In this issue
OSCE Confidence-Building Measures for Cyberspace

The EU Takes One Step Forward (And Then One Back) in Data Protection Reform

‘Montevideo Statement’ and ‘Global Government Surveillance Reform’: Responses to Government Surveillance Activities

October 2013 Focused on Global Cyber Security Awareness Activities

CoE Stepping up Global Action on Cybercrime

Interesting reads

Contact
publications@ccdcoe.org
www.ccdcoe.org

About
Given the cross-border nature of cyberspace, cyber security has become a relevant issue for everyone, whether from an international, regional or domestic perspective. In addition to Nation States, numerous international and regional organisations and other international entities have launched initiatives related to cyber security. Documents on cyber security have been issued, both in the form of non-binding instruments, such as declarations, recommendations, policies and strategies, and binding documents, such as conventions, directives, regulations and action plans. One way or another, all of these developments feed into (inter)national organisations’ and other stakeholders’ planning, strategy and capability development, as well as their cyber security investment analysis and decision-making; whilst for the wider audience, they reflect overall trends and the nature of national interests regarding cyber security.

Due to the growing number of entities active in cyber security, orientation within the flow of legal and policy documents can be challenging. Therefore, NATO CCD COE’s Cyber Security Status Watch project focuses on the work of international organisations, and brings together knowledge of all the relevant legal and policy instruments in order to improve overall awareness of international developments, and, most importantly, to serve as a central hub for easy access to the wide range of different legal and policy instruments that make up the contemporary domain of cyber security.

Cyber Security Status Watch will be updated quarterly, highlighting any recent international developments in the area of cyber security as well as new initiatives from international organisations.

The 2013 Q4 issue reports on Confidence-Building Measures for cyberspace, recently developed by the Organization for Security and Cooperation in Europe; gives a review of the developments in the European Union on data protection; notes private sector responses to government surveillance activities; and reports on the different cyber security awareness activities of international organisations and on recent Council of Europe initiatives aimed at countering cyber crime. This report also highlights some of the most relevant recent publications in the area of cyber security.
OSCE Confidence-Building Measures for Cyberspace

The OSCE Ministerial Council welcomed an initial set of Confidence-Building Measures aimed at reducing conflict stemming from the use of information and communication technologies.

The ministers of foreign affairs of the participating States of the Organization for Security and Cooperation in Europe (OSCE), at their 20th Ministerial Council, held on 5-6 December 2013 in Kiev, welcomed a set of Confidence-Building Measures (CBMs) for Cyberspace. The CBMs are laid down in Decision No. 1106, dated 3 December 2013, of the Permanent Council, the political decision-making body of the OSCE, comprising the ambassadors of the participating States. The CBMs aim to reduce conflict stemming from the use of information and communication technologies.

The activities of the OSCE with regard to cyber security in the past few years have mainly focussed on counter-terrorism, addressing the abuse of cyber means by terrorists. Lately it has started working on ‘Cyber CBMs’. The OSCE has a long tradition in the area of CBMs with regard to nuclear weapons. In 2012 the Parliamentary Assembly of the OSCE issued a Resolution calling for the OSCE to “organize an exchange of views and best practice on confidence- and security-building measures, including in the area of cyber security and counter-terrorism, with a view to exploring the possibility of building new OSCE commitments.” This Resolution initiated more concrete cyber security policies.

Decision No. 1106 of the Permanent Council of the OSCE, the “Initial set of OSCE Confidence–Building Measures to reduce the risks of conflict stemming from the use of information and communication technologies,” defines the measures the participating States agreed to take. In summary, the States:

- will, on a voluntary basis, provide national views on aspects of national and transnational threats to and in the use of ICTs, facilitate co-operation among the competent national bodies, exchange information in relation with the security of and in the use of ICTs, hold consultations in order to reduce the risks of misperception, and of the possible emergence of political or military tension or conflict that may stem from the use of ICTs, protect critical national and international ICT infrastructures, including their integrity, and share information on measures that they have taken to ensure an open, interoperable, secure and reliable Internet;
- will use the OSCE as a platform for dialogue, exchange of best practices, awareness-raising and information on capacity-building with regard to the security of and in the use of ICTs, including effective responses to related threats, and further explore the role of the OSCE in this regard;
- are encouraged to have in place national legislation to facilitate on a voluntary basis bilateral co-operation and

---

1 See OSCE website: http://www.osce.org/event/mc_2013
information exchange between competent authorities, including law enforcement agencies, in order to counter terrorist or criminal use of ICTs;

- will voluntarily share information on their national organisation, strategies, policies and programmes, including information about co-operation between the public and the private sector relevant to the security of and in the use of ICTs;

- will nominate a contact point to facilitate pertinent communications and dialogue on the security of and in the use of ICTs, voluntarily provide contact data for existing official national structures that manage ICT-related incidents and co-ordinate responses to enable a direct dialogue, and facilitate interaction among responsible national bodies and experts.

