October, 2009

LAW ENFORCEMENT DUE DILIGENCE RECOMMENDATIONS FOR ICANN - SEOUL

Summary of due diligence recommendations for ICANN to adopt in accrediting registrars and registries and proposed amendments to the RAA, supported by international law enforcement.

Introduction: Below is a summary of due diligence recommendations for ICANN to adopt in accrediting registrars and registries and proposed amendments to the Registrar Accreditation Agreement (RAA), supported by the following international law enforcement agencies:

- Australian Federal Police;
- Department of Justice (US);
- Federal Bureau of Investigation (US);
- New Zealand Police;
- Royal Canadian Mounted Police;
- Serious Organised Crime Agency (UK)

The recommendations are considered to be required in order to aid the prevention and disruption of efforts to exploit domain registration procedures by Criminal Groups for criminal purposes. The proposed amendments take account of existing EU, US, Canadian and Australian legislation and those countries commitment to preserving the individual's rights to privacy.

1) Due Diligence

a. ICANN should perform due diligence investigations on all Registrars and Registries upon accreditation and periodically thereafter;
b. The RAA should require Registrars to collect accurate and complete data of all Registrants upon domain name registration and periodically thereafter, in which the Registrar will validate to ensure such Registrant data is accurate and complete.

2) WHOIS

In accordance with the ICANN's 2006 JPA Affirmation of Responsibilities, and the 2009 Affirmation of Commitments, all gTLD domain name WHOIS information must be accurate, detailed and public. Although LE does not support the use of proxy/privacy registrations, the LE agencies urge ICANN to exercise the following on proxy/privacy registrations:

a. The proxy/privacy registrant is a private individual using the domain name for non-commercial purposes only, and ;
b. The proxy/privacy registration service has been accredited by ICANN using the same due diligence process as a Registrar/Registry, and
c. Information from the WHOIS database can be provided to law enforcement authorities when the information will assist in the prevention, detection, investigation prosecution or punishment of criminal offences or breaches of laws imposing penalties, or when authorised or required by law.

3) Transparency and Accountability

a. ICANN should require all domain name resellers and all third party beneficiaries to be held to the same terms and conditions and due diligence requirements as Registrars and Registries;
b. ICANN should require all registrars, registries, proxy services, resellers and all third party beneficiaries of any contracts, policies of ICANN to publicly display ownership, parent companies, subsidiaries and business associations.

Conclusion: The international law enforcement community views the above-referenced recommendations as vital in preventing crimes involving the DNS. The law enforcement community has consulted with the Registrar and Registry community in preparing this document. It is imperative that law enforcement and ICANN work together to ensure a safe and secure Internet.

Law Enforcement Recommended RAA Amendments and ICANN Due Diligence

Detailed Version

Introduction: Below are: 1) suggested amendments to the RAA and; 2) due diligence recommendations for ICANN to adopt in accrediting registrars and registries. Both are supported by the following international law enforcement agencies:

- Australian Federal Police;
- Department of Justice (US);
- Federal Bureau of Investigation (US);
- New Zealand Police;
- Royal Canadian Mounted Police;
- Serious Organised Crime Agency (UK)

The amendments are considered to be required in order to aid the prevention and disruption of efforts to exploit domain registration procedures by Criminal Groups for criminal purposes. The proposed amendments take account of existing EU, US, Canadian and Australian legislation and those countries commitment to preserving individual's rights to privacy. These amendments would maintain these protections whilst facilitating effective investigation of Internet related crime.

I. Proposed Amendments to the RAA (May 21, 2009 version)

1) The RAA should not explicitly condone or encourage the use of Proxy Registrations or Privacy Services, as it appears in paragraphs 3.4.1 and 3.12.4. This goes directly against the Joint Project Agreement (JPA) ICANN signed with the United States Department of Commerce on September 25, 2006 which specifically states "*ICANN shall continue to enforce existing (Whois) policy*", i.e., totally open and public WHOIS, and the September 30, 2009, Affirmation of Commitments, paragraph 9.3.1 which states "*ICANN implement measures to maintain timely, unrestricted and public access to accurate and complete WHOIS information, including registrant, technical, billing, and administrative contact information*." Lastly, proxy and privacy registrations contravene the 2007 GAC Principles on WHOIS.

   If there are proxy and/or privacy domain name registrations, the following is recommended concerning their use:

a. Registrars are to accept proxy/privacy registrations only from ICANN accredited Proxy Registration Services;[13]

b. Registrants using privacy/proxy registration services will have authentic WHOIS information immediately published by the Registrar when registrant is found to be violating terms of service, including but not limited to the use of false data, fraudulent use, spamming and/or criminal activity.

