Parliamentary Assembly
Assemblée parlementaire
http://assembly.coe.int

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Doc.
12 March 2014

Improving user protection and security in cyberspace

Report[1]
Committee on Culture, Science, Education and Media
Rapporteur: Mr Axel E. FISCHER, Germany, Group of the European People's Party

A. Draft resolution[2]

1. The Parliamentary Assembly is concerned that the further development and exploitation of cyberspace is still taking place without an adequate protection of the rights and interests of the weakest stakeholder in this process: the individual user.

2. Users of online services have been alarmed by numerous intrusions into their personal data and correspondence by public authorities, commercial companies as well as private individuals. Widely publicised examples have been the interception of communication and the screening of user data through national security services in Europe and the USA, the professional data-mining of social online networks, the commercial profiling of users by online service providers through Internet access data and geo-localisation data, as well as the large-scale hacking into user accounts and passwords for fraudulent purposes.

3. The Assembly regrets that those attacks on the security and integrity of online and mobile communication services have deeply undermined the trust of users in cyber services. Therefore, the Assembly calls on all member and observer States to immediately launch, in co-operation with the Internet and online industry, a global initiative for improving user protection and security in cyberspace. The Internet has no national borders; therefore we must act together.

4. The Assembly therefore welcomes the Resolution on the right to privacy in the digital age, which was adopted by the United Nations General Assembly on 18 December 2013. The Assembly concurs that the same rights which people have offline must also be protected online, in particular the right to privacy as expressed in its Resolution 1843 (2011) on the protection of privacy and personal data on the Internet and online media.

5. Welcoming the Montevideo Statement on the Future of Internet Cooperation of 7 October 2013, the Assembly agrees that the globalisation of the Internet Corporation for Assigned Names and Numbers (ICANN) and its Internet Assigned Numbers Authority (IANA) must be accelerated, towards an environment in which all stakeholders, including governments, participate on an equal footing.

6. The Assembly recommends that all member and observer States ensure the effective implementation of the following principles:

6.1. everyone's private life, correspondence and personal data must be protected online; interception, surveillance, profiling and storage of user data by public authorities, commercial entities or private persons is only permissible where allowed by law in accordance with Article 8 of the European Convention on Human Rights (ETS No. 5); member States have a positive obligation to ensure adequate legal protection against the interception, surveillance, profiling and storage of user data; personal data archives must employ precautionary measures to protect their data base against data theft and abuse;

6.2. producers of access devices and online service providers should automatically apply encryption and conditional access technologies as well as tools against online viruses and automatic signs ("cookies"); special protection should be afforded by providers of wireless access points ("hotspots") as well as to

[1] Reference to committee: Doc 12585, Reference 3772 of 27.05.2011.
[2] Draft resolution adopted by the committee on 11 March 2014.

personal data produced through the “Internet of things”; ISO (International Organization for Standardization) standards should be developed in this respect;

6.3. criminal activities on or through online services must be combated effectively by competent state authorities in accordance with Article 8 of the European Convention on Human Rights; law-abiding users have the right to remain anonymous, while law-infringing users must be identifiable;

6.4. online hotlines or other help-systems for children and persons with special needs should be established by public authorities and online service providers, in particular as regards cyber-mobbing and online child abuse;

6.5. the protection of property must be respected online; online service providers should offer the possibility to attach electronic signatures or apply electronic authentication tools to online content and services; providers of “cloud computing” services should automatically apply special protection measures for property stored with them, including conditional access tools and regular back-up filing;

6.6. providers of “cloud computing” services must not lower their users’ rights and protection by delocalising their “data cloud” outside the jurisdiction otherwise applicable to their company;

6.7. member States should set-up an adequate regulatory framework for online gambling services irrespective of whether such gambling services are offered by public or private companies; online gambling services seated in a country, which are accessible for, and targeted at, users in another country, should fall under the jurisdiction of the latter;

6.8. commercial or institutional service providers must have the legal obligation to inform their users of their name, legal seat and legal representative or director as well as their policies concerning user protection and security, in particular as regards their protection of a user’s private life, correspondence, personal data and property;

6.9. users of online services must be adequately informed of their rights by their service providers, irrespective of whether such services are provided by a public authority or a private entity; the waiver of any rights by users in favour of service providers must require the prior, informed and express consent by those users;

6.10. users of online services must have an effective legal remedy before a national authority or court against violations of their rights, having regard to Articles 6 and 13 of the European Convention on Human Rights as well as Article 2 of the United Nations International Covenant on Civil and Political Rights;

6.11. commercial or institutional service providers should offer their users the possibility to submit complaints and settle disputes voluntarily out-of-court, for instance through national or European consumer protection centres, bodies for online dispute resolution and in-house ombudspersons;

6.12. the secrecy of private correspondence of employees through their employer’s communication devices is protected by Article 8 of the European Convention on Human Rights, and employment contracts should prohibit any interference in accordance with the Committee of Ministers Recommendation No R (89) 2 concerning the protection of personal data used for employment purposes.

7. The Assembly calls on the European Internet Service Providers Association (EuroISPA) and their national members to establish a common code of conduct in view of the above basic principles on user protection and security in cyberspace. Internet service providers and law enforcement authorities should have a legal framework for practical co-operation against attacks on the rights and the security of users of the Internet and online media.

8. The Assembly invites the United Nations High Commissioner for Human Rights to co-operate with the Council of Europe and refer to this resolution as well as Resolution 1843 (2011) on the protection of privacy and personal data on the Internet and online media, when preparing her report on the protection and promotion of the right to privacy for the UN Human Rights Council and the sixty-ninth session of the UN General Assembly in 2014 – 2015.

