Most controversial cybercrime regulations – such as „telecommunication data retention“\(^1\) or the so-called „hacker paragraph“ (§ 202c StGB)\(^2\) – were not an invention of the German legislature, or German government. Instead, their roots can easily be traced to the European Union and the Council of Europe: The European Union's Council Framework Decision attacks against information systems,\(^3\) the Council of Europe Convention on Cybercrime\(^4\) and the Directive on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks.\(^5\) But how does national law – and especially national criminal law and criminal procedure – interact with European law, with International law? What „news“, which new provisions loom around the corner? What will this mean to the open-source approach to software and cyberspace? These are some of the questions I will address in the following presentation.

**Europeanization of Cybercrime Law - an overview**

When analyzing the Europeanization of criminal law, five different methods or approaches can be distinguished:

---

* This written presentation was last updated on 11 April 2010; any later developments regarding the Europeanization of cybercrime law will be discussed in the talk at the LinuxTag 2010 in Berlin. All documents relating to the Europeanization of criminal law mentioned in this presentation (e.g. Commission [COM, SEC], Council documents and a non-authoritative copy of the Official Journal [OJ]) may be found in the eurocrim database by the Eberhard Karls Universität Tübingen, available at [http://www.eurocrim.org/](http://www.eurocrim.org/).

1 While the German Constitutional Court (Judgement of 3 March 2010 – 1 BvR 256/08; 1 BvR 263/08; 1 BvR 586/08) held that the German implementation of data retention to be unconstitutional, it did not consider the basis in European law to be disproportionate.

2 Cf. the German Constitutional Court decision on „dual-use tools“, JR 2010, 79 and the commentary by Valerius, JR 2010, 84.


4 CETS No. 185.

• first, the harmonization of Criminal Law or – in future\(^6\) – of Criminal Procedure,

• second, the convergence of Criminal Law or Criminal Procedure by „soft law“ or the Open Method of Coordination,

• third, an improved „horizontal“ cooperation between the member states' criminal justice systems,

• fourth, a „vertical“ coordination of criminal investigations and proceedings by European institutions such as Europol and Eurojust, and

• fifth, actually lifting criminal investigations and proceedings to a true European level.

Up to now, the Europeanization of cybercrime law made use of the first four methods just described.

**Harmonization**

The European Union cannot define crimes on its own, but it can require member states to criminalize some acts in their own national criminal laws, for example, when the behaviour in question relates to „computer crime“.\(^2\) A prime example for this is the crime of „computer sabotage“, § 303b StGB, which was modified to implement the aforementioned 2005 Framework Decision on attacks against information systems.\(^3\) This Framework Decision includes requirements to criminalize illegal access to information systems (Art. 2), illegal system interference (Art. 3) and illegal data interference (Art. 4).\(^4\) Up to December 2014, the European Union cannot fine member states if they do not honour their requirements under this Framework Decision;\(^5\) therefore it is not at all surprising that the Commission has found improper implementations in several member states, with seven states not even notifying the Commission at all about their implementation.\(^6\) The German implementation, however, is

---

\(^6\) The Lisbon Treaty, which entered into force on 1 December 2009, contains an unprecedented harmonization competence relating to criminal procedure in Art. 82 para. 2 TFEU (Treaty on the Functioning of the European Union; consolidated version available in OJ C 115 of 09.05.2008, p. 1).

\(^2\) Art. 83 para. 1 TFEU. Before the Lisbon Treaty entered into force (see supra footnote 6), such regulations were based on the broadly interpreted competence to deal with „organized crime“, Art. 31 para. 1 lit. (e) TEU (Treaty on European Union – old version).