2) To RAA paragraph 5.3.2.1, language should be added to the effect "or knowingly and/or through gross negligence permit criminal activity in the registration of domain names or provision of domain name WHOIS information…"

3) All Accredited Registrars must submit to ICANN accurate and verifiable contact details of their main operational and physical office location, including country, phone number (with international prefix), street address, city, and region, to be publicly disclosed in ICANN web directory. Address must also be posted clearly on the Registrar's main website. Post Office boxes, incorporation addresses, mail-drop, and mail-forwarding locations will not be acceptable. In addition, Registrar must submit URL and location of Port 43 WHOIS server.

4) Registrars must publicly display of the name of CEO, President, and/or other responsible officer(s).

5) Registrars with multiple accreditations must disclose and publicly display on their website parent ownership or corporate relationship, i.e., identify controlling interests.

6) Registrar must notify ICANN immediately of the following and concurrently update Registrar website:

a. any and all changes to a Registrar's location;
b. changes to presiding officer(s);
c. bankruptcy filing;
d. change of ownership;
e. criminal convictions ;
f. legal/civil actions

[13] ICANN to implement accreditation system for Proxy Services using the same stringent checks and assurances as provided in these points, to ensure that all proxy services used are traceable and can supply correct details of registrant to relevant authorities.

7) Registrar should be legal entity within the country of operation, and should provide ICANN with official certification of business registration or license.

8) Resellers must be held completely accountable to ALL provisions of the RAA. Registrars must contractually obligate all its Resellers to comply and enforce all RAA provisions. The Registrar will be held directly liable for any breach of the RAA a Reseller commits in which the Registrar does not remediate immediately. All Registrar resellers and third-party beneficiaries should be listed and reported to ICANN who shall maintain accurate and updated records.

9) Registrars and all associated third-party beneficiaries to Registrars are required to collect and securely maintain the following data[14]:

(i) Source IP address

(ii) HTTP Request Headers

(a) From

(b) Accept

(c) Accept-Encoding

(d) Accept-Language

(e) User-Agent

(f) Referrer

(g) Authorization

(h) Charge-To

(i) If-Modified-Since

(iii) Collect and store the following data from registrants:

(a) First Name:

(b) Last Name:

[14] Anti-Phishing Working Group (AGWG) "Anti-Phishing Best Practices Recommendations for Registrars", October 2008

(c) E-mail Address:

(d) Alternate E-mail address

(e) Company Name:

(f) Position:

(g) Address 1:

(h) Address 2:

(i) City:

(j) Country:

(k) State:

(l) Enter State:

(m) Zip:

(n) Phone Number:

(o) Additional Phone:

(p) Fax:

(q) Alternative Contact First Name:

(r) Alternative Contact Last Name:

(s) Alternative Contact E-mail:

(t) Alternative Contact Phone:

(iv) Collect data on all additional add-on services purchased during the registration process.

(v) All financial transactions, including, but not limited to credit card, payment information.

10) Each registrar is required to validate the following data upon receipt from a registrant[15]:

(1) Technical Data

(a) IP addresses used to register domain names.

(b) E-mail Address

(i) Verify that registration e-mail address(es) are valid.

(2) Billing Data

(a) Validate billing data based on the payment card industry (PCI standards), at a minimum, the latest version of the PCI Data Security Standard (DSS).

(3) Contact Data

(a) Validate data is being provided by a human by using some anti-automatic form submission technology (such as dynamic imaging) to ensure registrations are done by humans.

(b) Validate current address WHOIS data and correlate with in-house fraudulent data for domain contact information and registrant's IP address.

(4) Phone Numbers

[15] Anti-Phishing Working Group (AGWG) "Anti-Phishing Best Practices Recommendations for Registrars", October 2008

(i) Confirm that point of contact phone numbers are valid using an automated system.
(ii) (ii) Cross validate the phone number area code with the provided address and credit card billing address.

11) Registrar must provide abuse contact information, including the SSAC SAC 038 recommendations below[16]:

- Registrars must prominently publish abuse contact information on their website and WHOIS.

1. The registrar identified in the sponsoring registrar field of a Whois entry should have an abuse contact listed prominently on its web page. To assist the community in locating this page, registrars should use uniform naming convention to facilitate (automated and rapid) discovery of this page, i.e., http://www.<registar>.<TLD>/abuse.html.
2. Registrars should provide ICANN with their abuse contact information and ICANN should publish this information at http://www.internic.net/regist.html.

