



Strasbourg, 07 June 2013

PC-GR-COT (2013) 3 EN

**AD HOC DRAFTING GROUP ON TRANSNATIONAL ORGANISED CRIME
(PC-GR-COT)**

Report prepared by Mr Michael LEVI
Cardiff University

Introduction

The principal aims of the Group are:

1. the identification of relevant and emerging transnational organised crime issues which require a criminal law response;
2. the development, in close co-ordination with strategic partners, of pan-European strategies, and where possible, common policies on preventing and combating transnational organised crime;
3. the collection, assessment and exchange of best practices in the prevention of, and fight against, transnational organised crime from all Council of Europe member States; and
4. the preparation of a White Paper for consideration by the Committee of Ministers, after validation by the CDPC, on selected trends and developments in transnational organised crime in the Council of Europe member States which may be considered as priority areas, focusing on developing an integrated strategic approach to combating transnational organised crime and identifying common responses to major threats to the rule of law and security of citizens.

In discharging its tasks, the PC-GR-COT shall consider the previous and current work carried out in this field by the relevant international and supranational organisations, notably the European Union, and the previous work of the Council of Europe in this area.

Selected Trends and Developments

An Interpretative Framework

Our knowledge of organised crime is necessarily imperfect. Indeed that imperfection may even be desirable, since if it was perfect we might be living in a totalitarian society in which such crimes were officially tolerated because they were committed by or with the support of a 'rent-seeking' elite. The notion of a trend in organised crime contains two elements which are separable in principle but often mixed up in practice. The first is the evolution of how criminals organise themselves and relate to each other – the 'organised' part. The second is the evolution of what sorts of crimes are being committed, in what quantities, and with what social effects – the 'crime' and 'harm' parts. When we consider why organised crime is worse than just 'crime' it is because we think that organised criminals have a greater capacity to do more harm and to be more resilient to counter-measures than do 'unorganised' or individual criminals.

Year on year, there may be only modest changes in crime patterns, but the big shifts tends to be in (a) the use of ICT to commit offences and to facilitate communication between offenders (far less in the money laundering process itself); and (b) in the substitution of 'legal highs' for illegal drugs (other than opiates). There may often be shifts in the geographic patterns of supply routes, in response to our control efforts. Finally, there may be shifts in our efforts against organised crime, and these efforts may generate insights into problems in the mutual legal assistance process, at the points of investigation, charge, and prosecution (including the freezing/seizure and the confiscation of proceeds of crime).

The organisation of crime might be considered to deal with a number of stages, which also offer points of intervention:¹

1. Finding co-offenders (if needed)
2. Purchasing materials and other logistics for crime commission (or in the case of people smuggling/trafficking, being paid for and/or deceiving/kidnapping persons for export)
3. Funding lifestyle while awaiting crime completion
4. Converting product of crime into funds
5. Spending and storing proceeds of crimes
6. Safely integrating/re-investing saved proceeds
7. Avoiding severe criminal and financial sanctions, if necessary by bribery

When describing *changes* or trends in organised crime, we must allow for these merely to be changes in our own focus, technologies and human sources of knowing and tracking, and not always changes in the phenomena. Sometimes things may seem worse only because we know more or are trying to do more, rather than because they have actually become worse. Our awareness of trends is only as good as the underpinning data, derived usually from policing intelligence but also sometimes from academic and civil society research. Therefore variations in intelligence efforts between Council of Europe MS *and* in the penetrability of their targets are a constraint that we should appreciate. More practical issues of trends in financial intelligence, police or judicial cooperation are usually less contentious, but are only indirect measures of organised crime, e.g. there is only a weak relationship between money laundering itself and the number of suspicious activity reports or the amounts seized and confiscated. They are however important not just because of the balance of human rights and crime control within and between MS but also because a well-functioning cooperation process is essential to contemporary organised and economic crime control.

