Presentation to the Civil Liberties Committee hearing on the proposed Directive on Attacks Against Computer Systems

Introduction

Thank you for giving me the opportunity to speak to you today on a complex issue of importance to both the fundamental rights and the economic interests of European citizens.

European Digital Rights is an association of 28 digital civil rights associations from 18 European countries. We work on issues such as data protection, data retention, intellectual property and, of course, cybercrime – any issue, in fact, that impacts on civil rights in the digital environment.

General comments

The first general comment that must be made is that the preparation of this dossier in all three institutions has been exemplary.

The European Commission kept civil society groups informed from the earliest stages in their preparations and regularly updated EDRi on progress. We welcome the fact that it adopted a narrow and targeted approach placed emphasis on improved cooperation. We support the proposed obligations on Member States with regard to monitoring and statistics. This will permit maximum opportunities for evidence-based decision-making in the future. Similarly, in this house, the measured, inclusive and diligent approach to the file has been a case study in democratic decision-making.

Some of the points that are of concern to us have already been addressed and provisionally agreed by the Council, but there is still some room for improvement.

The key issues that we would like to see clarified by the Parliament are:

–A more coherent approach to “minor” offences is needed**.** It is not acceptable for the default position to be that these should be criminalised in the absence of an active decision to the contrary by Member States;
–A clear exception for possession of software that could be used for cyber-attacks in the absence of clear criminal intent – particularly, but not only to ensure that researchers can work in a secure legal environment;
–A clarification on unintentional aiding and abetting to ensure legal certainty for intermediaries. A harmonised definition of “instigation” is also needed;
–The wording of Article 10.2 appears to be excessively vague, with words like “considerable,' “significant” and “tool” being open for very wide interpretation. Also, we assume that “loss of personal data” is meant to mean “loss or unauthorised access to personal data';
–The proposal on data exchange needs to be coupled with adequate data protection safeguards.

International attacks against computer systems

During previous debates**,** the rapporteur made reference to the problem of states that launch cyber attacks. Attacks by or for states are a growing problem. The EU's approach to this topic is very important for the

legitimacy, coherence and credibility of our efforts to fight attacks against computer systems. Unfortunately, there is a major contradiction in EU policies on this topic and I would like to focus on this key point.

In this context, one would tend to imagine stuxnet-type attacks, which was an attack on one country by others in the traditional sense. However, there is also an increasing danger of domain names and IP addresses, which are key elements in the functioning of the Internet and the world wide web, being used as very blunt tools in extra-territorial enforcement by the United States and European Union.

The United States has, up until recently, never sought to exploit its theoretical jurisdiction over the companies and infrastructure that are at the core of the Internet. Now, however, particularly as a result of, for example, the so-called PROTECT IP[1] and COICA[2] acts, this is changing. The result of these and other measures is that the US is giving itself, and private companies in some cases, the power to render inaccessible computer data outside its jurisdiction. As these systems are outside the USA these actions are, by definition, "without right" in the sense of the draft Directive and the Cybercrime Convention, which the US claims to have ratified.

How sustainable are the definitions in this Directive if state-sponsored and state-protected attacks on computer systems are both permitted and encouraged in the United States? This is creating increasing legal uncertainty for European citizens and businesses. It is creating a permanent risk of defenselessly being subjected to actions defined as criminal acts by the draft Directive. This danger is clearly illustrated by the case of mooo.com last year where the US authorities, while seeking to disable ten allegedly child abuse websites accidentally removed the web domains of 84,0000 innocent sites – rendering them inaccessible - and replacing them with a notice accusing the users of crimes against children.