- The information a registrar publishes for the abuse point of contact should be consistent with contact details currently proposed as an amendment to Section 3.16 of the RAA. Each contact method (telephone, email, postal address) should reach an individual at the Registrar who will be able to promptly and competently attend to an abuse claim; for example, no contact should intentionally reject postal or email submissions.

- Registrars should provide complainants with a well-defined, auditable way to track abuse complaints (e.g. a ticketing or similar tracking system).

12) ICANN should require Registrars to have a Service Level Agreement for their Port 43 servers.

[16] ICANN SSAC SAC 038: Registrar Abuse Point of Contact, 25 February 2009

II. Proposed ICANN Due Diligence on current and new gTLD Registrars and Registries

a. ICANN to conduct enhanced due diligence on all Registrars and Registries (including but not limited to owners, officers, board of directors) ICANN accredits, or has accredited, to include, but not limited to:

- criminal checks;
- credit checks;
- financial history and solvency;
- corporate/company structure and ownership.

For example: Dunn and Bradstreet, Lexis-Nexis, Clear, World-Check, etc.

b. Such due diligence shall be documented by ICANN, in detail, in a written report that can be provided upon request to appropriate auditors.

c. ICANN should provide complainants with well-defined and auditable way to track complaints against Registrars and Registries.

i. ICANN should publish annual detailed reports of reported complaints.

d. ICANN should conduct WHOIS compliance audits , at least once a year, and publish results on:

i. Port 43
ii. WHOIS accuracy

Governmental Advisory Committee
Chairman

ICANN

Mr. Peter Dengate Thrush
Chairman of the Board
ICANN

Paris, 12 April 2010

Re: LEA RAA Amendment/Due Diligence Proposals

Dear Peter,

As per the GAC Nairobi Communiqué, I am very pleased to forward statements of support for the "Law Enforcement Due Diligence Recommendations for ICANN" proposals developed by law enforcement agencies from Australia, Canada, New Zealand, the UK and the U.S. for due diligence on accredited registrars and amendments to the Registrar Accreditation Agreement (RAA) from the Interpol Working Party on IT Crime-Europe and the G8 Lyon-Roma Group's High Tech Crime Subgroup. As you will recall, the law enforcement proposals were shared with the GAC, the ICANN Board and broader ICANN community, including the RAA Working Group under the Generic Names Supporting Organization (GNSO), during the October 2009 ICANN meeting in Seoul, Korea.

Also attached are recommendations developed by the participants in the Council of Europe (COE) Octopus Interface Conference, held March 23-25, 2010 as part of the COE Project on Cybercrime. These recommendations include a specific reference the law enforcement proposals noted above. It is notable that all three documents urge ICANN to implement the law enforcement recommendations.

The GNSO Council Chair, Chuck Gomes, is copied on this letter to ensure that the attached statements are circulated to the GNSO RAA Working Group. The GAC expects that these proposals, and the attached statements of support, will be thoroughly examined and taken into consideration by ICANN.

I anticipate that many GAC members will be joined by their law enforcement colleagues from capitals at the Brussels meeting in June 2010, and have no doubt that those law enforcement representatives present at the Brussels meeting will make themselves available to discuss their proposals further and to answer any outstanding questions.

Yours sincerely

Janis Karklins
Chairman of the Governmental Advisory Committee,
Ambassador of Latvia to France

Cc: Mr. Chuck Gomes, GNSO Council Chair

Attachments:
Interpol Working Party on IT Crime-Europe Statement
G8 Lyon-Roma Group High Tech Crime Subgroup Statement
Council of Europe Project on Cybercrime, "Messages from the Octopus Conference"

ICANN Governmental Advisory Committee; GAC Secretariat
1016, Electronics Niketan, 6 CGO Complex, Lodi Road, New Delhi, – 110 003, India
Telephone: +91 11 2430 1116. *Fax*: +91 11 2436 3126 *E-mail*: gacsec@gac.icann.org
Website: http://www.gac.icann.org

ICANN
Governmental Advisory Committee

Nairobi, 10 March 2010

GAC Communiqué – Nairobi

I. INTRODUCTION

The Governmental Advisory Committee (GAC) of the Internet Corporation for Assigned Names and Numbers (ICANN) met in Nairobi, during March 6 - 10, 2010.

36 members and 3 observers participated in the meeting, whereas 2 members participated remotely.