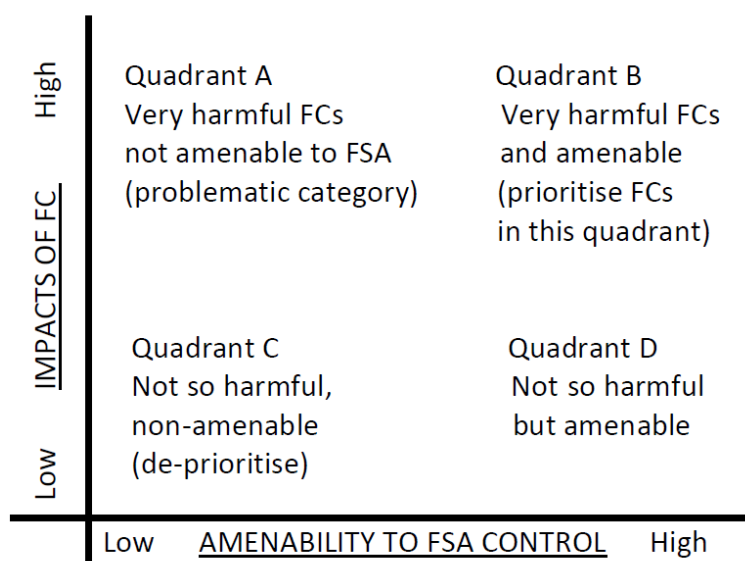
Organised crime in Europe, as normally understood, involves both predatory crimes (art and antiquities theft, coerced trafficking, extortion, fraud, robbery and other violence such as drug/gang-related woundings/homicides) and consensual or transit crimes (e.g. some forms of corruption, drugs and people smuggling, money laundering). Data are poor about most of these offences, which have large 'dark figures' of unreported and undetected crimes, though the EMCDDA does maintain data on drug *use* in many MS (which arguably mostly originates from organised crime), and there are global corporate surveys of frauds against large business, commercial bribery and – at least in the EU27 - some limited surveys of fraud against individuals, which likewise is mostly committed by organised crime. Annex A contains a discussion of some of these issues. But trends in crimes and in how they are organised are connected issues that we must try to combine, using official sources, academic sources and investigative journalism/other civil society sources. This will be important in a number of contexts. For example, the new FATF 2013 methodology requires countries (and evaluators) to analyse their money laundering risks and for this to be done properly, they will need a fuller appreciation of their countries' domestic crime problems and their role in laundering the proceeds of other countries' crimes than they have needed to know in the past. As the modern regulatory environment moves towards 'outcomes-focused regulation', it is harder to justify even

¹ Transnational and domestic bribery/extortion for contracts follows a different logical chain.

law enforcement actions in terms solely of the importance of the task, but also the contribution made to attaining measurable institutional objectives and outcomes.

A strategic approach to combating organised crime involves reviewing the factors that facilitate social harms and what can be done about them, whether by CoE MS acting alone or collectively, and/or in collaboration with other bodies. Thus, a study of the scale and impact of financial crimes for what is now the Financial Conduct (formerly, Financial Services) Authority suggested the following as an evidence-based model for interventions and prioritisations (FC = Financial Crime)²:

Figure 1. Outline typology of FSA priorities in terms of financial crime impacts and amenability to FSA control



This can be applied to many other sorts of crime problems. So at a practical level, it is important to judge not only what are the most serious harms to focus on, but also to work out what one can do about them, alone or in collaboration. It is this that may be useful for the Committee to develop. A set of possible directions for development will be listed at the end. What follows is a short report on some few areas of organised crime activity that are relevant to the work of the Committee, but it is not claimed that these should be the priority areas: only that they contain some data.

Trends in Organised Crime

There is no forum or mechanism for gathering data about organised trends in all of the CoE MS since 2005, when the last of the CoE annual organised crime situation reports was published.³ The EU SOCTA 2013 highlights the continuing evolution of an allegedly new breed of ‘network-style’ organised crime groups, defined much less by their ethnicity or nationality than has been the case hitherto, and much more by their capacity to operate on an international basis, with multiple

² p.11, *Impacts of Financial Crimes and Amenability to Control by the FSA: Proposed framework for generating data in a comparative manner*, Dorn, N., Levi, M., Artingstall, D. and Howell, J., London: Financial Services Authority. http://www.fsa.gov.uk/pubs/other/scale_and_impact_paper.pdf.

³ The PC-GR-COT Scientific Expert prepared that report on economic crimes in Europe, and also worked on the earlier ones. The reports, 1996-2005, are available at <http://www.coe.int/t/dgh/cooperation/economiccrime/organisedcrime/>.

partners and in multiple crime areas and countries. Europol states that this calls for a shift in our strategic response in the EU, away from one centred on individual ethnic types, or even individual crime areas, towards a more flexible, heterogeneous model of targeting these dynamic organised crime networks, through a more effective use of cross-border mechanisms to exchange information and coordinate operational activity. These can be proposed also for the CoE, and should be politically unproblematic for those MS who have ratified the Palermo Convention.

