CONTENTS

SPECIAL EDITION
THE FUTURE OF CRIMINALISATION AFTER LISBON

EDITORIAL

The Future of Criminalisation after Lisbon
VALSAMIS MITSILEGAS 225

ARTICLES

Criminalisation as a Last Resort: A National Principle under the Pressure of Europeanisation?
JANNEMIEKE W. OUWERKERK 228

The Criminalisation Power of the European Union after Lisbon and the Principle of Democratic Legitimacy
PERRINE SIMON 242

The Criminal Sanctions against the Illicit Proceeds of Criminal Organisations
Anna Maria Maugeri 257

Implementing Action against Trafficking of Human Beings under the TFEU: A Preliminary Analysis
Tom Obokata and Brian Payne 298

The European Harmonisation in the Sector of Protection of the Environment through Criminal Law: The Results Achieved and Further Needs for Intervention
GRAZIA MARIA VAGLIASINDI 320

Gearing up the Fight against Cybercrime in the European Union: A New Set of Rules and the Establishment of the European Cybercrime Centre (EC3)
LAVIERO BUONO 332

<table>
<thead>
<tr>
<th>Title</th>
<th>Authors</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>The New European Commission Anti-Corruption Package:</td>
<td>Emilija Taseva</td>
<td>344</td>
</tr>
<tr>
<td>Towards a More Efficient Fight against Corruption?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>The Europeanisation of Polish Substantive Criminal Law:</td>
<td>Celina Nowak</td>
<td>363</td>
</tr>
<tr>
<td>How the European Instruments Influenced Criminalisation in Polish Law</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Behind the Scenes in the Negotiation of EU Criminal Justice Legislation</td>
<td>Harriet Nowell-Smith</td>
<td>381</td>
</tr>
<tr>
<td>Testing the Principle of Subsidiarity in EU Criminal Policy: The Omitted Exercise in the Recent EU Documents on Principles for Substantive European Criminal Law</td>
<td>Paul De Hert and Irene Wieczorek</td>
<td>394</td>
</tr>
</tbody>
</table>

ANALYSIS AND OPINION

Italian Court of Cassation Delivers Its Ruling on the Abu Omar Case: What to Expect from the Decision? | Irene Wieczorek | 412  |
GEARING UP THE FIGHT AGAINST CYBERCRIME IN THE EUROPEAN UNION: A NEW SET OF RULES AND THE ESTABLISHMENT OF THE EUROPEAN CYBERCRIME CENTRE (EC3)

Laviero Buono*

ABSTRACT

In the never-ending cat-and-mouse game between the law and the (r)evolution of technologies there always seems to be new mice around. Botnet attacks, phishing, social networks, Voice over Internet Protocols (VoIPs) and geo-locative software are posing new menaces that were unknown, or largely underestimated, only few years ago. Although technology neutral, the legislation should, to the extent possible, respond to these constantly changing trends and threats. This article focuses on the European Union’s new approach to fight cybercrime giving a preliminary assessment of the new proposal for a Directive on attacks against information systems, intended to replace the 2005 Framework Decision. The article also explores the establishment of the European Cybercrime Centre (EC3) by 2013 and its key features.

Keywords: child pornography on the internet; cybercrime; European Cybercrime Centre (EC3); EU legislation; EU policy

1. INTRODUCTION

For the past ten years the European Union (EU) has made important efforts to develop an adequate legal framework to address the challenge of cybercrime. The two major ‘hard law’ legal instruments addressing this issue were adopted in mid-2000s and

* Laviero Buono is Head of Section for European Criminal Law at the Academy of European Law (ERA), Trier, Germany. All comments and views expressed in this article are those of the author alone.
consisted of two EU Framework Decisions.\(^1\) Both measures aimed at establishing minimum rules concerning the definition of criminal offences and sanctions in the areas of attacks against information systems and child pornography on the internet. However, recently, in light of the profound changes brought by Information and Communication Technologies (ICTs), both instruments have been under intensive discussion among EU Member States. In 2011 the Directive on combating the sexual abuse and sexual exploitation of children and child pornography\(^2\) was adopted. The new proposal for a Directive to repeal the 2005 Framework Decision on attacks against information systems is currently heading towards formal adoption\(^3\) in accordance with the new ordinary procedure set by the Lisbon Treaty in Article 82 that places the European Parliament on an equal footing with the Council of the EU. After its adoption, EU Member States will have two years to bring into force the laws, regulations and administrative provisions necessary to comply with both Directives (‘transposition’ phase).