- will, in order to reduce the risk of misunderstandings in the absence of agreed terminology and to further a continuing dialogue, as a first step, voluntarily provide a list of national terminology related to the security of and in the use of ICTs, accompanied by an explanation or definition of each term; and

- intend to conduct the first information exchange by October 31, 2014.

It is to be noted that most of the activities are to be undertaken on a voluntary basis. Russia has added an interpretative guidance that says that “the Russian Federation will be guided in its implementation by a firm commitment to the principles of non-interference in the internal affairs of States, their equality in the process of Internet governance and the sovereign right of States to Internet governance in their national information space, to international law and to the observance of fundamental human rights and freedoms.”

The EU Takes One Step Forward (And Then One Back) in Data Protection Reform

The European Commission initiated the data protection legislation reform in January 2012. Despite strong support from the Committee for Civil Liberties, Justice and Home Affairs (LIBE) of the European Parliament in October 2013, the Council of Ministers did not grant the reform proposals a green light in December 2013.

In order to modernise and harmonise the fragmented data protection standards across its Member States, the European Commission is in the process of reforming the current regulation aiming to substitute the Data Protection Directive 95/46/EC of 1995. The proposals focus on the draft text of the general Data Protection Regulation and on the Data Protection Directive for law enforcement situations. The Data Protection Regulation, once adopted, would establish a single pan-European set of rules that would be obligatory for all Member States, and will thus lose the need to interpret the data protections laws of all 28 countries.


For example, the proposals put forward include the new principle that both foreign and EU-based companies must adhere to the same set of rules, instead of the former application of stricter standards on EU businesses. For private citizens, the reform aims to protect individuals’ rights online more strongly, e.g. by putting more emphasis on the concepts of “the right to be forgotten” and “privacy by design”, allowing personal data to be transferred more easily between service providers, and making the meaning of “data subject’s consent” more explicit.6

The reform proposals have had to go through complex rounds of discussions in different EU institutions. After the positive vote from the Civil Liberties, Justice and Home Affairs (LIBE) of the European Parliament in October, where the voting results were seen as a strong sign of progress of the reform, the text moved on to the next round of discussions at the Council of Ministers. Despite high hopes for quick progress, the Council expressed its concerns about a number of aspects and called for reconsideration of the proposals.

**Issues discussed at the Council**

One of the main developments offered by the reform would be the creation of a single supervisory data protection authority for all companies, instead of the current practice, which has 28 different national data protection authorities. This solution has been labelled as the “one-stop-shop” and is designed to “bring simplicity and cost-savings to pan-European data controllers and processors”.7 However, in its current form and wording, it is opposed by a number of EU Member States, such as Germany.8

Also, despite an agreement having been reached by the LIBE of the European Parliament, the Member States are still discussing the form of the data protection framework (either a Directive or a Regulation) and the consolidation of the data protection supervisory powers into a single EU entity, especially with regard to the authority to order fines and penalties, as well as the more practical mechanisms for consumer redress.9 For example, it is feared that the one-stop-shop system may impose linguistic and financial barriers to those EU citizens whose data had been mishandled by a company based in another member state, and thus may discourage the citizens from going to court.10

There are no concrete signs on the expected date of adoption on the reform proposals. The European Commission has, however, expressed hope that “An agreement on the reform is possible before the end of this year”.11

---


9 “Progress falters on EU Data Protection Regulation at Council meeting,” supra note 10.


‘Montevideo Statement’ and ‘Global Government Surveillance Reform’: Responses to Government Surveillance Activities

Organisations responsible for the coordination of the Internet’s technical infrastructure, like ICANN, and major IT companies have expressed concerns about government surveillance activities in cyberspace.

The disclosure by former US National Security Agency (NSA) contractor Edward Snowden of large amounts of data resulting from surveillance activities by the NSA and the British Government Communications Headquarters (GCHQ) led to a worldwide debate about the legitimacy of these surveillance programs. The topic dominated the media headlines in the second half of 2013. The ‘Montevideo Statement’ and the ‘Global Government Surveillance Reform’ show that this issue is also on the agenda of the organisations that coordinate Internet infrastructure and some of the larger IT companies.

