Parliamentary Assembly
Assemblée parlementaire
https://pace.coe.int

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Resolution 1565 (2007)[1]

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

Parliamentary Assembly

1. The Parliamentary Assembly recalls its Opinion No. 226 (2001) on the draft convention on cybercrime 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 democratic stability and national security, and raises fundamental issues as regards the respect for human rights and the rule of law. Thus, this issue should be treated as a matter of top priority.

3. Politically-motivated attacks against military or government websites of a number of Council of Europe member and observer states are increasingly frequent and sophisticated. Indeed, for the first time, criminal cyber attacks have targeted a state as a whole, attempting to paralyse the functioning of infrastructure vital 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. This threat can emanate from private individuals, organised groups or states.

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 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 also recalls that the Council of Europe Convention on the Prevention of Terrorism (CETS No. 196) offers an additional instrument in the fight against cyberterrorism, as well as against the use of the Internet for terrorist purposes.

8. The Assembly deplores the fact that a large number of member and observer states have not yet ratified these important conventions.

9. The Assembly notes that the fight against cybercrime requires urgent international co-operation between governments, the private sector and non-governmental organisations, as cybercriminals rely on their ability to operate across borders and to exploit differences in national law. The lack of co-operation by the member states exposes them to considerable danger.

---

1. Assembly debate on 28 June 2007 (25th Sitting) (see Doc. 11325, report of the Committee on Legal Affairs and Human Rights, rapporteur: Mr Sasi; Doc. 11335, opinion of the Political Affairs Committee, rapporteur: Mr Agramunt; and Doc. 11333, opinion of the Committee on Economic Affairs and Development, rapporteur: Mrs Lilliehöök). Text adopted by the Assembly on 28 June 2007 (25th Sitting).

10. 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.

11. 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 the "Check the Web" programme, 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.

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

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

14. 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. In doing so, they should involve private actors, including computer, networking and software industries.

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

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

15.2. sign and ratify the Council of Europe Convention on the Prevention of Terrorism and the Convention on Cybercrime and its Additional Protocol concerning the Criminalisation of Acts of a Racist and Xenophobic Nature committed through Computer Systems (ETS No. 189) without delay, and fully implement them as soon as possible;

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

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

15.5. develop a framework for facilitating urgent political consultations and exchange of information, at all necessary levels of the countries concerned, in situations of extensive cyber attacks;

15.6. 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;

15.7. associate the private sector more closely, notably by building public-private partnerships for more effective and cross-sector international co-operation against cybercrime;

15.8. take effective national measures to prevent cybercrime activities;

15.9. give every assistance to the Government of Estonia in ensuring that a full and exhaustive investigation of the recent cyber attacks in that country is undertaken so as to inform future international efforts to combat cybercrime.

16. While considering that the convention should be regularly examined in the light of technological advances and new challenges, the Assembly awaits eagerly 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. The Assembly resolves to return to this matter as soon as possible.