Version 16 Feb 2012

# The Budapest Convention on Cybercrime 10 years on:

# Lessons learnt or the web is a web[1]

**Alexander Seger[2]**

The 10th anniversary of the Budapest Convention on Cybercrime was the focus of the Council of Europe's annual Octopus Conference on Cooperation against Cybercrime in Strasbourg from 21 to 23 November 2011. [3]

The presentations and debates during that event and the lessons learnt since this treaty was opened for signature in Budapest on 23 November 2001 provide valuable insights not only with respect to the functioning of this specific Convention, but with regard to international cooperation against cybercrime in general.

Having been involved in the promotion and implementation of this treaty from 2002 onwards, I am offering here my views on what the Budapest Convention is all about, on key achievements ten years on, on lessons learnt and on the need to weave a web of responses to challenges on the web.[4]

## ABOUT THE BUDAPEST CONVENTION

The Budapest Convention basically requires state parties to this treaty to do the following:

- To establish specific types of conduct as criminal offences in domestic legislation. This includes offences against computer data and systems, that is, the so-called offences against the "confidentiality, integrity and availability" of computers, such as illegal access, data and system interference and others. In addition to these "c-i-a" offences, it includes offences by means of computers. However, as any crime these days may involve computer systems, the Budapest Convention focuses on the criminalization of specific conduct that acquires a new quality or scope when committed through computers. Thus, it stipulates the criminalization of computer-related forgery and fraud, of child pornography and of intellectual property related offences.

- To provide criminal justice authorities with effective means for investigations through procedural law tools such as search and seizure, expedited preservation of volatile data, interception of communications and others. It is important to note that these investigative means are to apply to the evidence on computer systems related to any criminal offence and not only for offences against and by means of computers. This gives the Convention a very broad scope. Article 15 requires Parties to establish conditions and safeguards to limit and prevent abuse of law enforcement powers and to protect human rights.[5]

---

[1] Based on the presentation made in Session IV (New national and international legal responses to cybercrime) at the International Conference on Cybercrime: Global Phenomenon and its Challenges organized by ISPAC/CNPDS/Courmayeur Foundation/UNODC/KIC in Courmayeur Mont Blanc, Italy, 2-4 December 2011.

[2] Head of Data Protection and Cybercrime Division, Council of Europe. The views are those of the author and do not necessarily reflect official positions of the Council of Europe. Feedback is welcome to Alexander.seger@coe.int

[3] For presentations, videos and other materials see www.coe.octopus

[4] As an interested party, I do not claim my views to be "scientific".

[5] For a discussion on article 15 see:
http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/Octopus2011/2467_SafeguardsRep_v16_8nov11.pdf
For an overview of Internet case-law of the European Court of Human Rights see:
http://www.echr.coe.int/NR/rdonlyres/E3B11782-7E42-418B-AC04-A29BEDC0400F/0/RAPPORT_RECHERCHE_Internet_Freedom_Expression_EN.pdf

– To engage in efficient international cooperation through a combination of urgent provisional measures (such as expedited preservation), and police and judicial cooperation.

Cybercrime is thus understood as offences against and by means of computers. It is also understood that any crime may involve electronic evidence and that this needs to be addressed in procedural law.[6]

The Budapest Convention is a criminal justice treaty that establishes criminal law measures based on rule of law and human rights principles. While measures against cybercrime certainly contribute to national security and to cybersecurity, and while international cooperation against cybercrime based on this treaty can contribute to confidence and trust between states and de-escalate incidents of cross-border cyberattacks, the Budapest Convention is not an agreement aimed at the politico-military dimension of international relations and it is not a cybersecurity treaty.[7]

The Budapest Convention does serve as a guideline and many countries have used it as a "model law" when preparing domestic legislation. Unlike other "model laws", however, it is a negotiated and formally adopted international agreement and thus also a legal framework for cooperation between state parties.