\(^3\) Cf. supra footnote 3.


considered to be mostly adequate, with the notable exception of § 303b StGB (German Penal Code) – computer sabotage. This crime is limited to information systems „of considerable importance for a third party“, which is contrary to the requirements of the Framework Decision.\(^1\)

The same requirements are also found in the 2001 Council of Europe Cybercrime Convention,\(^2\) which also adds criminalization requirements regarding illegal interception of data, misuse of devices, computer-related forgery or fraud. Germany ratified this Convention in 2009.\(^3\) There is no „real“ enforcement mechanism at all regarding this convention – as is typical for true public international law treaties.\(^4\)

**Convergence**

Convergence – or the Open Method of Coordination (OMC) – makes use of „soft law“, such as communications, reports, conclusions and other non-binding instruments. These instruments may then be utilized as arguments in policy discussions, as basis for reflection, and as ground work for „hard law“. Typically, convergence has very limited influence in the short term, but it may set much in motion, which is hard to stop afterwards. Relating to cybercrime, the European Commission utilized this approach in a 2006 communication „A strategy for a Secure Information Society“\(^5\) and a 2007 communication „Towards a general policy on the fight against cyber crime“\(^6\); the Council of the European Union followed with 2008 conclusions „on a concerted work strategy and practical measures against cybercrime“.\(^7\) It focuses, among other things, on better training for stakeholders, on public-private-cooperation, and on „invitation[s]“ to bring forward proposals for easier mutual legal assistance. Let me quote one issue from the last instrument:

---


\(^2\) Cf. supra footnote 4.

\(^3\) BGBl 2009 II p. 1242.


\(^7\) Council Conclusions of 27 November 2008 on a concerted work strategy and practical measures against cybercrime, OJ C 62 of 17.03.2009, p. 16.
“The Council ... invites ... member states to introduce ... mechanisms for blocking ... child pornography .... Service providers should be encouraged to adopt these measures“.

This is exactly which followed one year later in Germany: First there was an attempt to use public-private-cooperation to „filter“ the internet; now we have the so-called „Zugangserschwerungsgesetz“\(^1\), a law obliging ISPs to filter the Internet, which is in force but shall not be utilized at the moment, according to the Ministry of the Interior.\(^2\)

**Cooperation**

The true strength of the European Union legislation is in its enhancement of cooperation between judicial authorities. Cooperation is essential to prosecute transnational cases, such as where evidence is located in a different state – which is more the rule than the exception in cybercrime cases. Such mutual legal assistance (abbreviated „MLA“) currently focuses on the judicial and enforcement phase – easing access to suspects or convicts, for example by means of a European Arrest Warrant.\(^3\) A new focus of mutual legal instruments is, in contrast, on how to obtain evidence locate in another member state – thus, the investigation phase. Typically, such transnational obtaining of evidence is based on a „classical“ concept: sovereign states grant legal assistance case-by-case after a judicial and also an administrative-political decision. For example, a search warrant needed for a prosecution in Malawi may only be issued if the conduct in question is also a crime in Germany, all other requirements of German Criminal procedure are fulfilled, and the German authorities agree to grant legal assistance. Within Europe, mutual legal assistance may be directed or bound by treaties and conventions such as the 1959 Council of Europe Convention on Mutual Assistance in Criminal Matters,\(^4\) but that convention is hardly of interest here. Instead, let us briefly touch the so-called 2000 MLA convention by the European Union\(^5\): This convention, ratified by Germany in 2006, allows for easier cross-border interception of telecommunication, and lifts double

---

\(^1\) Gesetz zur Erschwerung des Zugangs zu kinderpornographischen Inhalten in Kommunikationsnetzen (Zugangserschwerungsgesetz – ZugErschwG), BGBl I 2010 p. 78.


\(^4\) European Convention on Mutual Assistance in Criminal Matters of 20 April 1959, CETS No. 030.

criminality requirements in some cases. Nonetheless, Europe also provides for specific safeguards against such interception of telecommunication: The awareness for the European principle of proportionality is increasing as we speak, and the right to privacy as specified in Art. 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms is interpreted by the European Court of Human Rights to mean that telecommunication interception may only be ordered for a limited duration, only in cases where a severe crime is presumed, only if a deletion procedure exists, and only if sufficient independent oversight is guaranteed.

