Canada's response to UNODC note verbales CU 2016/50/DTA/OCB/CSS and CU 2016/133/DTA/OCB/CSS pertaining to the February 2013 Draft Comprehensive Study on Cybercrime

Canada is pleased to provide its comments on the February 2013 Draft Comprehensive Study on Cybercrime developed by UNODC for the open-ended intergovernmental expert group (IEG) convened pursuant to paragraph 9 of General Assembly Resolution 65/230 of 21 December 2010[1] (Draft Study).

At the outset, Canada wishes to thank the UNODC for its work to develop the Draft Study with limited resources under difficult conditions. As the challenges that the transnational nature of cybercrime poses to all jurisdictions by cybercrime increase, it is important to discuss these challenges and Canada hopes that the IEG will be able to continue its work in this regard.

Mandate Issues

Canada is concerned that the findings, options, key results and conclusions made in the Draft Study go beyond what the UNODC was mandated by the IEG to do. Canada highly values the work of the UNODC, particularly its professionalism in organizing, running and reporting on intergovernmental and technical expert processes. However, in an intergovernmental process, the role of the UNODC is to collect evidence from Member States, the private sector and other sources and present it to the intergovernmental body in a neutral manner which does not suggest or presume any specific policy direction or prejudice intergovernmental deliberations based on the evidence. Attempting to accelerate the process by presenting the IEG with predetermined conclusions and recommendations in the form of sections on key findings, options and key results, is prejudicial to the balance and autonomy of the IEG process.

Canada's concerns arise, in part, from the fact that cybercrime poses very difficult and complex technical challenges of law, policy and technology. We believe that solutions will come only through expert deliberations and consensus on the entirety of the factual information that we have all worked so hard to accumulate. In Canada's view, those parts of the Draft Study which draw conclusions about the facts, particularly the various "Key Findings and Options" and "Key Results" sections or any other text that develops

[1] A/RES/65/230, para.9:

> 9. *Requests* the Commission on Crime Prevention and Criminal Justice to establish, in line with paragraph 42 of the Salvador Declaration, an open-ended intergovernmental expert group, to be convened prior to the twentieth session of the Commission, to conduct a comprehensive study of the problem of cybercrime and responses to it by Member States, the international community and the private sector, including the exchange of information on national legislation, best practices, technical assistance and international cooperation, with a view to examining options to strengthen existing and to propose new national and international legal or other responses to cybercrime;

policy recommendations or options should be removed and examples are set out in Annex 1. In addition, the Green Boxes at the beginning of each chapter should be reviewed to ensure that they contain a factual summary of the content of each chapter rather than integrating judgements and findings into the summaries.

General comments

Canada provides additional comments, and some proposed text, in Annex 2 on substantive areas addressed in the Draft Study, including addressing relevant human rights considerations.

Canada agrees with the Draft Study including a review of human rights issues relating to cybercrime, including criminalization and enforcement, as human rights protections will be an important element of future IEG discussions. While Member States differ on what types of content should be criminalized and on the applicable human rights protections of expression or content, human rights issues also arise in contexts other than the criminalization of content (e.g. in discussing the privacy interests and the use of law enforcement techniques) and should also be explored.

For example, the Draft Study makes numerous references to the need to "balance" privacy (and other values) against security, law enforcement or due process considerations. This characterization suggests a trade-off between interests is inevitable. Some states take the view that human rights and privacy interests complement security and law enforcement interests and they should be approached as mutually reinforcing objectives. It would be preferable to refer to the different considerations in a neutral way (i.e. the relationship between privacy and security) to avoid the implication that interests are necessarily competing.

Another comment pertains to chapters 1 and 2 of the Draft Study which present a 'snapshot' in time, as mentioned on page x. Canada is of the view that a caveat should be incorporated into the Draft Study to clearly indicate data was compiled as of a certain date and to recognize that while more up-to-date information may be available, it is not incorporated into the Draft Study.

References and Sources

The Draft Study should focus on factual evidence concerning cybercrime, the response of Member States and other stakeholders based on the results of the Questionnaire and academic sources reviewed by the UNODC. Where appropriate, the UNODC should also provide their expert assessment as to the validity and reliability of the data.

The Draft Study also cites reports from other United Nations bodies (e.g., the International Telecommunications Union) that are considering the same or parallel issues under consideration by the IEG and the United Nations Commission on Crime Prevention and Criminal Justice. These are valid sources that should be reflected, bearing in mind that the IEG is not bound by them.

For the IEG to properly review different sources and base its conclusions on the evidence presented, citations must properly reflect their source. Annex 3 sets out areas of the Draft Study in which the sources and citations could be clarified.

Canada is also of the view that the source data should be either released as an annex to the Draft Study or shared with participants in more detailed fashion (i.e., specific input from the surveys). This would enable Member States, private sector, academics and others gain a more in-depth understanding of the issues at stake. As with any study, its ultimate validity depends to a large degree on the ability of others to independently review the empirical data.

Minor errors

Typographical and other minor errors were also noted and are set out in Annex 4.

Way Forward

In summary, Canada believes that the Draft Study should be revised to focus on the evidence collected from Member States, the private sector, and academic and other expert sources, as well as the practices reported by Member States in the survey. In accordance with its mandate, the IEG should only then consider the revised draft, the implications of the data in it and develop consensus-based recommendations for transmission to the General Assembly, via the Commission on Crime Prevention and Criminal Justice and the Economic and Social Council.

Enclosures:

