]

7.6 A definition of the term electronic communication is neither contained in the ITU Toolkit for Cybercrime Legislation, nor in the Budapest Convention. The definition narrows electronic communication to an interaction with the public or part of the public. This excludes non-public individual communication such as VoIP or E-Mail communication.[55] As the term "electronic communication" is only used in Art. 31 with regard to supplementary sanctions it is uncertain if the intensive restriction of the term was intended. A review should be taken into consideration.

8 Art. 2 – Fraudulent access to computer systems

8.1 Illegal access is one of the traditional computer crimes.[56] Ever since computer networks were developed, their ability to connect computers and offer users access to other computer systems have been abused for criminal purposes.[57] The motivation of the offenders vary. Within the scope of recognised offences, wide ranges of perpetrator's motivations have been discovered. [58] Very often the offenders are accessing computer systems and networks to obtain stored information. If the target computer is protected against unauthorised access, the offender needs to circumvent the protection measures securing the network.[59] Very often security systems protecting physical location of the IT

> Article 2: Fraudulent access to computer systems
>
> The act by which a person fraudulently accesses or attempts to access the whole or part of a computer system.

[50] Addition Protocol on cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems. ETS No. 189. Regarding the development of the Additional Protocol see: Understanding Cybercrime: A Guide for Developing Countries, page 97.

[51] Regarding the definition see: Understanding Cybercrime: A Guide for Developing Countries, page 134 et seq.

[52] Regarding the criminalisation of fictional images see: Understanding Cybercrime: A Guide for Developing Countries, page 136.

[53] Regarding the intention of the drafters to exclude child pornography see: ITU Toolkit for Cybercrime Legislation, page 32.

[54] UN Convention on the Protection of the Child**,** Document A/RES/44/25, 12 December 1989.

[55] Regarding the importance of protecting individual communication see: Understanding Cybercrime: A Guide for Developing Countries, page 25.

[56] Understanding Cybercrime: A Guide for Developing Countries, page 20.

[57] *Sieber*, Multimedia Handbook, Chapter 19, page 17. For an overview of victims of early hacking attacks see: http://en.wikipedia.org/wiki/Timeline_of_computer_security_hacker_history; *Joyner/Lotrionte*, Information Warfare as International Coercion: Elements of a Legal Framework, EJIL 2002, No5 – page 825 et sqq.

[58] They are ranging from the simple proof that technical protection measures can be circumvented, to the intention of obtaining data stored on the victimised computer. Even political motivations were discovered. See: *Anderson*, Hacktivism and Politically Motivated Computer Crime, 2005 – available at: http://www.aracnet.com/~kea/Papers/Politically%20Motivated%20Computer%20Crime.pdf;

59 These can for example be passwords or fingerprint authorisation. In addition there are several tools available that can be used to circumvent protection measures. For an overview about the tools used see *Ealy*, A New Evolution in Hack

infrastructure are much more sophisticated than the security systems protecting sensitive information on networks, even within the same building.[60] This makes it easier for the offender to remotely access the computer system than access the building.

There are legal approaches to criminalise activities related to illegal access.[61] Some countries criminalise the mere access to a computer system, while others limit the criminalisation by prosecuting these offences only in cases where the accessed system is protected by security measures, or where the perpetrator has harmful intentions, or where data was obtained, modified or damaged. Others legal systems do not criminalise mere access, but only subsequent offences.[62]

8.2 Art. 2 Draft Directive criminalises the fraudulent access to computer systems. The provision was drafted similar to Art. 2 Budapest Convention.[63] Sec. 2 b) ITU Toolkit for Cybercrime Legislation provides a modified and more complex provision.

8.3 Regarding the use of the term "fraudulent" instead of "illegal" or "without authorisation" see above: Chapter 6.1.

8.4 Regarding the fact that the provision does not explicitly define the requirements with regard to the mental element see above: Chapter 6.2.

8.5. Art. 2 Draft Directive incorporates a criminalisation of attempts to access computer systems. This approach is in line with Sec. 9 ITU Toolkit for Cybercrime Legislation and Art. 11 Budapest Convention.

9 Art. 3 – Fraudulently remaining in a computer systems

Article 3: Fraudulently remaining in a computer system

> The act by which a person fraudulently remains or attempts to remain within the whole or part of a computer system.

9.1 Art. 3 Draft Directive criminalises the act of fraudulently remaining in a computer system as well as the attempt to such act.

9.2 Such offence can neither be found in ITU Toolkit for Cybercrime Legislation, nor in the Budapest Convention. As those only provide sample language (ITU Toolkit for Cybercrime Legislation) or minimum standards (Budapest Convention) there is in general no concern related to creation of new offences.

Attacks: A General Overview of Types, Methods, Tools, and Prevention – available at: http://www.212cafe.com/download/e-book/A.pdf.

[60] Regarding the supportive aspects of missing technical protection measures see *Wilson*, Computer Attacks and Cyber Terrorism, Cybercrime & Security, IIV-3, page 5. The importance of implementing effective security measures to prevent illegal access is as well highlighted by the drafters of the Convention on Cybercrime. See: Explanatory Report to the Council of Europe Convention on Cybercrime, No. 45.