Although adjusted a number of times during the negotiations to accommodate the positions expressed by Member States’ delegations and the European Parliament, compared to the old Framework Decisions, both Directives contain new key elements.

The proposal for a Directive on attacks against information systems makes clear reference to large scale attacks and botnets,\(^4\) it introduces the criminalisation of ‘illegal interception’, it strengthens the existing structure of 24/7 contact points, including an obligation to answer within eight hours to urgent requests, it includes the obligation for EU Member States to collect basic statistical data on cybercrimes and, all in all, it raises the level of criminal penalties. Among the most important new features of the Directive on combating the sexual abuse, sexual exploitation of children and child pornography, it is certainly worth noticing, also here, the overall increase of penalties (which can now range from one to ten years in prison), the criminalisation of ‘grooming’, i.e. the solicitation of children on the internet for sexual purposes, and the introduction of new measures against websites containing or


\(^{3}\) At the time of writing, a ‘compromise package’ proposal for Directive on attacks against information systems has been provisionally endorsed by the Council of the EU.

\(^{4}\) In the context of the Proposal for Directive of the European Parliament and the Council on Attacks against Information Systems, replacing Council Framework Decision 2005/222/JHA – General Approach (Council of the EU, Interinstitutional file 2010/0273 COD) botnets are defined as ‘network of computers that have been infected by malicious software (computer virus). Such a network of compromised computers (“zombies”) may be activated to perform specific actions, such as attacking information systems (cyber attacks). These “zombies” can be controlled – often without the knowledge of the users of the compromised computers – by another computer. This ‘controlling’ computer is also known as the “command-and-control centre”’.

disseminating child pornography, mainly consisting in prompt removal at source and (voluntary) blocking by EU Member States.\(^5\)

These new elements clearly show that emerging technologies challenged the existing EU legal regime and created a need for a legal reform. The European Union responded to it, showing great flexibility, by amending legal instruments that were adopted ‘only’ five-six years ago. It remains to be seen however, whether this new EU legal regime evolved in response to new technological trends will be fit enough, from a substantive and procedural criminal law point of view, to face the challenges posed by peer-to-peer traffic, encryption software and circumvention blocking tools.

This paper considers the main features of the new proposed Directive on attacks against information systems and the recent launch of the European Cybercrime Centre (EC3) intended to serve as focal point in the fight against cybercrime. First, the main EU initiatives launched in this field are chronicled leading from the ‘eEurope’ Communication of 1999\(^6\) right up to the 2012 proposals (Sections 2 and 3). This flashback will shed interesting light on how and why the European Union decided to gear up its fight against the illegal use of internet, to strike harder on paedophiles and to set up an ad hoc dedicated Cybercrime Centre.

## 2. TEN YEARS OF EU EFFORTS TO TACKLE CYBERCRIME (FIRST PHASE: 1999–2005)

It is surely difficult to indicate the precise date when the European Union decided to address the cybercrime phenomenon. Already in the late 90s the European Commission published a Communication on the illegal and harmful content on the internet.\(^7\) It was a first attempt trying to develop a legal framework to clarify the rules and regulations governing the liability of access and host service providers. On the wave of this Communication and upon request of the 1997 European Council of Amsterdam,\(^8\) the European Commission then contracted the University of Würzburg, in Germany, to conduct a study which could provide up-to-date information on the legal issues of

\(^5\) To this extent, it has to be noted that the original proposal of the European Commission had it mandatory to have law to block websites containing or disseminating child pornography. However, during the negotiations with the European Parliament, amendments made it voluntary to introduce blocking in Member States. Therefore, according to the new wording: ‘Member States may set up procedures to block access by Internet users in their territory to Internet pages containing or disseminating child pornography in accordance with national law’.