1. Annex 1
2. Annex 2
3. Annex 3
4. Annex 4

Annex 1 – Changes relating to Mandate Issues			
Section	**Page**	**Paragraph**	**Comments**
Introduction	p. x	1st full paragraph ("As required…")	The full UNODC mandate should be provided. The text states that the Study was prepared "with a view to examining options to strengthen existing and to propose… responses to cybercrime", while the full mandate of the IEG is "to conduct a comprehensive study of the problem of cybercrime and responses to it by Member States, the international community and the private sector, including the exchange of information on national legislation, best practices, technical assistance and international cooperation, with a view to examining options to strengthen existing and to propose new national and international legal or other responses to cybercrime.". . The mandate of the IEG was a negotiated compromise text and should be included *verbatim* at the beginning of the text to avoid any bias or misleading impressions. The mandate to conduct a complete "study" is that of the IEG; the text produced by UNODC is, in our view, only part of the final product. The Study's final wording will be a matter for the IEG to decide.
KEY FINDINGS AND OPTIONS	xi - xv	Entire section	Consistent with Canada's covering comments on the mandate for the study, this section of the report should be removed. Accordingly, the 'Key Results' boxes, as well as any policy options or recommendations embedded in the text, should also be deleted throughout the study. Specific page numbers and references are included in this Annex.
1.1 1.2 1.3 1.4	p. 1 p. 4 p. 6 p.11	Key Results boxes and the Green box	Consistent with Canada's covering comments on the mandate for the study, all 'Key Results' should be removed from the draft and the Green box should be reviewed.
1.1	p. 3		The chapter contains various policy statements from a variety of organizations (see for example, page 3: *The persisting digital divide*) which may reflect policy positions and particular historical contexts. The notion of "digital divide" may be characterized from differing perspectives (e.g. technological disparity among geographic regions of the world as opposed to local or regional inequalities arising from educational opportunities, class differences, household incomes and/or competitive advantage). As such, reference to particular studies and comparison of their high level findings should be approached carefully and citations documented. In addition, care must be taken to reflect the responses received from Member States rather than a

			particular policy perspective.
1.4 and 2.1	pp. 11-21, and 24		Canada agrees with the basic assessment and suggestion that cybercrime falls into 3 groups. Regarding the second suggested category (thus far known as "computer-related crime") and agree that it "risks becoming extensive" (p. 24). Nevertheless, we believe that computer-related crime needs to remain part of the agenda. We do not think that the difficulty in drawing lines based on the extent of information and technology or network involvement should be a problem. We agree that the approach has to be to first, collect data on specific acts, to the extent possible defined by thematic descriptions like the ones used in the IEG Survey Instrument. We would also suggest that the text be changed to say that, while the range of "computer related" crime issues is broad and can be open-ended, future study of specific crimes and crime patterns will be needed as the technologies and offences evolve. As well, many forms of "computer-related" crimes, such as drug trafficking, organised crime and money-laundering are already the subject of existing mandates and study, and future study could include a focus on similarities of the computer related elements for these different types of crime. A threshold issue will be reporting from a diverse range of State and other sources as to what "computer-related" offences are being encountered and which of these are seen by Member States as the most serious and in need of legislative or technical assistance responses.
1.4	p. 20-p.21	last 3 lines of p. 20 and top of p. 21	The characterization of cybercrimes based on the questionnaire does not support the conclusion that there is a consensus on core issues, namely what should be addressed as a computer crime and what should be addressed by either using or extending pre-existing offences. The different views should be included here.
1.4	p. 22	Last paragraph ("As the world…")	Consistent with Canada's comments on the mandate of the Draft Study, the paragraph should be deleted. The IEG should discuss and include its opinion if it finds consensus or the text should express the range of views if there is no consensus.
2.1 2.2 2.3	p. 23 p. 25 p. 39	Key Results boxes and Green box	Consistent with Canada's covering comments on the mandate for the study, all 'Key Results' should be removed from the draft.
2.1	pp.	Section on	Canada has no issue with the content presented in the Draft

	24-25	"*What information can be gathered?"*	Study but in our view, expert opinion is also an important source, especially given the obvious difficulty in collecting internationally-comparable statistical data. One or two sentences to this effect should be added. As noted in our covering comments, Canada is also of the view that the source data should be either released as an annex to the Draft Study or shared with participants in more detailed fashion (i.e., specific input from the surveys). This would enable Member States, private sector, academics and others gain a more in-depth understanding of the issues at stake. As with any study, its ultimate validity depends to a large degree on the ability of others to independently review the empirical data
2.2	pp.28-29		In general, the facts and statistics have been assembled into patterns of consistency, based on what may be possible or plausible explanations for the data (e.g. the discussion of differences in victimisation rates at pp.28-29). The conclusions may mask or under emphasize data that do not fit or contradict those patterns. Consistent with Canada's comments general comments, looking at all of the data is a function of the IEG and should also be possible for outside professional and academic experts.
2.2	p.28	2nd paragraph ("*Consumer victimization…")*, second last sentence	The statement that "One factor responsible for this difference [higher victimisation for cyber offences than conventional offences] ~~is likely~~ **may be** the 'bulk' nature of many cybercrime acts. For acts such as phishing, or 'brute-forcing' email passwords to gain unauthorized access, a single individual can simultaneously target many victims in a way not possible in forms of conventional crime", should be reworded to identify possible explanations but not comment on probability.
2.2	p. 28	2nd paragraph ("*Consumer victimization…")*	The drafting does not always make clear what the "base line" comparator is. In the text discussing victimisation (p.28), for example, cyber-offences are given as a percent "of the on-line population", whereas conventional offences are just set out as percentages. Do these refer to percentages of the entire national population? Depending on the comparators above, a discussion of whether comparing victimisation rates based on the on-line and general populations is valid or not should be raised as an issue for the IEG.
3.1 3.2	p. 51 p. 56	Key Results boxes and	Consistent with Canada's covering comments on the mandate for the study, all 'Key Results' should be removed

3.3 3.4	p. 63 p. 72	Green box	from the draft and the Green box should be reviewed.
3.1	p. 55	Paragraph - Jurisdiction and International Cooperation	The paragraph is presently phrased as a conclusion about what sorts of jurisdictional extension Member States need. The question of extraterritorial extension of jurisdiction (whether they are needed and on what basis) is an issue for Member States and the IEG. The text should discuss the investigative and national sovereignty aspects on both sides of the issue, including problems with both extending investigative (executive or enforcement) jurisdiction and the use of consent-based cooperative investigations and sharing of evidence collected by territorial States through mutual legal assistance channels. To the extent that some of the Member States responded to the effect that they felt extensions of jurisdiction were needed, this should be reported as such. Canada would suggest something along the following lines: *Jurisdiction and international cooperation* – More than half of responding countries reported that between 50 and 100 per cent of cybercrime acts encountered by police involved a 'transnational element.'15 <u>The prosecution of transnational or extraterritorial offences requires that the prosecuting State have adjudicative jurisdiction over the offences involved based on factors such as having elements of the offence, offenders, victims or effects in its territory, or that some essential State interest be threatened by an entirely-extraterritorial offence. In practical terms, such prosecutions also require that the State concerned have custody of, and thus personal enforcement jurisdiction over, the accused offender, commonly accomplished by extradition, and sufficient evidence to prosecute the case and meet any procedural requirements regarding admissibility (e.g. authenticity, human rights and disclosure requirements) in criminal proceedings, often obtained through mutual legal assistance frameworks. The fundamental gap between the practical requirements for the effective investigation and prosecution of cybercrime cases and the need to respect the sovereign independence and equality of States, including the rule of law within each State, the integrity of their penal laws and human rights protections, is a critical challenge for the effective suppression of global cybercrime in national criminal justice systems. On one hand, investigators require rapid access to trace offenders</u>

