Parliamentary **Assembly**
**Assemblée** parlementaire

Parliamentary Assembly
Assemblée parlementaire
COUNCIL OF EUROPE CONSEIL DE L'EUROPE

**Doc. 11325**
26 June 2007

# How to prevent cybercrime against state institutions in member and observer states?

Report
Committee on Legal Affairs and Human Rights
Rapporteur: Mr Kimmo SASI, Finland, Group of the European People's Party

*Summary*

Cybercrime is a dangerous reality which has to be taken seriously at the highest level. It represents a real threat to states, whose technology-based infrastructures can be paralysed or even destroyed. This matter must be given the utmost priority.

The Parliamentary Assembly emphasises the importance and relevance of the Convention on Cybercrime (ETS No. 185) – the only binding legal instrument on this subject to date – and calls on all member and observer states of the Council of Europe to sign, ratify and implement its provisions without delay.

The Assembly notes that the fight against cybercrime requires international co-operation most urgently, as cyber criminals rely on being able to operate across borders and to exploit differences in national law.

Moreover, cyber attacks are not only a legal challenge; countries should develop policies and strategies to effectively protect their critical infrastructures, an undertaking which entails providing the necessary human, financial and technical resources for that purpose.

The Assembly eagerly awaits the findings of the Committee of Experts on Terrorism (CODEXTER), which is currently examining the question of whether gaps in existing instruments (including the Convention on Cybercrime) require the development of additional instruments, before addressing its recommendations to the Committee of Ministers.



F – 67075 Strasbourg Cedex, e-mail: assembly@coe.int
tel : + 33 3 88 41 2000, fax + 33 3 88 41 2776

## A. Draft resolution

1. The Parliamentary Assembly recalls its Opinion No. 226 (2001) in which it considered the fight against cybercrime to be a crucially important challenge in view of the obstacles which this form of crime may pose to the development of new technologies and, more generally, to legal and economic security.

2. The Assembly considers that cybercrime is a real threat to democracy, human rights, the rule of law, and that this issue should be treated as a matter of top priority.

3. Indeed, for the first time, criminal cyber attacks have targeted a State as a whole, attempting to paralyse the functioning of infrastructure vitally important to the Republic of Estonia. A few attacks have also been noted in other countries at the same time.

4. This shows that cybercrime is a dangerous reality which has to be taken seriously at the highest level and that it represents a real threat to states whose technology-based infrastructures can be paralysed or even destroyed.

5. As all states are vulnerable in the face of this danger; it is of utmost importance that an efficient protection and reaction system be developed at the international level.

6. The Assembly recalls that the Convention on Cybercrime, ETS No. 185 (hereinafter "the Convention"), contains extensive legislative provisions to counter cyber attacks against critical infrastructure. This treaty – the only binding one on this subject to date – has received widespread international support and therefore, in order to fight such crime effectively, all member states of the Council of Europe should urgently sign and ratify it and, more importantly, fully implement its provisions.

7. The Assembly deplores the fact that a large number of member states have not yet ratified this important Convention.

8. The Assembly notes that cybercrime requires international co-operation most urgently, as cyber criminals rely on being able to operate across borders and to exploit differences in national law. The lack of co-operation by member states exposes them to considerable danger.

9. The Assembly recalls that the Convention is an open treaty and therefore invites non member states to accede to it as soon as possible to reinforce international co-operation on this important subject.

10. In this context, the Assembly welcomes the various initiatives taken in order to enhance international co-operation and co-ordination in the fight against cybercrime, *inter alia* the 24/7 points of contact and "Check the web", and strongly encourages member states to continue to reinforce their efforts, to strengthen international co-operation and to support concrete co-ordinated measures for more efficient protection.

11. In so doing, the Assembly emphasises that measures to fight and to prevent cybercrime must be based on laws that fully respect human rights and civil liberties.

12. Furthermore, the relevant laws need to be standardised, or at least compatible with one another, to permit the required level of international co-operation.