It is proposed that this Committee should not be too obsessed by focusing only on emerging or new threats. Many of the threats are old but are not being dealt with satisfactorily, and that is a sufficient basis for our activities. For example, based on extensive police material, a recent Spanish study provides a sobering account of the criminal organisations identified that avoids 'new trends'.⁴ As far as the organisational structures in their sample of Spanish gangs are concerned, hierarchical and non-hierarchical organisations were equally present, but the hierarchical ones appear to be much smaller. The simple reason, according to the authors, is the difficulties of management when hierarchical organisations expand. Horizontal and network 'organisations' are more flexible and adaptable without the burden of management. Concerning the level of sophistication, the authors mention some identified technical high-level devices, but in general the technical level and knowledge were not conspicuously sophisticated. The same applies to money laundering that consists mainly in the physical moving around of cash. A Bulgarian study in the same volume explores the *criminal market approach* that focuses on "*the number and types of actors that populate these illegal markets*". As examples they elaborate the heroin market and the illegal cigarette market. They demonstrate that by collecting data on the structure, actors (traders and customers), turnover and market value, one arrives at a more realistic assessment of illicit markets than is provided by other approaches to the study of organised crime.⁵ Crime, in other words, needs to be only as sophisticated as we force it to be. We are not in a position to replicate the Europol or indeed national assessments, nor is it necessary for us to do so.

⁴ 'The profile of a sample of criminal organisations acting in Spain during last decade', Andrea Gimenez-Salinas, Laura Requena Espada and Luis de la Corte Ibáñez, in *Human Dimensions In Organised Crime, Money Laundering And Corruption*, Wolf Legal, 2013.

⁵ 'European lessons from the Bulgarian Serious Organised Crime Threat Assessment', A. Rusev, P Gounev and T. Bezlov, Wolf Legal, 2013.

Drug Markets

Some key findings of the EU drug markets report:⁶

Drug trafficking is a highly profitable commercial activity and a core business for organised crime groups across Europe today. Understanding the reality of the European drug market requires a holistic approach, following the economic chain from production, via trafficking, to consumption. Describing how Europe is entering a new phase regarding the supply and demand for drugs, the agencies identify key action points to inform future policies (see Chapter 10 of the report and a selection below), which our Committee might consider also and might develop for the CoE.

1. Drivers of change (see also [IP/13/73](#))

The changing face of organised crime

The report describes the changing face of organised crime in Europe and a more 'polymorphous, dynamic and fluid' market. Contributing factors to this change include: criminals' multi-commodity perspective; the diversification of trafficking; and the exploitation of legitimate transportation options (e.g. containers, couriers, postal services).

Action points: coordinate targeted, intelligence-led law-enforcement actions focusing on 'high-value' criminals and groups; interrupt criminal money flows; forge partnerships with industry to tackle the misuse of commercial channels for drug trafficking.

The impact of global developments on the European drug market

It is impossible to understand the European drug market without locating it within a global context. There is a changing global marketplace (demand for drugs in the developing world); the role of Africa (transit, storage) and the need for cooperation between EU and non-EU countries. The EU is also a major drug *producer* as well as consumer, and criminal gangs in North-West Europe play a pivotal role in intra-European trafficking.

Action points: boost positive engagement with a larger number of producer and transit countries; improve analysis of supply and demand trends outside the EU; focus on Africa; continue to target drug production in the EU and to suppress trafficking of drugs and precursor chemicals from the region.

Technology and innovation

Technology is a 'significant game-changer' in the trafficking, production and distribution of drugs, with the Internet having a profound impact as communication tool and marketplace. But innovation is also seen in the area of production (EU as a key 'source of expertise and know how' on cannabis cultivation, synthetic drug production).

Action points: improve knowledge of the online drug market; create barriers to Internet sales via partnerships with credit card companies and online payment providers.