			and prevent the loss of evidence, while on the other, basic human rights and other safeguards depend on respect for domestic rule of law requirements such as judicial approvals, which take time. Chapter Seven (International cooperation) examines this area in detail.
3.4	p.72-73		The text accompanying pp. 72-73 does not lead to this conclusion in the box's text and Canada suggests deleting the last portion of the sentence. If there is data supporting the assertion, the data should be sourced. "Membership of a multilateral cybercrime instrument corresponds with the perception of increased sufficiency of national criminal and procedural law. ~~*indicating that current multilateral provisions in these areas are generally considered effective.*~~"
3.4	p. 76	Last paragraph ("Ultimately, however…")	Consistent with Canada's comments on the mandate of the Draft Study, the paragraph should be deleted. This paragraph concludes that greater harmonisation is needed to respond to the global challenge of cybercrime and that binding and non-binding international instruments have significant potential for positive progress in this direction. This is a debate among Member States about the need for further international legal instruments which should be discussed by the IEG.
4.1 4.2 4.3	p. 77 p. 81 p.107	Key Results boxes and Green box	Consistent with Canada's covering comments on the mandate for the study, all 'Key Results' should be removed from the draft and the Green box should be reviewed.
4.1	p.77-78	Fig. 4.1	Some qualifying language should be added to indicate that the conduct descriptions in the chapter were developed by UNODC and the IEG and set out in the survey questionnaire. A short footnote explaining how the categories and descriptions were developed might be of assistance.
4.3	p. 116	Bottom of page	The sentence which says "Where content is illegal in one country, but legal to produce and disseminate in another, States will need to focus criminal justice responses on persons accessing content within the national jurisdiction, rather than on content produced outside of the country" should be removed as the draft study should not guess as to policy response of states.
4.3	p. 116	Last paragraph ("Moreover, where…")	Consistent with Canada's comments on the mandate of the Draft Study, the paragraph should be deleted. For example, the first sentence states a conclusion about future developments in international law. Assertions of

			extraterritorial jurisdiction over content raise policy issues that are within the mandate of the IEG.
5.1 5.2 5.3 5.4 5.5 5.6	p. 117 p. 122 p. 134 p. 142 p. 144 p. 152	Key Results boxes and the Green box	Consistent with Canada's covering comments on the mandate for the study, all 'Key Results' should be removed from the draft and the Green box should be reviewed.
5.1	p. 118	Last paragraph ("As discussed…")	The paragraph draws or summarises conclusions about what the "critical elements of a consistent law enforcement response are". In Canada's view, the literature paints a more complex and nuanced picture and should be reviewed and included for balance. For example, sources could include: support for the conclusions suggested in this chapter (e.g. Susan Brenner, *Cybercrime: Criminal Threats from Cyberspace*, 2010); for more complex public/private models of policing (David S. Wall, *Cybercrime* 2007) and some opinion that the problems are over-stated and do not require extensive law enforcement (McGuire M.R., *Technology Crime and Justice* 2012).
5.1	p. 120	2nd paragraph ("Country responses also…")	The conclusions, "Country responses also showed the need for law enforcement authorities to work closely with other stakeholders, such as the private sector – in order to increase reporting and for intelligence purposes." and "Overall, however, the comparatively low proportion of cybercrime acts reported by company victims or internet service providers, suggests that additional outreach and development of public-private partnerships may be needed, in order to strengthen reporting of cybercrime acts from these sources" should be either re-worked to reflect that they were based on expert evidence, suggested by respondents to the survey or deleted if they are conclusions drawn by the drafters.
5.3	p.141	("Recent work by…"), 3rd sentence	The sentence that reads: As countries work to promulgate laws that address the delicate balance between individual privacy and the prevention and control of crime, it is critical that national laws reflect common rule of law and human rights principles for law enforcement investigative actions. While Canada has no difficulty with the conclusion, the text should be revised to simply state the problem in terms of finding ways to effectively protect human rights in

			transnational investigative scenarios while at the same time enabling effective cybercrime investigations. The European Court of Human Rights text in the box on p. 141 can then be cited as an example of responses developed for this problem.
5.3	p.141	3rd paragraph ("One strong starting…"), last sentence	As there is no general consensus about the application of national privacy standards or causes of action, Canada suggests the sentence be deleted or revised to read: "This may entail considering whether (i) support to foreign law enforcement is or should be fully subject to national privacy standards; and (ii) causes of action are or should be available to persons outside of national jurisdictions that are affected by the actions of the law enforcement authorities of that country."
6.1	p. 157 p. 162 p. 168 p. 172 p. 178	Key Results boxes	Consistent with Canada's covering comments on the mandate for the study, all 'Key Results' should be removed from the draft.
7.1 7.2 7.3 7.4 7.5	p. 183 p. 189 p. 197 p. 208 p. 216	Key Results boxes and Green box	Consistent with Canada's covering comments on the mandate for the study, all 'Key Results' should be removed from the draft and the Green box should be reviewed.
7.1	p.183-184		Canada does not believe that the text accurately characterizes the jurisdictional issues arising from cybercrime cases. All aspects of the issue should be included for discussion by the IEG. The customary law requirement for consent for any exercise of enforcement jurisdiction (including investigative measures) and the national safeguards required to obtain that consent should be addressed. National sovereignty, the rule of law and procedural requirements based on national human rights and other protections must generally be followed in the form of judicial and executive reviews before cooperation can be provided. The text should reflect the reasons behind the respect for formal channels of consent requirements.
7.1	p. 185	Table	In Canada's view, caution should be exercised in making assessments of the "effects doctrine" in the context of cybercrime. The nature of computer crime and computer networks may mean that many of the offences, especially "computer crime" offences that target computers, networks or data, would become the subject of something approaching universal jurisdiction based on their effects or potential effects in every country where the Internet is