\(^7\) Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions on illegal and harmful content on the Internet (COM(1996)487).

computer-related crime, especially with respect to substantive criminal law and procedural criminal law.\(^9\) Based on this study, and in order to ensure that the goals set by the 2000 Lisbon European Council\(^10\) were achieved, in June 2000, the European Commission, together with the Council, prepared the ‘eEurope Action Plan’.\(^11\) However, at political level, it was the Tampere Programme that for the first time, in 1999, acknowledged that ‘high-tech crime’ had to be included in efforts to reach agreement on common definitions and penalties for a number of criminal offences.\(^12\) Following the Tampere political guidelines, the European Commission issued in 2001 the first ‘soft law’ instrument to specifically tackle cybercrime: ‘Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating computer-related crimes’,\(^13\) also known as the Communication on cybercrime. To this extent, it is worth noticing that at the beginning of 2000 there was a clear semantic confusion: whereas the Tampere Programme addressed this phenomenon as ‘high-tech crime’, the official Communication of the European Commission addressed it as ‘computer-related crime’ and the jargon referred to is as ‘cybercrime’. All three terms were used interchangeably to picture the same typology of crime, namely: a crime that had its key feature in the use of ICT facilities regardless of whether the computer or device was the target (such as in cracking cases\(^14\) or Denial of Service Attacks – DOS\(^15\)) or merely a tool used to eventually commit the criminal offence (like in child pornography cases).

The year 2001 marked a very important date in the fight against cybercrime not only at the European but also at the global level. In Budapest, on 23 November 2001, the Council of Europe Convention on Cybercrime\(^16\) was signed by 30 Countries,
including non-members of the Council of Europe such as Canada, United States, Japan and South Africa. After ten years, the Council of Europe Convention on Cybercrime remains today a key instrument providing minimal legal and procedural standards for fighting cybercrime. The European Union, on several occasions, acknowledged the importance of the Cybercrime Convention and encouraged EU Member States which have not yet ratified it to do so as soon as possible. In light of this new European framework, the EU started internal discussions on a new legal instrument to tackle cybercrime. The discussions ended with the adoption in 2005 of the Framework Decision on attacks against information systems. However, contrary to the Council of Europe Convention on Cybercrime, which addresses the fight against cybercrime 

\textit{sensu lato}, issues related to content-related crimes (such as child pornography), computer-related offences (such as fraud and forgery on line) and copyright violations were kept out of the EU Framework Decision and addressed by other legal instruments.

3. **TEN YEARS OF EU EFFORTS TO TACKLE CYBERCRIME (SECOND PHASE: 2006–2012)**

The second half of the 2000s marked a decisive change of pace in the EU fight against cybercrime. After the Estonian cyber attack in April-May 2007, the European Union started focusing on issues such as ‘large scale cyber attacks’ and ‘botnets’. The Commission Communication ‘Towards a general strategy on the fight against cybercrime’, adopted on 22 May 2007 indicated as key operational priorities an effective dialogue with industry (public/private partnership) and a coordinated financial support for training and research activities in the field of cybercrime. This Communication was echoed by the October 2008 Justice and Home Affairs Council that discussed cybercrime in the context of European cooperation on internal security. It adopted conclusions on setting up national alert platforms and a European alert platform for reporting offences detected on the internet, and conclusions on promoting closer operational cooperation among the law enforcement authorities of the Member

---

17 See Communication from the Commission to the European Parliament, the Council and the Committee of the Regions – Towards a general policy on the fight against cyber crime (COM(2007)267 final), p. 6: ‘Considering the agreed importance of the Convention, the Commission will encourage Member States and relevant third countries to ratify the Convention and consider the possibility for the European Community to become a party to the Convention’.  