13. Cyber attacks are not only a legal challenge; countries should develop policies and strategies to effectively protect their critical infrastructures, an undertaking which entails providing the necessary human, financial and technical resources for that purpose.

14. The Assembly consequently invites member and observer states to:

14.1. consider the question of fighting against and preventing cybercrimes as a matter of priority;

14.2. sign and ratify the Convention on Cybercrime and its Additional Protocol without delay, and fully implement them as soon as possible;

14.3. evaluate their respective legal frameworks to assess whether they provide appropriate sanctions, including provisions for cases of computer-based terrorist attacks, for cybercrime, and to amend their legislation if necessary, while fully respecting individual freedoms, in particular the freedoms of expression and information;

14.4. ensure that their relevant legislation is compatible with that of other states in order to facilitate international co-operation and exchange of information;

14.5. develop policies and strategies, on the basis of relevant technical studies, to effectively protect their critical infrastructures and to provide the necessary human, financial and technical resources for that purpose;

14.6. take effective national measures to prevent cybercrime activities.

15. While considering that the Convention should be regularly examined in the light of technological advances, the Assembly eagerly awaits the findings of the Committee of Experts on Terrorism (CODEXTER) – which is currently examining the question of whether gaps in existing instruments (including the Convention on Cybercrime) require the development of additional instruments – before addressing its recommendations to the Committee of Ministers.

## B. Explanatory memorandum by Mr Kimmo Sasi, rapporteur

**Contents**



* * *

### I. Introduction

1. On 25 June 2007, following the request by myself and others, the Bureau has decided to ask the Committee on Legal Affairs and Human Rights to prepare a report on "How to prevent cybercrime against state institutions in member states".

2. On the same day, the Committee appointed me Rapporteur.

3. I would like to outline, in a few sentences, the context for this initiative.

4. In the past few weeks, a member state of the Council of Europe – Estonia – has been subjected to extensive cyber-attacks[1]. These reached a peak on 8 and 9 May 2007. This has caused disruptions in the functioning of many Estonian data transmission networks and web pages of the public sector. The first attacks were launched against the web pages of state agencies (Government, ministries, Office of the President, Riigikogu, police, etc), but were later extended to mass media, internet environments, telecommunication companies, banks and other electronic infrastructures. The attacks were clearly malicious and there is reasonable cause to suspect that their launch shortly after the mass disorder in Tallinn at the end of April was not a coincidence.

5. As already stated in the letter from the Rapporteur and others[2], the feature that renders these attacks unique and particularly severe is the fact that for the first time a state is targeted as a whole, involving attempts to paralyse the functioning of vitally important infrastructure of the Republic of Estonia.

6. It seems that the bulk of the attacks originated from outside Estonia – at first mainly from Russia[3], but later also from various locations around the world. Mostly Russian-language internet sites have published explicit incitations and instructions for carrying out cyber-attacks. A few attacks have also been felt in other member states.

[1] These events gave rise to numbers of reactions. Although the European Network and Information Agency (ENISA) does not cover fighting cybercrime, since it is not within its mandate, the ENISA commented on the cyber attacks in Estonia:
http://www.enisa.europa.eu/pages/02_01_press_2007_05_24_ENISA_commenting_on_massive_cyber_attacks_in_Estonia.html

[2] See letter dated 22.05.2007 from Kimmo Sasi and others.

[3] See Herald Tribune, Estonia says cyber-assault may involve the Kremlin, 17.05.2007 at http://www.iht.com/articles/2007/05/17/news/estonia.php.

7. Cybercrime represents a threat to democracy, human rights, the rule of law, and, last but not least, security. Potential threats include cyber-terrorism, that is the shutting down of entire essential infrastructures or the use of computers as weapons – disabling critical systems or threatening whole populations.

8. The recent events in Estonia show that these are not only paranoid conjectures but have become reality. No state is safe in the face of such a danger; it is therefore of utmost importance that an efficient protection and reaction system be developed at the international level.

