International Journal of Advanced Research and Development
ISSN: 2455-4030; Impact Factor: RJIF 5.24
Received: 19-05-2019; Accepted: 22-06-2019
www.advancedjournal.com
Volume 4; Issue 4; July 2019; Page No. 74-78

International conventions on cybercrime and the challenges of harmonisation

Kshamendra Mathur
Research Scholar, Department of Law, JNV University, Jodhpur, Rajasthan, India

Abstract
The adoption of consistent computer crime or Cyber Crime definitions and a consistent taxonomy is needed in order to assist in the activities like sharing information, reporting and accurate monitoring of computer crime cooperation and collaboration and cooperation on combating computer crime. Finally, the acceptance of common computer crime definitions and a common taxonomy will assist progress in harmonizing computer crime and Cyber Crime regulation and legislation. Therefore, in the current research papers systematic understanding of International Conventions on Cyber Crime and the Challenges of Harmonisationare explained.

Keywords: ICT (information and communication technologies), cyber-crimes, cyber security, convention

1. Introduction

Despite near universal support for international action against Cyber Crime, there is currently no binding international Cyber Crime agreement. If the Convention is not to fulfil this role, the question arises as to how such international consensus is to be achieved. The United Nations is the obvious choice, with its resolutions on Combating the Criminal Misuse of Information Technologies [1] raising many of the issues addressed by the Convention. However, none of these measures were binding, with member states invited to take them into account in developing their own efforts to combat the criminal misuse of information technologies. Out of the first phase of the World Summit on the Information Society, held in Geneva in 2003 [2], came the Geneva Declaration of Principles and the Geneva Plan of Action [3]. The latter included action line C5, 'Building Confidence and Security in the use of ICTs', Art 12(b) of which contained a number of measures that government should take, in cooperation with the private sector, to 'prevent, detect and respond to cyber-crime and misuse of ICTs'. The second phase held in 2005 produced the Tunis Agenda for the Information Society. In the context of legislative reform, this called upon governments 'to develop necessary legislation for the investigation and prosecution of Cyber Crime' taking into account existing frameworks and regional initiatives 'including, but not limited to, the Council of Europe's Convention on Cyber Crime'.

In 2007 the International Telecommunication Union (ITU), which is responsible for facilitating action line C5, launched its Global Cybersecurity Agenda (GCA) [4]. The GCA is divided into five pillars/work areas: Legal Measures, Technical and Procedural Measures, Organizational Structures, Capacity Building and International Cooperation. In respect of legal measures, it highlights the importance of international harmonisation and, in what would seem a thinly veiled reference to the Convention, notes that 'some efforts to address this challenge have been undertaken, and although very valuable, they are still insufficient. The Internet is an international communication tool and, consequently, any solution to secure it must be sought at the global level'. Yet the GCA does not pursue a binding global initiative. The first of the seven strategic goals 'calls for the elaboration of strategies for the development of Cyber Crime legislation that is globally applicable and interoperable with existing national and regional legislative measures.' Harmonisation of laws and facilitation of international cooperation is seen as essential to achieving global cybersecurity. However, the mechanism whereby such harmonisation can be achieved remains contested. The Convention is the only non-United Nations initiative referred to by the General Assembly as a regional initiative to which countries should have regard in ascertaining whether they have developed the necessary legislation for the investigation and prosecution of Cyber Crime [5].

The Twelfth United Nations Congress on Crime Prevention and Criminal Justice produced a clear division of opinion as to whether to proceed with negotiation of a global convention on Cyber Crime [6]. On the one hand, countries such as the Russian Federation and China supported the negotiation of a global convention [7]. The broader notion of an international agreement also finds support in African [8], Asian and Pacific [9], Latin American and Caribbean [10] nations. On the other hand, the United States, United Kingdom [11] and European Union argued that the Convention is sufficient and that the focus should be on capacity building.

The Commission on Crime Prevention and Criminal Justice was then invited to convene 'an open-ended intergovernmental expert group to conduct a comprehensive study of the problem of Cyber Crime' [12]. In addition, it was recommended 'that the United Nations Office on Drugs and Crime, upon request, provide, in cooperation with Member States, relevant international organizations and the private sector, technical assistance and training' in order to deal with Cyber Crime.