The Governmental Advisory Committee expresses utmost gratitude to the Communications Commission of Kenya (CCK) and Kenya Network Information Centre (KENIC) for hosting the meeting in Nairobi and thanks ICANN for supporting the GAC meeting.

II. IDN ccTLD

After discussions with ccNSO, the GAC adopted "GAC Interim Principles on IDN ccTLDs" (Annex A) as a contribution to the ongoing policy development process.

III. New gTLDs

The GAC is grateful to receive updates on progress with the new gTLDs initiative, in particular with regard to the root scaling studies being undertaken and the Special Trade Mark Issues Review Team recommendations currently out for public consultation.

The GAC discussed a number of outstanding issues which it believes require resolution before the gTLD program should be launched. The Chair of the GAC sent the GAC comments on the Draft Applicant Guidebook v3 to the Chair of ICANN Board (Annex B) and the GAC is looking forward to the ongoing dialogue.

The GAC reiterates "the need to explore track differentiation between categories" as indicated in its Seoul communiqué. The Nairobi meeting has also revealed growing awareness in the community of the importance of further exploring this approach. The GAC therefore welcomes the proposal for the creation of a cross-community group to explore this topic and to report on it at the latest one month before the Brussels meeting.

The GAC appreciates the exchange of views on these issues with the GNSO.

IV. EoI

The mandatory nature of the currently proposed Expression of Interest (EOI) model turns it into a slot reservation step and not a mere data-gathering exercise as initially intended and presented. Opening slot reservation and conferring certain rights to the participants against payment of a fee would constitute a *de facto* launch of the new gTLD application process. Should the Board intend to use an EOI mechanism as proposed, the GAC, after interaction

with the rest of the community, formally advises the Board to launch it only after the overarching issues have been resolved and the Draft Applicant Guidebook (DAG) finalized.

In that context, the GAC questions the benefits of pursuing further a separate EOI process, which could distract attention and resources from finalizing the new gTLD program. The GAC believes that public forum comments on the EOI and face-to-face discussions in Nairobi have helped identify ideas and concerns that can usefully inform the development of DAG v4, on which the community should focus.

V. Morality and public order issues

The GAC continues to have concerns regarding the procedures outlined in DAG v3 for objections on the basis of morality and public order. The GAC questions the appropriateness of the phrase "morality and public order" and is unclear how the proposed mechanism would work in practice. The GAC believes this item should not be listed on the "closed items" list with respect to the new gTLD process and requests a more detailed briefing from the ICANN staff on the anticipated practical implementation of the approach.

VI. Law enforcement Due Diligence Recommendations

The GAC received an update from law enforcement representatives on domain name abuse and their proposals to mitigate the negative effects of such abuse on consumers, including through further amendments to the Registrar Accreditation Agreement (RAA).

The GAC is aware that these proposals have been favorably reviewed by the high tech crime experts in the G8 and Interpol and will forward their statements of support to the Board separately. These law enforcement RAA amendment proposals will also be shared with the GNSO RAA working group. The GAC expects that these proposals will be thoroughly examined and taken into consideration.

VII. Security and Stability issues

The GAC welcomes the update by ICANN staff regarding ICANN Strategic Initiatives for Security, Stability and Resiliency as well as the SSAC update on root scaling issues.

The GAC welcomes information about the "Global DNS-CERT Business Case" and the initiative to launch a global strategy concerning the medium-long term planning about security of the DNS presented in the recently published documents "Proposed Initiatives for Improved DNS Security and Resiliency".

Concerning the DNS CERT, the GAC recommends that ICANN informs the relevant GAC Representatives about its consultations with national and regional CERTs and is concerned about possible duplication of efforts.

The GAC notes progress on the analysis of the factors that provoke the expansion of the root zone file.

In the context of scaling the root, the increasing adoption of DNSSEC will be the major factor; an important milestone will be July 2010 with the anticipated signing of the root going live.

In particular the GAC notes that, in the context of the root scaling issue, "anycast" related questions have been identified as an additional element to be considered.

Furthermore, the GAC notes that, in the context of IDNs, the concept of "variants" requires further clarification.

The GAC finally notes that, in order to take a position on the technical limits to the number of new gTLDs that can be added over a certain time, SSAC needs further analysis with the actors involved.

VIII. Board/ GAC Joint Working Group on the Review of the Role of the GAC at ICANN

The Board /GAC Joint Working Group (JWG) met at the Nairobi meeting. The Working Group discussed provision of GAC advice to the Board; the role of GAC liaisons; travel support to GAC members from developing countries and secretariat support for the GAC.