## II. Terms of reference

9. Cyberterrorism can target the internet (as was the case in Estonia), and/or be conducted by means of the internet. The attacks can consist in: cyber attacks aimed at disabling vital electronic systems *via* the internet; dissemination of illegal content; use of IT systems by terrorists or other criminal groups for communications and other logistical uses.

## III. The relevant existing instruments to fight against and prevent cybercrime

### *i. The Convention on Cybercrime (ETS No. 185)*

10. The Council of Europe Convention on Cybercrime (hereinafter "the Convention"), dated 23 November 2001, is the only binding and the most comprehensive international treaty on the subject to date. It entered into force in July 2004 and provides guidelines for all governments wishing to develop comprehensive legislation against cybercrime. It has been supplemented by an Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems (CETS No. 189).

11. The Convention on Cybercrime – in Section 1 on substantive criminal law – criminalises "data" (Article 4) and "system interference" (Article 5) which cover attacks against critical infrastructures. Countries may go beyond these provisions and be more specific in their national legislation if they so wish.

12. The Convention provides for the criminalisation of certain conduct (substantive criminal law) including illegal access, illegal interception, data interference, system interference, misuse of devices, computer-related forgery, computer related fraud, offences related to child pornography and offences related to infringements of copyright and related rights (Articles 2 to 10).

13. It also outlines procedural rules for the investigation of cybercrimes and other offences committed through computer systems (Articles 16 to 21).

14. The Convention also intends to foster effective international cooperation on the protection of society against cybercrime (Articles 29 to 35).

15. It is important to note that the scope of the procedural provisions covers all criminal offences committed by means of a computer system as well as covering the collecting of electronic evidence (see Article 14). These provisions therefore apply not only to conduct criminalized in accordance with the provisions of the Convention (Section 1) but also to all other acts criminalised under national law. These acts include terrorism, money laundering and other offences as long as computer systems (which include modern mobile telephones etc) are involved.

16. At its recent meeting (13-14 June 2007) the Cybercrime Convention Committee (T-CY), which holds periodic consultations of the Parties to the Convention, examined issues related to terrorism. Many participants felt, although the Convention does not specifically refer to those matters, that there was no need to have specific provisions dealing with terrorism. The Committee of Experts on Terrorism (CODEXTER) is also considering the question of whether gaps in existing instruments (including the Convention on Cybercrime) require the development of additional instruments.

### *ii. Other relevant legal instruments*

17. The Convention on the Prevention of Terrorism (ETS No. 196) requires states parties to criminalise, *inter alia*, public provocation to commit a terrorist offence, as well as terrorist recruitment and training. This covers the use of the internet, since the Convention does not specify by which means the dissemination must occur.

18. The EU Council Framework Decision on attacks against information systems[4], based on the Convention on Cybercrime, aims to strengthen criminal judicial cooperation on attacks against information systems by developing effective tools and procedures. The criminal offences punishable under the framework decision are: illegal access to information systems; illegal system interference (the intentional serious hindering or interruption of the functioning of an information system by inputting, transmitting, damaging, deleting, deteriorating, altering, suppressing or rendering inaccessible computer data); illegal data interference.

19. Cyberterrorism is also addressed in the EU Council Framework Decision on Combating Terrorism[5].

20. A number UN Conventions and Protocols against specific acts of terrorism could also be applied in the case of attacks committed *via* computer based manipulation or *via* email[6].

## IV. The relative weaknesses in the current protection system: for the countries to act

### *i. Insufficient number of ratifications of the Convention on Cybercrime*

21. The clearest weakness of the current international protection system against cybercrime is the low number of ratifications of the legal instruments.

22. Since it is clear that cybercrime requires coordinated action at the international level and harmonised legal provisions, only a full implementation of the relevant international legal instruments can provide a satisfactory and efficient answer to this threat.

23. The Convention on Cybercrime has been so far ratified by 21 countries (member States of the COE[7] and the USA)[8] and signed by another 22 (member states[9] as well as Canada, Japan and South

---

[4] See Council Framework Decision 2005/222/JHA of 24.02.2005 on attacks against information systems (OJ L 69/67 of 16.03.2005).