9. The Assembly invites the Multistakeholder Advisory Group preparing the next UN Internet Governance Forum (Istanbul, 2-5 September 2014) to pay particular attention to questions regarding user protection and security in cyberspace, in particular the human right to protection of privacy and personal data.

10. The Assembly invites the International Telecommunications Union to elaborate global technical standards on the integrity, security and secrecy of online and mobile communications, which are based on Article 17 of the United Nations International Covenant on Civil and Political Rights as well as the Council of Europe's Convention on Cybercrime (ETS No. 185) and the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 180).

B. Draft recommendation[3]

1. The Parliamentary Assembly refers to its Resolution …. (2014) on improving user protection and security in cyberspace and emphasises the importance of increasing the intergovernmental action by the Council of Europe in this field.

2. Welcoming the Committee of Ministers' Internet Governance Strategy 2012-2015 and its numerous prior initiatives in this field, the Assembly recommends that the Committee of Ministers:

2.1. consider the feasibility of drafting an additional protocol to the Convention on Cybercrime (ETS No. 185) regarding serious violations of fundamental rights of users of online services;

2.2. analyse in how far the European Convention on Mutual Assistance in Criminal Matters (ETS No. 30) needs to be up-dated in order to deal with legal assistance in matters concerning transnational cybercrime and cyber evidence;

2.3. analyse in how far the Convention on the Legal Protection of Services based on, or consisting of, Conditional Access (ETS No. 178) can be utilised in order to increase the security of conditional access systems for online services, in particular as regards "cloud computing" services;

2.4. assist member States in the implementation of the Convention on Cybercrime as well as the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108);

2.5. complete as a matter of urgency the current revision of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, taking into account Assembly Recommendation 1984 (2011);

2.6. support and coordinate a pan-European approach to the globalisation of the Internet Corporation for Assigned Names and Numbers (ICANN) and its Internet Assigned Numbers Authority (IANA) as outlined in the Montevideo Statement on the Future of Internet Cooperation of 7 October 2013;

2.7. invite its observer States to work actively with the Council of Europe towards improving user protection and security in cyberspace, and ask them to set-up joint initiatives with the Council of Europe in this respect;

2.8. invite the European Union to accede to the Convention on Cybercrime as well as the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data and call upon the parties to these conventions to prepare actively this process.

[3] Draft recommendation adopted by the committee on 11 March 2014.

C. Explanatory Memorandum by Mr Axel E. Fischer (Germany, EPP/CD), rapporteur

1. Mandate for this report

1. Having tabled the Motion for a resolution on "improving user protection and security" (doc. 12585), I was subsequently appointed rapporteur of the Committee on Culture, Science, Education and Media on 23 June 2011.

2. As a result of the current affairs debate on "state interference with privacy on the Internet" by the Parliamentary Assembly on 27 June 2013, the Assembly Bureau decided that follow-up to this debate and subject should be part of this report. The Assembly debate of 27 June had been triggered by the PRISM/Snowden affair.

2. Preparatory work

3. The Assembly´s Sub-Committee on Media and Information Society organised a hearing in Strasbourg on 25 January 2012 with Mr John Carr OBE (Secretary of the Children's Charities' Coalition on Internet Safety, London), Dr Catarina Katzer (President of the Association against Cyber Mobbing, Cologne) and Mr Stefan Herwig (Partner, Mindbase Strategic Consulting, Gelsenkirchen).

4. Following my thematic instructions, a technical background report was subsequently commissioned from Dr Kei Ishii (Technical University Berlin) and a legal background report from Professor Hans Schulte-Nölke (University of Osnabrück). Both reports were presented to the Sub-Committee on Media and Information Society on 2 October 2012 by these experts and constitute the basis for parts of this memorandum. I am particularly grateful to both experts and the members of the Sub-Committee for their contributions.

5. The Committee on Culture, Science, Education and Media considered my preliminary draft report in Paris on 11 March 2013 and held an exchange of views with Professor Wolfgang Schulz, Director of the Hans Bredow Institute for Media Research (Hamburg) and Mr Thomas Spiller, Vice President for Global Public Policy EMEA at the Walt Disney Company (Brussels) speaking as an expert of the International Chamber of Commerce (Paris).

6. On 1 October 2013, the Committee organised a hearing in Strasbourg on State interference with privacy on the Internet with the participation of Mrs Dorothee Belz, Vice President of Microsoft Europe, Mr Duncan Campbell, journalist and forensic expert as well as Mr Lawrence Early, Jurisconsult of the European Court of Human Rights.

7. I have also built on my national parliamentary work as chairperson of the Enquête Commission on Internet and Digital Society of the German Parliament, which concluded its work on 28 January 2013 and adopted inter alia a report on user protection.[4]

3. Council of Europe standards and other international standards

8. The European Convention on Human Rights and its first protocol (ETS No. 5 and 9) guarantee also to users of online services the right to freedom of expression and information, the right to the protection of private life and personal data as well as the right to the protection of property.

9. Additional protection is afforded by the Convention on Cybercrime (ETS No. 185), making it a criminal offense to illegally access, intercept, or interfere with, computer systems or computer data, as well as by the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data and its additional protocol (ETS No. 108 and 181). Both conventions have defined legal standards on mutual assistance between parties to those conventions.

10. The European Convention on Mutual Assistance in Criminal Matters (ETS No. 30) of 1959 sets the framework for legal assistance in transnational criminal matters including cybercrime matters. In this context, important related work is currently pursued under the Convention on Cybercrime in order to draft an additional protocol on jurisdiction and transborder access to data and data flows. The latter will clarify and expand Article 32 of the Convention on Cybercrime, which deals with trans-border access to stored computer data with consent or where publicly available.