Most recently, the Open-Ended Intergovernmental Expert Group to Conduct a Comprehensive Study of the Problem of Cyber Crime ('Expert Group') met in January 2011 [13], and again in February 2013, at which time it considered the United Nations Office on Drugs and Crime's

Comprehensive Study on Cyber Crime. In December 2012, the United Nations General Assembly noted with appreciation the work of the Expert Group, and encouraged it 'to enhance its efforts to complete its work and to present the outcome of the study to the Commission on Crime Prevention and Criminal Justice in due course' [14]. At the subsequent meeting of the Commission on Crime Prevention and Criminal Justice in April 2013, the issue of international agreement was once again deferred, with a draft resolution inviting member states 'to continue to consider … ways and means to strengthen international cooperation in combating Cyber Crime', and requesting an open-ended intergovernmental working group to be convened to further examine the problem of Cyber Crime and responses to it by member states [15]. A further draft resolution requested the United Nations Office on Drugs and Crime (UNODC) 'to strengthen partnerships for technical assistance and capacity-building with Member States, relevant organizations, the private sector and civil society', and 'to serve as a central repository of Cyber Crime laws and good practices' [16]. Although over 10 years has passed since the idea was seriously mooted, we are no closer to a United Nations convention nor to international acceptance of the Convention.

There are a number of advantages to pursuing a convention through the United Nations. The first and most significant is that it would have the broadest geographic scope, being open to all member states. Second, it would provide an opportunity to address issues not included in the Convention, or to improve on provisions requiring amendment. Third, it would potentially allow amendment or removal of the provisions that have provided an obstacle to wider acceptance of the Convention.

There are, however, a number of significant disadvantages. Principal among them is the time taken to reach international agreement, if agreement can in fact be reached. It has been estimated that having signed the Convention it takes a country, on average, more than five years to ratify. Should a comprehensive binding international Cyber Crime agreement be implemented, there is no reason to believe that ratification would occur more quickly. In an area where we are constantly told of how rapidly technology outpaces attempts at regulation, there seems to be a blithe acceptance that we can wait a few more years before international agreement is reached. Even assuming international agreement can be reached, it is not clear that it would add a great deal to the Convention. In fact, in order to ensure international agreement, it is likely to provide less. The influence of the Convention 'has now been so pervasive on Cyber Crime laws throughout the world that any international agreement would largely have to mirror its terms'. Were it to depart significantly, it would be unlikely to achieve agreement from those countries that have implemented legislation based on the Convention. Equally, to ensure agreement from those countries that have objected to terms of the Convention, it would need to provide less. Human rights and privacy protections, for example, may have to be diluted or removed, while certain substantive offences may not be included.

As an illustration of the difficulties of achieving international agreement in this area, as recently as 2012 agreement could not be reached on the International Telecommunication Regulations. Although signed by 89 member states, a number of countries including Australia, Canada, the United Kingdom and the United States refused to sign [17], in part due to an addition to the preamble proposed by African countries which states that 'these regulations recognize the right of access of member states to international telecommunication services'. This was seen by some countries as expanding the regulations beyond their current remit to cover Internet governance and content.

Overall, the global picture is one of a certain degree of fragmentation in membership of international and regional instruments related to Cyber Crime. Regional patterns are particularly clear. Countries in some parts of the world benefit from membership of binding Cyber Crime instruments -- including more than one instrument for some countries -- while other regions do not participate in any binding framework. An international convention is, of course, only one approach to harmonisation, and recent years have seen a flurry of activity in relation to Cyber Crime at the international, regional and national level. The UNODC has identified five 'clusters' of international and regional instruments addressing the challenges of Cyber Crime.

The first are those which have been developed in the context of the Convention, the most significant being the Commonwealth Model Law on Computer and Computer Related Crime. Second, those developed by the Commonwealth of Independent States (CIS) [18] and the Shanghai Cooperation Organisation (SCO) [19]. The third is the League of Arab States' Arab Convention on Combating Information Technology Offences [20] and associated Model Law. Fourth is the Draft African Union Convention on the Establishment of a Legal Framework Conducive to Cyber Security in Africa [21]. If ratified, this last instrument will make a particularly significant contribution to the development of Cyber Crime laws globally, being a binding instrument, which encompasses the 54 member states of the African Union [22].