In particular, the JWG agreed that further consideration of the nature of GAC advice to Board, and its treatment once it has been generated, would assist the JWG in making any recommendations for improvements.

The JWG aims at finalizing its report at the Brussels meeting.

The GAC discussed various models for a secretariat where independence and sustainability would be fundamental considerations. A "hybrid" model, the details of which need to be refined – where a secretariat would be co-funded by governments and ICANN - was viewed as the most promising way forward. At the meeting The Netherlands, Brazil and Norway committed to contribute to fund such a hybrid model, if adopted, for an initial period of 5 years. The proposal will be worked on further inter-sessionally and a detailed proposal will be presented at the Brussels meeting with the purpose of seeking GAC approval.

IX. GAC Operating Principles

The GAC adopted amendments to the Article IX of the Operating Principles (Annex C).

The GAC decided to engage in further revisions of its Operating Principles as a consequence of the work of the GAC/Board Joint Working Group and in this regard is considering the establishment of an ad hoc Group in the near future.

* * * *

The GAC warmly thanks all those among the ICANN community who have contributed to the dialogue with the GAC in Nairobi.

The next GAC meeting will take place during the period of the ICANN meeting in Brussels, Belgium.

G8 Lyon-Roma Group
High Tech Crime Subgroup

In October 2009, a series of recommendations for amendments to ICANN's Registrar Accreditation Agreement (RAA) was proposed to ICANN by law enforcement agencies from the US, UK, Canada, Australia and New Zealand.

The principle aim of these proposals is to implement stronger controls around domain name registration and to ensure a mandatory and rigorous regulatory framework to govern ICANN's contracts with domain registrars. They include requirements for effective due diligence on accredited registrars, controls to ensure more accurate WHOIS information and availability for Law Enforcement, in addition to improved transparency around domain name resellers and third party beneficiaries.

The recommendations are considered to be necessary to aid the prevention and disruption of efforts to exploit domain registration procedures for criminal purposes. The international law enforcement community views these recommendations as vital in preventing crimes involving the Domain Name System.

The G8 High Technology Crime Subgroup (HTCSG), which comprises representatives from law enforcement, justice departments and other governmental bodies of the G8 countries, is in support of these recommendations and recommends their implementation.

International Criminal Police Organization
Organización Internacional de Policía Criminal

Organisation internationale de police criminelle
المنظمة الدولية للشرطة الجنائية

INTERPOL

200, quai Charles de Gaulle
69006 LYON - FRANCE
Telephone : +33 4 72 44 70 00
Facsimile : + 33 4 72 44 71 63
http://www.interpol.int

General Secretariat
Secrétariat général
Secretaría General
الأمانة العامة

26 March 2010

Subject:
Law Enforcement Due Diligence Recommendations for ICANN

In October 2009, a series of recommendations for amendments to ICANN's Registrar Accreditation Agreement (RAA) was proposed to ICANN by law enforcement agencies from the US, UK, Canada, Australia and New Zealand.

The principle aim of these proposals is to implement stronger controls around domain name registration and to ensure a mandatory and rigorous regulatory framework to govern ICANN's contracts with domain registrars. They include requirements for effective due diligence on accredited registrars, controls to ensure more accurate WHOIS information and availability for Law Enforcement, in addition to improved transparency around domain name resellers and third party beneficiaries.

The recommendations are considered to be necessary to aid the prevention and disruption of efforts to exploit domain registration procedures for criminal purposes. The international law enforcement community views these recommendations as vital in preventing crimes involving the Domain Name System.

The Interpol Working Party on IT Crime - Europe, which comprises representatives from law enforcement bodies of 15 European countries, is in support of these recommendations and recommends their implementation.

Wolfgang Schreiber
Chairperson
Interpol Working Party
on IT Crime – Europe

Project on Cybercrime
www.coe.int/cybercrime

COUNCIL OF EUROPE CONSEIL DE L'EUROPE

Octopus Interface conference
Cooperation against cybercrime
23 – 25 March 2010
Council of Europe, Strasbourg, France

25 March 10/provisional

Messages from the Octopus conference

More than 300 cybercrime experts representing countries from all continents, international organisations and the private sector met at the Council of Europe in Strasbourg from 23 to 25 March 2010 to enhance their cooperation against cybercrime. At the close of the conference participants adopted key messages aimed a guiding further action.

Participants share a common interest in pursuing the most effective approaches against the growing threat of cybercrime that societies worldwide are faced with.