Heroin

Europe's heroin problem has its roots largely in the 1990s and is characterised today by a relatively small and ageing population of users. While heroin use continues to be responsible for severe health

⁶ *EU drug markets: a strategic analysis*, EMCDDA, Lisbon, 2013

and social problems, recent data suggest that use of the drug in the EU is in decline. Here vigorous policing along the heroin routes bordering the EU, and the success of Member States in engaging those with heroin problems in effective drug treatment programmes, are both likely to have played a significant role. The European heroin market therefore appears less important today in global terms, with non-EU heroin markets now larger and easier to penetrate. Turkey still plays a central role in heroin trafficking along the Balkan route, but there are signs of new routes being used as organised criminals respond to interdiction successes (e.g. Western Balkans). Organised crime groups linked to heroin now appear more active in markets for other drugs (e.g. cocaine). A specific risk highlighted is the potential diversification of heroin networks into methamphetamine production and trafficking. Europe remains a key source of the heroin precursor acetic anhydride.

Action points: invest in intelligence-led operations along classical heroin trafficking routes; build strategic partnerships with non-EU countries (e.g. in Africa); ensure joined-up law-enforcement against a joined-up threat (interaction between markets).

Cocaine

Over the last decade, cocaine has established itself as the most commonly used illicit stimulant drug in Europe, yet most users are found in a small number of western EU countries. Although demand for the drug remains high, indicators of cocaine use at EU level peaked around 2008 and have since fallen slightly. Spain and Portugal are the main points of entry for cocaine into Europe (with trafficking through West Africa a particular concern). New routes are also emerging. Cocaine concealed in container shipments is becoming more common, and recent major seizures have been made in the Black Sea and Eastern Baltic Sea areas. Interaction between cocaine and cannabis resin trafficking networks is well established, but interaction is also being seen between cocaine and heroin traffickers. To avoid detection, traffickers use sophisticated chemical techniques to incorporate cocaine into legitimate products (e.g. clothing, plastics). Most of the cocaine laboratories dismantled in the EU are 'secondary extraction labs' used to remove cocaine from materials in which it has been incorporated before exportation to Europe.

Action points: assess new threats (Black Sea; Balkan areas); focus on containers and develop partnerships between customs, port authorities and commercial transport bodies; support precursor control in producer countries.

Cannabis

The diversity and sophistication of cannabis products, producers and sources, and the sheer scale of demand for the drug, makes it relatively resilient to interdiction efforts. Herbal cannabis production is now widespread throughout the EU, a shift that has been accompanied by developments in cultivation technologies that may result in increased yield and potency. Being cultivated close to the intended consumer market, domestically grown herbal cannabis is more difficult to intercept and poses a new challenge for law enforcement. Trafficking of cannabis resin, principally from Morocco, remains a key concern and is sometimes linked to the importation of other illegal cargoes.

Action points: share know-how between countries on domestic cannabis production and improve monitoring of yields and potency; act in key areas (Morocco; S-E Europe).

Synthetic drugs (amphetamine, methamphetamine, ecstasy)

Recent developments in the synthetic drug market include a bounce-back of ecstasy (MDMA) availability; increased availability of methamphetamine; greater technical sophistication; and evidence of a scaling-up of production processes. There is increasing evidence of synthetic

substances being used as replacements for both heroin and cocaine and signs of more interplay with the market for non-controlled new psychoactive substances. Ecstasy use over the medium term has stabilised or even declined, due in large part to successful enforcement. The increased availability of MDMA in tablets, and now powders, may, however, see renewed interest in this drug. Demand for synthetic drugs in Europe is met largely by laboratories located intraregionally, particularly in the Netherlands and, to a lesser extent, Belgium, Poland and Lithuania. However, trafficking in precursors (and pre-precursors) occurs on a global basis, and producers are proving versatile in finding new production methods. The EU remains an important exporter of amphetamine and ecstasy.

Action points: target the intra-regional production of synthetic drugs through coordinated law-enforcement actions; identify key producers; restrict access to precursor chemicals; strengthen the international framework for restricting new precursors and pre-precursors.

New psychoactive substances

New psychoactive substances (new drugs) comprise a broad range of substances that are not controlled by international drug laws. In recent years, there has been a dramatic growth in their number, type and availability. Much of the policy focus on new drugs has concerned their legal status. However, it is also important to see them in the context of the overall drug market (interplay between the 'legal high' and illicit drug market). New drugs are usually synthesised outside the EU, while EU-based 'entrepreneurs', operating in a grey area, play an important role in importing, packaging and marketing. The report stresses the challenge of identifying new drugs which belong to diverse chemical groups, emerge rapidly and are sold in products that may contain mixtures of substances that change over time (meaning that users are exposed to substances of unknown toxicity). The Internet is a source of supply and information to consumers, traders and producers.