[4] See http://www.bundestag.de/internetenquete/dokumentation/Sitzungen/20130128/20_Sitzung_2013-01-28_PGVS_Zwischenbericht.pdf

11. Personal data, correspondence and property of users are often protected through conditional access systems to online services, such as passwords or electronic authentication tools. The illicit reproduction or use of such conditional access devices is to be punished by law under the Convention on the Legal Protection of Services based on, or consisting of, Conditional Access (ETS No. 178).

12. As counterfeit medical products are often sold through the Internet, related user protection is achieved through the Convention on the Counterfeiting of Medical Products and Similar Crimes involving Threats to Public Health (CETS No. 211).

13. The physical and moral integrity of children is protected under the Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (CETS No. 201) and Article 9 of the Convention on Cyberspace.

14. The Committee of Ministers of the Council of Europe adopted recommendations on:

- the protection of freedom of expression and freedom of assembly and association with regard to privately operated internet platforms and online service providers (2011)
- the protection and promotion of the internet's universality, integrity and openness (2011)
- the protection of human rights with regard to social platforms (2012)
- the protection of human rights with regard to search engines (2012)

as well as guidelines for:

- internet service providers (2008), developed in co-operation with the European Internet Service Providers Association,
- online games providers (2008), developed in co-operation with the Interactive Software Federation of Europe.

15. The Organisation for Economic Cooperation and Development (OECD) produced non-binding, but directly relevant standards: the Guidelines for Consumer Protection in the Context of Electronic Commerce (1999), the Guidelines for Protecting Consumers from Fraudulent and Deceptive Commercial Practices across Borders (2003) and the Recommendation on Consumer Dispute Resolution and Redress (2007).

16. Within the European Union, relevant legislation comprises the Consumer Sales Directive (1999/44/EC), the E-Signatures Directive (1999/93/EC), the E-Commerce Directive (2000/31/EC), the E-Privacy Directive 2002/58/EC (as amended by Directive 2009/136/EC), the Unfair Commercial Practices Directive (2005/29/EC), the Consumer Rights Directive (2011/83/EU) and the Directive on attacks against information systems (2013/40/EU).

4. State interference with privacy on the Internet

17. The current public debate about the PRISM programme of the National Security Agency of the USA and related co-operation with security services in Europe reflects different international approaches to the protection of personal data vis-à-vis the protection of national security and law enforcement. Based allegedly on documents disclosed by Edward Snowden to The Observer, The Guardian reported that "in addition to the UK – Denmark, the Netherlands, France, Germany, Spain, and Italy have all had formal agreements to provide communications data to the US. They state that the EU countries have had "second and third party status" under decades-old signal intelligence (Sigint) agreements that compel them to hand over data which, in later years, experts believe, has come to include mobile phone and internet data."[5]

18. In this context, reference must be made to the work of the Assembly which had led to Resolution 1843 and Recommendation 1984 (2011) on the protection of privacy and personal data on the Internet and online media, based on a report by Ms Andreja Rihter (Slovenia, SOC), as well as Resolution 1877 and Recommendation 1998 (2012) on the protection of freedom of expression and information on the Internet and online media, based on a report by Ms Zaruhi Postanjyan (Armenia, EPP/CD).

19. More than a decade ago, a similar public debate had been held about the alleged interception of radio and satellite communication by the USA, the United Kingdom, Canada, Australia and New Zealand. This situation had been analysed by the European Parliament in its report and resolution of 2001 on the existence of a global system for the interception of private and commercial communications (ECHELON interception system).[6] Although the possibilities for the large-scale screening of online communication data,

[5] See, The Guardian (30 June 2013), at http://www.theguardian.com/world/2013/jun/30/nsa-spying-europe-claims-us-eu-trade

[6] See http://www.europarl.europa.eu/comparl/tempcom/echelon/pdf/rapport_echelon_en.pdf

traffic data and other meta data had been less developed then, the results of the ECHELON debate are still of relevance to the PRISM debate today.

20. The rapid development of IT communication globally has enabled national security services and law-enforcement authorities to focus on IT services in order to identify and trace terrorists or other serious criminals who use such IT services. Benjamin Franklin, the former President of the USA, had said: “He who sacrifices freedom for security deserves neither.” In a modern human rights debate, one would not sacrifice one human right for another, but define both through their correlation.

21. While Article 8 of the European Convention on Human Rights protects also personal data online, national security can limit such right. The USA is not party to the European Convention on Human Rights, but committed under the corresponding Article 17 of the United Nations International Covenant on Civil and Political Rights. Member States of the Council of Europe collaborating in the alleged PRISM programme are bound by the European Convention. Any interference on grounds of national security must be prescribed by law and proportionate to the protection of national security.

22. The European Court of Human Rights has defined the requirements in this regard: “In its case-law on secret measures of surveillance, the Court has developed the following minimum safeguards that should be set out in statute law in order to avoid abuses of power: the nature of the offences which may give rise to an interception order; a definition of the categories of people liable to have their telephones tapped; a limit on the duration of telephone tapping; the procedure to be followed for examining, using and storing the data obtained; the precautions to be taken when communicating the data to other parties; and the circumstances in which recordings may or must be erased or the tapes destroyed.”[7]

23. Although the facts of the PRISM programme are not fully known, it seems that vast amounts of IT communication data were intercepted, stored and analysed in collaboration with national security services by States in Europe. Such processing or screening of personal data was allegedly done, once keywords were used in IT communication, which were part of a huge list of words typically used by terrorists or criminals. In the end, a huge number of users must have been screened and profiled. In this context, commercial espionage was also alleged.