			present. In the present context, the merits and demerits of effects-based jurisdiction over cybercrime is an issue that should be considered by the IEG and should be framed in the text as an open question to support such a discussion.
7.2	p. 190-191		More discussion is needed of what constitutes an "extraterritorial offence" in the context of transnational computer and communications networks. If there is more information in the survey data (e.g. how Member States interpreted the term in their responses) it should be added, and if not this is an issue that should be flagged for discussion by the IEG.
7.2	p. 196	1st paragraph ("Overall, analysis…")	The opening paragraph observes that the analysis undertaken suggests that "cybercrime jurisdictional challenges can be resolved by ensuring clarity and *innovative application of existing principles*.' It is not entirely clear what the latter refers to and if there is consensus amongst Member States that the resolution reached through "innovative application of existing principles" would be appropriate. If so, the evidence should be sourced.
7.2	p. 196	Last paragraph ("As discussed…")	Consistent with Canada's comments on the mandate of the Draft Study, the text that begins "*Whether [jurisdiction] is viewed … coordination of extraterritorial criminal justice actions."* should be deleted. The issue of the required threshold is a matter for the IEG to discuss.
7.3	p. 205	1st full paragraph ("While a number…), second last sentence	The second last sentence ends with a speculative comment about the basis of a particular country reply. That should be deleted.
7.4	p. 215	Last paragraph ("Many such challenges…")	The last section ("Sufficient cooperation?") includes findings/speculation that are not directly tied to the results of the questionnaire (e.g., speculation such as "The current international cooperation picture risks the emergence of country clusters…"). Canada requests that such text be removed.
7.5	p. 218	First full sentence ("In effect, the interests…")	The sentence is conclusory in nature and could be softened by suggesting that the approach highlights the tension between the interests of the state in which the cloud data is stored vs. the state on whose territory the data is controlled. The responses of Member States, if any, on this issue could be addressed.
7.5	p. 218	International and regional	The bulk of this section analyzes Article 32 of the Budapest Convention (on transborder access to open source computer

		approaches	data and access to such data on consent of the person with lawful authority to disclose it). Members States responses, if any, on this issue should be reviewed.
7.5	p. 223	Last paragraph ("From a crime…")	The paragraph should be deleted as it is not a result or finding of the study, it is a recommendation.
8.1 8.2 8.3	p. 225 p. 234 p. 239	Key Results boxes and the Green box	Consistent with Canada's covering comments on the mandate for the study, all 'Key Results' should be removed from the draft and the Green box should be reviewed.
8.3	p. 248	3rd full paragraph, 3rd sentence ("Data processing..")	The text should be reviewed for language that reflects recommendations "should" rather than describing the domestic laws of states.

Annex 2 – General comments			
Section	**Page**	**Paragraph**	**Comments**
1.1	p. 1 and following, as well as p. 165		As reflected on p. x, the Draft Study "represents a 'snapshot' in time" as it reflects the practice and views of Member States at a specific point in time. Canada notes that much of the data is at least 5 years old or based on projections from 2012 or earlier. Such "statistics", estimates, and projections have already been superseded by later (similar) snapshots. For example, a May 2015 ITU snapshot which uses similar types of headings: http://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2015.pdf. Canada is of the view that a caveat should be incorporated into the Draft Study to clearly indicate data was compiled as of a certain date and to recognize that while more up-to-date information may be available, it is not incorporated into the Draft Study.
1.1	p. 2 and following		Section 1.1 fails to discuss several issues with legal and political implications: • The focus on rates and trends in "cybercrime" assumes that a consistent criminological environment has existed over the entire period, which is not the case. Only with the advent of computers and criminalization did cybercrime arise. Important environmental elements affecting cybercrime such as interconnectedness and the speed and capacity of data processing, storage and transfer have been changing ever since. That the definitions of cybercrime are still changing is a variable that needs to be discussed. • Advances in technology also create new opportunities for criminal innovation, reduce risks and increase potential benefits to offenders. These in turn affect the extent (increases in volume) and scope (increases in the range of types of crime) of cybercrimes committed. • As the threat of cybercrime and related risk increases, states have also tended to understand and define cybercrime as a national security issues, which then raises the issue of the definition and scope of what constitutes a crime (and/or a national security threat).
1.1	p. 2	Last paragraph ("Africa and the Arab…"), 2nd last	Care should be taken to ensure that estimates or projections are not incorporated that are tied to dates that have already passed or may be projected to be prior to the study's

		sentence	release.
1.3	p.7	2nd paragraph ("In the past five…")	The statement that compares media reporting of homicide and cybercrime requires some clarification. The intended meaning may be to address the public reporting of the problems as opposed to actual occurrence rates but the fact that homicide is much more visible than cybercrime, much of which is never detected and/or never reported or publicly discussed, is also important. The other significant variable is that the legitimate and criminal use of information technologies has evolved significantly in the period 2005-2012, whereas homicide has not. Whether the cluster of phenomena that constitute "cybercrime" will eventually stabilise in the way that long-established offences have remains to be seen and is something that could be discussed by the IEG and included in the final text. The following changes could be made to the text: Between the years 2005 and 2012, public media references to cybercrime have increased by up to 600 per cent, compared with around 80 per cent in the case of references to homicide. [33] Such measurements obviously reflect the public attention paid to cybercrime more than they reflect the underlying problems and actual offending rates, but they may partly reflect real increases. Comparing cybercrime and homicide also illustrates the challenges of gaining an accurate picture. Homicide figures are used because the offence is highly visible, almost always reported and substantially similar from one jurisdiction and legal system to another. Cybercrime is often never detected and may not be reported when it is detected. Further, while homicide rates may be relatively stable for decades in some countries, in other countries it may abruptly increase and even double in the course of ten years. The contrast between stability or rapid transformation is often linked to underlying structural conditions – whether political, economic or social – ranging from shifts in sources or distribution of wealth, war or internecine conflicts, industrializing versus industrialized countries, major changes in unemployment, escalating or declining organised crime, relative aging of populations, or changing police practices. Long-term studies in homicide rates or violent crime are more prevalent than comparable studies for cybercrime offences and this may be structurally inevitable at this point in history. In part this is because cybercrime only emerged as a phenomenon fairly recently in the 1960s; in part it is because the underlying technologies have been evolving constantly since then; and, more compellingly, the market penetration and