[5] See EU Council Framework Decision on Combating Terrorism of 13.06.2002, 2002/475/JHA, OJ L 164/3 of 22.06.2002; see Article 1 (d) : "*1. Each Member State shall take the necessary measures to ensure that the intentional acts referred to below in points (a) to (i), as defined as offences under national law, which, given their nature or context, may seriously damage a country or an international organisation where committed with the aim of:*
*- seriously intimidating a population, or*
*- unduly compelling a Government or international organisation to perform or abstain from performing any act, or*
*- seriously destabilising or destroying the fundamental political, constitutional, economic or social structures of a country or an international organisation,*
*shall be deemed to be terrorist offences:*
*(…)*
*(d) causing extensive destruction to a Government or public facility, a transport system, an infrastructure facility, **including an information system**, a fixed platform located on the continental shelf, a public place or private property likely to endanger human life or result in major economic loss;*" (emphasis added).

[6] For example, the Convention of Unlawful Seizure of Aircraft, the Convention for the Suppression of Unlawful Acts Against the Safety of civil Aviation, the Protocol for the Suppression of Unlawful Acts of Violence at Airports serving International Aviation, The Convention on the Prevention and Punishment of Crimes Against Internationally Protected Persons, The International Convention Against the Taking of Hostages, etc.

[7] Albania, Armenia, Bosnia and Herzegovina, Bulgaria, Croatia, Cyprus, Denmark, Estonia, Finland, France, Hungary, Iceland, Latvia, Lithuania, Netherlands, Norway, Romania, Slovenia, "the former Yugoslav Republic of Macedonia", Ukraine (as at 22.06.2007).

[8] Finland ratified in May 2007. Discussions with the Russian Federation are underway with regard to the interpretation of one particular Article so that the Russian Federation can also sign and ratify this treaty as soon as possible.

Africa). Costa Rica and Mexico have been invited to accede. Many other countries from around the world are reforming their legislation in line with the Convention (e.g. Argentina, Brazil, Costa Rica, Egypt, India, Mexico, Philippines).

24. The Assembly should call on member states which have not yet done so, to sign, ratify and implement this Convention, and its Additional Protocol, as soon as possible.

***ii. Need for a coordinated response to cybercrime***

25. The issue of Cybercrime is currently the subject of intensive discussion at the international level. On 11 and 12 June, the Octopus Interface Conference on Cybercrime[10], held in Strasbourg, dealt with:

- The identification of new cybercrime threats,
- The effectiveness of cybercrime legislation,
- Initiatives of other organisations and stakeholders,
- Public-private partnerships,
- International cooperation and the functioning of 24/7 points of contact[11].

26. The Convention on Cybercrime puts great emphasis on practical cooperation (see *inter alia* Article 35). As stated in the Preamble of the Convention, the fight against cybercrime requires "increased, rapid and well-functioning international co-operation in criminal matters"[12].

27. The German Presidency of the European Council has recently launched an initiative called "Check the web". It aims at taking resolute action against the use of the Internet by terrorist structures[13]. In this context, the Rapporteur would like to draw attention to Europol's future information portal which should become a real technical platform for information exchange among Member states.

28. Following the cyber attacks in Estonia, the European Commission also urged coordinated efforts against cybercrime at the international level[14]. Furthermore, at its meeting on 21 and 22 June 2007, the European Council called for the development of a policy framework in the field of the fight against cybercrime[15].

29. It is clear that cybercrime requires, more than other crimes, real and effective international cooperation. Efforts have been undertaken to strengthen this cooperation and need to be followed by concrete action. The harmonisation of relevant legislation must be one of the priorities, to ensure that there is no legislative hindrance to cooperation.

***iii. Need for "effective, proportionate and dissuasive sanctions"***

30. As required in Article 13 of the Convention on Cybercrime, the national legislations should provide for sanctions in cases involving attacks, including terrorist ones, against computer systems. The sanctions are to be "effective, proportionate and dissuasive".