[61] Understanding Cybercrime: A Guide for Developing Countries, page 113 et seq.

[62] An example for this is the German Criminal Code that criminalised only the act of obtaining data (Section 202a). The provision was changed in 2007. The following text is the old version:

Section 202a - Data Espionage

(1) Whoever, without authorization, obtains data for himself or another, which was not intended for him and was specially protected against unauthorized access, shall be punished with imprisonment for not more than three years or a fine.

(2) Within the meaning of subsection (1), data shall only be those which stored or transmitted electronically or magnetically or otherwise in a not immediately perceivable manner.

[63] Regarding the interpretation of the provision see: Understanding Cybercrime: A Guide for Developing Countries, page 114.

9.3 With regard to the specific approach of Art. 3, a couple of questions remain that could be discussed with the help of regional experts to avoid difficulties with regard to the application of the provision.

- What is the protected legal interest?[64]
- Does the provision intend to close gaps or will it mandatorily go along with other offences (e.g. Art. 2 Draft Directive). If there are no cases, where Art. 3 can be committed without prior committing Art. 2 this leads to the question if Art. 3 is a separate offence or shall only enable an aggravation of penalty.
- How can the act of remaining be further defined? Does it require certain activities or would it be sufficient to stay logged on without carrying out any operations. Is acertain duration of remaining in a system necessary? If not every act of illegal access will at the same time very likely be covered by Art. 3 Draft Directive: If the offender successfully enters the system he at the same time starts to remain in the system or at least attempts to remain there.

9.4 Regarding the use of the term "fraudulent" instead of "illegal" or "without authorisation" see above: Chapter 6.1.

9.5 Regarding the fact that the provision does not explicitly define the requirements with regard to the mental element see above: Chapter 6.2.

10 Art. 4 – Interfering with the operation of a computer system

Article 4: Interfering with the operation of a computer system

The act by which a person impedes, alters or attempts to impede or alter the functioning of a computer system.

10.1 Art. 4 Draft Directive criminalises the hindering of computer systems.

10.2 Computer operations do in general require access to the relevant data and software as well as proper hardware.[65] More and more businesses are running either Internet Services or at least incorporate Internet Services in their production services. If the offenders successfully hinder the computer systems from operating this can lead to great financial losses for the victims.[66]

An attack can be carried out by a physical impact on the computer system.[67] If the offenders are able to get access to the computer system they can easily destroy the damageable hardware. For most criminal law systems these cases are not a major challenge as they are very close to the classic cases of damage of property. Difficulties might only arise with regard to the fact that especially when it comes to attacks against computer systems from highly profitable e-commerce businesses, the financial damage caused by destroying the computer system is likely to be much higher than the price of the affected computer hardware. More challenging for the legal systems are current scams of web-based attacks. Examples of attacks against computer systems that do not require the presence of the offender at the location of computer system are "Computer Worms"[68] and "Denial-of-Service Attacks"[69]. People or businesses that

[64] Very likely it is the integrity of the computer system.
[65] Understanding Cybercrime: A Guide for Developing Countries, page 28.
[66] Regarding the possible financial consequences see: *Campbell/Gordon/Loeb/Zhou*, The Economic Cost of Publicly Announced Information Security Breaches: Empirical Evidence From the Stock Market, Journal of Computer Security, Vol. 11, page 431-448.
[67] Examples are: Inserting metal objects in computer devices to cause electrical shorts, blowing hair spray into sensitive devices, cutting cables. For more examples see *Sieber*, Council of Europe Organised Crime Report 2004, page 107.
[68] *Sieber*, Council of Europe Organised Crime Report 2004, page 107.
[69] A Denial-of-Service (DoS) attacks aims to make a computer system unavailable by saturating it with external communications requests, such that it cannot respond to legitimate traffic. For more information see: US-CERT, Understanding Denial-of-Service Attacks, available at: http://www.us-cert.gov/cas/tips/ST04-015.html; *Paxson*, An

offer services based on computer technology depend on the functioning of their computer systems. The temporary unavailability of famous web pages that were victims of so called "Denial-of-Service (DOS) Attacks" shows how serious the threat of attacks is.[70] Attacks like these can cause serious financial losses for the companies involved.

10.3 Art. 4 Draft Law does not require that the act is committed "fraudulent", "illegal" or "without authorisation". This leads to concern that the provision could even cover legal acts such as the work of system administrators and computer technicians whose work could lead to a temporary hindering of the operation of a computer system.

The ITU Toolkit for Cybercrime Legislation contains a similar provision that is more restricted as it requires that the act is committed without authorization or in excess of authorization or by infringement of security measures.[71] Furthermore it is limited to acts that lead to a disruption as defined by Sec. 1 (j) ITU Toolkit on Cybercrime Legislation. The Budapest Convention contains an approach that limits the criminalisation to certain acts ("by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data") that are carried out intentionally and lead to serious consequences. The limitation to certain acts excludes physical damages to a computer system. Taking into account that the Budapest Convention only defines minimum there is no need to limit the criminalisation to the text of the Budapest Convention but a clarification related to the mental element as well as the consequences, as suggested by both the ITU Toolkit for Cybercrime Legislation as well as the Budapest Convention should be taken into consideration.