The fifth category is United Nations instruments. Although there is no United Nations convention on Cyber Crime, the UNTOC can and has been utilised in the context of Cyber Crime. The UNTOC applies to the 'prevention, investigation and prosecution' of a number of specific offences required to be criminalised under Arts 5, 6, 8 and 23 [23], as well as 'serious crime' where the offence is 'transnational in nature and involves an organized criminal group'. The UNTOC has been ratified by 181 countries [24] and requires parties to 'afford one another the widest measure of mutual legal assistance in investigations, prosecutions and judicial proceedings. It may also be used as the basis for extradition in those cases to which it applies. Although the United Nations' Model Treaty on Mutual Assistance in Criminal Matters [25] and Model Treaty on Extradition [26] do not deal specifically with Cyber Crime investigations or prosecutions, they can be applied or adapted to computer searches. For example, the revised Model Law on Mutual Assistance in Criminal Matters contains model provisions for expedited preservation and disclosure of stored computer data, production of stored computer data and search and seizure of computer data. They do not, however, contain provisions relating to electronic surveillance and interception, these being matters which parties may consider including in any treaty between them.

These are, of course, not discrete clusters, and there is considerable overlap. The Convention, in particular, has

played a significant role in influencing the drafting of other instruments. In the Commonwealth, for example, beyond those countries which are parties, the Convention and the Commonwealth Model Law on Computer and Computer Related Crime have influenced the Cyber Crime legislation of a significant number of countries [27]. For example, although Australia is now a party, its Cyber Crime laws had already been influenced by the terms of the Convention [28]. Its influence further extends to countries such as Argentina, Pakistan, the Philippines, Egypt, New Zealand and Nigeria. Adoption of the Convention has been recommended by the Organization of American States and the Financial Action Task Force [29], and its influence on the United Nations' ITU Toolkit further expands its reach. Even within Russia it is acknowledged as the 'most important international legal instrument aimed at combating crime against computer security'. Overall it is claimed to have influenced approximately 100 countries in the drafting of their Cyber Crime laws, though such claims are very difficult to verify, and may conceal considerable divergence in levels of implementation [30].

Beyond the Convention, the ITU has been active in promoting model legislation in a number of areas including Africa, the Caribbean [31] and the Pacific. Africa, in particular, has seen a raft of initiatives, including the East African Community's Draft EAC Legal Framework for Cyberlaws, the Economic Community of West African States' Directive on Fighting Cyber Crime Within ECOWAS, the Common Market for Eastern and Southern Africa's (COMESA) Cybersecurity Draft Model Bill (2011) and the South African Development Community's Computer Crime and Cyber Crime Model Law [32].

Although it is positive to see so many global initiatives addressing the challenges of Cyber Crime, there is the very real danger of fragmentation. While a comparative analysis is beyond the scope of this article, it is sufficient to note that there are significant differences. For example, while the Convention, the Commonwealth Model Law on Computer and Computer Related Crime, the CIS Agreement and the Arab Convention all focus on a criminal justice response to Cyber Crime, others address Cyber Crime as part of a broader attempt to deal with international information security. The Draft African Union Convention for example, includes provisions relating to electronic transactions, cybersecurity and e-governance as well as Cyber Crime. Similarly, the SCO's Agreement on Cooperation in the Field of Information Security provides for international cooperation in relation to information warfare, terrorism and other threats to international information infrastructure. Even within a criminal justice response, only the Convention and the Arab Convention cover substantive law, procedural law, jurisdiction and mutual assistance. Some provide for substantive offences on which it would be difficult to obtain broad international agreement, such as pornography and public order offences. Electronic evidence, which is vital to successful Cyber Crime prosecutions, is covered by relatively few instruments.

Ultimately, however, the use of both binding and non-binding international and regional instruments has significant potential for positive progress towards greater sufficiency and harmonization of national laws -- and, in the long run, enhanced international cooperation against a global challenge. On the one hand, the current global situation is one in which Cyber Crime is clearly on the international agenda, with a broad range of international, regional and national models for countries to draw upon. On the other hand, there is the danger that divergence 'may lead to the emergence of country cooperation "clusters" that are not always well suited to the global nature of Cyber Crime'. While the United Nations process continues, it is conceivable that no international agreement will be reached on this issue in the near future. An international agreement will face the same challenges as the Convention -- plus the additional issues that it does not address -- all to be agreed between the member states of the United Nations. The 'window of opportunity' during which such an agreement could be reached may have passed, and it would now be 'very difficult to bring all interests under an international agreement of the scope and depth of the Budapest Convention'.

In the absence of international agreement, the Convention remains 'the most complete international standard to date'. As of 2013, 82 countries had signed and/or ratified a binding Cyber Crime instrument. While no one instrument could be said to have global reach, the Convention has by far the largest influence, with 53 signatures/ratifications [33]. Although falling short of a 'global standard', amongst countries responding to the UNODC's Comprehensive Study on Cyber Crime it has by far the greatest influence on existing or planned Cyber Crime legislation.