Within the European Union and its Area of Freedom, Security and Justice, this classical model is being replaced by the principle of mutual recognition: In theory, any order of a court of any member state shall be honoured as if it were an order of the same member state. So far, there are two Framework Decisions implementing this principle which focus on the obtaining and transfer of evidence: the 2003 European Freezing Order and the 2008 European Evidence Warrant Framework Decisions. Critics such as the Commission consider these – underrated – instruments to be „somewhat `virtual’“ and therefore of few use.

What do these instruments allow for, and what are their safeguards? The European Freezing Order applies to any „data which could be produced as evidence in criminal proceedings“ (Art. 2 lit. (e)); such evidence may quickly be „frozen” or seized on behalf of another member state. Practitioners and politicians alike still aren't fully aware of the extent of the Freezing Order, which is broader than many think: It covers any location – data stored on a

---

1 For example, there is no double criminality requirement when state A (Germany) needs the help of state B (Luxembourg) to intercept telecommunications (an outgoing Skype call) from a suspect residing in state C (Italy).


3 CETS No 5. Generally speaking, the Union – while not yet directly bound by this Convention (but see Art. 6 para. 2, para. 3 TEU [Treaty on European Union]) – adheres at least to the standard specified by it, and the Charter of Fundamental Rights „reaffirms“ the rights specified by the Convention; cf. its Preamble and its Art. 52 para 3.


suspect’s computer, or in an e-mail-account at an ISP – and any content – communication data or confidential data are not excluded. In addition, there is no double criminality requirement for a long list of offences including „computer-related crime“. However, the actual „freezing“ or „seizing“ of data must be done in open, not secretly; national laws (Art. 5 para. 2) – such as the German standards on obtaining access to e-mail accounts – and its immunities (Art. 7 para. 1 lit. (b)) are to be honoured, and the European ordre public – and its principle of proportionality – is a final safeguard against overly broad uses of the Freezing Order.¹

For the actual transfer of the „frozen“ evidence, member states may either make use of the „classical“ mutual legal assistance regime,² or use the European Evidence Warrant, which still needs to be implemented in German law. Once this is done, a European Evidence Warrant itself may be used to call for a search or seizure in any cases a state presumes a „computer-related crime“. However, real-time interceptions are not covered by this instrument. In its safeguards, the European Evidence Warrant spells out, for the first time, specific and firm rules regarding the proportionality principle (Art. 7).

Coordination

The European institutions Eurojust³, Europol⁴, and – to a lesser extent – also the European Judicial Network⁵ enter the field to coordinate proceedings throughout the European Union. For example, there is now a semi-formalized procedure to determine which state shall prosecute a crime – and that one crime is indeed only prosecuted once.⁶ However, if the member states do not agree which one shall prosecute, there is no mechanism for a final decision; similarly, suspects and accused have no chance to review such a decision, even though it opens the door to „forum shopping“.

Lifting to an European level

Up to today,⁷ all criminal proceedings in the European Union are actually proceedings by the member states – there is no European „penal code“, no

² However, the far-reaching § 97 IRG (German law on mutual legal assistance) is to be noted.
European Public Prosecutor actually prosecuting crimes, and no European court of law actually judging on criminals.\(^1\) There is only one notable exception to this rule, which hardly relates to cybercrime: Some parts of investigations relating to the financial interests of the European Union are already conducted by an institution called OLAF.

**„Patches in the queue” – current developments in the Europeanization of Cybercrime Law**

The European Union is, nowadays, at a turning point in time. A few months ago, the Lisbon Treaty entered into force;\(^2\) around the same date, a new five-year programme regarding the Area of Freedom, Security and Justice was agreed upon – the so-called „Stockholm Programme – An open and secure Europe serving and protecting the citizens“\(^3\). Three major cornerstones can be discerned regarding any future Europeanization of cybercrime law:

- **First**, the Union is increasingly aware of fundamental rights, such as the proportionality principle and the right on privacy.\(^4\) For example, the statement by Commissioner Reding to evaluate the data retention directive in the next months must be seen in this light.\(^5\)

- **Second**, the Union has realized that the mutual recognition principle requires mutual trust.\(^6\) Member states – and their courts – will only execute court orders from another state if they trust the other state to honour human rights, if they trust the other state to honour the principle