			relative adoption of specific constellations of technologies has changed significantly and variably from country to country in the past two decades alone. Determining the relevant factors and establishing meaningful base-lines in the case of cybercrime is still nascent.
2.1	p. 24-25	Last paragraph, "What information can be gathered?"	Canada has no issue with the content presented in the Draft, but in our view expert opinion is also an important information source, given the obvious difficulty in collecting internationally-comparable statistical data. Care should be taken to include the full range of expert opinion and underlying empirical evidence available on each issue.
2.2	p. 27	Figures 2.2 and 2.3	Any information behind the differences, particularly in the significance of computer-related copyright and trademark offences would be useful to include, particularly if significant differences were reported depending on the region.
2.2	p.32-35	*Criminal tools – the botnet*	The use of botnets is a major problem but the study needs to cover the entire range of cybercrime tools, and not just focus on a single tool or category. There are other types of malware that raise legislative, enforcement and prevention challenges, and a range of "hacking" applications for example.
2.2	p.36	*Last sentence before Child pornography*	The nature of the threshold required to limit freedom of expression should be cited as a point of international law or the respective laws of Member States and not just expressed as an opinion. The issue should be flagged for the IEG to discuss.
3.1	p. 52	3rd full paragraph ("While *criminal law*…")	The reference to "constitutional or rights-based laws" should be replaced with "human rights laws".
3.1	p. 55		The text reads "Firstly, states must be able to assert that their national criminal law applies to an act that takes place only partly, or even not at all, within its national territory." For states like Canada, territorial jurisdiction must apply to some element of the offence, such that there can be said to be a reasonable and substantial connection to Canada. In our view, extending jurisdiction more broadly raises sovereignty and comity issues that could adversely affect international relations, including existing forms of formal and informal cooperation in criminal matters. Only in a very limited number of offences will Canadian criminal laws apply where there an offence is wholly committed outside of

			Canada, and often this is in furtherance of an international treaty obligation. Other Member States may have other views, but we believe the issue of extending extraterritorial jurisdiction should be raised in a neutral manner for discussion in the IEG. Suggest rewording as: "Firstly, states ~~must be able to assert~~ should ensure that their national criminal law applies to an act that takes place only partly~~, or even not at all~~, within its national territory and may, in certain circumstances, extend its application extraterritorially."
3.1	p.55	1st sentence ("Thus, the gathering…")	The reference to "chain of custody" issues for electronic evidence should be expanded to refer to '"forensic standards for the collection, handling and presentation of electronic evidence from the time it is seized or collected until all legal proceedings are exhausted, including what is sometimes called the "chain of custody" process." Including "forensics" would note that there is more to the challenge than chain of custody matters after the evidence is collected. Unlike physical seizures ensuring the completeness and authenticity of evidence is also a challenge during the actual search. The addition is useful for policy-making and technical assistance aspects.
3.1	p.55	First paragraph ("*Regulation and risk*")	The paragraph should be expanded to *Regulation and risk-mitigation* as the current wording is not clear. Also the reference to "proactive actions against criminal infrastructure" in the second sentence should either be explained or deleted, depending on what meaning was intended. If the reference addresses legal powers to make proactive interventions to take down illegal content or web sites, this should be clarified. If referring to actions independent of legal powers, it should not be in the segment dealing with legal frameworks.
3.3	p. 63-73		The analysis should mention the *Palermo Convention*, as well as bilateral instruments, that address mutual legal assistance, extradition and other important issues which apply to cybercrime in many scenarios.
4.1	pp. 79 and 91	2nd paragraph ("In addition to…)	In relation to mental elements, the study seems to equate recklessness (a criminal standard) with a non-intentional culpability (strict liability). In many common law states there is no criminal culpability for strict liability offences. This same confusion is found again at page 91 and should be

			clarified.
4.2	p. 87 and following		To the extent that the content of survey responses supports it, it might be useful to add a short explanation of what is meant by some of the basic terms used in the questionnaire and in Member State responses, both for greater clarity in English and to support any future translations. An example of the explanation needed is the description of what "transmission" means or includes on p.87. Where meanings were ambiguous (i.e., that Member States may have responded to the questionnaire based on different assumptions) this should be pointed out. For example, in English the concept of "intercepting" physical items usually refers to an intervention that prevents them from reaching a destination, whereas when used in references to data or communications it may refer both to stopping or interrupting a transmission and/or "intercepting" the content in the sense that the transmission is copied, recorded, read or listened to, without otherwise interfering with its passage from source to destination. Similarly, what was meant by the Member States who reported offences of "remaining in" a computer system is not very clear. There is some discussion of different responses concerning "interference" with data and computer systems, but this also could be explained more clearly. Interference with a computer system generally requires interference with its functions or operations, whereas "interference" with data could mean either alteration, deletion or damage to the data, or interference with access to the data or its transmission from source to legitimate user. If Member States were given a specific meaning it should be footnoted, and if not the text should qualify that responses may have been made based on different laws or interpretations.
4.2	p. 81	1st full paragraph ("This section…")	The term "primary source legislation" which is found in chapter 4 and other parts of the Draft Study should be defined.
Ch. 3 4.2 4.3 Ch. 5	throughout p.109 throughout throughout	Last paragraph	Canada agrees with the Draft Study including a review of human rights issues relating to cybercrime, including criminalization and enforcement, as human rights protections will be an important element of future IEG

Ch. 7	throughout		discussions. While Member States differ on what types of content should be criminalized and on the applicable human rights protections of expression or content, human rights issues also arise in contexts other than the criminalization of content (e.g. in discussing the privacy interests and the use of law enforcement techniques) and should also be explored. For example, the Draft Study makes numerous references to the need to "balance" privacy (and other values) against security, law enforcement or due process considerations. This characterization suggests a trade-off between interests is inevitable. Some states take the view that human rights and privacy interests complement security and law enforcement interests and they should be approached as mutually reinforcing objectives. It would be preferable to refer to the different considerations in a neutral way (i.e. the relationship between privacy and security) to avoid the implication that interests are necessarily competing.
5.2	p. 122	2nd paragraph ("While some of these…"), last sentence	It would be better to reference the actor that must address the issues identified rather than the powers. It should read "In addition, police must be able to address challenges…".
5.2	p.123	2nd para. ("During information gathering…")	This paragraph discusses legal frameworks, and clear definitions, but does not mention the difficulties inherent in defining terms such as for example "data at rest" and "data in transit". This paragraph could be improved by adding a reference to these difficulties, such as "It should be noted however that defining these terms in a constantly evolving technological environment, in a way that is both clear and resilient in the face of change, can pose a significant challenge."
5.2	p. 127	*Preservation of computer data*	This section would benefit from a quick introduction on what is meant by data preservation. The intro paragraph in this section refers to storing computer data, but clarity could be brought to clearly distinguish data preservation from data retention.
5.2	p.128	Last paragraph ("As discussed in Chapter 1…"), last sentence	Suggest adding the following at the end to clarify the meaning: "…obtaining electronic evidence that achieves the goal of obtaining necessary evidence in a way that is less disruptive for legitimate business activity and more efficient for law enforcement."
5.2	p. 129	First paragraph ("In many	The sentence is not clear. As an IP address is identifying information, the procedural challenges should be more fully