States. A few months later, as a result of a high-level Ministerial conference held under the auspices of the Czech Presidency of the EU in Prague on 20 April 2009, entitled: ‘Safer Internet for Children – fighting together against illegal content and conduct on-line’, the so called ‘Prague Declaration’ was adopted. The Declaration is to a large extent dedicated to the process of improving cooperation between all stakeholders in the field of promoting safer internet and mobile communications, especially for children.

Still, at political level, precise reference to the fight against cybercrime was made in the third multi-annual Programme in the area of freedom, security and justice, known as ‘the Stockholm Programme’, which was endorsed by the European Council in December 2009. The Programme priorities were reflected in the 2010 European Commission’s Action Plan setting out concrete implementing measures and actions together with a timetable for their adoption. Regarding the fight against cybercrime, as general orientations set out in the Programme, the European Commission and Europol were invited to take measures for enhancing/improving public private partnerships and to step up strategic analysis on cybercrime, while all Member States were called upon to improve judicial cooperation in cybercrime cases.

However, cybercrime was established as serious crime with a cross-border dimension in 2009, by including ‘computer crime’ in Article 83(2) of the new Lisbon Treaty, in the same category as similarly severe crimes: terrorism, trafficking in human beings and sexual exploitation of women and children, illicit drug trafficking, illicit arms trafficking, money laundering, corruption, counterfeiting of means of payment and organised crime.

Finally, in recent years, the fight against cybercrime was addressed by two other important EU policy documents. In 2010, the EU presented the Digital Agenda for

---

24 Some EU Member States attach particular importance to the fight against cybercrime. This is the case of The Netherlands which recently announced its readiness to devote additional public funds to internet trend watching and to tracing and prosecution of cybercrime. See Council of the EU document: ‘Position of the Netherlands on fighting cyber crime’ (Council of the EU, CRIMORG 117, 12225/09).
Europe, the first flagship initiative adopted under the Europe 2020 strategy. The Agenda recognised the need to address the rise of new forms of crime, in particular cybercrime, at European level. In 2011, on the basis of Article 71 of the Lisbon Treaty, the Standing Committee on Operational Cooperation on Internal Security (COSI) was established. The Standing Committee consists of high-level officials from EU States’ ministries of the interior, the Commission, Eurojust, Europol, Frontex and other relevant bodies’ representatives and serves to develop, monitor and implement the EU Internal Security Strategy which identifies five strategic objectives including, for 2013, the establishment of the European Cybercrime Centre (see chapter 5).

4. KEY FEATURES OF THE NEW PROPOSAL FOR AN EU DIRECTIVE ON ATTACKS AGAINST INFORMATION SYSTEMS

In the second half of the 2000s, several emerging cyber threats materialised in attacks across Europe, in particular in the emergence of large-scale simultaneous attacks against information systems. Such attacks had not been the centre of attention when the 2005 Framework Decision was adopted. In response to these developments, the European Union deemed it appropriate to consider actions aimed at devising better responses to these new threats.

As a general rule and in an effort to avoid being outpaced by rapidly changing technology, any piece of legislation in the field of cybercrime at national, European and international level, should be as technologically neutral as possible. To this extent, for example, although the proposal for the EU Directive on attacks against information systems does not specifically refer to ‘botnets’, it still takes into account the damages that can be caused by a ‘significant number of information systems’, indirectly referring to the effects provoked by a network of compromised computers. In the explanatory memorandum of the proposal it is emphasised that large-scale attacks (attacks that can either be carried out with the use of tools affecting significant numbers of information systems or attacks that cause considerable damage, e.g. in terms of disrupted system services, financial cost, loss of personal data, etc.) have a major impact on the functioning of the target itself and on society as a whole. The

---

27 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions – A Digital Agenda for Europe (COM(2010)245, 19 May 2010).
30 To this extent, it has to be noted that the need to updated the EU legislation was mainly triggered by the Estonian cyber attack of April-May 2007.
2005 EU Framework Decision clearly did not fully address the potential threat posed to society by large scale attacks nor did it take sufficient account of the gravity of the crimes and sanctions against them.