10.4 Regarding the use of the term "fraudulent" instead of "illegal" or "without authorisation" see above: Chapter 6.1.

10.5 Regarding the fact that the provision does not explicitly define the requirements with regard to the mental element see above: Chapter 6.2.

11 Art. 5 – Fraudulent input of data in a computer system

Article 5: Fraudulent input of data in a computer system

The act by which a person fraudulently inputs or attempts to input data into a computer system.

11.1 Art. 5 Draft Directive criminalises the fraudulent input of data in a computer system.

11.2 Such offence can at least in the specific form neither be found in ITU Toolkit for Cybercrime Legislation, nor in the Budapest Convention. Sec. 4 a) – c) in combination with Sec. 1 (l) ITU Toolkit for Cybercrime Legislation criminalises – among others – the authorised input of computer data that causes interference or disruption of a computer system. Art. 5 Budapest Convention contains a similar approach.

11.3 Art. 5 Draft Directive differs from those approaches at it does require that the input of data causes an interference or disruption. As both above mentioned approaches only provide sample language (ITU Toolkit for Cybercrime Legislation) or minimum standards (Budapest Convention) there is in general no concern related to creation of new offences. But with regard to the specific approach of Art. 5 a couple of questions remain, that could be discussed with the help of regional experts to avoid difficulties with regard to the application of the provision.

Analysis of Using Reflectors for Distributed Denial-of-Service Attacks – available at: http://www.icir.org/vern/papers/reflectors.CCR.01/reflectors.html; *Schuba/Krsul/Kuhn/Spafford/Sundaram/Zamboni*, Analysis of a Denial of Service Attack on TCP; Houle/Weaver, Trends in Denial of Service Attack Technology, 2001 – available at: http://www.cert.org/archive/pdf/DoS_trends.pdf.

[70] In 2004 the web-services of the German Airline Lufthansa was affected by such a DOS-attack. As a result the use of the online booking-service was not or only with delay available for the period of 2 hours.

[71] See Sec. 4a) ITU Toolkit for Cybercrime Legislation.

- What is the protected legal interest?
- Why does the provision not include inputting files on part of a computer system but only on computer systems itself?
- Is it necessary that the act (inputting) leads to consequences regarding the computer system (e.g. denial of service attack[72]) or data (alteration of the existing data by inputting data).

11.4 Regarding the fact that the provision does not explicitly define the requirements with regard to the mental element see above: Chapter 6.2.

12 Art. 6 – Fraudulent interception of computer data

Article 6: Fraudulent interception of computer data

The act by which a person fraudulently intercepts or attempts to intercept computerised data during their non-public transmission to, from or within a computer system through technical means.

12.1 Art. 6 Draft Directive criminalises the interception of computer data as well the attempt to intercept computer data.

12.2 Data cannot only be obtained while they are stored on a computer system.[73] Offenders can intercept the communication between users and record the information they exchange.[74] The interception of data transfer processes does not only allow the offenders to record data that are exchanged between two users (e.g. e-mails) – the offenders can also intercept the data transferred when one user uploads data on a web-server or accesses a web-based external storage media.[75] They can target any communication infrastructure (fixed lines, wireless) and any Internet service (e.g. e-mail, chat, voice-over-IP communication).[76] Examples for the interception of data exchange[77] are the interception of communication performed via wireless networks (Wifi / Wireless LAN)[78] and the intercepting Voice-over-IP[79] conversations.

[72] A Denial-of-Service (DoS) attacks aims to make a computer system unavailable by saturating it with external communications requests, so it cannot respond to legitimate traffic. For more information, see: US-CERT, "Understanding Denial-of-Service Attacks", available at: http://www.us-cert.gov/cas/tips/ST04-015.html; *Paxson*, "An Analysis of Using Reflectors for Distributed Denial-of-Service Attacks", available at: http://www.icir.org/vern/papers/reflectors.CCR.01/reflectors.html.

[73] Understanding Cybercrime: A Guide for Developing Countries, page 25.

[74] *Leprevost*, Encryption and cryptosystems in electronic surveillance: a survey of the technology assessment issues, Development of surveillance technology and risk of abuse of economic information, 2.4 – available at: http://cryptome.org/stoa-r3-5.htm.

[75] With the dropping prices of server storage space the external storage of information becomes more and more popular. Another advantage of the external storage is the fact that information can be accessed from every Internet connection.

[76] With regard to the fact that it is in general much more difficult to intercept phone conversations made using the classic land lines it is important to highlight, that more and more telecommunication companies do switch to IP-Technology.

[77] For more information about the modus operandi see *Sieber*, Council of Europe Organised Crime Report 2004, page 97 et seqq.

[78] *Sieber*, Council of Europe Organised Crime Report 2004, page 99; Regarding the difficulties in Cybercrime investigations that include wireless networks see *Kang*, Wireless Network Security – Yet another hurdle in fighting Cybercrime.

[79] Regarding the interception of VoIP to assist law enforcement agencies see *Bellovin and others*, Security Implications of Applying the Communications Assistance to Law Enforcement Act to Voice over IP – available at http://www.itaa.org/news/docs/CALEAVOIPreport.pdf; Simon/Slay, Voice over IP: Forensic Computing Implications, 2006 - available at: http://scissec.scis.ecu.edu.au/wordpress/conference_proceedings/2006/forensics/Simon%20Slay%20-%20Voice%20over%20IP-%20Forensic%20Computing%20Implications.pdf.