\footnote{Under the Lisbon Treaty (supra footnote 6), Art. 86 para. 1 TFEU allows a group of at least nine member states to empower Eurojust (supra footnote 33) to become the European Public Prosecutor’s Office (EPP). Its competence is at first limited to the protection of the Union’s financial interests, but it may be extended to include other “serious crimes having a cross-border dimension” (Art. 86 para. 4 TFEU), such as international, high-profile cybercrime with its intrinsic borderless character. See further Brodowski in: Bellini/Brunst/Jähnke (eds.), Current Issues in IT Security, 2010, p. 121, 135.}

\footnote{However, for more than a few member states, the still applicable Art. 35 TEU – old version – allows the European Court of Justice to decide certain matters of European criminal law, if so asked by national courts (preliminary ruling procedure). For future instruments, and from December 2014 on, this will be governed by Art. 19 para. 3 lit. (b) TEU, Art. 267 TFEU.}

\footnote{Cf. supra footnote 6.}


\footnote{Cf. supra footnote 26 and Art. 8, Art. 9 Charter of Fundamental Rights.}

\footnote{See heise online, http://www.heise.de/newsticker/meldung/EU-will-Pflicht-zur-Vorratsdatenspeicherung-neu-pruefen-942207.html (accessed 17 March 2010).}

\footnote{Cf., inter alia, the Stockholm Programme (supra footnote 40), Council Document 17024/09 of 02.12.2009, pp. 5 et seq., 17 et seq., 21 et seq., 25 et seq., 28, 37; and considerations 8 and 9 of the „Roadmap“ (infra footnote 52).}
of proportionality, and if they trust the instruments aren't misused, for example for economic espionage.

- Third, the Union recognizes a primacy of prevention.¹ This means the Union prefers a proactive approach against crimes, and if this fails, it will attempt to ensure effective prosecution of crimes. There will be no „safe harbours“ for criminals in the European Union, and there will be increasing pressure to avert the commission of crimes – which, in the Union's eyes, includes the utilization of Internet „filtering“ and the banning of „hacking tools“.

Let us now look at some specific actions in the pipeline, which focus on the harmonization and cooperation aspects described above.

**Harmonization**

**Criminal Law**

The European Union is becoming more and more critical of the effectiveness and usefulness of the harmonization of criminal law. While there may be some need to define what constitutes „computer-related crimes“ – a term which is used in several instruments on legal assistance – the Stockholm Programme hardly contains any references to the harmonization of crimes.

Therefore, it seems quite unlikely that the European Union intends to use the „back door“ of the ongoing, secret negotiations on the Anti-Counterfeiting Trade Agreement² to broaden the criminal protection of intellectual property. Furthermore, the European Parliament has already used its new teeth – that international agreements now need to pass a vote in parliament – when it rejected the „SWIFT“-Agreement with the USA. If the European Parliament is not included properly in the negotiations, the chances are actually quite high that an overly broad ACTA treaty may never enter into force.

Also, I doubt the need for an updated „Directive on the fight against cybercrime“.³ Already the current framework decision seems to adequately criminalize all severe forms of cybercrime; other forms of cybercrime may be – and are – punished by member states. Therefore, current issued issues not explicitly covered by the existing framework decision – such as „cyber terrorism“, botnets, denial of service attacks, „phishing“, „pharming“ and „identity theft“ – do not require an European reaction.

---


³ A „presentation“ of such a draft Directive was mentioned in the provisional agenda for the Justice and Home Affairs Council on 25 and 26 February 2010, cf. Council Document 5006/10 of 06.01.2010; but has not taken place so far.
New harmonization legislation is suggested, however, for the fight against child pornography. The Commission proposed to update the existing Framework Decision on combating child pornography in March 2009 and March 2010.\(^1\) Besides a new obligation to criminalize certain forms of „grooming“, it also contains a new provision to criminalize to „[k]nowingly obtaining access, by means of information and communication technology, to child pornography“.\(^2\)