The Convention is scalable in terms of membership. It is true that it has been prepared by the member states of the Council of Europe.[8] However, Canada, Japan, South Africa and the USA participated in it negotiations. The treaty is open for accession by any country that is prepared to fully implement it and cooperate with other parties. Eight states have been invited to accede so far.[9]

It is also scalable in terms of content. In 2003, a Protocol on Xenophobia and Racism committed through computer systems was adopted. In February 2012, the Cybercrime Convention Committee (T-CY) began work on a solution to transborder access to data within the context of cloud computing. This may result in another protocol to the Convention or a soft-law guideline. Implementation of the Budapest Convention in conjunction with other instruments allows addressing challenges such as the sexual exploitation and abuse of children on the Internet, the terrorist use of the Internet, criminal money flows and money laundering on the Internet,[10] the need to protect privacy and personal data, and others.

The Budapest Convention can be backed up or complemented by additional tools, guidelines and good practices. In recent years, the Council of Europe began to weave a web of tools around the Convention, such as on law enforcement/service provider cooperation[11], on judicial training[12], on law enforcement training strategies[13], on cybercrime strategies[14], on criminal money flows, and on

[6] This has practical consequences for crime prevention and criminal justice policies and strategies: all law enforcement, prosecutors and judges need to have at least basic training in matters related to cybercrime and electronic evidence.
[7] For a distinction between cybercrime and cybersecurity strategies see: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079_cy_strats_rep_V20_14oct11.pdf
[8] Currently the Council of Europe has 47 member states (www.coe.int).
[9] By February 2012, Argentina, Australia, Chile, Costa Rica, Dominican Republic, Mexico, Philippines and Senegal.
[10] For example, on 16 February 2012, the Financial Action Task Force (FATF) published the revised consolidated 40 Recommendations. Recommendation 36 encourages accession to the Budapest Convention.
[11] http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/567_prov-d-guidelines_provisional2_3April2008_en.pdf
[12] http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Training/2079_train_concept_4_provisional_8oct09.pdf
[13] http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/Documents/Cyber%20IPA%20reports/2467_LEA_Training_Strategy_Fin1.pdf

specialized services.[15] In fact, training and materials developed by other organizations often take the Budapest Convention as the starting point as well.

The Budapest Convention is a mature treaty. By the time it was opened for signature in November 2001 it had been preceded by more than twelve years of preparatory work and precursors in the form of soft-law recommendations. The ten years that followed its adoption showed that it has proven to work, that due to its technology-neutral language it is still most relevant, and that with each new party it is becoming more effective.

## NOVEMBER 2001 – NOVEMBER 2011: KEY ACHIEVEMENTS

The adoption of the Budapest Convention is a major achievement in itself. Cybercrime has been around from the late 1970s, and from the late 1980s onwards work on computer crime and information security had been underway at the level of the OECD[16] and the Council of Europe.[17] However, until 2001 there had not been sufficient experience and pressure to negotiate a binding international agreement. I would argue that in 2001 the Council of Europe exploited a window of opportunity when finalizing and adopting a treaty as comprehensive as the Budapest Convention on Cybercrime. I also believe that that window closed soon afterwards. Ten years later, information and communication technology have become far too important for governments and societies and involve such a large number of stakeholders that it would seem very difficult to bring all interests under an international agreement of the scope and depth of the Budapest Convention.[18]

The approach of the Council of Europe and of the current state parties to the Budapest Convention of building on this treaty and gradually rolling it out across the globe seems to be more promising than trying to negotiate a new agreement.

Key achievements since it adoption in November 2001, can be summarized as follows:

- The Budapest Convention reinforced a process of legislative reform worldwide. This is particularly true since around 2006.[19] An inventory would suggest that such reforms have been carried out or are underway in at least 120 states. The Budapest Convention has served as a guideline to most of these countries.[20] The Convention thus facilitated a minimum of harmonization of legislation around the world.[21] The United Nations General Assembly[22]

---

[14] http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079_cy_strats_rep_V20_14oct11.pdf

[15] http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/Octopus2011/2467_HTCU_study_V30_9Nov11.pdf

[16] Leading in 1992 to the first version of the Guidelines for the Security of Information Systems http://www.oecd.org/dataoecd/16/22/15582260.pdf

[17] Leading in 1989 to Recommendation R(89)9 on Computer-related Crime https://wcd.coe.int/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet&InstranetImage=610660&SecMode=1&DocId=702280&Usage=2
And in 1995 to Recommendation R(95)13 on Problems of Criminal Procedure Law connected with Information Technology
https://wcd.coe.int/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet&InstranetImage=1900870&SecMode=1&DocId=528034&Usage=2