24. If such screening and profiling were pursued without sufficient grounds of national security concerns, a violation of Article 8 of the European Convention on Human Rights could be assumed. The recent Motion on massive eavesdropping in Europe (Assembly doc. 13288) may lead to further analysis and discussion of this particular case and its wider implications concerning the correlation between national security and the protection of privacy.

25. Edward Snowden had worked for the private security companies Booz Allen Hamilton and Dell, which had been contracted by the National Security Agency of the USA. Such outsourcing of Internet surveillance for national security purposes may seriously lower the protection of privacy and personal data. Edward Snowden is cited by The Guardian: "The government has granted itself power it is not entitled to. There is no public oversight. The result is people like myself have the latitude to go further than they are allowed to."[8] Although with a different focus, one might refer in this context also to Assembly Recommendation 1858 (2009) on private military and security firms and erosion of the state monopoly on the use of force.

26. Edward Snowden disclosed to The Guardian a large amount of secret information about the activities of national security services in the USA, the United Kingdom and other NATO countries. The Guardian journalist Glenn Greenwald testified before a Brazilian Senate foreign relations committee that he had up to 20.000 secret government files, which he had received from Edward Snowden.[9] The disclosure of these files was labelled as “whistle-blowing”. Following these events, the President of Brazil decided to postpone her state visit to the USA until the situation would be clarified. After a month in Hong Kong, China, Mr Snowden is now in Russia since June 2013.

27. Following Mr Snowden’s revelations of pervasive surveillance of email correspondence in France as well as the interception of the mobile phone and SMS communication of the Federal Chancellor of Germany by the national security service of the USA for many years, the governments of France and Germany are

[7] See, ECtHR in Liberty and others v. the United Kingdom (Appl. No. 58243/00) citing its decision in Weber and Saravia v. Germany (Appl. no. 54934/00), reproduced at http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-87207
[8] See, The Guardian (11 June 2013), at http://www.theguardian.com/world/2013/jun/10/obama-pressured-explain-nsa-surveillance
[9] See http://rt.com/news/journalist-thousands-snowden-documents-143/

leading an initiative within the Council of the European Union in order to clarify the level of privacy intrusion committed by the USA and to develop mutual standards on surveillance and co-operation in the field of national security. In addition, the Civil Liberties, Justice and Home Affairs Committee of the European Parliament established an inquiry on electronic mass surveillance of EU citizens, which held hearings since 5 September 2013 and produced its final report on 21 February 2014.[10] The Parliamentary Assembly of the Council of Europe referred on 30 September 2013 the Motion on massive eavesdropping in Europe (Doc. 13288) to its Committee on Legal Affairs and Human Rights for report. At the level of the United Nations, Brazil and Germany have, on 8 November 2013, introduced to the Third Committee of the UN General Assembly a draft resolution calling for the protection of privacy in accordance with international human rights law and the cessation of excessive electronic surveillance. The latter Resolution on the right to privacy in the digital age was adopted on 18 December 2013 by the UN General Assembly.

28. Assembly Resolution 1729 (2010) on the protection of "whistle-blowers" outlined in § 6.1.1: "the definition of protected disclosures shall include all bona fide warnings against various types of unlawful acts, including all serious human rights violations which affect or threaten the life, health, liberty and any other legitimate interests of individuals as subjects of public administration or taxpayers, or as shareholders, employees or customers of private companies." Such whistle-blowing could as an ultima ratio be done through the media, as stated in § 6.2.3 of Resolution 1729: "Where internal channels either do not exist, have not functioned properly or could reasonably be expected not to function properly given the nature of the problem raised by the whistle-blower, external whistle-blowing, including through the media, should likewise be protected."

29. In any case, Article 8 would not permit the screening and profiling of IT users by public authorities on purely political grounds, for instance targeting political opponents. While most states in the world might possess the technological and human resources to do so, and while it could be assumed that non-democratic and oppressive governments would wish to do this, factual indications have not been revealed to this end with regard to the PRISM case.

30. In Klass and others v. Germany (Application no. 5029/71), the European Court of Human Rights accepted under Article 8 "that the existence of some legislation granting powers of secret surveillance over the mail, post and telecommunications is, under exceptional conditions, necessary in a democratic society in the interests of national security and/or for the prevention of disorder or crime. (…) The Court, being aware of the danger such a law poses of undermining or even destroying democracy on the ground of defending it, affirms that the Contracting States may not, in the name of the struggle against espionage and terrorism, adopt whatever measures they deem appropriate. The Court must be satisfied that, whatever system of surveillance is adopted, there exist adequate and effective guarantees against abuse. This assessment has only a relative character: it depends on all the circumstances of the case, such as the nature, scope and duration of the possible measures, the grounds required for ordering such measures, the authorities competent to permit, carry out and supervise such measures, and the kind of remedy provided by the national law." [11]

31. In conclusion, it is necessary to have an adequate and efficient internal oversight within, and judicial review over, national security services and law-enforcement authorities, in order to prevent abuse and hence violations of Article 8 of the European Convention on Human Rights. The possible damage done by irresponsible access and use of such data is obvious.

32. Although at a smaller scale, the technological possibilities for the screening and profiling of users are in principle also available to commercial companies and private individuals, who might wish to exploit such data for personal gain. States must therefore afford users adequate protection also in this regard. The surveillance of employees by their employers is restricted by the Committee of Ministers Recommendation No R (89) 2 concerning the protection of personal data used for employment purposes.

5. Developments in IT security

33. IT security has become an important research area in computing, aimed at developing sophisticated ways of avoiding intrusion, manipulation or destruction of databases, but also impede hackers to take over the control of home or business IT systems or threaten public administration IT systems (e.g. police, judiciary or defence) or information-based critical infrastructure which is essential to the daily life of our societies (e.g. finance and banking, transports and energy).