This is not to suggest that all countries should accede to the Convention. The reality is that many will not or cannot. The Convention does, however, provide an important touchstone against which a country's response to Cyber Crime may be measured, providing a 'guideline or reference' even for those countries which do not want to become parties.

Perhaps the most promising development over recent years has been the increased emphasis on capacity building, and the willingness of international, regional and national agencies to assist countries in developing an appropriate response to Cyber Crime. At the international level, there is increased cooperation between the UNODC and other relevant organisations including INTERPOL, the ITU, the European Commission and the Council of Europe, as well as the private sector [34].

In 2012, the UNODC finalised its 'Global Programme on Cyber Crime' which is intended to take an 'holistic approach' including 'enhanced national, regional and international cooperation in addressing Cyber Crime'. In this it is supported by the ITU [35] whose Cybersecurity Gateway lists a range of initiatives drawing upon the expertise of national, regional and international agencies and bodies. In addition, the ITU has produced two resources, the ITU Toolkit and Understanding Cyber Crime: Phenomena, Challenges and Legal Response. The UNODC also participates as an observer with the Council of Europe Convention Committee, the Commonwealth Cyber Crime Initiative and others.

The 'Octopus' programme is part of the Council of Europe's 'Global Project on Cyber Crime' [36]. The 'Octopus Conference' on Cyber Crime was first run in 2007 to encourage ratification and accession to the Convention and aimed to promote the use of the Convention as a guide in developing national legislation. Today the conference still addresses the implementation of the Convention and 'threats and trends' in Cyber Crime, but also takes a unique focus each year. For instance, in 2012 the key focuses of the conference were jurisdiction and cloud computing and

information sharing. The Council of Europe also facilitates the 'Octopus Cyber Crime Community', which links Cyber Crime experts from around the globe with an aim of strengthening cooperation against Cyber Crime.

2. Conclusion

To see harmonisation as a destination is unrealistic; it is a process. As the technology evolves and changes so too our responses will need to evolve and change. The ideal that all member states will have comprehensive Cyber Crime laws is a noble goal, but one that is many years off. With almost 60 per cent of reporting countries in the UNODC's Comprehensive Study on Cyber Crime indicating new or planned Cyber Crime legislation, it is vital that support be provided. Rather than focusing on differences as an impediment to harmonisation, the focus should be on how those differences may be resolved in working towards the common goal of effective international cooperation against a global challenge.

The binary debate about the Convention versus a United Nations Convention in some way presents a false dichotomy. Each country will determine what it considers necessary to effectively combat Cyber Crime, looking to national, regional and international standards in enacting laws that best suit its national circumstances. Nonetheless, the Convention provides a crucial benchmark against which such efforts can be measured, providing an internationally recognised framework for the harmonisation of Cyber Crime laws. For those countries that are unable to, or choose not to ratify, it provides an important model against which their own laws can be compared. Discussions about what the Convention does not cover are equally important for parties and non-parties alike. The UNODC and Council of Europe, as well as other regional and national initiatives, play an extremely valuable role in information sharing and capacity building. In this way, difference and diversity becomes a driver of change; the focus on what needs to be achieved rather than how difficult it will be. In a world now connected by technology, we may find that 'what unites us is far greater than what divides us' [37].

