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

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Resolution 2070 (2015)[1]

Increasing co-operation against cyberterrorism and other large-scale attacks on the Internet

Parliamentary Assembly

1. The Parliamentary Assembly is aware of the positive impact of this era of new information technologies on all aspects of modern societies and human life. However, besides these positive effects, new vulnerabilities in our societies have emerged through the growth of the Internet and other computer networks. The Assembly is alarmed by the number and magnitude of criminal attacks perpetrated in cyberspace over the past few years which have undermined public trust in technological development.

2. Deeply concerned by apparently politically motivated cyberattacks against a Polish airline and the German Parliament recently, against websites in Ukraine in the wake of the military conflict that started in 2014, against websites in Georgia in the wake of the war between Russia and Georgia in 2008, as well as against the web infrastructure in Estonia in 2007, the Assembly recalls its Resolution 1565 (2007) on how to prevent cybercrime against state institutions in member and observer states? and emphasises the urgency of reacting against such large-scale attacks and securing evidence in order to establish the origins, perpetrators and political instigators of those attacks.

3. The Council of Europe has set important international legal standards in this field though its Conventions on Mutual Assistance in Criminal Matters (ETS Nos. 30, 99 and 182), on the Suppression of Terrorism (ETS Nos. 90 and 190), on the Prevention of Terrorism (CETS No. 196) and on Cybercrime (ETS Nos. 185 and 189). Nevertheless, serious obstacles still hamper the investigation and prosecution of cyberoffences, particularly in the context of cross-border networks, and the sanctions provided for by national legislations are not always adequate. The Assembly therefore believes that further work is necessary at European and international levels in order to address adequately the challenges posed by cyberterrorism and other forms of large-scale attacks on and through computer systems, which threaten the national security, public safety or the economic well-being of States.

4. Having regard to the relevant European Union legislation, in particular the European Union Convention on Mutual Assistance in Criminal Matters between Member States, the Assembly emphasises the need to further develop international legal and practical aspects, including the following principles:

4.1. requests for mutual assistance should be executed by the requested State as soon as possible, taking as full account as possible of the deadlines indicated by the requesting State. If a request cannot be executed fully in accordance with the requirements of the requesting State, the authorities of the requested State should promptly indicate the estimated time needed for execution of the request and the conditions under which it might be possible to execute it;

4.2. each member State should ensure that systems of telecommunications services operated via a gateway on its territory, and which for the lawful interception of the communications of a subject present in another State are not directly accessible on the territory of the latter, may be made directly accessible for the lawful interception by the latter State through the intermediary of a designated service provider present on its territory. Such a procedure should be accompanied by safeguards against espionage by third States;

---

1. *Assembly debate* on 26 June 2015 (27th Sitting) (see Doc. 13802, report of the Committee on Culture, Science, Education and Media, rapporteur: Mr Hans Franken). *Text adopted by the Assembly* on 26 June 2015 (27th Sitting).
See also Recommendation 2077 (2015) .

4.3. member States should define a minimum level of criminalisation of large-scale cyberattacks, including aggravating circumstances of those attacks, as well as minimum standards for penalties for such attacks.

5. Although mutual legal assistance of law-enforcement authorities has to be improved and adapted with regard to technological developments, the Assembly is aware that other fundamental rights must not be compromised, in particular the right to protection of private life and personal data under Article 8 of the European Convention on Human Rights (ETS No. 5) and the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108).

6. Aware that certain services and infrastructure are critical for the national security, public safety or the economic well-being of States, the Assembly recommends that member States:

6.1. draw up Internet-independent emergency plans against cyberattacks on critical services and infrastructure, such as electricity services, gas and oil pipelines, power plants, waterworks, telecommunication networks, airports, railways, hospitals, fire brigades, security services and the military;

6.2. install technical security measures for the protection of critical services and infrastructure on their national territory, such as the creation of closed back-up computer systems and networks which can be used if open Internet connections are attacked or blocked;

6.3. conclude bilateral emergency agreements with neighbouring States, in order to ensure mutual assistance in case of a cyberattack on critical services or infrastructure;

6.4. establish an adequate legal framework for public–private co-operation in the defence against large-scale cyberattacks;

6.5. recognise that States are internationally responsible for taking all reasonable measures to prevent large-scale cyberattacks from being launched by persons under their jurisdiction or emanating from their national territory;

6.6. criminalise the production, distribution and use of malware which is intended to enable individuals to prepare or launch large-scale cyberattacks.

7. Providers of critical services or infrastructure should be obliged to immediately report any large-scale cyberattack on them to the competent law-enforcement authorities of the State where they have their registered seat, as well as of the State where the attack occurred. In addition, natural or legal persons should be made aware of how to report cyberattacks on them to their competent law-enforcement authorities.

8. Producers of hardware and software should immediately inform their customers if a systemic weakness is detected which allows large-scale cyberattacks, such as through botnets, electronic viruses or other malware.

9. Providers of cloud computing services should set up security measures to protect their cloud against attacks on its security and integrity which could lead to large-scale cyberattacks, such as botclouds.

10. Providers of public websites should ensure that their sites do not contain electronic viruses or other malware which could lead to large-scale cyberattacks. For this purpose, their webmasters should regularly apply technical devices to prevent such malware.

11. Producers and sellers of computers or software should regularly inform computer owners about their possibilities, and ultimate responsibility, for ensuring the technical safety of their computers when connecting them to the Internet or other public computer networks.

12. Member States should develop binding security standards for protection against large-scale cyberattacks, as well as the public certification of such standards, if possible at European or international level.

13. The Assembly invites the Secretary General of the Council of Europe to initiate and co-ordinate intergovernmental action of the Council of Europe, establish co-operation programmes with the information technology industry and Internet service providers, and ensure closer co-operation with the European Union and the United Nations in this field of utmost importance.