[10] See http://www.europarl.europa.eu/document/activities/cont/201403/20140306ATT80632/20140306ATT80632EN.pdf
[11] See http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-57510

34. The latter has resulted in international co-operation such as the International Cyber Security Protection Alliance[12] as well as the recent establishment by the EU of the European Cybercrime Centre at Europol in The Hague.[13]

35. However, despite decade-long efforts, protecting IT systems against malicious threats still poses a challenge for organisations, as media coverage of numerous break-ins into their IT systems indicates. And with more powerful networked devices and e-services available to the individual user, they become lucrative targets for malicious attackers as well. IT security appears even less prepared here, as regular news coverage about virus attacks illustrates.

36. Computers are accessible from remote places and data and software can be rapidly exchanged. This leads to the development of technological means to cope with the new IT security challenges – such as firewalls, anti-virus software, or cryptographic tools. But the growing system complexity combined with everyday actions (or inactions) of the users constantly expose vulnerabilities which attackers could exploit.

37. As technological-only means cannot provide a complete solution, the focus shifted from technological solutions to the organisational factors. Technologically secured devices and software still can be compromised if no sound security policies and procedures exist, and if these policies are not properly enforced and supported. Policy frameworks and certifications were developed which allow organisations to systematically evaluate their IT security needs and implement the necessary products, policies and procedures. In this way, *organisational IT security* was recognised as an important element of IT security.

38. Even when technological and organisational security measures were put in place, IT security problems remained. The user is often overwhelmed by security procedures or unaware of security consequences of their action. Also, the growing need of users outside organisations to protect their private IT environment has led to scrutinise the role of the end user in IT security.

39. Therefore, research recently shifted to *personal IT security* as a crucial element of the overall security of IT system and "Usable [privacy and] security" has developed into a hot topic. It appears that the *mental model* elaborated to assess the user's risk and actions might not be adequate. Understanding better the role of mental models and formulating more appropriate ones carries the promise to enhance the effectiveness of user IT security. The shape of technology must be "usable" in the sense that it supports both the user and the IT security. It remains to be seen how the research results can be translated into future devices, software and services as well as educational efforts and home user support.

6. Current state of IT security

40. With the rapid increase in Internet services in all areas of life, the crime rate has equally grown exponentially. The 2012 Norton Symantec Cybercrime Report estimates 1.5 million victims of cybercrime daily with an estimated annual value of 110 billion US-$ worldwide and 16 billion US-$ in Europe.[14] Parallel to the growth in mobile Internet access, the number of cybercrime attacks has doubled from 2010 to 2011.

41. Widely publicised cases have concerned the massive hacking into user data, for instance by a group called Lulz Security into the servers of Sony and Nintendo in 2011, the hacking attack on the telephone directory Truecaller by a group called Syrian Electronic Army in July 2013 as well as the theft of 2 million user data stored on a Vodafone server in Germany in September 2013. In March 2011, the Internet security firm McAfee reported that Internet hackers in China had committed massive commercial espionage of several multinational oil companies since 2009 called “operation night dragon”.

42. Another spectacular case was the use of stolen credit card data to withdraw 45 million US-Dollars from banking machines in New York and other cities around the world in December 2012 and February 2013. In May 2013, the Liberty Reserve online money transfer service was closed by law enforcement authorities in the USA and 16 other countries on suspicion of having run a massive money laundering scheme through the Internet of up to 6 billion US-Dollars. While those spectacular cases may hint at Internet security risks, the smaller but more frequent attacks on individual Internet users are more harmful in absolute terms and should therefore guide our analysis in this report.

[12] See https://www.icspa.org/
[13] See https://www.europol.europa.eu/ec3
[14] See http://now-static.norton.com/now/en/pu/images/Promotions/2012/cybercrimeReport/2012_Norton_Cybercrime_Report_Master_FINAL_050912.pdf

43. Drawing from the experience with a German user-oriented Internet information portal for IT security and privacy ("*Verbraucher sicher online*"),[15] IT security can be outlined from the vantage point of both attacker and user. The attacker is looking for vulnerabilities which enable him or her to gain access to the system. The user must take the appropriate actions against these vulnerabilities to minimise the risks of being attacked.

44. One can distinguish four different components of a user IT environment which show different vulnerabilities and responses: An attack can be raised against any of the *devices* (computers, smart phones, etc.) of the user or against the *networks* (Internet, mobile networks) the devices connect to, in order to interact with the *e-services* employed by the user. Finally, the *users* themselves can be targeted by an attack as well.

6.1. Attacks against devices

45. Devices comprise the computers, laptops, smart phones etc. that the user directly interacts with. They consist of the hardware, the operating system and application software, and are usually connected to local or mobile networks, and through these to the Internet.

46. Attacks against devices use one or more technical *vulnerabilities* such as software defects in the operating system and applications, so called *exploits*, in order to install or 'infect' it with malicious software. Once infected, the malware regularly gains absolute control over the device. All data can be accessed, all user actions intercepted (for example the typing of passwords) and altered, and the device can be used to infect or attack other devices and e-services.

47. The *technological responses* against these kinds of attacks are: (1) maintaining current backups of the data on the device, in order to protect against data theft and alteration, (2) active and up-to-date malware protection software which protects against malicious e-mails or websites, and (3) continuously updating application and operating system software in order to close known software defects, which may otherwise be used by viruses in order to infect the system.