A side-note to the non-criminal law aspect of Internet filtering: this Directive proposal also contains a requirement for member states to „take the necessary measures to obtain the blocking of access by Internet users in their territory to Internet pages containing or disseminating child pornography“\(^3\). Similarly, the Spanish presidency asked member states in early 2010 relating to the „[i]nfringement[] of intellectual property rights, xenophobic and racist content, and child pornography: how do we combat these crimes on the internet?“\(^4\) The three questions asked relate to the current abilities of the member states – do they include a way to „block access to websites“? –, to ideas on future regulation by the European Union, and on how to „combat this type of content from servers broadcasting from States outside the European Union“. As measures such as filtering only require qualified majority votes in the Council and in the European Parliament, we will likely see more action in this field, even though the purely national, German approach to filtering the internet is not pursued at the moment.\(^5\)

**Criminal Procedure**

Based on the Lisbon Treaty, the European Union can also begin to harmonize criminal procedure. Most notable is the step-by-step approach spelled out in the Roadmap for strengthening procedural rights of suspected or accused persons in criminal proceedings\(^6\). While this does not relate to cybercrime prosecutions specifically, it does underline a new approach to fundamental rights and the principle of proportionality within the Union.


\(^2\) Art. 5 para. 3 of the 2010 proposal (supra footnote 47); and – in almost exactly the same words – Art. 4 lit (e) of the 2009 proposal (supra footnote 47). The latter was wrongly translated in the 2009 proposal into German with „... bewusste[m] Zugänglichmachren von Kinderpornographie mittels eines Informationssystems ...“; it should read „... zumindest wissentlich mittels eines Informationssystem Zugang verschafft ...“ instead.

\(^3\) Art. 21 para. 1 of the 2010 proposal (supra footnote 47); and – again in almost exactly the same words – Art. 18 of the 2009 proposal (supra footnote 47).


\(^5\) See supra footnotes 19 and 20.

However, there are also initiatives to require member states to allow for specific investigation techniques in criminal investigations. The aforementioned Proposal for a Directive on combating child pornography states that „member states shall take the necessary measures to ensure that effective investigation tools are available … allowing the possibility of covert operations at least in those cases where the use of information and communication technology is involved” (Art. 14 para. 3). While „covert operations” definitely includes „covert investigations” – „investigations into crimes by officers acting under covert or false identities” (Art. 14 para. 1, 2000 MLA Convention) –, the lack of any further specifics leaves open whether it also means covert, technical means such as the installation of key loggers, Trojan horses or the hacking into computer systems, the so-called „Online-Durchsuchung”.

**Cooperation**

The centrepiece of current discussions regarding the Europeanization of criminal law relates to a new European Evidence Warrant II, sometimes also called European Investigation Order. Such an instrument is to be based on the principle of mutual recognition. Member states are to fulfill investigation orders for any other member state; this may lead to search and seizure operations, to wiretapping and also to the obtaining of fingerprints. This new concept calls for very few grounds for refusal – the „issuing“ member state shall honour the fundamental rights and the principle of proportionality; the „executing“ member state shall trust the „issuing“ state that everything is in order. Let me first note that such is exactly what happens within Germany, or within most states: a wiretap is executed in southern Bavaria regardless whether it was issued by a near-by court or a court in Berlin.

Nonetheless, there are different, European issues at stake here, which NGOs but also member states such as Germany point out: The European Evidence Warrant I – which is still quite young and fresh, and not implemented in many member states – needs to be implemented first. Only through an evaluation of the European Evidence Warrant I the Union can indeed adhere to an „evidence-

---


2 See supra footnote 47. The 2009 proposal (supra footnote 47) also contained a similar requirement in Art. 12 para. 5.

3 The German Constitutional Court held that such measures may be constitutional, BVerfGE 120, 274.

4 For the German legislature, see BR-Drs. 906/09; BT-Ausschussdrs. 17(6)003; for NGOs the Statement by the German Federal Bar (BRAK) No. 2/2010. See also Schünemann/Roger ZIS 2010, 92; Brodowski in: Bellini/Brunst/Jähnke (eds.), Current Issues in IT Security, 2010, pp. 121, 129 et seq.
based criminal policy”. Furthermore, the mutual trust between member states must be strengthened before investigation orders may be mutually recognized. Introducing an European Evidence Warrant II too fast and with too few safeguards opens the door for economic espionage, and disregards the right to effective defence also in transnational criminal defence. Despite these strong objections, shared by the German government and the German legislature, it must be noted that such an European Investigation Order might be agreed upon by a qualified majority of member states and the European Parliament. Therefore, this European issue requires a thoughtful discussion on the European level – a „no“ by Berlin isn't sufficient at all to block new developments in the Area of Security, Freedom and Justice.