12.3 Art. 6 Draft Directive is based on Art. 3 Budapest Convention. Sec. 5 ITU Toolkit for Cybercrime Legislation contains a similar approach.

12.4 Regarding the use of the term "fraudulent" instead of "illegal" or "without authorisation" see above: Chapter 6.1.

12.5 Regarding the fact that the provision does not explicitly define the requirements with regard to the mental element see above: Chapter 6.2.

13 Art. 7 - Fraudulent modification of computer data

Article 7: Fraudulent modification of computer data

The act by which a person fraudulently damages or attempts to damage, delete or attempts to delete, deteriorate or attempting to deteriorate, alter or attempts to alter, modify or attempt to modify computer data.

13.2 Computer data are vital for private users, businesses and administrations, all of which depend on the integrity and availability of data.[80] Lack of access to data can result in considerable (financial) damage. Offenders can violate the integrity of data and interfere with them by deleting, altering or suppressing them. One of the most common examples of the deletion of data is the computer virus.[81] Ever since computer technology was first developed, computer viruses have threatened users who failed to install proper protection.[82] Since then, the number of computer viruses has risen significantly.[83] The computer worm SQL Slammer[84] was estimated to have infected 90 percent of vulnerable computer systems within the first 10 minutes of its distribution.[85] The financial damage caused by virus attacks in 2000 alone was estimated to amount to some 17 billion USD.[86] In 2003 it was still more than 12 billion USD.[87]

13.3 Apart from the missing criminalisation of the suppression of computer data Art. 7 Draft Directive is following a similar approach as defined by Art. 4 Budapest Convention. Sec. 4 b) ITU Toolkit for Cybercrime Legislation contains a similar approach.

13.4 Regarding the use of the term "fraudulent" instead of "illegal" or "without authorisation" see above: Chapter 6.1.

13.5 Regarding the fact that the provision does not explicitly define the requirements with regard to the mental element see above: Chapter 6.2.

---

[80] See in this context as well: ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 32, available at: http://www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

[81] A computer virus is software that is able to replicate itself and infect a computer, without the permission of the user to harm the computer system. See *Spafford*, "The Internet Worm Program: An Analysis", page 3; *Cohen*, "Computer Viruses - Theory and Experiments", available at: http://all.net/books/virus/index.html. *Cohen*, "Computer Viruses"; *Adleman*, "An Abstract Theory of Computer Viruses". Regarding the economic impact of computer viruses, see *Cashell/Jackson/Jickling/Webel*, "The Economic Impact of Cyber-Attacks", page 12; Symantec "Internet Security Threat Report", Trends for July-December 2006, available at: http://eval.symantec.com/mktginfo/enterprise/white_papers/ent-whitepaper_internet_security_threat_report_xi_03_2007.en-us.pdf

[82] One of the first computer virus was called (c)Brain and was created by *Basit* and *Amjad Farooq Alvi*. For further details, see: http://en.wikipedia.org/wiki/Computer_virus.

[83] *White/Kephart/Chess*, Computer Viruses: A Global Perspective, available at: http://www.research.ibm.com/antivirus/SciPapers/White/VB95/vb95.distrib.html.

[84] See BBC News, "Virus-like attack hits web traffic", 25.01.2003, http://news.bbc.co.uk/2/hi/technology/2693925.stm;

[85] Critical Infrastructure Protection Department Of Homeland Security Faces Challenges In Fulfilling Cybersecurity Responsibilities, GAO, 2005 GAO-05-434, page 12, available at: http://www.gao.gov/new.items/d05434.pdf.

[86] *Cashell/Jackson/Jickling/Webel*, "The Economic Impact of Cyber-Attacks", page 12, available at: http://www.cisco.com/warp/public/779/govtaffairs/images/CRS_Cyber_Attacks.pdf.

[87] *Cashell/Jackson/Jickling/Webel*, "The Economic Impact of Cyber-Attacks", page 12, available at: http://www.cisco.com/warp/public/779/govtaffairs/images/CRS_Cyber_Attacks.pdf.

14 Art. 8 - Fraudulent production of computer data

Article 8: Fraudulent production of computer data

The act by which a person produces or manufactures a set of digital data through fraudulent input, deletion or suppression of computerized data stored, processed or transmitted by a computer system, resulting in counterfeit data, with the intent that it be considered or used for legal purposes as if it were genuine.

14.2 Ever since classic documents were used to prove legal relations those documents were forged. The falsification of passports and official documents are just two examples. Computer related forgery describes the manipulation of digital documents. In the past, criminal proceedings involving computer-related forgery were rare because most documents with legal relevance were tangible documents. With the ongoing process of digitalisation this situation is changing. The development towards digital documents is supported by the creation of a legal background for their use – e.g. by legislation regarding digital signatures.

One of the most well known examples of computer related forgery is related to a scam called "phishing".[88] The term "phishing" describes an act that is carried out to make the victim disclose personal/secret information.[89] Very often the offenders are sending out e-mails that look like an e-mail from a legitimate financial institution used by the victim.[90] The e-mails are designed in a way that it is impossible or at least difficult for the victim to identify it as a falsified e-mail. In the e-mail the recipient is ordered to disclose certain secret information.