48. As there is no central authority for the protection of devices, any security policies or procedures can only rely on *personal responses*, i.e. the knowledge and awareness of the user itself. In this respect, the *usability* of the security features has improved in recent years. With the media attention to IT security issues, device and software makers have stepped up their efforts to integrate security considerations in their development and offer timely security updates. Also, more and more software can be configured to install security updates automatically, relieving the user from this task. Still, the user has to actively follow security news, and actively install and maintain backups and anti-malware software. In addition, constant attention is required in order to recognise and prevent attacks through e-mail, websites etc., which may lead to the infection of the device.

6.2. Attacks against networks

49. Devices connect to various networks in order to reach e-services over the Internet. It is more and more common to make these connections wirelessly. Generally, entry points to networks are either home routers, or public or private hotspots.

50. Common attacks against home routers try to gain access to the router and either intercept the connections going through it, or use the connection to raise further attacks against local or remote devices. The main *technological responses* for routers consist of enabling strong encryption of the wireless connections (currently WPA2) with a strong password, securing the administrative interface with a (different) strong password, and regular updates of the router firmware. A recent *usability response* by router manufacturers is the default activation of the wireless connection encryption, which has led to a noticeable reduction of unsecured wireless home networks.

51. Attacks through public or private hotspots generally take one of two forms: either the attacker gains controlling access to the hotspot router, or he sets up another hotspot pretending to be the legitimate one. In both cases, connections going through the router can be intercepted. Hotspots are attractive targets for attackers as many users are enticed especially by cost free hotspots, and underestimate the risks associated with them. Although *technical responses* such as the employment of virtual private networks (VPN) exist which might alleviate the risks connected to hotspots, they are cumbersome or even blocked by the hotspot.

[15] See http://www.verbraucher-sicher-online.de/

52. Therefore the sensible *personal response* would be to find an alternative, more secure means to connect to the Internet. In the medium term, the proliferation of fast mobile Internet access might lessen the problem with hotspots.

6.3. Attacks against e-services

53. Gaining unauthorised access to the users' e-services is certainly a main target for attackers. Access to most of these services is still only dependent on simple security credentials, such as username and a password, although some, notably e-banking services, have developed more intricate schemes including single-use passwords (transaction authentication numbers, TAN) and multi-factor authentication (additional security credentials through different technical means, such as mobile phone or TAN generators).

54. An often overlooked risk concerns the availability of the user data stored by the e-service. Service providers might for example not guarantee the confidentiality, integrity or availability of the data, which leaves a risk that a direct attack against the e-service itself might cause the loss of the user data. The appropriate *technical response* is to have the data stored (backup) in more than one place and to require the e-service provider to use regularly up-dated security measures against attacks.

6.4. Attacks against users

55. From the vantage point of an attacker, the user can be successfully targeted just as a device, network, or e-service. These attacks are often subsumed under the term "social engineering" which can be defined as any "attack that uses social means such as deception and manipulation in order to gain access to information technology". The phishing attacks, where malicious e-mails try to entice the user to open an attachment containing malware, respond to a scam or enter security credentials into a fake e-service-website fall into this category. For example, a fake e-service website or a fake support e-mail is asking to send back the username and password "for security reasons".

56. The most effective security response is *non-technological* in nature, namely the secure handling of the username and password, and caution against "phishing". In contrast, technological responses (e.g. automatic detection of phishing e-mails) so far have proven largely ineffective against the countless variations of these attacks.

57. Security risks may also stem from publicly accessible Internet content which has been generated voluntarily by users. Such content can be screened and collected by specific data-mining software. A recent example is the Rapid Information Overlay Technology (RIOT), which was developed by the US-American company Raytheon and has even been used by public authorities for searching social networks in order to profile persons.[16]

7. Future risks: mobile, cloud and Internet of Things

58. Mobile phones, especially smart phones, are computers such as laptop or desktop computers. Therefore, they share similar vulnerabilities, threats and risks such as malware attacks. But a number of characteristics of smart phones aggravate the challenges inherent in mobile IT security.

59. These include;

- their size, both in terms of physical size (ease of loss or theft) and – compared to desktop or laptop computers – limited computing capabilities;
- the multitude of networking (mobile network, Wi-Fi, Bluetooth) and other technical built-in capabilities (GPS, electronic payments through near field communication);
- consequently, the complexity of the mobile operating system with a heightened chance for vulnerabilities; and the large number of applications ("Apps") and uses.

60. Whereas cloud computing in general is aimed at business users who might gain economic advantages by outsourcing various computing resources (e.g., software, storage, execution time) to cloud computing providers, current service offerings such as Google services or Apple's iCloud can be seen as the "consumer side" of cloud computing.

61. These offerings integrate several otherwise independently available services (e-mail, photo and video sharing, social networking, remote storage, etc.) into one centrally accessed "cloud" ecosphere.

[16] See the criticism raised by the American Civil Liberties Union, accessible at: http://www.aclu.org/blog/technology-and-liberty-national-security/raytheons-riot-social-network-data-mining-software

Another characteristic is the tight integration of software (web browser, operating system) and devices (smartphone) into that ecosphere.

62. The consequences for IT security of cloud computing are twofold. On one hand, there are claims that the personal data is better protected against destruction in the cloud, as it is stored independently from one device. Also, specific security features such as the remote deletion of stolen devices or the centralised authentication relieving the user from memorising numerous passwords (assumed that the centralised authentication is secure) can be found as security benefits of cloud services.

63. On the other hand, some anecdotic evidences hint at possible IT security problems. For example, a successful attack against the centralised authentication opens access to all user data and services available to the user. In the case of the incident involving the Apple iCloud service, the attackers who successfully gained access to the journalist's iCloud in summer 2012 were able to delete the complete data stored on all his connected devices, including his smartphone and laptop. This feature, offered as a security feature against theft, turned out to entail a severe security risk.