31. The state parties are called on to broadly criminalise IT-based terrorist attacks, as well as attacks on other interests that depend on computers. It is worth noting that the Convention on

---

[9] Austria, Belgium, Czech Republic, Germany, Greece, Ireland, Italy, Luxembourg, Malta, Moldova, Montenegro, Poland, Portugal, Serbia, Slovakia, Spain, Sweden, Switzerland, United Kingdom (as at 22.06.2007).

[10] for further details see http://www.coe.int/t/dc/files/themes/cybercrime/default_en.asp.

[11] "24/7 network ": contact available on a 24 hours, 7 day-a-week basis.

[12] The European Convention on Mutual Assistance in Criminal Matters (ETS No.. 30) and its two additional protocols provide a legal framework for international cooperation but also include many possibilities for refusal to cooperate.

[13] See Council Conclusions on cooperation to combat terrorist use of the Internet (« Check the web »), 8457/3/07 REV 3, ENFOPOL 66, 29.05.2007.

[14] See http://www.infoworld.com/article/07/05/22/EC-urges-effort-against-cybercrime_1.html and Business Week, Brussels to wage war on Cybercrime, 23.05.2007 under :
http://www.businessweek.com/globalbiz/content/may2007/gb20070523_811592.htm?chan=globalbiz_europe+index+page_top+stories

[15] See the Presidency Conclusions of 21 and 22.06.2007, § 31,
http://www.consilium.europa.eu/ueDocs/cms_Data/docs/pressData/en/ec/94932.pdf.

Cybercrime does not require harm to property or human life and well-being as a precondition for imposing sanctions.

32. The Council Framework Decision also states that member states will have to create effective, proportionate and dissuasive criminal penalties for illegally accessing information systems, illegally interfering with systems and illegally interfering with data. The decision also requires that instigating, aiding and abetting as well as attempting to commit any of the above offences shall also be liable to punishment (Article 5).

33. Therefore, the Assembly should encourage member states to evaluate their respective legal frameworks in order to assess whether they provide appropriate sanctions for cybercrime, including provisions for cases of computer-based terrorist attacks, and to amend their legislation if necessary.

## V. Conclusions

34. Cooperation at the international level is the key element for the efficient protection and prevention of cybercrime. The response of only some member states is *per se* "destined to failure" since cyber criminals know no borders. The current and future efforts at the international level should concentrate on the prevention and repression of cybercrime *via* adequate and harmonised provisions in national legislations. This should of course be achieved while respecting civil liberties[16].

35. The Assembly's duty is to call on member states to make coordinated use of the existing instruments. Of course, given the very essence of cybercrime, a crime based on daily evolving technology, flexibility of response is absolutely necessary. The Convention on Cybercrime should therefore be examined regularly in order to assess whether it satisfactorily addresses new challenges resulting from technological advances.

36. Considering that the international protection provided by existing international instruments appears to be quite comprehensive, covering all serious cyber attacks, and since the Council of Europe's CODEXTER is currently examining possible gaps in the protection, the Assembly should at this stage refrain from recommending the drafting of an Additional Protocol to the Convention on Cybercrime and await the conclusions of the CODEXTER.

[16] See for example Weber and Saravia v Germany (Application No. 54934/00 of 29.06.2006) regarding the interception of telecommunications by the state authorities (especially § 95). This case is indirectly relevant, since the Court has not yet decided on a case directly concerning cybercrime. The case involves the provisions of the German Act of 13.08.1968 on Restrictions on the Secrecy of Mail, Post and Telecommunications; the applicant, who had several telephone messages intercepted, argues that her fundamental rights were disregarded. The main question is whether the government overstepped its bounds in monitoring certain data for the purposes of catching terrorists. One can consider that "telecommunications" also includes the internet, since it is most commonly defined as "the transmission of information, as words, sounds, or images, usually over great distances, in the form of electromagnetic signals, as by telegraph, telephone, radio or television." The Court also speaks in rather general terms about the "transmission of personal data" and does not specifically only refer to telephone communications. The Court held that there had been no violation of the Convention and declared the case inadmissible.