However, before opting for a new Directive, in the framework of a general impact assessment, the European Union examined various policy options among which were also to keep the status quo (option 1), to introduce brand new comprehensive EU legislation against cybercrime (option 4) and to update the Council of Europe Convention on Cybercrime (option 5).\(^{31}\) It was eventually decided to go for a targeted update of the 2005 Framework Decision.

Aside from botnets and large scale attacks, other new elements were contemplated by the new proposal for a Directive. Among these were the introduction of ‘illegal interception’ of information systems as a criminal offence (mainly aligning the EU legislation with the Council of Europe standards), the strengthening of the existing 24/7 contact points (including an obligation to answer within eight hours to urgent requests) and the obligation to collect basic statistical data on cybercrimes. Furthermore, the proposed Directive raises considerably the level of criminal penalties. Once formally adopted, EU Member States will have two years to transpose these legal measures into national legislation. However, for this new EU instrument, contrary to the 2005 Framework Decision which was adopted under the so-called ‘third pillar’, the Lisbon Treaty allows the Commission to take legal action to make sure that Member States enforce these rules.

Although the proposed EU Directive cannot be seen as a panacea for all crimes committed on the Internet, it can be considered as an important tool in the fight against cybercrime. At global level, there has been such a mushrooming of cyber initiatives\(^{32}\) that harmonising legislation and penalties in one of the healthiest Regions of the World should be greeted as a big step forward for the EU community and a great deterrent for potential perpetrators.

5. THE ESTABLISHING OF THE EUROPEAN CYBERCRIME CENTRE (EC3)

In April 2010, in adopting an Action Plan to implement the concerted strategy to combat cybercrime,\(^{33}\) the Council invited the European Commission to draw up a


\(^{33}\) Draft Council conclusions on an Action Plan to implement the concerted strategy to combat cybercrime (Council of the EU, 5957/2/10 CRIMORG 22 ENFOPOL 32).
feasibility study on the possibility of creating a Cybercrime Centre to perform a number of tasks in the fight against cybercrime. Based on the study, published in February 2012, on 28 March 2012 the European Commission adopted a Communication titled: ‘Tackling Crime in our Digital Age: Establishing a European Cybercrime Centre’. The Centre, commonly referred as ‘EC3’ will be established within Europol in The Hague. To this extent, it has to be noted that the 2009 Council Decision establishing Europol already conferred to the EU Agency the competence to cover computer crime and that the Europol Organised Crime Threat Assessment (OCTA) 2011 identified cybercrime as a criminal phenomenon which required high levels of intelligence coordination and analysis in the framework of law enforcement cooperation in order to gain accurate insight and provide targeted responses.

The EC3 should become the European Union’s focal point in the fight against cybercrime, responding to queries on specific technical issues from cybercrime investigators, prosecutors and judges, as well as the private sector, and providing operational support in concrete investigations. The EC3’s added value should lie in its focus on major strands of cybercrime, such as fighting online fraud generating large criminal profits, online child sexual abuse material, and cyber-attacks affecting critical infrastructure and information systems in the EU.

In terms of EC3’s work, the Communication lists four main tasks:

- Serve as the European cybercrime information focal point
- Pool European cybercrime expertise to support Members States in capacity building
- Provide support to Member States’ cybercrime investigations
- Become the collective voice of European cybercrime investigators across law enforcement and the judiciary.