[18] Considering not only the interests of different governments (some want to control content and the internet infrastructure, others promote a free and open Internet and fundamental rights, some want to address not only cybercrime but also cyberwarfare and cyberterrorism, others want to address cybersecurity, etc.) but also the "Internet street" (see the mobilization of protest against the SOPA and PIPA proposals in the US Congress in January 2012 or against the Anti-Counterfeit Trade Agreement in many countries of Europe in February 2012 or against the law on blocking access to child abuse materials in Germany in 2010 which led to the abolishment of that law in 2011). Governments and politicians are likely to be reluctant to be seen promoting a new meaningful treaty on cybercrime.

[19] In 2006, the Council of Europe launched its Global Project on Cybercrime that assists countries in the implementation of the Budapest Convention.

[20] Which does not mean that all of them have implemented it in full.

[21] See for example the country profiles prepared under the Council of Europe's Global Project on Cybercrime http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/Documents/CountryProfiles/default_en.asp

recommended that UN member states use the Budapest Convention to "Ascertain whether your country has developed necessary legislation for the investigation and prosecution of cybercrime". This may further support harmonization.

- The treaty had a reach beyond Europe. 55 countries had ratified or signed it or been invited to accede, including 14 non-European countries. The Council of Europe engaged with at least another 55 countries in technical cooperation on the basis of the Budapest Convention.

- The Convention served as a catalyst for technical cooperation. Not only the Council of Europe, but also major donors such as the European Union now recognize that measures against cybercrime contribute to the rule of law and help countries make use of the development opportunities of information and communication technologies.

- In countries that have implemented the Budapest Convention an increase in criminal justice measures against cybercrime is noted.[23]

- Police-to-police and judicial cooperation increased considerably between many of the parties to the Budapest Convention. Ratification of this treaty by the United States of America in 2006 was essential in this respect. All parties now have functioning 24/7 points of contact in line with Article 35.

- The Budapest Convention has been one of the Council of Europe's main contributions to multi-stakeholder cooperation for Internet governance. This has been most visible during the Internet Governance Fora since 2006,[24] the European Dialogue on Internet Governance [25] or the Octopus Conferences since 2004.[26] Multi-stakeholder cooperation includes in particular public-private cooperation. The private sector has supported the implementation of the Budapest Convention.[27] Practical results included the guidelines on law enforcement/service provider cooperation in the investigation of cybercrime of 2008.[28]

- Governments have a positive obligation to protect people through effective laws and law enforcement measures, for example, by implementing the Budapest Convention as noted by the European Court of Human Rights.[29] Article 15 helps strike a fair balance between the need for effective law enforcement and procedural safeguards. The Convention is thus about "protecting you and your rights".[30]

---

Presentations at the Courmayeur Conference showed that also countries such as Iran based much of their law on the Budapest Convention or that China is using it as benchmark to identify gaps in domestic legislation.

[22] UN General Assembly Resolution 64/2011 of 17 March 2010 on Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical infrastructures.

[23] In Germany, for example, changes in legislation in line with Article 8 (computer-related fraud) of the Budapest Convention closed a gap in legislation. Computer-related fraud now accounts for the largest number of cases recorded by the police (27,292 in 2010).
http://www.bka.de/nn_193360/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrime__node.html?__nnn=true

[24] http://www.intgovforum.org/cms/

[25] http://www.eurodig.org/

[26] www.coe.int/cybercrime

[27] Microsoft in particular, but also McAfee and Visa Europe have been partners in project activities.

[28] http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/567_prov-d-guidelines_provisional2_3April2008_en.pdf

[29] See the case K.U. v.Finland
http://cmiskp.echr.coe.int/tkp197/view.asp?action=html&documentId=843777&portal=hbkm&source=externalbydocnumber&table=F69A27FD8FB86142BF01C1166DEA39864919
Regarding Article 15 see
http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/Octopus2011/2467_SafeguardsRep_v16_8nov11.pdf

[30] See Octopus conference 2011 – Outlook Panel 1
http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/cy_Octopus_Interface_2011/Presentations/default_en.asp

In short, during the first ten years of its existence, the Budapest Convention became an essential element of norms of behaviour for cyberspace.