14.3 Apart from the missing criminalisation of the act of alteration Art. 8 Draft Directive is following a similar approach as defined by Art. 7 Budapest Convention. Sec. 7 ITU Toolkit for Cybercrime Legislation contains a similar approach.

14.4 Regarding the use of the term "fraudulent" instead of "illegal" or "without authorisation" see above: Chapter 6.1.

14.5 Regarding the fact that the provision does not explicitly define the requirements with regards to the mental element see above: Chapter 6.2.

15 Art. 9 - Use of fraudulently obtained data

Article 9: Use of fraudulently obtained data

The Member States shall undertake to adopt such legislative measures as may be necessary to establish as a criminal offence the act of knowingly using data thus obtained.

15.1 Art. 9 Draft Directive criminalises the use of fraudulently obtained data.

15.2 Such offence can at least in the specific form neither be found in ITU Toolkit for Cybercrime Legislation, nor in the Budapest Convention. The very broad criminalisation of of illegal use raises a number of questions that could be discussed with the help of regional experts to avoid difficulties with regard to the application of the provision.

[88] Regarding the phenomenon phishing see. *Dhamija/Tygar/Hearst*, Why Phishing Works – available at: http://people.seas.harvard.edu/~rachna/papers/why_phishing_works.pdf; Report on Phishing, A Report to the Minister of Public Safety and Emergency Preparedness Canada and the Attorney General of the United States, 2006 – available at: http://www.usdoj.gov/opa/report_on_phishing.pdf

[89] The term "phishing" originally described the use of emails to "phish" for passwords and financial data from a sea of Internet users. The use of "ph" linked to popular hacker naming conventions. See *Gercke*, CR, 2005, 606; *Ollmann*, The Phishing Guide Understanding & Preventing Phishing Attacks – available at: http://www.nextgenss.com/papers/NISR-WP-Phishing.pdf.

[90] With regard to this aspect the "phishing" scam shows a number of similarities to spam e-mails. It is therefore likely that those organised crime groups that are involved in spam are also involved in phishing scams as they have access to spam databases.

- Is the intention of the provision to criminalise "broker" that buy and sell illegally obtained information?
- When is the information used?[91]
- Is the provision only applicable to offenders other than the one who has obtained the information?
- Is there a specific reason why this provision – unlike the others – is introduced with "Member States shall undertake to adopt such legislative measures"

15.4 Regarding the use of the term "fraudulent" instead of "illegal" or "without authorisation" see above: Chapter 6.1.

15.5 Regarding the fact that the provision does not explicitly define the requirements with regard to the mental element see above: Chapter 6.2.

Article 10: Fraudulently obtaining any benefit whatsoever

The act by which a person fraudulently obtains any benefit for oneself or for another person through the input, alteration, deletion or suppression of computerized data or through any other form of interference with the functioning of a computer system.

16 Art. 10 - Fraudulently obtaining any benefit whatsoever

16.1 Art. 10 Draft Directive criminalises the act of fraudulently obtaining any benefit.

16.2 Computer-related fraud is still among the most popular crimes in the Internet.[92] Especially the success of Online Shopping and Internet Auctions increased the opportunities of offenders. Apart from that the possibilities connected to automation are causing great difficulties as the automation enables the offenders to make great profit with a number of rather small acts. [93] If they succeed to keep the loss of each victim below a certain limit there is good chance that due to the time and energy they would need to invest to start an investigation these crimes are not reported by the victim. One example for such scam is the "Nigeria Advanced Fee Fraud".[94] Another common fraud scam is the "Auction Fraud[95]". Apart from that the development of assets administered in computer systems (electronic funds, deposit money, e-gold) has become the target of manipulations similar to traditional forms of property. To avoid these criminal acts especially with regard to Internet Auctions a number of confidence-building measures have been taken on the technical side.[96] But the missing personal contact between the seller and customer limits the possibilities of possible victims for a self-protection.

[91] Very likely it is an act following the act of obtaining the information as this is a requirement established by Art. 9

[92] In 2006 the US Federal Trade Commission received nearly 205.000 internet-related fraud complains. See Consumer Fraud and Identity Theft Complain Data – January – December 2006, Federal Trade Commission – available at: http://www.consumer.gov/sentinel/pubs/Top10Fraud2006.pdf.

[93] In 2006 Nearly 50% of all fraud complains reported to the US Federal Trade Commission are related to a amount paid between 0 and 25 US Dollar. See Consumer Fraud and Identity Theft Complain Data – January – December 2006, Federal Trade Commission – available at: http://www.consumer.gov/sentinel/pubs/Top10Fraud2006.pdf.

[94] The term advance fee fraud describes an offence in which the offender is trying to convince the victim to advance a small sum of money in the hope of receiving a much larger sum afterwards. For more information see: *Reich*, Advance Fee Fraud Scams in-country and across borders, Cybercrime & Security, IF-1, page 1; *Smith/Holmes/Kaufmann*, Nigerian Advance Fee Fraud, Trends & Issues in Crime and Criminal Justice, No. 121 – available at: http://www.aic.gov.au/publications/tandi/ti121.pdf; *Oriola*, Advance fee fraud on the Internet: Nigeria's regulatory response, Computer Law & Security Report, Volume 21, Issue 3, 237.