3. References

1. Combating Criminal Misuse, no 1, UN Doc A/RES/55/63; Combating Criminal Misuse No 2, UN Doc A/RES/56/121
2. World Summit on the Information Society, GA Res 56/183, Agenda Item 95(c), UN Doc A/RES/56/183 (31 January 2002, adopted 21 December 2001)
3. World Summit on the Information Society, 'Plan of Action' (Document No WSIS-03/GENEVA/ DOC/5-E, International Telecommunication Union, 12 December 2003) ('Geneva Plan of Action').
4. International Telecommunication Union, Global Cybersecurity Agenda. http://www.cybersecurity-gateway.org/pdf/new-gca-brochure.pdf
5. Creation of a Global Culture of Cybersecurity and Taking Stock of National Efforts to Protect Critical Information Infrastructures, Agenda Item 55(c), UN Doc A/RES/64/211 (17 March 2010, adopted 21 December 2009).
6. Report of the Twelfth United Nations Congress on Crime Prevention and Criminal Justice, UN Doc A/ CONF.213/18 (18 May 2010) 56–7 [202]– [204].
7. Greg Masters, 'Global Cybercrime Treaty Rejected at UN', SC Magazine (online). http://www.scmagazineus.com/global-cybercrime-treaty-rejected-at-un/article/168630/
8. Report of the African Regional Preparatory Meeting for the Twelfth United Nations Congress on Crime Prevention and Criminal Justice, Held in Nairobi from 8 to 10 September 2009, UN Doc A/CONF.213/ RPM.4/1 (24 February 2010) 8–9 [40].
9. Report of the Asian and Pacific Regional Preparatory Meeting for the Twelfth United Nations Congress on Crime Prevention and Criminal Justice, Held in Bangkok from 1 to 3 July 2009, UN Doc A/ CONF.213/RPM.3/1 (8 September 2009) 7–8 [298]; Report of the Western Asian Regional Preparatory Meeting for the Twelfth United Nations Congress on Crime Prevention and Criminal Justice, Held in Doha from 1 to 3 June 2009, UN Doc A/CONF.213/RPM.2/1.
10. Report of the Latin American and Caribbean Regional Preparatory Meeting for the Twelfth United Nations Congress on Crime Prevention and Criminal Justice, Held in San Jose, from 25 to 27 May 2009, UN Doc A/CONF.213/RPM.1/1
11. The Quintet of Attorneys-General from Australia, Canada, New Zealand, the United Kingdom and the United States have resolved to 'promote the Convention as the key international instrument for dealing with Cyber Crime and use the Convention as a basis for delivering capacity building and awareness raising activities': US Reference Service, Communiqué Quintet of Attorneys General: Action Plan to Fight Cyber Crime.
12. Salvador Declaration on Comprehensive Strategies for Global Challenges: Crime Prevention and Criminal Justice Systems and Their Development in a Changing World, para 42 ('Salvador Declaration'). Paragraph 42 of the Salvador Declaration was adopted by the Commission on Crime Prevention and Criminal Justice and then by the Economic and Social Council: Twelfth United Nations Congress on Crime Prevention and Criminal Justice. It was also adopted by the General Assembly: Twelfth United Nations Congress on Crime Prevention and Criminal Justice
13. Report on the Meeting of the Open-Ended Intergovernmental Expert Group to Conduct a Comprehensive Study of the Problem of Cybercrime, Held in Vienna from 17 to 21 January 2011, Doc No UNODC/ CCPCJ/EG.4/2011/3
14. Strengthening the United Nations Crime Prevention and Criminal Justice Programme, in Particular Its Technical Cooperation Capacity, Agenda Item 103, UN Doc A/RES/67/189 (27 March 2013, adopted 20 December 2012) para 6.
15. Commission on Crime Prevention and Criminal Justice, Strengthening International Cooperation to Combat Cybercrime, Agenda Item 7, UN Doc d E/CN.15/2013/L.14 para 3.
16. Commission on Crime Prevention and Criminal Justice, Enabling International Cooperation against Cybercrime through Technical Assistance and Capacity-Building, Agenda Item d 7, UN Doc E/CN.15/2013/L.16 (2 April 2013) paras 3–4.
17. International Telecommunication Union, Signatories of the Final Acts: 89. See also 'US and UK Refuse to Sign UN's Communications Treaty' BBC News (online).