Finally, after an era of enhancing cooperation between the member states of the European Union, the Union now also takes a look beyond it's own nose: Be it the agreements on mutual legal assistance with the United States\(^1\) or with Japan\(^2\); be it the (failed) „SWIFT“-Agreement with the United States\(^3\): Prosecuting cross-border crime – such as cybercrime – will also be made more effective beyond the European Union. However, let me name just two examples for existing and effective safeguards against overly broad criminal prosecution by foreign states: first, it is unlikely that in the near or medium term Germany will assist non-member states in prosecuting behaviour which is not a crime in Germany; the „double criminality“ requirement will persist in such third-state constellations. Second, while Germans may be extradited to other member states of the European Union, they may not be extradited to third countries.\(^4\)

**Consequences for Open-Source Software?**

But what does all this mean for Open-Source Software? Let me briefly address three major aspects: the protection of intellectual property, the primacy of prevention, and an increasing awareness for safe and secure software.

---

1 OJ 181 of 17.07.2003, p. 34.
3 OJ 8 of 13.01.2010, p. 9.
4 Art. 16 para. 2 Fundamental Law (Grundgesetz). However, this does not protect Germans travelling abroad (e.g. to the United Kingdom) to be extradited to a third state (e.g. the United States).
**Protection of Intellectual Property?**

First of all – and probably most controversial to those following this presentation – the European Union strongly emphasises the value of intellectual property and acknowledges a need for its protection. This is something, however, at least large parts of the Open-Source Community agree upon: If companies sell products which use modified GPL-licensed software, the Open-Source Community is forcefully protecting their own copyrights. So this is, in principle, nothing to fear.

A distinct point relates to the field of „software patents“ – and the enforcement of such „software patents“ by means of criminal law. Much has been talked about this issue, and much will still be talked about it in future, for there is large disagreement whether „software“ can be patented at all. Let me just point out one aspect: part of the issue might be the overly long protection period – about twenty years – not fitting to the fast evolving development of software.

And yet another, controversial aspect relates to „digital rights management“ – or, more pointedly, criminal law provisions against the circumvention of intellectual property protection. The much-feared „hacker paragraph“ – § 202c German Penal Code – turned out not to be a threat in practice; further criminalization does not seem to loom around the corner.

**Primacy of Prevention**

The European Union acknowledges a primacy of prevention. This means there is a need for better training of police with regard to the Internet – so that they can better discern what is allowed, and what is not; so that they can better realize what is proportionate, and what is not. Furthermore, there are calls for hundreds if not thousands new police officers specifically addressing crimes committed by means of the Internet. The focus of such a „policing” is not low-key infringements of intellectual property – the focus of such initiatives seems to be the protection of minors, for example against „grooming”; the protection against fraud, identity theft, and other forms of economic crimes.

Furthermore, the primacy of prevention also calls for „hardened“ software and „hardened“ hardware. Safe and secure software – which is not exploitable, which warns users on unsafe actions – is one of the best methods to raise the bar for criminals. The security of Open-Source Software is one of its greatest strengths, and this strength should be made much use of under the „primacy of prevention“.

**Awareness**

Closely related with this is my last point: Citizens are more aware than ever of the need for software which focuses on security, reliability and anonymity as well as data protection. More than ever they seem willing to try out Open-
Source Software, for it promises to provide and honour these values more than any other software.

To summarize: While there are indeed many risks associated with the Europeanization of cybercrime law, the safeguards are evolving, too – and using and writing good software is one of the best safeguards there are.