		countries…"), 3rd sentence	explained.
5.2	p. 131	1st paragraph ("privacy and investigations…")	The first paragraph refers to "compelling a service provider, within its existing technical capability, to collect or record computer data, or to co-operate and assist authorities to do so". The text should reflect that in some states, there is no such requirement and that other states require the creation of such a capability, whether pursuant to a multilateral instrument or domestic legislation.
5.3	p.135		The sentence that reads: "While the often covert and/or electronic surveillance nature of cybercrime investigative techniques may raise particular privacy challenges, it is important to remember that the proportionality requirements of privacy rights apply equally to 'simple' search and seizure measures" is based on European law/treaty obligations. As this is a UN Study applicable beyond just the European context, it may be important to consider that the proportionality requirement may not be applicable to all responding countries. The same concern arises with the sentence "Procedural law limits and safeguards must therefore reflect the varying intrusiveness of investigative measures - ensuring that each measure is only used as necessary in a democratic society", necessity being a requirement in European law.
5.3	p. 140	Footnote 101	This footnote refers to *R. v. Ward* 2012 ONCA 660, a decision that is not a leading case in this area. This reference should be deleted.
Ch. 7	p.206	1st full paragraph	Text should be added to discuss the practice of seeking the preservation of electronic evidence (noted in the table on p. 198) as the preservation of electronic evidence can assist the investigation of some cybercrime cases.
7.1	p. 184	1st paragraph ("The starting point…")	Canada recommends adding the following to the first paragraph: The starting point for state jurisdiction and international cooperation is sovereignty. The sovereign equality of states is protected by rules of customary public international law. These include the obligation on states not to *'interfere in any form or for any reason whatsoever in the internal and external affairs of other States.'*9 In the context of

			cybercrime, this is important because territorial sovereignty is the basis of the rule of law in general, as well as the enactment and enforcement of laws respecting criminal offences, law enforcement and other powers, and human rights and other safeguards. Extraterritorial intrusions may weaken the rule of law, and risk circumventing human rights and other safeguards, all of which rely on domestic laws of the territorial State for enforcement. This is the basis of distinction between principles of international and domestic law governing the exercises of *prescriptive jurisdiction* (the power to enact offences and procedural laws), *adjudicative jurisdiction* (the authority to hear and decide cases with foreign elements if the parties and evidence are before the Court) and *enforcement jurisdiction*, also called "executive jurisdiction" (the authority to apply, enforce and administer legal and other rules).* Elements of adjudicative and enforcement jurisdiction are sometimes described as overlapping or intertwined in the sense that court orders must be enforced to take effect or the power to try criminal cases usually requires the presence of the accused within the territorial jurisdiction of the court and enforcement powers can then be applied to compel appearance and impose sentencing and other orders during and as a result of the trial. The critical difference in cybercrime and other transnational criminal investigations is that any sort of extraterritorial investigative actions are considered exercises of executive or enforcement jurisdiction, especially if they involve an element of intrusion or coercion that would engage criminal offences, human rights protections or other substantive or procedural laws of the State in whose territory they take place. *Prominent authorities that can be cited for this proposition include Akehurst, M. "Jurisdiction in International Law" (1974) 46 *British Yearbook of Int'l Law*, pp.145-257, and Crawford, J.,, *Brownlie's Principles of International Law* (8th ed., 2012), chapter 21 and (on exclusivity of enforcement jurisdiction) Simma, B. and Müller, A.T. "Exercise and Limits of Jurisdiction", chapt.6 of Crawford, J. and Koskenniemi, M., (eds.), *Cambridge Companion to International Law*, Cambridge, 2012, pp.134-57 at p.150.
7.1	p. 184	3rd paragraph ("Law enforcement and criminal…")	The text could clarify the relevant principle of customary law rather than being stated as an opinion of the drafters. The following revision and elaboration is proposed: Law enforcement and criminal justice matters fall

			within this exclusive domain of the sovereign (territorial) state – with the result that, traditionally, criminal *jurisdiction* has been linked to geographical territory. ~~States must therefore refrain from bringing pressure to bear on other states regarding the behaviour of specific national bodies, such as law enforcement agencies or the judiciary.10~~ Territorial exclusivity generally extends to the enactment of criminal law and the administration of criminal justice as elements of each State's constitutional rule of law framework, bearing in mind that States can and do assert prescriptive jurisdiction to address transnational or extraterritorial offences where their national interests are seen as sufficiently engaged. They also engage in diplomatic efforts to influence criminal justice policy in areas such as the establishment of cybercrime offences and the allocation of prosecutorial or law enforcement resources or priorities. Interference with rule of law functions, such as the independent decision-making of prosecutors or judges, however, would generally be regarded as unacceptable intrusions on sovereignty. The basic principle of customary law insofar as executive or enforcement actions outside of diplomatic channels are concerned is that no enforcement can be carried out without the consent of the territorial State. Persons may not be arrested…** ** The authority given (footnote 11) for exclusivity of enforcement jurisdiction could also be updated. The same text in the most recent (8th) edition of Brownlie is at: Crawford, J.,, *Brownlie's Principles of International Law* (8th ed., 2012), chapter 21, pp.478-79.
7.1	p. 185	The table ("Principle of territoriality")	Objective territoriality includes where an element of an offence, or element of an offence that has a "real and substantial connection" with the territorial state, takes place within the territorial state. This is not the same as scenarios where a wholly-extraterritorial offence has effects in the State that seeks to prosecute. As the "effects doctrine" is discussed as a separate issue in the subsequent point, Canada suggests deleting the reference to effects from the first point.