36 Before opting for the establishing of the EC3 within Europol in The Hague, a broad range of possible options stemming from maintaining the status quo to a wholly EU new agency were scrutinised in the feasibility study. These options also considered the setting up of the EC3 within Eurojust, ENISA and the EC3 as ‘virtual centre’. For a complete analysis of all options considered see chapter 6 and 7 of the study.
Besides the decision to increase, overall, the financial and human resources to more efficiently combat cybercrime for the years ahead, a key novelty of the EC3 will be its preparedness to exchange information with (and respond to queries from) partners that go beyond the law enforcement community, namely judicial authorities (that in this context have to be interpreted sensu lato, i.e. including judges and prosecutors) and the private sector/internet industry. Such a shared cross-community approach (that will embrace also the know-how of other partners such as Eurojust, CEPOL, ENISA and others) to tackling cybercrime is without doubt one of the key features of the EC3.

Through the use of information and communication technologies, potentially almost all forms of ‘traditional’ crimes can be committed via internet in the future. This is the case as regards, inter alia, the recruitment and training of terrorists, illegal online gambling, fraud committed using cloned credit cards and the trade of sexual images of children. If potentially all crimes can be committed with the use of Internet, bilateral cooperation between law enforcement authorities in different countries is insufficient. Large-scale cross-border operations to tackle cybercrime cannot be successfully conducted by police forces alone. Their meritorious efforts can vanish if the ‘investigative’ circle is not ideally closed by the presence of judges and prosecutors equipped with the adequate skills necessary to cope with internet-related offenses. This means focussing on the development of overall awareness-raising initiatives combined with basic and specialised training for prosecutors and judges who will ultimately investigate and adjudicate upon cybercrime cases. Without such training, cases related to online fraud and forgery offences, dissemination of child sexual abuse material on the internet, cybercrimes affecting critical infrastructure and information systems in the EU and all other crimes that can be committed using ICT facilities will be exacerbated by the lack of knowledge of internet fundamentals and cyber-criminals’ modus operandi.40 To this extent, the European Commission Communication establishing the EC3 stresses that: ‘Effective involvement of the judiciary in tackling cybercrime is of paramount importance for improving the prosecution or serious cybercriminals across the Member States’.41

High-tech crimes cannot be adequately investigated, prosecuted and adjudicated upon without cooperation with the private sector. Dialogue with internet service providers and internet industry players will be key for law enforcement authorities, judges and prosecutors to be able to prevent, detect and respond to crimes committed using information and communication technologies facilities. Therefore it is crucial to initiate such dialogue and start facing new complex issues of international relations related to national sovereignty and territoriality. Also this issue seems to be adequately

---

40 On the need to train judges and prosecutors on cybercrime-related issues see L. Buono, ‘Investigating and prosecuting crimes in the cyberspace: European training schemes for judges and prosecutors’ (ERA Forum, Volume 10, Number 2, August 2010).

stressed by the Communication on the establishing of the EC3 that clearly states: 'Building trust and confidence between the private sector and law enforcement authorities is of utmost importance in the fight against cybercrime'.

Finally, in setting up the EC3, one of the key challenges is to preserve and increase security whilst paying due respect to privacy protection and other fundamental rights. There is little doubt that EC3’s operations will require vast processing of data which often involves risks for citizens’ privacy. To safeguard and ensure high standards of data protection, Europol already has a robust and tested regime in place. Different ad hoc projects carried out by Europol (such as CYBORG, TERMINAL and TWINS) process data where computers and networks are involved. That data protection must be an essential element in the creation of the EC3 has been clearly stressed by the European Data Protection Supervisor (EDPS) which called on the European Commission to consider that activities of the EC3 should be based on a solid data protection scheme, and that this must be reflected in its establishment.