[95] The term auction fraud describes fraudulent activities involving electronic auction platforms in the Internet.

[96] An example for this is the service offered by PAYPAL: PAYPAL is an internet business that is enabling the user to transfer money, avoiding traditional paper methods such as money orders. It also performs payment processing for auction sites.

16.3 The provision shows similarities to Art. 8 Budapest Convention and Sec. 8 ITU Toolkit for Cybercrime Legislation but significant differences remain. The most important differences are related to the dogmatic structure of the offence. Like most national approaches Art. 8 Budapest Convention contains four main elements:[97]

- Definition of the act (input, input, alteration, deletion or suppression of computer data or any interference with the functioning of a computer system)
- Economic loss as a consequence of the act
- General Intent
- Specific fraudulent or dishonest intent to gain economic or other benefits for oneself or another

Apart from similarities within the definition of the act, Art. 10 Draft Directive follows a different structure:

- Definition of the act (input, alteration, deletion or suppression of computerized data or through any other form of interference with the functioning of a computer system)
- Obtaining a benefit for the offender or for another person (instead of an economic loss for another person)

16.4 As the structure of the offence varies significantly from Art. 8 Budapest Convention and Sec. 8 ITU Toolkit for Cybercrime Legislation a review should be taken into consideration. The review should especially focus on the mental element. Regarding the fact that most of the provision do not explicitly define the requirements with regard to the mental element see above: Chapter 6.2.

17 Art. 11 - Fraudulent manipulation of personal data

Article 11: Fraudulent manipulation of personal data

The act by which a person, even through negligence, processes, personal data or causes personal data to be processed without having complied with the prerequisite conditions stipulated by the relevant law on personal data provided for in each Member Stateof a computer system.

17.1 Art. 11 Draft Directive criminalises the acts of data manipulation. The reference to the relevant laws on personal data links the offences to data protection violations.

17.2 Neither the ITU Toolkit for Cybercrime Legislation, nor in the Budapest Convention contains such an offence. One of the main reasons for an exclusion of such broad criminalisation of data protection violations is the fact that it in general needs to be based on a solid data protection legislation that is not necessarily in place in all countries. As indicated in the request from ECOWAS[98] the situation is different as legislation on data protection was recently developed for all ECOWAS countries.

17.3 One issue that could be taken into consideration within a review of Art. 11 is the fact that – very likely unlike all other offences developed by the Draft Directive - the provision currently even criminalises the negligence procession of personal data.

18 Art. 12 - Obtaining equipment to commit an offence

[97] Understanding Cybercrime: A Guide for Developing Countries, page 165 et seq.
[98] See Annex 1.

Article 12: Obtaining equipment to commit an offence

The act by which a person produces, sells, imports, possesses, distributes, offers, transfers or makes available equipment, a computer programme, or any device or data designed or specially adapted for committing an offence, or any password, access code or similar computer data by which the whole or any part of a computer system can be accessed.

18.1 Art. 12 Draft Directive criminalises interaction with illegal devices.

18.2 The availability of tools designed to carry out sophisticated cybercrime has become a serious challenge in the fight against cybercrime.[99] Most of these devices are available on a large scale. The majority, distributed for free, are easy to operate and can therefore even be run by users without any specific technical knowledge. Apart from the proliferation of "hacking devices", the exchange of passwords that enable the unauthorised user to access a computer system can be seen as a challenge in the fight against Cybercrime. Once published a single password can grant access to restricted information to hundreds of users instead of only one. With regard to the potential threat of these devices it seems to be necessary to discuss if it is necessary to criminalise the distribution of such tools in addition to the criminalisation of the use of tools to commit crimes. Very often the national criminal law systems do criminalise the "attempt of an offence" or in addition at least contain some provision related to the criminalisation of preparatory acts. An approach to fight against the distribution of such devices is the criminalisation of the production of the tools used. In general this criminalisation goes along with an extensive forward displacement of criminal liability. It is therefore often limited to the most serious crimes. Especially in the legislation of the European Union there are tendencies to extend the criminalisation for preparatory acts to less grave offences. [100]

18.3 Art. 12 Draft Directive was drafted similar to the requirements of Art. 6 Budapest Convention and the solution provided by Sec. 6 b) and c) ITU Toolkit for Cybercrime Legislation. The main difference to the Budapest Convention and the ITU Toolkit for Cybercrime Legislation is the fact that the Draft Directive does not include the requirement of a special intent that the tool shall be used for the purpose of committing any of the offences. The missing requirements with regard to the mental element could lead to difficulties in the application of the provision as the mental element plays an important role in avoiding an over-criminalisation regarding the possession of illegal devices. In Art. 5 Budapest Convention the criminalisation of the possession of these devices is limited by the requirement of an intent to use the device to commit a crime as set out in Articles 2 to 5 of the Convention.[101] The Explanatory Report points out that this special intent was included to "avoid the danger of over-criminalisation where devices are produced and put on the market for legitimate purposes, e.g. to counter attacks against computer systems".[102] Within the ITU Toolkit for Cybercrime Legislation the special intent has a similar function. Taking into account the importance of the mental element a review of the provision should be taken into consideration. Regarding the fact that most of the provision do not explicitly define the requirements with regard to the mental element see above: Chapter 6.2.