7.1	p. 187	1st paragraph ("An evolving alternative…), 2nd sentence	The sentence asserts that traditional mutual legal assistance typically requires lengthy verification of the validity of the request – including with respect to which the object of the request is an offence under the domestic law of the requested state (e.g., dual criminality). While dual criminality is generally a feature of extradition agreements, dual criminality is not as consistent a feature under MLA and is generally discouraged unless the domestic criminal law of the requested state makes it a requirement. The footnoted reference used in support of this assertion is Article 18(9) of the UNTOC which allows dual criminality to be used as a ground of refusal but it not a mandatory ground of refusal and the text of the provision makes it clear that MLA can still be provided at the discretion of the requested state even in the absence of dual criminality. Canada recommends that the sentence simply be deleted as it is not necessary for the paragraph to be complete.
7.2	p. 191	2nd paragraph ("Country responses…), last sentence	The statement that "Respondent countries often reported that if the crime is committed *entirely* outside of the country, with no effects within the territory, then criminalization and prosecution can be particularly challenging." is puzzling and may require some explanation. If a cybercrime offence is committed entirely outside of a country and has no effects there, why would that country *want* jurisdiction to prosecute the case? One response might be States whose nationals committed a cybercrime from another country against a third country, and having returned, cannot be extradited for constitutional reasons, but in that scenario there seems no obvious reason why the challenges of criminalising or prosecuting the cybercrime offences would be more challenging than the exercise of nationality based jurisdiction over any other offence.
7.2	p. 193	2nd paragraph ("Finally, some countries…"), first sentence	The first sentence requires clarification. In our view questions of "territoriality" deal with physical location and the application of domestic laws, whereas "nationality" is an attribute that attaches to natural and in some systems legal persons, wherever they are. These are conceptually distinct and the distinction is important. Nationality may affect *jurisdiction*, or at least the willingness of some States to assert jurisdiction and prosecute cases, but this may be more likely to be a matter of prosecutorial discretion than of jurisdictional law. In Canada's view customary law vests comprehensive prescriptive, adjudicative and enforcement jurisdiction over all persons, things and events within a

			State's territory. The *Vienna Convention of Diplomatic Relations*, for example, makes clear that diplomatic privileges and immunities are a bar to the *exercise* of jurisdiction and not to the existence of jurisdiction *simpliciter*.
7.2	p. 193	2nd paragraph ("Finally, some countries…"), 2nd sentence	The reference to an "extraterritorial perpetrator" should be clarified. Territorial jurisdiction to adjudicate an offence depends on where the offence takes place, not where the offender is located, either at the time or later on. If an offender commits an offence in a State's territory, then the state would have clear jurisdiction, and if other States are involved, usually the strongest claim. It does not make a difference whether the offender was outside of that territory when the offence was committed or he or she fled there afterward, these being merely questions of whether the other States involved will cooperate with mutual legal assistance and extradition and not jurisdictional constraints.
7.3	p. 202	3rd paragraph ("Use of international…"), 5th sentence and 4th paragraph, 2nd and 3rd sentences	The text addressing dual criminality is inaccurate. The mutual legal assistance provisions of the Budapest Convention (e.g. Article 29(4)) refer to dual criminality where this is a requirement under the laws of the Contracting Party. The Convention does not itself impose a dual criminality requirement and is similar to other multilateral instruments which include mutual legal assistance requirements. The text should be clarified in this regard.
7.3	p. 203	3rd paragraph ("In addition, dual…")	"The Council of Europe Cybercrime Convention, for example, allows that States Parties can apply dual criminality requirements to requests for preservation of computer data" should more properly reflect article 29(4) of the *Budapest Convention.* The text should clarify that dual criminality is limited to those specific circumstances.
7.3	p. 204-5	p. 204, final paragraph ("The constraint of dual…") and p. 205, first paragraph ("While a number..")	The text notes the impediment posed by dual criminality as regards both extradition and MLA. Figure 7.6 supports this assertion as regards extradition – and dual criminal in extradition context is generally acceptable. However, the text should be clarified as there is no similar support for the assertion about mutual legal assistance.
7.4	p. 212	Last paragraph "*24/7*	The draft study states that "Perhaps unexpectedly, the most common requests reported to be received by 24/7 contact

		Contact…")	points were for identity or subscriber information, followed by requests for expedited preservation of data and supply of stored traffic data." It is not clear why these results are unexpected. These two words "Perhaps unexpectedly" should be deleted.
Chapter 8			"Information sharing" might mean different things to different people, therefore a definition would be useful; for example, depending on its usage in the document, it is not always clear if it includes aspects related to: o "intelligence" sharing on page 246; o sharing technical indicators of compromise; o general threat information sharing; and o if the sharing is manual, or automated.

Annex 3 – Changes relating to Citation of Sources			
Section	**Page**	**Paragraph**	**Comments**
	p. x		Chapters 1 and 2 of the Draft Study present a 'snapshot' in time as mentioned on page x. Canada is of the view that a caveat should be incorporated into the Draft Study to clearly indicate data was compiled as of a certain date and to recognize that while more up-to-date information may be available, it is not incorporated into the Draft Study.
	p. xviii, (and pp. 25 and 37)		A statistic (i.e., that almost 24 per cent of total global internet traffic is estimated to infringe copyright, with downloads of shared peer-to-peer (P2P) material particularly high in countries in Africa, South America, and Western and South Asia) is referenced several times before the source is cited on p. 37. The source should be put when first cited. Note also that it may be prudent to caveat this statistic as: • the study was commissioned by NBC Universal to analyse bandwidth usage across the internet with the specific aim of assessing how much of that usage infringed upon copyright; and • the results seem to be based on a limited sample that was significantly extrapolated in relation to the US market.
Chapter 1			Generally in Chapters 1 and 2, data is often unattributed and sources should be referenced.
1.1	p. 2	Diagram	The diagram is attributed to an ITU 2012 document. Such data derives from the ITU World Telecommunication/ICT Indicators database. It has been updated, on an annual basis since 1975. The site, which should be referenced, provides some of the caveats associated with particular data sets (See http://www.itu.int/en/ITU-D/Statistics/Pages/publications/wtid.aspx).
1.4	p. 20	Text Box	For the text box commenting on the INCB (illicit drug sales), the original INCB study on the use of ICTS for international narcotics trafficking should be cited. Cite to read: *Report of the International Narcotics Control Board for 2001* (United Nations publication, Sales No. E.02.XI.1, Part I. While the Draft Study is criminal law focused, it may be worth noting that drug matters are also dealt with by the World Health Organization in Geneva. A couple of sentences could be added at the beginning:

			Since the founding of the United Nations and convening of the Commission on Narcotic Drugs in 1949 there has been consensus that some aspects of national and global policy on narcotic and other drugs required a criminal law focus under the Commission and other aspects required a health-based approach under the World Health Organization. As it has become a vehicle for global commerce in the mid-1990s, the role of the Internet both in public health matters and the production of and trafficking in narcotic drugs and their precursor chemicals has paralleled its development and use in other areas. Since the mid-1990s, it has been increasingly used by drug traffickers…
Chapter 2			
2.2	pp. 26-28, 28-32	*Distribution of cybercrime acts and Prevalence and impact of cybercrime acts* e.g., footnote 10	The presentation of the actual survey data should be more precise if possible. References to "some countries" or "a number of countries" are important when summarising opinions expressed or positions taken, where the requirement is to give an accurate picture without taking a vote or pre-judging the direction of consensus. But in reporting what Member States actually said on the survey, more accurate information is needed, and the use of descriptions (e.g., "about 1/3" or percentages) should be provided. More footnotes are needed indicating the source of information cited. For example, does the statement "According to law enforcement perceptions…", last paragraph of p. 26 refer to law enforcement responses in the survey or some other sources? If sources include both the survey and the literature review, the text should so state and whether all of the sources that could be found agreed or not is important.
2.2	p. 38	Figure 2.13	It is not clear what methods, if any, were used to account for virtual private networks (which allow IP addresses to appear to be coming from another state) in the creation of this data. Such services could artificially inflate or deflate the numbers represented here and state actors are clearly not the source of this data.
2.3	pp. 40-43	*Typical offender profiles* (pp. 40-43) and *Child pornography perpetrators* (pp. 43-44)	Results from the Member State survey should be incorporated. If the data is inconclusive, the fact that they were inconclusive would be relevant as it would suggest a need for better research and tabulation.

Chapter 3			
3.3	p. 67	1st full paragraph	The Report states "Founding states have the advantage of influencing the content of the treaty, yet may face certain costs in the process of treaty negotiation and drafting. Accession to treaties at a later stage avoids such costs but offers limited opportunities for renegotiation of treaty obligations and content. In so far as treaties are often concluded by states with similar preferences, treaties may not be acceptable to states that were not involved in negotiations, even if the treaty is left open for accession." Although the inclusion of academic sources is important, using a single source to draw this conclusion is not appropriate. Additional sources and the responses of Members States, if any, should be referenced.
Chapter 4			
4.1	pp. 77-78		Some qualifying language should be added pointing out to readers that the conduct descriptions in the chapter (e.g., as listed in Fig 4.1 on p. 78) are the ones developed by UNODC and the IEG itself and set out in the survey questionnaire. A short footnote explaining how the categories and descriptions were developed might be of assistance to future users of the data.
Chapter 7			
7.3	p. 201	Final paragraph	The basis for the finding in the final paragraph is not clear, its source should be noted.

Annex 4 – Minor Errors (Typographical, etc.)			
Section	**Page**	**Paragraph**	**Comments**
3.1	p.53	1st full paragraph ("This breadth of areas…")	The reference to "laws on wiretapping" should be changed to "laws on electronic surveillance or investigation (e.g. "wiretapping")". The term "wiretapping" originates in mid-20th century US law and is still used in some countries with laws based on the US precedent. The term does not include the range of electronic investigative techniques and controls that have evolved since the 1980s expansion of the Internet.
	p. 134-137		• p.134, last paragraph, first sentence, typos: "A range of rights…including rights to liberty and security of the person, and rights to a fair trial." • p.136, first paragraph, first sentence, typo: "Nonetheless, computer data and electronic communications in these countries were reported to…" • p.136, fourth paragraph, first sentence, typo: "Reported safeguards….by the court or a prosecutor." • p.137, second paragraph, first sentence, typo: "The majority of countries….safeguards were built into primary…"
	p.100		The statement regarding child pornography "At the national level, over 80 per cent of countries responding to the Study questionnaire indicated that child pornography is a criminal offence" is unclear. It should either refer to specific conduct (e.g. that making or possessing child pornography is an offence) or be generalized (e.g. "…over 80 per cent of countries…had offences relating to child pornography…")
	p.118		The reference to desktop technologies for gaining access to mobile phone data could be misinterpreted as referring to remote searches. It could be clarified to read: In some countries, for example, local police stations have been routinely equipped with desktop technology for extracting data from mobile phones seized from arrested suspects.
5.2	p. 128	1st paragraph, 1st sentence	Suggest deleting the word "arguably". The text that follows does not make an argument that preservation is equally prejudicial to privacy as disclosure, only that there remains a privacy interest to be protected in the context of preservation. The view that disclosure is more invasive than preservation is not one that is highly disputed so as to merit the use of the word "arguably".
5.2	p. 128	2nd paragraph,	Suggest deleting "Nonetheless" and beginning with "Preservation of data…." as the preceding paragraph does not make an argument that

		1st sentence:	would justify "nonetheless" and its inclusion (as with "arguably") suggests a level of debate that is not indicated in the text, nor exists outside this text.
5.2	p. 128	2nd paragraph, last sentence	It is not clear from the sentence why the statement is made that the separation of the two obligations is a key element. The sentence could be amended perhaps to add "to ensure effectiveness" if this is consistent with the view of the academic cited in the footnote, or otherwise amended as appropriate to convey the justification for the statement
5.2	p.128	4th paragraph, second last sentence	Recommend it be amended to read: "The use of coercive measures…are impractical…" i.e. delete the word "unfeasible" and replace it with "impractical" as it would be more accurate to state that the volume and disruption concerns render it impractical.
	p.129	2nd paragraph, 5th sentence	The sentence that begins: "The existence of such investigative powers alone…" contains what appears to be a typo at the end: "…would not otherwise so process." it should perhaps be: "…would not otherwise so possess."
	p.130	last paragraph, 2nd last sentence	The sentence reads: "This distinction relates, not least, to differences…" Recommend deleting "not least" as it begs the question, what else? and is not needed.
5.2	p. 131	Footnote 59	The reference should be to Article 21 (interception of content data), and not Article 20.
	p. 147	1st paragraph, last sentence	Suggest the beginning of the sentence be reworded: "In addition, many private sector policies are publicly available…" (currently reads "polices")
	p. 198	1st paragraph	In the last part of the sentence, the scope of the international cooperation provisions is described as either "biting" on the offences themselves and/or having wider scope. The term "bite" is not very clear and it is suggested this phrase be reworded.
	p. 201	Last sentence	The reference to "unwritten rules" should be clarified.
	p. 203		The text incorrectly reference Article 28(4) in footnote 126 and it should read Article 29(4).
	p. 210	1st paragraph, 2nd last sentence	A new term, "focal point", is used and repeated frequently in the pages that follow. All previous references in this section (section 7.4) had been to "contact points". It is unclear if these are intended to be "interchangeable" terms or not. Suggest staying with the term contact point throughout, or defining both terms.