64. As cloud services include new IT security features, it might be possible that they mitigate the inherent IT risks of such centralised services. In any case, the user should carefully assess the risks involved into such services.

65. Given the current problems with IT security, and the foreseeable problems in already available technologies such as mobile Internet access or cloud computing services, one may speculate what form the IT security challenges will take with such potentially disruptive technologies as the "Internet of Things". Once every day’s physical things from home appliances to cars will incorporate networked computing capabilities, they may become targets or additional entry-points for attacks. As those “things” with Internet are typically commercial goods which require commercial services and allow the profiling of a user (e.g. automated impulses for servicing the car, repairing the heating, or replacing the toner in the printer), the economic interest in an attack is obviously increased.

66. "Pervasive" or "ambient computing" may reach further into the life of users, as computing and networking will be tightly integrated to things, activities or even the human body, and "disappear" as distinguishable technologies.

8. Steps towards enhanced user protection and security

67. For nearly a century, consumer protection principles have been established for traditional commerce of goods and services. However, they are more or less absent in modern cyberspace. User protection principles have been developed in some areas by the OECD and UNCITRAL. A few legal principles have been established by the United Nations, the Council of Europe and, in particular, the European Union.

68. Co-operation between law-enforcement authorities should be increased. This may require wider use of the Budapest Convention on Cybercrime (ETS No. 185) as well as international treaties on legal assistance such as the European Convention on Mutual Assistance in Criminal Matters (ETS No. 30).

69. Awareness of the latter norms and principles is rather low among Internet service providers as well as users. In addition, their legal force is rather limited, except for the EU law in force in all EU member States. Therefore, it seems necessary to increase awareness of the already established legal standards and seek to develop additional ones where there is a need.

70. Users buy computers or other devices and they subscribe to Internet services. Those are typically commercial transactions between a user and a commercial company. Based on this, users may have a legitimate expectation that the goods and services they receive are without defect and not potentially dangerous. Such a legitimate expectation may require companies to sell their goods and services with certain precautionary measures taken in favour of the security of their users.

71. For example, service providers can be expected to provide encryption tools automatically (i.e. as a default option) and free of charge. This will increase the security of users with regard to passwords or other sensitive data. Modern computers or other devices should have advanced anti-virus programmes set-up automatically. In addition, websites should disclose in a transparent manner if they apply automatic signs or cookies to the access devices of users.

72. Companies may meet such standards voluntarily, but states can usefully encourage or even prescribe them where deemed necessary. In a globalised world, it is important to co-ordinate those approaches among states, especially within Europe.

73. The Council of Europe has been the first, and so far the unique, international organisation to address cybercrime through an international convention. The Budapest Convention on Cybercrime has also been signed by many states outside Europe and is a model for more than 100 states worldwide. At the recent Council of Europe conference on strategic priorities in the cooperation against cybercrime (Dubrovnik, 15 February 2013), the ministers participating adopted the following objectives:

- Pursue cybercrime strategies to ensure an effective criminal justice response to offences against and by means of computers as well as to any offence involving electronic evidence;
- Adopt complete and effective legislation on cybercrime that meets human rights and rule of law requirements;
- Strengthen specialised law enforcement units and the specialisation of prosecution services with respect to cybercrime and electronic evidence;
- Implement sustainable law enforcement training strategies;
- Support the training of judges and prosecutors on cybercrime and electronic evidence;
- Pursue comprehensive strategies to protect children against online sexual exploitation and sexual abuse in line with the Lanzarote Convention;
- Promote financial investigations and the prevention and control of fraud and money laundering on the Internet;
- Strengthen cooperation with the private sector, in particular between law enforcement authorities and Internet service providers;
- Engage in efficient regional and international cooperation;
- Share our experience with other regions of the world to support capacity building against cybercrime;
- Promote adherence to the Budapest Convention on Cybercrime at the global level.

9. Examples of self-regulation by market actors

74. In 2011, the European Advertising Standards Alliance (EASA) released its Best Practice Recommendation on Online Behavioural Advertising which aims at ensuring privacy protection across Europe.[17] The basic idea is to allow users to identify online behavioural advertising via a uniform European-wide icon. The icon shall be included in or around all online behavioural advertisements and will signal to users that online behavioural advertising is being used. The icon will be interactive, allowing users to find out which companies are involved in serving the ad and also to click through to a European-wide website. The website shall provide information about online behavioural advertising in general and means for users, in their national language, to exercise their choice about whether they want to receive online behavioural advertising ads.

75. This system however, is not very effective, especially for inexperienced users. Several dozens of companies have so far signed the commitment – but by far not all providers of behavioural advertising. The user would have to visit the many websites of the participating companies and object to cookies used by these providers. He or she would have to do this from all computers including mobile phones. In addition, there is no regulation for the most stubborn "flash cookies", which do not embed themselves in the browser, but deeper in the computer system and are very difficult to delete.

76. The Safer Social Networking Principles of the EU (2009) have been developed by a number of social networking service providers in consultation with the European Commission, as part of its Safer Internet Plus Programme, and several NGOs. They aim to provide good practice recommendations for the providers of social networking and other user interactive sites, to enhance the safety of children and young people using their services. The seven basic principles are:

- Principle 1: Raise awareness of safety education messages and acceptable use policies to users, parents, teachers and carers in a prominent, clear and age-appropriate manner
- Principle 2: Work towards ensuring that services are age-appropriate for the intended audience
- Principle 3: Empower users through tools and technology
- Principle 4: Provide easy-to-use mechanisms to report conduct or content that violates the Terms of Service
- Principle 5: Respond to notifications of illegal content or conduct
- Principle 6: Enable and encourage users to employ a safe approach to personal information and privacy

[17] Available at: http://www.easa-alliance.org/page.aspx/386.