6. CONCLUSIONS

The above analysis of the recent development of computer crime has illustrated a complex pattern of crimes as well as a multitude of different new problems, which, until now, within the European Union, seem to have been addressed in practice independently from each other and without a solid basic legal and policy concept. The two EU Framework Decisions which addressed issues of tackling child pornography and attacks against information systems, adopted in the mid-2000s under the ‘third pillar’ regime, were not adequately transposed into the EU Member States’ legislation. With the entry into force of the Lisbon Treaty in December 2009, the European Union received a clear mandate to deal with computer crime offences. As a direct result, in

43 For an overview of Europol’s systems and tools in fighting cybercrime and their data protection’s implications see D. Drewer and J. Ellermann, ‘Europol’s data protection framework as an asset in the fight against cybercrime’ (forthcoming Issue ERA Forum, Volume 12, Number 3, October-November 2012).
44 Opinion of the European Data Protection Supervisor on the Communication from the European Commission to the Council and the European Parliament on the establishment of a European Cybercrime Centre (Council of the EU, 12404/12, 10 July 2012).
45 Article 12(2) of the EU Framework Decision on attacks against information systems placed an obligation on Member States to transmit, by 16 March 2007, the text of any provisions transposing the obligations imposed under the FD into their national law. According to the European Commission, by that date, only one State (Sweden) had transmitted a national text and even that was incomplete. On this point see: Report from the Commission to the Council based on Article 12 of the Council Framework Decision of 24 February 2005 on attacks against information systems (COM(2008)448 final, 14 July 2008, p. 2).
the past months, important developments within the EU took place, at both the legal and policy levels.

At legal level, two new legal instruments were (re)launched. The first is the new Directive on combating the sexual abuse and sexual exploitation of children and child pornography, adopted in November 2011, which substantially improved the EU rules by addressing new forms of abuse and exploitation of children using information technology, meeting specific needs of child victims and introducing adequate measure to prevent offences. The second is the new (proposed) Directive on attacks against information systems which makes clear reference to large scale attacks, it introduces the criminalisation of ‘illegal interception’, it strengthens the existing structure of 24/7 contact points, it includes the obligation for EU Member States to collect basic statistical data on cybercrimes and, all in all, it raises the level of criminal penalties. The formal adoption of this latter instrument is expected by the end of 2012.

At policy level, the major breakthrough in fighting cybercrime at EU level is surely represented by the launch of the European Cybercrime Centre (expected to start operations in January 2013) to help protect European citizens and businesses against mounting cyber-threats. The Centre will serve as a platform for European cybercrime law enforcement and judicial authorities, where they can have a collective voice in discussions with internet industry players, the research community, users’ associations and civil society organisations.

The two levels are interchangeable and complement each other. They are essential axes of the holistic EU approach to fighting cybercrime. This means that there can barely be effective legislation without a body set to pool expertise, provide support and become the collective voice of the EU in the fight against cybercrime. A body that, in the years ahead, on the basis of concrete needs analysis and unique expertise in the area, can ultimately advise EU policy makers in drafting and reviewing legal instruments. But it also means that the work of the new EU cybercrime ‘focal point’ will be greatly facilitated if at least minimum rules concerning the definition of criminal offences and related sanctions in certain cybercrime-related areas are in place, fully transposed and legally binding, in all EU Member States.
The New Journal of European Criminal law is the leading international journal on European criminal law. It analyses, discusses, defines, develops and improves criminal law in Europe and in particular criminal law as it is drawn up by the European Union and the Council of Europe.

European criminal law is an established and recognised legal discipline. It is not confined to the European Union, but it extends to all forty-seven States of the Council of Europe. Institutionally speaking European criminal law is driven by both the EU and the Council of Europe under the supervision and influence of the Court of Justice of the European Communities as far as the EU is concerned and by the European Court of Human Rights as regards the Council of Europe.

Although European criminal law is a recognised body of law, it constitutes by no means a perfect system and it requires analysis and discussion, so that it may develop and improve. Analysis and discussion cannot be the exclusive preserve of the legislative and judicial bodies; others must contribute to ensure balanced solutions.

Nor is European criminal law confined to what is traditionally considered as criminal law. It extends to and complements environmental law and competition law. As regards competition law the New Journal of European Criminal Law is running a section dedicated to the criminalisation of competition law and of hardcore cartels in particular. It is the first ever legal journal to treat criminal and competition law disciplines related at their interface.