The European Parliament[3] has already reacted very coherently and clearly to this approach. In June of last year, in its resolution on Internet governance, it voiced its opposition to the manipulation of global Internet architecture. It argued that governments should protect "the integrity of the global Internet and freedom of communication by avoiding any regional measures, such as revocation of IP addresses or domain names in third countries". This position was supported only three weeks ago by the Committee of Ministers of the Council of Europe. The ministers cautioned[4] that Member States must "protect and promote the universality, integrity and openness of the Internet"

As a Spanish MEP, the rapporteur, Mr Sosa Wagner, will have seen this problem first hand. In 2009 a British citizen living and working in Spain, running a travel company specialising in trips to Cuba had his online presence simply deleted from the Internet from one day to the next. This was done without warning, without breaking Spanish law and without due process. The European company – with no activity in the USA, no targeting of activity at US citizens and no ambitions of doing business in the USA – had been put on a blacklist by the US Treasury. As a result, the web company that had registered his domain names unilaterally revoked all of them – leaving him without his websites, without e-mail, without reservations and, therefore, without income.

Similarly, the United States has – again in the absence of due process of law - also removed the domain name of a Spanish website on the basis of accusations of copyright violations – accusations that have already found to be without merit in the Spanish courts.

To make matters worse, the United States Immigration and Customs Enforcement Agency recently claimed

1 http://en.wikipedia.org/wiki/Protect_IP_Act
2 http://en.wikipedia.org/wiki/Combating_Online_Infringement_and_Counterfeits_Act
3 Internet Governance: the next steps. Resolution adopted on 15 June 2010. See http://www.europarl.europa.eu/sides/getDoc.do?type=TA&language=EN&reference=P7-TA-2010-0208
4 https://wcd.coe.int/wcd/ViewDoc.jsp?Ref=CM/Rec%282011%298&Language=lanEnglish&Ver=original&BackColorInternet=C3C3C3&BackColorIntranet=EDB021&BackColorLogged=F5D383

American jurisdiction on all .COM and .NET domain names worldwide.[5]

For the moment, as anticipated by the European Parliament resolution, the integrity of the global Internet is being undermined as worries grow about such extra-territorial land-grabs.

The response of the European Commission and Council

The response of the European Commission and Council to these attacks and threats of attacks against European citizens and European web resources is possibly not what one might expect. Instead of protesting at these attacks, it has enthusiastically endorsed this approach.

The Commission reacted positively to an American proposal to launch an US/EU[6] project not only on the revocation of domain names, but on IP addresses too. The logic is clear – while the US has very strong control over domain names, its IP address registry only covers North America. By contrast, the European registry RIPE covers a far wider region – stretching across Asia.

The proposal for the European Union to give itself powers on revoking domain names and IP addresses was first made in the Communication on the Stockholm Programme[7] in June 2009. This approach was rejected by the Swedish Presidency but it reappeared under the Spanish Presidency in Conclusions[8] on Cybercrime adopted by EU Foreign Affairs Ministers in the General Affairs Council of April 2010.

This proposal specifically referred to shutting down ISPs and websites outside Europe. Being outside Europe and outside European jurisdiction, such powers can only be used unlawfully by reaching into the country where the allegedly infringing service is operating - a criminal offence under the definitions of the Directive. One has to wonder how the European Union can simultaneously be giving itself powers to unlawfully disable information resources outside its own jurisdiction *and* be proposing criminal sanctions against the unlawful disabling of information resources.

Conclusions

Particularly, but not only, due to the increased importance of online content due to cloud computing, it is very important for the European Parliament to re-affirm its position on state-sponsored attacks against computer systems via abuses of Internet infrastructure. As we have seen, it was all too correct when it adopted its resolution on Internet governance last year. Failure to do this threatens, as the Parliament has already said, the integrity of the global Internet.

Failure to do this will leave European citizens and businesses without any legal certainty. Risk management for their online resources will be based on guesses about the possible policies of their service provider, their own government, the governments in countries where their providers are active, the policies of the company that registered the domain names of the companies that provide them online services, the activities of other users of the same service and so on. This is unacceptable.

The Commission's strategy for this Directive is broadly solid and proportionate, pending the improvements mentioned earlier. The Parliament needs to demand, using all of the legal tools at its disposal, that the Commission remain consistent with this approach and neither give itself the power to take the kinds of measures that it is seeking to criminalise nor support or accept any third country government that seeks to do this.

5 http://californiareview.net/tag/immigration-and-customs-enforcement/
6 At least two meetings of this working group have been held this year, one in Brussels and one in Washington.
7 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0262:FIN:EN:PDF
8 http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/jha/114028.pdf