Action points: strengthen the EU early-warning mechanism on new drugs to keep pace with challenges; boost forensic capacity to improve detection; keep up-to-speed with new Internet trends; respond to the interplay between the 'legal highs' and illicit drug market; take rapid action to protect public health via fast-track EU-wide alerts.

Fraud in the context of financial crimes

Fraud is a deceptively simple word covering a very broad territory. It is a way of making money illegally via deception, whether that deception is directly person-to-person in real space or occurs in virtual space, usually without physical contact between offender and victim. Fraud is committed by spreading false stories or via the use of deceptive physical or e-documents or via Personal Identification Numbers. It may be committed using everyday transactions and stories, sometimes using genuine or phoney businesses as tools for the deed.

Fraud is a partially overlapping sub-set of 'financial crime' (which in many European countries is given the label 'economic crime'⁷). The latter is a heterogeneous term whose denotation has been expanding substantially over time, and now includes:

1. frauds of different types (*modus operandi*) with different victims (from wealthy corporations and High Net Worth Individuals to the very poor and from very rich to very poor governments);

⁷ See Council of Europe report for 2005.

2. 'market abuse' such as insider dealing/trading (which covers a range from corrupt relationships between investors and insiders to giving talks about company prospects to some important analysts before releasing results to the general market, giving the former an unlawful competitive advantage);
3. money laundering (of all crimes, increasingly including tax fraud);
4. financing of terrorism (mostly since 2001) and (since 2008) of Weapons of Mass Destruction proliferation, sometimes using deceptive documents; and
5. (transnational) bribery (usually by corporates paying public officials in developing countries, but also paying officials in their own – wealthy or poor – countries), covering up the act and money transfers by deceptive documents.

Some of these offences – like fraud – have existed in some form for centuries though even there, legislative changes have been needed to qualify them as criminal, for example to cope with the evolution of technology or moral awareness. This is the case with offences which are new since the 1980s (such as insider dealing/trading and money laundering). Others still typically are only a few years old or are in a process of major adaptation (like the financing of terrorism and of the proliferation of weapons of mass destruction, and transnational bribery). In addition, offences involving Intellectual Property, environmental crimes, etc. can be treated as part of 'financial crime', if only via their role (with all other offences) as part of the ever-extending list of 'predicate crimes' for money laundering offences. Indeed, to the extent that most crimes for gain lead to concealment or transformation of *some* proceeds, it is arguable that all such crimes *ipso facto* become 'financial crimes'. Consequently those who facilitate them and the movement of moneys from them are liable to increased risks of 'criminalisation', at least in principle. This implies a huge extension of what 'financial crime' and its subdivisions constitute.

Fraudsters are more diverse in terms of socio-economic status and age than are other 'organised offenders', though they sometimes operate in national or ethnic networks transnationally (Levi, 2008a, 2008b). Very serious frauds can be committed by solo actors. According to reviews of its forensic cases by KPMG (2007), typical internal fraudsters act alone, are middle aged and have usually been employed by the company for six or more years. By 2011, though this may merely reflect changing composition of reports to KPMG rather than real changes in the organisation of fraud, this had changed to the typical fraudster acting in collusion and being employed for more than 10 years (KPMG, 2011). Over half commit twenty or more frauds, usually over some years (though these are all people whose frauds are serious enough and whose victims are wealthy enough to engage KPMG).

Software advances have shown that what would previously have been seen as isolated frauds, if fraud at all, are actually part of an 'organised' network. For example between accident management companies, car hire firms, valuers, and a pool of people willing to make false claims for whiplash and other injuries. Thus it is tempting to see these trends as an effect of the Global Financial Crisis (GFC) and (at least partly independently) of the inexorable movement of 'organised crime' into fraud, but many 'organised frauds' preceded the GFC undetected, and in any event, this looks more like the dissemination of techniques by imitation.