## LEASONS LEARNT

Standards, norms and good practices to meet the challenge of cybercrime have been and are being developed by public and private sector and international organizations. The main problem is that while they are available they are not sufficiently implemented in all regions of the world. Widest possible implementation of existing standards such as the Budapest Convention and other tools would seem the most effective way ahead. Discussions at the 2010 United Nations Congress on Crime Prevention and Criminal Justice (Salvador, Brazil) clearly underlined the need for technical assistance for capacity building against cybercrime. [31]

The Budapest Convention de facto serves as the guideline or reference for cybercrime legislation worldwide, even in countries that for political reasons may not want to become parties.

In most countries, those responsible for legislation (ministries of justice, parliaments) and those responsible for criminal law measures (law enforcement, prosecutors, judges) see the benefits of this treaty. In some countries ministries of foreign affairs sometimes oppose it. The reasons brought forward concern less the substance of the treaty but the fact that their respective country did not participate in the negotiation of the Convention.[32] The historical fact that this treaty was prepared by the Council of Europe and not by the United Nations is difficult to correct retroactively. For some, this problem is that serious that it prevails over the benefits of urgent international cooperation against cybercrime and the practical and legal value of the treaty.

For many other countries, this is not a major obstacle. They consider it in their national interest to cooperate against cybercrime, and consider that the Budapest Convention offers an existing and functioning framework to that effect. They also recognize that once they are parties they will participate in the operation of the treaty and, as members of the Cybercrime Convention Committee, will participate in its further development, for example, through protocols. They acknowledge that the treaty has the support of a significant number of countries and organizations gathering a very large share of Internet users, of the Internet industry and of the ICT infrastructure worldwide. For them, these advantages outweigh the fact that they had not been involved in negotiating it.

The effectiveness of the treaty increases with each new party. However, ratification or accession to the Budapest Convention has been slower than expected. There are several explanations. The expectation is that by the time of ratification or accession, all provisions are reflected in domestic legislation. The treaty comprises a range of procedural law measures, which means that states not only need to amend their criminal codes but also their criminal procedure codes. It is legitimate that governments and parliaments take time to make such amendments. But this is not the only cause for slow implementation. Within the European Union, member states often attempt to combine the ratification of the Budapest Convention with implementation of European Union instruments, such as the 2005 Framework Decision on Attacks against Information Systems,[33] the Data Retention Directive of 2006[34] or the Directive on Attacks against Information Systems which is expected to be adopted in mid-2012.[35] This causes delays. There is a further important reason:

[31] http://www.unodc.org/unodc/en/crime-congress/12th-crime-congress-documents.html
While there was full consensus on the need for technical assistance, there was much disagreement on the need for a new treaty on cybercrime.
[32] An anecdote for illustration: at the UN Crime Congress in Salvador I mentioned to the head of delegation from a G77 country strongly opposed to the Budapest Convention, that the legislation of his country had been guided by this treaty. His reply was: "What do you mean guided? We copied it word by word!" To my question why then he opposed it, he answered: "you don't understand: it's political!"
[33] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32005F0222:EN:HTML
[34] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32006L0024:EN:HTML
[35] http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/10/463

for many decision-makers in governments and parliaments the question of cybercrime has simply not been high enough on their agenda. The 2007 attacks against Estonia and subsequent attacks against other states started to change this. It is expected that by the end of 2012 the number of parties will have increased significantly.[36] This will enhance the Budapest Convention as a framework for trusted international cooperation against cybercrime.

Measures against cybercrime must be designed to protect rule of law and human rights principles. This means full implementation of Article 15 Budapest Convention on safeguards and conditions for law enforcement powers but also effective measures to protect privacy and personal data. The protection of personal data has become a key challenge of information societies. It is noteworthy that in many countries data protection legislation is adopted in conjunction with cybercrime legislation. The Council of Europe's Data Protection Convention 108[37] is open for accession to third countries, and in 2011 Uruguay was the first non-member state invited to accede.