https://www.bbc.co.uk/news/technology-20717774
18. Commonwealth of Independent States, Agreement on Cooperation among the States Members of the Commonwealth of Independent States in Combating Offences Relating to Computer Information (2001) ('CIS Agreement'). The CIS consists of former Soviet republics of Azerbaijan, Armenia, Belarus, Georgia, Kazakhstan, Kyrgyzstan, Moldova, Russia, Tajikistan, Turkmenistan, Uzbekistan and Ukraine: Common wealth of Independent States, About Commonwealth of Independent States www.cisstat.com/eng/cis.htm
19. Shanghai Cooperation Organisation, Agreement on Cooperation in the Field of Information Security (2010). The SCO consists of member states of Kazakhstan, China, Russia, Kyrgyzstan, Tajikistan and Uzbekistan, as well as observer states of Afghanistan, India, Iran, Mongolia and Pakistan, and dialogue partners of Belarus, Turkey and Sri Lanka: Official Website of Russia's Presidency in the Shanghai Cooperation Organisation 2014–2015, Brief Introduction to the Shanghai Cooperation Organization http://en.sco-russia.ru/about_sco/20140905/ 1013180761.html
20. League of Arab States, Arab Convention on Combatting Information Technology Offences, opened for signature 21 December 2012 ('Arab Convention')
21. African Union, Draft African Union Convention on the Establishment of a Legal Framework Conducive to Cyber Security in Africa (1 September 2012) ('Draft African Union Convention')
22. African Union, Member States. The convention is only open to members of the African Union: ibid art IV-2(1). For a discussion of responses to cybercrime in Africa, see Uchenna Jerome Orji, Cybersecurity Law and Regulation (Wolf Legal Publishers, 2012).
23. UNTOC art 3(1). These are offences relating to participation in an organised criminal group, laundering of proceeds of crime, corruption and the obstruction of justice.
24. United Nations Office on Drugs and Crime, Signatories to the United Nations Convention against Transnational Crime and its Protocols. https://www.unodc.org/unodc/ en/treaties/CTOC/signatures.html
25. United Nations Office on Drugs and Crime, Model Treaty on Mutual Assistance in Criminal Matters. This model treaty was subsequently adopted in Model Treaty on Mutual Assistance in Criminal Matters, GA Res 45/117, UN GAOR, Agenda Item 100, UN Doc A/RES/45/117 (14 December 1990) and amended in Mutual Assistance and International Cooperation in Criminal Matters, GA Res, 53/112, UN GAOR, Agenda Item 101, UN Doc A/RES/53/112 (20 January 1999)
26. United Nations Office on Drugs and Crime, Model Treaty on Extradition. This model treaty was subsequently adopted in Model Treaty on Extradition, GA Res 45/116, UN GAOR, 45th sess, 68th plen mtg, Agenda Item 100, UN Doc A/ RES/45/116 (14 December 1990) and amended in International Cooperation in Criminal Matters, GA Res 52/88, UN GAOR, 45th sess, 70th plen mtg, Agenda Item 103, UN Doc A/RES/52/88 (4 February 1998).
27. See discussion on Commonwealth States' use of the Convention: Council of Europe, 'Cybercrime Legislation of Commonwealth States', above n 299. At the meeting of Commonwealth Law Ministers in Sydney in 2011, ministers mandated the Commonwealth Secretariat to form a multidisciplinary working group of experts to review the practical implications of cybercrime in the Commonwealth and identify the most effective means of international co-operation and enforcement, taking into account, amongst others, the Council of Europe Convention on Cybercrime, without duplicating the work of other international bodies … Commonwealth Working Group of Experts on Cybercrime, 'Report to Commonwealth Law Ministers 2014 (Report, Commonwealth Secretariat, 2014)
28. Model Criminal Code Officers Committee of the Standing Committee of Attorneys-General, 'Model Criminal Code Chapter 4: Damage and Computer Offences' (Report, January 2001) 89.
29. Financial Action Task Force, 'International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation: The FATF Recommendations' (Report, February 2012) 27.
30. Gercke, '10 Years Convention on Cybercrime', above n 37, 143. The cybercrime profile of a number of countries can be found at: Council of Europe, Cybercrime Legislation Country Profiles www.coe.int/t/dg1/legalcooperation/economiccrime/cybercrime/Documents/CountryProfi les/default.en.asp
31. International Telecommunication Union, 'Cybercrime / e-Crimes: Model Policy Guidelines and Legislative Texts' (2012).
32. International Telecommunication Union, 'Computer Crime and Cybercrime: Southern African Development Community (SADC) Model Law' (2013) https://www.itu.int/en/ITU-D/Cybersecurity/Pages/default.aspx ('Computer Crime and Cybercrime Model Law').
33. Council of Europe, Convention on Cybercrime CETS No: 185, above n 237. Compare with the Arab Convention (18 countries/territories), CIS (10 countries/territories) and SCO (six countries/territories).
34. Commission on Crime Prevention and Criminal Justice, Promotion of Activities Relating to Combating Cybercrime, Including Technical Assistance and Capacity-Building: Report of the Secretary General, UN ESCOR, Agenda Item 7, UN Doc E/CN.15/2013/24 (5 March 2013) 2 [3] ('Promotion of Activities Relating to Combating Cybercrime').
35. United Nations Office on Drugs and Crime, UNODC and ITU Join Forces to Make Internet Safer (19 May 2011). https://www.unodc.org/unodc/en/frontpage/ 2011/May/unodc-and-itu-to-cooperate-more-closely-to-make-the-internet-safer.html
36. Council of Europe, Octopus 2013. For a summary of the development of the Octopus Program, see Council of Europe, Roots: The History of Octopus. https://www.coe.int/en/web/human-rights-rule-of-law/home
37. John F Kennedy, 'Address before the Canadian Parliament in Ottawa' (Speech delivered at the Canadian Parliament, Ottowa, 17 May 1961).