*Reporting committee*: Committee on Legal Affairs and Human Rights

*Reference to committee*: Request for an urgent debate, Reference No. 3365 of 25 June 2007

*Draft resolution* adopted unanimously by the Committee on 26 June 2007

*Members of the Committee*: Mr Dick **Marty** (Chairperson), Mr Erik **Jurgens**, Mr György Frunda, Mrs Herta Däubler-Gmelin (Vice-Chairpersons), Mr Athanasios **Alevras**, Mr Miguel Arias (alternate: Mr Miguel **Barceló Pérez**), Mrs Aneliya Atanasova, Mr Abdülkadir Ateş, Mr Jaume **Bartumeu Cassany**, Mrs Meritxell Batet, Mrs Soledad Becerril, Mrs Marie-Louise **Bemelmans-Videc**, Mr Erol Aslan Cebeci, Mrs Pia Christmas-Møller, Mrs Ingrīda **Circene**, Mrs Lydie Err, Mr Valeriy **Fedorov**, Mr Aniello Formisano, Mr Jean-Charles Gardetto, Mr József Gedei, Mr Stef Goris, Mr Valery Grebennikov, Mrs Carina Hägg, Mr Holger **Haibach**, Mrs Gultakin Hajiyeva, Mrs Karin Hakl, Mr Nick Harvey, Mr Andres **Herkel**, Mr Serhiy **Holovaty**, Mr Michel Hunault, Mr Rafael Huseynov, Mrs Fatme Ilyaz, Mr Kastriot Islami, Mr Željko Ivanji, Mrs Kateřina Jacques, Mr Karol Karski (alternate: Mrs Ewa **Tomaszewska**), Mr Hans Kaufmann, Mr András Kelemen, Mrs Kateřina Konečná, Mr Nikolay Kovalev (alternate: Mr Yuri **Sharandin**), Mr Jean-Pierre Kucheida, Mr Eduard Kukan, Mrs Darja **Lavtižar-Bebler**, Mr Andrzej Lepper (alternate: Mr Krzysztof **Lisek**), Mrs Sabine **Leutheusser-Schnarrenberger**, Mr Tony Lloyd, Mr Humfrey **Malins**, Mr Andrija Mandic, Mr Pietro Marcenaro, Mr Alberto Martins, Mr Andrew McIntosh, Mr Murat Mercan, Mrs Ilinka **Mitreva**, Mr Philippe Monfils, Mr João Bosco Mota Amaral, Mr Philippe Nachbar, Mrs Nino Nakashidzé, Mr Tomislav Nikolić, Ms Ann Ormonde, Mr Claudio Podeschi, Mr Ivan **Popescu**, Mrs Maria **Postoico**, Mrs Marietta **de Pourbaix-Lundin**, Mr Christos Pourgourides, Mr Jeffrey Pullicino Orlando, Mr Valeriy Pysarenko, Mr François Rochebloine, Mr Francesco Saverio Romano, Mr Armen Rustamyan, Mr Kimmo **Sasi**, Mr Ellert Schram, Mr Christoph **Strässer**, Mr Mihai Tudose, Mr Vasile Ioan Dănuț **Ungureanu**, Mr Øyvind **Vaksdal**, Mr Egidijus **Vareikis**, Mr Miltiadis **Varvitsiotis**, Mrs Renate **Wohlwend**, Mr Marco Zacchera, Mr Krysztof **Zaremba**, Mr Vladimir Zhirinovsky, Mr Miomir Žužul

N.B.: The names of the members who took part in the meeting are printed in **bold**

*Secretariat of the Committee*: Mr Drzemczewski, Mr Schirmer, Mrs Maffucci-Hugel, Ms Heurtin, Ms Schuetze-Reymann