The New Journal of European Criminal Law has two patrons: the European Criminal Bar Association (ECBA) and the European Criminal Law Academic Network (ECLAN). It serves as a forum for both legal practitioners and academics interested in issues related to European criminal law. Its editorial board comprises as wide a cross-section of the legal profession as possible. The New Journal of European Criminal Law solicits articles from all those involved in criminal law in its European dimension. It seeks a large variety of articles, on a spectrum ranging from short case notes with little or no comment, to opinionated comments on developments to long in-depth critiques of judgements and legislative measures with proposals for reform or change.

To ensure originality, the New Journal of European Criminal Law has a peer-review system which is applied to long in-depth articles. This is necessary to maintain the position of the New Journal of European Criminal Law as the pre-eminent journal in its field and to guarantee the continued quality of its contents. For the same reason an Advisory Committee, composed of several authorities on the subject of European criminal law, supervises the Journal and its future development.

Thus, each issue comprises i.a. an editorial, in-depth articles submitted to a peer review, cutting-edge and to-the-point analysis & opinions, case law notes and legislative updates.
New Journal of European Criminal law

General Editors
Scott Crosby, M.A., LL.B., LL.M., Advocate, Brussels (Editor in chief) – Professor RA Holger Matt, Johann Wolfgang Goethe University, Frankfurt/Main (Deputy editor) – Professor Paul de Hert, Vrije Universiteit Brussel, University of Tilburg (Deputy editor)

Advisory Board
Professor Sir Francis Jacobs QC, London, Honorary Chairman – Professor John Vervaele, University of Utrecht – Professor John Spencer QC, University of Cambridge – Professor Ulrich Sieber, Max-Plack-Institut, Feiburg im Breisgau – Professor Robert Roth, University of Geneva

Editorial Board

Assistant Editors
Karen Weis and Silvia Santoro, Brussels

Order form

Fax this form to Intersentia +32 3 658 71 21

☐ I would like to order ............... subscription(s) to New Journal of European Criminal law (NJECI) at 145 euro per subscription.

Please charge my credit card:
☐ Visa
☐ MasterCard

Name of cardholder:

Card number:

Expiry date:

Signature

Mr | Ms | Prof | Dr

Name: First name:

Company: Job description:

Street: No.:

Postal code: City:

Country:

Telephone: Fax:

E-mail: VAT no.:

Signature Date

Groenstraat 31
BE-2640 Mortsel
Belgium

T +32 3 680 15 50
F +32 3 658 71 21

www.intersentia.com
mail@intersentia.be

New Journal of European Criminal law

Fax this form to Intersentia +32 3 658 71 21

☐ I would like to order ............... subscription(s) to New Journal of European Criminal law (NJECI) at 145 euro per subscription.

Please charge my credit card:
☐ Visa
☐ MasterCard

Name of cardholder:

Card number:

Expiry date:

Signature

Mr | Ms | Prof | Dr

Name: First name:

Company: Job description:

Street: No.:

Postal code: City:

Country:

Telephone: Fax:

E-mail: VAT no.:

Signature Date

Groenstraat 31
BE-2640 Mortsel
Belgium

T +32 3 680 15 50
F +32 3 658 71 21

www.intersentia.com
mail@intersentia.be

New Journal of European Criminal law

Fax this form to Intersentia +32 3 658 71 21

☐ I would like to order ............... subscription(s) to New Journal of European Criminal law (NJECI) at 145 euro per subscription.

Please charge my credit card:
☐ Visa
☐ MasterCard

Name of cardholder:

Card number:

Expiry date:

Signature

Mr | Ms | Prof | Dr

Name: First name:

Company: Job description:

Street: No.:

Postal code: City:

Country:

Telephone: Fax:

E-mail: VAT no.:

Signature Date

Groenstraat 31
BE-2640 Mortsel
Belgium

T +32 3 680 15 50
F +32 3 658 71 21

www.intersentia.com
mail@intersentia.be