19 Art. 14 - Production of child pornography

Article 14: Production of child pornography or pornographic representation

The act by which a person produces, records, offers or makes available, distributes or transmits child pornography or pornographic representation through a computer system.

Sieber, Council of Europe Organised Crime Report 2004, page 143.

[100] An example is the EU Framework Decision ABl. EG Nr. L 149, 2.6.2001.

[101] *Gercke*, Cybercrime Training for Judges, 2009, page 39, available at: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079%20if09%20pres%20coe%20train%20manual%20judges6%20_4%20march%2009_.pdf.

[102] Explanatory Report to the Council of Europe Convention on Cybercrime No 76: "Paragraph 2 sets out clearly that those tools created for the authorised testing or the protection of a computer system are not covered by the provision. This concept is already contained in the expression 'without right'. For example, test-devices ('cracking-devices') and network analysis devices designed by industry to control the reliability of their information technology products or to test system security are produced for legitimate purposes, and would be considered to be 'with right'."

19.1 Art. 14 Draft Directive criminalises the production of child pornography.

19.2 International organisations are engaged in the fight against online child pornography[103] with several international legal initiatives including: the 1989 United Nations Convention on the Rights of the Child[104]; the 2003 European Union Council Framework Decision on combating the sexual exploitation of children and child pornography[105]; and the 2007 Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse, the ITU Child Online Protection initiative, among others.[106]

Sadly, initiatives seeking to control the network distribution of pornography have proved little deterrent to perpetrators, who use the Internet to communicate and exchange child pornography.[107] The sale of child pornography remains highly profitable[108], with collectors willing to pay great amounts for movies and pictures depicting children in a sexual context.[109]

19.3 Art. 14 Draft Directive was drafted similar to the requirements of Art. 9, paragraph 1 a) – c) Budapest Convention. The ITU Toolkit for Cybercrime Legislation intentionally does not provide sample language for child pornography offences and therefore does not contain such definition.[110] As with regard to Art. 10 and Art. 12 Draft Directive the main difference is related to the mental element. Art. 14 requires that the covered acts are committed through a computer system. With regard to the act of "producing child pornography" such link to a "computer system" might limit the application of the provision in a way not intended by the drafters. To avoid such limitation, Art. 9, paragraph 1 a) Budapest Convention requires that child pornography is produced "through a computer system" but "for the purpose of its distribution through a computer system". A review of the provision should with regard to the production of child pornography therefore be taken into consideration.

Article 15: Import or export of child pornography or pornographic representation

The act by which a person procures for oneself or for another person, imports or causes to be imported, exports or causes to be exported, child pornography through a computer system.

20 Art. 15 - Import or export of child pornography

[103] See for example the "G8 Communique", Genoa Summit, 2001, available at: http://www.g8.gc.ca/genoa/july-22-01-1-e.asp.

[104] United Nations Convention on the Right of the Child, A/RES/44/25, available at: http://www.hrweb.org/legal/child.html. Regarding the importance for Cybercrime legislation see: ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 35, available at: http://www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

[105] Council Framework Decision on combating the sexual exploitation of children and child pornography, 2004/68/JHA, available at: http://eur-lex.europa.eu/LexUriServ/site/en/oj/2004/l_013/l_01320040120en00440048.pdf.

[106] Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse, CETS No: 201, available at: http:// http://conventions.coe.int.

[107] *Sieber*, "Council of Europe Organised Crime Report 2004", page 135. Regarding the means of distribution, see: *Wortley/Smallbone*, Child Pornography on the Internet, page 10 et seq., available at: http://www.cops.usdoj.gov/mime/open.pdf?Item=1729.

[108] See *Walden*, "Computer Crimes and Digital Investigations", page 66.

[109] It is possible to make big profits in a rather short period of time by offering child pornography - this is one way how terrorist cells can finance their activities, without depending on donations.

[110] Regarding the intention of the drafters to exclude child pornography see: ITU Toolkit for Cybercrime Legislation, page 32.

20.1 Art. 15 Draft Directive criminalises the import and export of child pornography through a computer system.

20.2 Neither the Budapest Convention, nor the ITU Toolkit for Cybercrime Legislation covers such offence. The fact that the act of exporting child pornography through a computer system will likely already be covered by Art. 14 (transmitting through a computer system) limits the application of Art. 15 as a standalone offence to cases of importing child pornography.

21 Art. 16 - Possession of child pornography

Article 16: Possession of child pornography or pornographic representation

The act by which a person possesses child pornography or pornographic representation through a computer system or in any other computer-data storage medium.