While the Budapest Convention in its present form meets most needs, new challenges have emerged in recent years. These include issues related to cloud computing and the question as to how law enforcement can access data not stored on a specific computer system of a suspect but stored "somewhere" in the clouds, that is, possibly in foreign jurisdictions. As indicated above, in January 2012, the Cybercrime Convention Committee started its work on transborder access and jurisdiction in view of proposing a solution in the form of a protocol to the Budapest Convention or soft-law instrument providing guidance.

Governments around the world expect international organizations to provide support and coherent solutions. International organizations should therefore cooperate closely with each other to serve societies and help them meet the challenge of cybercrime. The experience of recent years suggests that there is much room for improvement. The main issue seems to have been the question of whether or not there should be another international treaty on cybercrime or cybersecurity or information security. While reflections on this are likely to continue in the foreseeable future, different international organizations could start engaging in closer cooperation in an area where there already is full international consensus, namely that of capacity building.

The controversy about future "cyber treaties" is partly due a confusion of the concepts of cybercrime as a crime prevention and criminal justice concept and that of cybersecurity with critical information infrastructure and national security as primary rationale. Given the difficulty in coming to international agreements in such sensitive areas, a clarification of these two complementary but different concepts may help separate the issues into more manageable portions. For cybercrime prevention and criminal justice a solution already exists with the Budapest Convention. For the politico-military dimension of cybersecurity a different solution may need to be negotiated in the coming years, possibly in the form of principles of state behaviour in cyberspace as discussed for example by the OSCE[38] or in fora such as the London Conference on Cyberspace.[39]

In any case, a major lesson learnt during the past ten years, is that while international treaties are essential to helping societies meet the challenge of cybercrime, they are only one element in a web of responses.

---

This Directive will bring EU law more in line with the Budapest Convention.

[36] The EU's "Stockholm Programme – An open and secure Europe serving and protecting citizens" foresees that all EU member states will be have ratified by the end of 2012.
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:115:0001:01:EN:HTML

[37] http://www.conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=108&CM=8&DF=12/02/2012&CL=ENG

[38] http://www.osce.org/cio/77317

[39] http://www.fco.gov.uk/en/global-issues/london-conference-cyberspace/

## CONCLUSION: THE WEB IS A WEB

The World Wide Web, or more broadly the cyberspace of interconnected computer systems, is a web linking up a huge number of stakeholders, billions of users and increasingly every "thing".[40] It is a web with many nodes that changes day by day.

It offers unique opportunities and at the same time poses huge challenges; cybercrime and threats to cybersecurity are among them. It is a web of innovation, and this includes innovative responses to threats and challenges by public and private sector stakeholders and individuals.

As stated above, international treaties provide important frameworks. However, where cyberspace is dynamic and organic, international treaty making is usually slow, static and mechanical. A single, stand-alone international agreement cannot represent the sole regulatory response to security challenges in cyberspace.

An organic approach combining a range of measures is needed. Soft-law instruments or good practices may be more responsive to needs and be equally if not more influential than formal treaties. In short, we need to weave a web of responses to threats in cyberspace – a web with many nodes.

In such a web, the Budapest Convention is a node linked to crime prevention and criminal justice in general, to law enforcement capabilities and to many other rule of law as well as human rights issues. It is linked to regulations on data protection, child protection, terrorism prevention, anti-money laundering measures, organized crime treaties, telecom regulations, domestic legislation, consumer protection, codes of conduct, self-regulation, guidelines, good practices and many others. It is connected to cybersecurity which in turn is connected to national security but also social and economic development opportunities. And, importantly, it is connected to the many measures taken by the private sector, by governments and by other international organizations.

The strength and effectiveness of the Budapest Convention – and of all other responses for that matter – depends on the strengths of its connections with other nodes. I would maintain that the Budapest Convention has made an impact because it is part of an organic multi-stakeholder approach.

From such a perspective it would seem futile to focus on re-negotiating the same node again and again.

It would seem much more productive to build on what already exists, to engage in capacity building worldwide and to reinforce the links and synergies between multiple stakeholders and initiatives. In short: we should all cooperate in the weaving of a web of responses to cybercrime.

AS/February 2012

_____

[40] See the "Internet of Things"