Effective approaches against cybercrime comprise a wide range of innovative initiatives and actions that need to be pursued in a dynamic and pragmatic manner by public and private sector stakeholders.

At the same time, measures against cybercrime are a shared responsibility and should be based on a set of common principles to allow for clear guidance to governments and organisations, to facilitate partnerships and to ensure the political commitment to cooperate.

In this connection, participants in the conference underline that:

- For security and the protection of rights to reinforce each other, measures against cybercrime must follow principles of human rights and the rule of law.
- Security and the protection of rights is the responsibility of both public authorities and private sector organisations.
- Broadest possible implementation of existing tools and instruments will have the most effective impact on cybercrime in the most efficient manner.

Following detailed discussions, participants recommend:

- Making decision makers aware of the risks of cybercrime and encouraging them to exercise their responsibility. Indicators of political commitment include steps towards the adoption of legislation and institution building, effective international cooperation and allocation of the necessary resources.
- Implementation of the Budapest Convention on Cybercrime worldwide to sustain legislative reforms already underway in a large number of countries. Countries should consider becoming parties to make use of the international cooperation provisions of this treaty. Consensus on this treaty as a common framework of reference helps mobilise resources and create partnerships among public and private sector organisations. In this connection, the ratification of the Budapest Convention by Azerbaijan, Montenegro and Portugal prior and during the conference, and the expression of interest to accede by Argentina and other countries serve as examples to other countries.
- Establishing the Budapest Convention as the global standard goes hand in hand with strengthening the Cybercrime Convention Committee (T-CY) as a forum for information-sharing network, policy-making and standard-setting. It is encouraged to address issues

not (exhaustively) regulated by the provisions of the Cybercrime Convention such as electronic evidence, jurisdiction and liability of ISP's.

- Coherent and systematic training of law enforcement, prosecutors and judges based on good practices, concepts and materials already available.
- The establishment and strengthening of high-tech crime and cybercrime units, and incidents response and reporting teams and systems.
- The development of cooperation procedures between law enforcement agencies, CERTs/CSIRTs as well as internet service providers and the IT industry.
- Due diligence by ICANN, registrars and registries and accurate WHOIS information. Endorsement of the "Law Enforcement Recommended Amendments to ICANN's Registrar Accreditation Agreement (RAA) and Due Diligence Recommendations" in line with data protection standards. ICANN is encouraged to implement these recommendations without delay.
- The many networks and initiatives against cybercrime that exist already create a dynamic and innovative environment involving a wide range of actors. Stronger networking among networks is encouraged to allow for synergies and reduce duplication. The mapping of networks exercise initiated by the Council of Europe should be continued.
- A contact list for enhanced cooperation between industry and law enforcement should be established. A proposal for a secure portal for interest parties is in preparation.
- Initiatives aimed at preventing, protecting and prosecuting the sexual exploitation and abuse of children are most valuable but require stronger support and consistency. The "Lanzarote" Convention of the Council of Europe (CETS 201) offers guidance in this respect and provides benchmarks to determine progress.
- Making use of the guidelines for law enforcement – ISP cooperation adopted at the Octopus Conference in 2008.
- Completion and broad dissemination of the results by the Council of Europe of the typology study on criminal money flows on the Internet that is currently underway.
- In order to meet the law enforcement and privacy challenges related to cloud computing existing instruments on international cooperation – such as the Data Protection Convention (CETS 108) and the Budapest Convention – need to be applied more widely and efficiently. Additional international standards on law enforcement access to data stored in the "clouds" may need to be considered. Globally trusted privacy and data protection standards and policies addressing those issues need to be put in place and the Council of Europe is encouraged to continue addressing these issues in its standard-setting activities as well as by the Global Project on Cybercrime.

Public authorities, international organisations, civil society (including non-governmental organisations) and the private sector should apply existing tools and instrument without delay and cooperate with each other to identify additional measures and responses to emerging threats and challenges.

In order to add impetus and resources to efforts against cybercrime and allow societies worldwide to make best possible use of tools, instruments, good practices and initiatives already available, a global action plan aimed at obtaining a clear picture of criminal justice capacities and pressing needs, mobilising resources and providing support, and assessing progress made should be launched, preferably by the United Nations and the Council of Europe in partnership with the European Union, Parties to the Budapest Convention, and other interested parties.

The results of the Octopus conference should be submitted to the United Nations Crime Congress in Salvador, Brazil (12-19 April 2010) for consideration.