- Principle 7: Assess the means for reviewing illegal or prohibited content/conduct

77. The document contains some more concrete specific recommendations for each principle. The document states, however, that, while providers will support all seven principles, "it is for each provider to judge where and how far to apply the document's specific recommendations."

78. The European Framework for Safer Mobile Use by Younger Teenagers and Children (2007) has been signed by many European mobile providers and content providers in order to ensure safer use of mobiles by younger teenagers and children. It contains recommendations on safer mobile use, in particular on access control mechanisms, raising awareness and education, classification of commercial content as well as illegal content on mobile community products or on the internet. Regular reports on the implementation published by industry show some progress made by mobile phone operators on their work to keep children safe while using mobile phones.

79. Internet service providers as well as producers of Internet access devices should be encouraged, supported and possibly obliged to set up precautionary measures for the protection and security of users and customers. This may be done through industry self-regulation or a co-regulation based on a legal framework to be implemented by industry action. Quality certification may be an important aspect in this regard, for instance for tools against attacks on devices, networks and services. The ISO (International Organization for Standardization) in Geneva has produced a number of international technical standards, such as the ISO/IEC 15408:1999, the Common Criteria for IT Security Evaluation. For an effective and transparent protection of users in a rapidly changing cyber environment, additional specific technical standards should be developed, for example on software and hardware security. Compliance with the latter ISO standards could serve as a quality label, which can be recognised and trusted by users.

10. Conclusions

80. Greater awareness, transparency and accountability are necessary for improving security in cyberspace. This is a challenge for all stakeholders alike, the Internet industry, users and the state.

81. For some IT security challenges, adequate technological responses exist, some of which also have improved in usability. But the capability of users to turn awareness and knowledge into appropriate actions hinges on appropriate mental models, which have to be developed for IT security. E-learning may be a useful and system-related tool in this respect. Trusted institutional structures have to be established, either by governments or the private sector, which support users in making the appropriate risk assessment and offer concrete help, similar to security policies and procedures and support staff in organisations.

82. Anonymity of users is an issue for their direct accountability. Large-scale surveying or monitoring of user behaviour on the Internet is neither not acceptable from a human rights perspective. Internet service providers generally know the identity of their users through their IP addresses or customer identification details. While law-abiding Internet users should remain anonymous, law-infringing Internet users must be identifiable. Where commercial web portals provide a platform for law-infringing users, the operators of these portals should be held liable unless they identify the law-infringing user.

83. National security services and law enforcement authorities can search and seize private online data within their jurisdiction in accordance with domestic law and Article 8 of the European Convention on Human Rights. Such interference must be proportionate to the legitimate aim pursued, with national security being a legitimate aim enumerated in Article 8, paragraph 2. As the European Court of Human Rights has consistently held, however, it is not enough that the interference should merely be useful or desirable. Permanent and random interceptions of private communications would be in violation of the principle of proportionality and hence not compatible with the European Convention on Human Rights.

84. User empowerment requires greater transparency of online service providers and intermediaries. A lack of such transparency compromises user protection and security. While transparency can be imposed on commercial service providers and intermediaries, this may be more difficult with regard to private social networks, peer-to-peer services and user generated content. Nevertheless, general principles of transparency should be developed.

85. The Convention on Cybercrime protects the integrity of computer networks. It may be necessary to analyse and possibly widen the remit of such protection, in order to include also attacks on the integrity through technical malware as well as an intentional lack of providing essential components necessary for the functioning of computer networks in the public domain. For example, technical attacks can stem from unsolicited messages or "spam", automatic signs or "cookies", malicious software such as the external

linking of computers through “botnets”, as well as "flash cookies" which are embedded deeper in the computer system and are very difficult to delete.

86. Public access points as well as “hotspots” for wireless Internet access are typically weak points for user security, because they can be used as an entry point for malicious software, hacking, data manipulation or other attacks on the security of users. Mobile Internet access may be more secure, where a single operator or service provider will function as contractual intermediary for a user.

87. Encryption can increase the secrecy of communications in cyberspace, especially in wireless connections. In order to keep up with the rapid progress in technical intrusions into communications, encryption software needs to be updated and enhanced regularly. A default activation of encryption will help less experienced users.

88. Commercial content should be made transparent and thus be classified. Commercial service providers and intermediaries should be barred from using fraudulent and deceptive commercial practices. In this regard, it may be helpful to agree on a list of prohibited commercial practices and on a Europe-wide benchmarking of quality standards. The same may be applied to fair business advertising and marketing practises. Sector-specific legislation can address advanced user protection and security in a more targeted way, for example for telecommunications, banking, insurance, financial instruments, electronic payments as well as travel contracts. The use and technical reliability of electronic signatures may be a relevant tool in this context.

89. Through the international reach of online services, user rights may be compromised by uncertainties in the jurisdiction of national courts and the applicability of national laws. Therefore, states should support mechanisms for online dispute resolution and redress and establish legal co-operation and assistance on the basis of public international law.

90. Children are a high-risk group. Harm for children might be caused by illegal or violent Internet content and contact with other Internet users. Children could harm themselves by posting private pictures or data on the Internet or by bullying. Private information and images are difficult to delete from the Internet, thus causing a potential endless victimisation. The Internet is also a potential entry point for outside dangers coming into a child’s room. Also adults could be a danger for children, especially regarding sexual abuse. It is therefore important to establish online help systems for parents and children as well as to support media education, teacher training and peer-to-peer education.