During their meeting in Montevideo, Uruguay, on 7 October 2013, the organisations responsible for the global coordination of the Internet’s technical infrastructure have discussed issues concerning the future of the Internet. The main player in this regard is ICANN, the Internet Corporation for Assigned Names and Numbers. One of the issues raised was the revelation of surveillance programmes by the US and British intelligence services. In what is called the ‘Montevideo Statement’, the organisations “expressed strong concern over the undermining of the trust and confidence of Internet users globally due to recent revelations of pervasive monitoring and surveillance.”12 Other issues that were discussed were “the importance of globally coherent Internet operations, the risk of Internet fragmentation at a national level, the need for Internet Governance and global multistakeholder Internet cooperation, further globalisation of ICANN and IANA functions and an environment in which all stakeholders, including governments, participate on an equal basis, and the transition to IPv6 as a top priority.”13

In parallel, a number of large IT companies and social media providers initiated the ‘Global Government Surveillance Reform.’14 AOL, Apple, Facebook, Google, LinkedIn, Microsoft, Twitter and Yahoo signed a statement in which they call upon governments “to limit 'government surveillance' of citizens and ensure free expression and privacy.” They list five principles: “(1) limiting governments’ authority to collect users’ information, (2) oversight and accountability, (3) transparency about government demands, (4) respecting the free flow of information, and (5) avoiding conflicts among governments.”

The US is currently reviewing its legislation concerning the activities of the NSA and other intelligence agencies.15

13 Id.
October 2013 Focused on Global Cyber Security Awareness Activities

Both the EU and the US have developed the tradition of celebrating Cyber Security Month every October. This year these activities coincided with events all around the world, including the campaign of the Singapore Cyber Security Awareness Alliance\(^\text{16}\) and the Asia Pacific Economic Cooperation Telecommunications and Information Working Group (APEC-TEL), Cyber Security Awareness Day.

October of 2013 witnessed several cyber security awareness activities around the world. One of the most prominent examples was the EU, which launched its Cyber Security Month (ECSM) that ran various events aimed at promoting cyber security education and the sharing of good practices in 27 participating countries. Some of the objectives of the ECSM 2013 were directly connected with recent legal and policy developments such as generating specific awareness of Network and Information Security (NIS) as addressed in the proposed EU NIS Directive, and enhancing attention and interest with regard to information security through political and media coordination.\(^\text{17}\)

The European Network and Information Security Agency (ENISA) has offered support for the ECSM through a number of publications. In 2011, ENISA conducted a feasibility study\(^\text{18}\) on the project. In October 2013, in coordination with global partners, the 12 mobile safety tips\(^\text{19}\) were announced. In December 2013, the Roadmap based on the results of the European Cyber Security Month\(^\text{20}\) was published, discussing the policy context, stakeholder model of engagement and the main achievements of ECSM, together with the country profiles of the participating EU Member States. As such, the Roadmap report introduces a model for a joint EU advocacy campaign which may serve as a useful example for other international and regional organisations.

In parallel, many other countries and organisations chose the month of October to underline the importance of cyber security awareness. For example, the US celebrated the 10th year of National Cyber Security Awareness Month,\(^\text{21}\) and the Asia Pacific Economic Cooperation Telecommunications and Information Working Group (APEC-TEL)\(^\text{22}\) held its 4th annual Cyber Security Awareness Day.

---

\(^\text{16}\) Singapore CS Awareness Alliance, read more at: [https://www.gosafeonline.sg/](https://www.gosafeonline.sg/)

\(^\text{17}\) About ECSM, read more at: [http://cybersecuritymonth.eu/whats-ecsm](http://cybersecuritymonth.eu/whats-ecsm)


CoE Stepping up Global Action on Cybercrime

The CoE is launching two three-year projects focusing on the fight against cybercrime.

Global Action on Cybercrime (GLACY)\(^{23}\) is a 36-month project funded by the EU and the CoE with the main aim to fight against organised crime. The project has a worldwide scope and focuses on supporting the countries that are prepared to implement the CoE Budapest Convention on Cybercrime. The specific objective of the project is to “enable criminal justice authorities to engage in international cooperation on cybercrime and electronic evidence on the basis of the Budapest Convention on Cybercrime”.\(^{24}\) The project has outlined an ambitious goal to have “up to 70 States participate in international efforts on cybercrime using the Budapest Convention as their common framework”.\(^{25}\)

Another CoE 36-month-long Octopus project is directed at the parties and observers of the CoE Convention of Cybercrime, as well as nations interested in joining the Convention. This project, to be launched in January 2014, focuses similarly to facilitating the implementation of the Convention and related instruments via organising the annual Octopus conference, supporting the Cybercrime Convention Committee (T-CY) and organising numerous events related to cybercrime.\(^{26}\)

Interesting reads

ENISA Publications

CoE publications
- Cybercrime Convention Committee (T-CY) Guidance Note #8 – ‘Obtaining subscriber information for an IP address used in a specific communication within a criminal investigation (draft for discussion) http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/TCY%202013/T-CY(2013)26_guidanceNote8_subscriber%20info_V10.pdf

---

\(^{25}\) GLACY, *ibid*.
\(^{26}\) CyberCrime@Octopus Project summary, available at: http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/CyberCrime@Octopus/3021_octo_summary_V7WEB.pdf