21.1 Art. 16 criminalises the possession of child pornography through a computer system.

21.2 Research into the behaviour of child pornography offenders shows that 15 per cent of arrested people with Internet-related child pornography in their possession had more than 1,000 pictures on their computer; 80 per cent had pictures of children between 6-12 years on their computer[111]; 19 per cent had pictures of children younger than the age of 3[112]; and 21 per cent had pictures depicting violence.[113] The degree of a criminalisation of possession of child pornography differs between national legal systems.[114] One of the reasons for a criminalisation is the fear that demand for such material could result in their production on an ongoing basis.[115] Another reason is the fact that possession of such material could encourage the sexual abuse of children, so drafters suggest that one effective way to curtail the production of child pornography is to make possession illegal.[116]

21.3 Art. 16 Draft Directive was drafted similar to the requirements of Art. 9, paragraph 1 e) Budapest Convention.

22. Art. 17 - Facilitation of access of minors to child pornography

Article 17: Facilitation of access of minors to child pornography, documents, sound or pornographic representation

The act by which a person facilitates access of a minor to pornographic pictures, sounds or representation.

22.1 Art. 17 criminalises the facilitation of access of minors to child pornography.

[111] See: *Wolak/ Finkelhor/ Mitchell*, "Child-Pornography Possessors Arrested in Internet-Related Crimes: Findings From the National Juvenile Online Victimization Study", 2005, page 5, available at: http://www.missingkids.com/en_US/publications/NC144.pdf.

[112] See: *Wolak/ Finkelhor/ Mitchell*, "Child-Pornography Possessors Arrested in Internet-Related Crimes: Findings From the National Juvenile Online Victimization Study", 2005, page 5, available at: http://www.missingkids.com/en_US/publications/NC144.pdf.

[113] For more information, see "Child Pornography: Model Legislation & Global Review", 2006, page 2, available at: http://www.icmec.org/en_X1/pdf/ModelLegislationFINAL.pdf.

[114] Regarding the criminalisation of the possession of child pornography in Australia, see: *Krone*, "Does thinking make it so? Defining online child pornography possession offences" in "Trends & Issues in Crime and Criminal Justice", No. 299; *Sieber*, Kinderpornographie, Jugendschutz und Providerverantwortlichkeit im Internet. This article compares various national laws regarding the criminalisation of child pornography.

[115] See: "Child Pornography: Model Legislation & Global Review", 2006, page 2, available at: http://www.icmec.org/en_X1/pdf/ModelLegislationFINAL.pdf.

[116] Explanatory Report to the Council of Europe Convention on Cybercrime No. 98.

22.2 Neither the Budapest Convention, nor the ITU Toolkit for Cybercrime Legislation cover such offence. With regard to the fact that the act of facilitating access of minors to child pornography through a computer system will in general already be covered by Art. 14 (making available child pornography through a computer system) limits the application of Art. 17 as a standalone offence. A review of the provision could be taken into consideration to determine if the provision is supposed to be a separate offence or shall only enable an aggravation of penalty.

23 Art. 18 - Possession of racist or xenophobic written documents

Article 18: Possession of racist or xenophobic written documents or pictures through a computer system

The act by which a person creates, downloads, disseminates, or make available in whatever form, written documents, messages, photographs, drawings or any other depictions of racist and xenophobic ideas and theories by means of a computer system.

23.1 The headline is slightly misleading. Art. 18 does not only cover the possession of racist or xenophobic material but various acts related to such content.

23.2 Art. 18 Draft Directive is following a similar approach as defined by Art. 3 of the first Additional Protocol to the Budapest Convention.[117] The ITU Toolkit for Cybercrime Legislation does not contain such an offence.

24 Art. 19 - Threat through a computer system

Article 19: Threat through a computer system

Any threat through a computer system to commit a criminal offence against a person by reason of his belonging to a group that is characterised by race, colour, ancestry or national or ethnic origin or religion, to the extent that this belonging serves as a pretext for such a threat to that person or a group of persons that is distinguished by one of the foregoing characteristics.

24.1 Art. 19 covers racist-motivated threat against members of a group.

24.2 Art. 19 Draft Directive is following a similar approach as defined by Art. 4 of the first Additional Protocol to the Budapest Convention.[118] The ITU Toolkit for Cybercrime Legislation does not contain such an offence.

25 Art. 20 - Insult through a computer system

Article 20: Insult through a computer system

Any insult to a person through a computer system by reason of his belonging to a group that is characterised by race, colour, ancestry or national or ethnic origin or religion, to the extent that this belonging serves as a pretext for such an insult to that person or a group of persons that is distinguished by one of the foregoing characteristics.

[117] Addition Protocol on cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems. ETS No. 189. Regarding the development of the Additional Protocol see: Understanding Cybercrime: A Guide for Developing Countries, page 97.

[118] Addition Protocol on cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems. ETS No. 189. Regarding the development of the Additional Protocol see: Understanding Cybercrime: A Guide for Developing Countries, page 97.

25.1 Art. 20 covers racist-motivated insult by means of computer systems.

25.2 Art. 20 Draft Directive is following a similar approach as defined by Art. 5 of the first Additional Protocol to the Budapest Convention.[119] The ITU Toolkit for Cybercrime Legislation does not contain such an offence.

[119] Addition Protocol on cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems. ETS No. 189. Regarding the development of the Additional Protocol see: Understanding Cybercrime: A Guide for Developing Countries, page 97.

International Telecommunication Union
Telecommunication Development Bureau (BDT)
Place des Nations
CH-1211 Geneva

E-mail: bdtmail@itu.int
www.itu.int/ITU-D/projects/ITU_EC_ACP/

Geneva, 2013