Fraud entails many different sorts of harm which were likely to be driven by different factors, including what we do to prevent them and prosecute them. A rise in crime rates can be an indication that the quality of life has got worse, but in this case, the substantially greater cost of fraud figure is

far more likely to reflect improved knowledge than a real rise. We should appreciate that any given sector of fraud risk consists of the interaction between motivation, criminal ingenuity and the opportunities that we give criminals by the way potential victims and 'third party guardians' watch over our assets and intervene (or otherwise). All three of these can change over time. Those expecting a rise in fraud due to the recession/GFC are not only loosely tempted by fears of 'Apocalypse Soon', but also by the alleged invasion of 'organised crime', the corruptibility of the professionals, 'teckies' (technology obsessives) and of the middle and working classes fearful of their jobs and wanting to make a quick profit before they lose their access to rich crime opportunities.

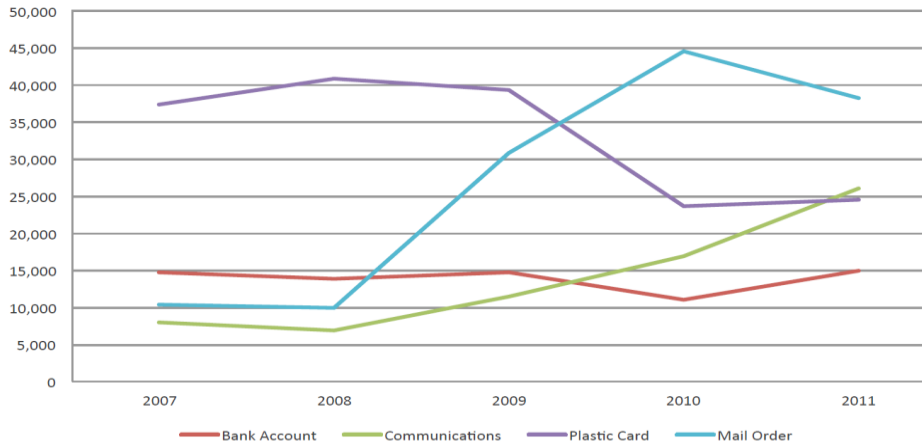
Payment card fraud in Europe generally increased after 2006, peaking in 2008. However, 2011 levels are €121 million more than in 2006. A notable exception is the UK, which accounted for 45 percent of the total in 2006 and now accounts for 29 percent, a reduction of €177 million. It has been asserted that criminals have shifted their focus to new opportunities within the European continent, as anti-fraud measures in the UK become stricter.⁸ In 2011, around 60% of payment card fraud losses were caused by card-not-present (CNP) fraud and totalled EUR 900 million. In some EU MS, losses to CNP already outstrip those of skimming.

The SOCTA 2013 notes that Cybercrime⁹ affects all MS and is linked primarily to financial fraud offences. According to research by the European Commission, 8% of internet users in the EU have experienced identity theft and 12% have suffered from some form of online fraud. In addition, malware affects millions of households and the general volume of banking fraud related to cybercrime is increasing year on year. The growing movement towards Bring Your Own Device (BYOD) in the corporate environment has major implications. The blurring of the boundary between company and private devices will potentially offer new opportunities for hackers to breach corporate environments and misuse - or hold hostage - the information within them. The mainstream adoption of processing in the Cloud is likely to present further challenges, in as much as consumers and corporate users will routinely access online resources using virtual computing environments with varying levels of personal data protection.

In the UK, data collected by fraud prevention service CIFAS – a not for profit organisation which acts as a rule-based clearing house and store for a variety of frauds on member organisations (many of which are also frauds on individuals) – indicate a rise in identity takeover frauds, as 'new credit' becomes harder to get, generating displacement to impersonating existing account-holders. Such frauds emerge quite quickly. An example of the different trajectories of identity frauds is given in the diagram overleaf, drawing on the CIFAS database for the UK:

⁸ (FICO, 2012, www.fico.com/fraudeurope)

⁹ For the purposes of the SOCTA, cybercrime comprises of both "specific" cybercrime offences such as hacking, phishing and malware, as well as internet enabled fraud. It does not include the distribution of copyright infringing material, although the internet remains the main method of accessing such material.



The crime triangle of motivation, opportunity, and capable guardians can be applied to fraud, and it is here in human and technological changes to these parameters that one may search for an explanatory framework. *A priori*, it would appear that different skill sets, commercial/personal background and formal qualifications will be needed for different fraud offences, and the barriers to entry depend on the starting point of any given individual or network *in relation to the practical opportunity and criminal justice obstacles that confront them*.

In most CoE MS and elsewhere, a distinction is made between laissez-faire opportunities to set up and work in commerce and some restrictions (normally simple criminal record and indebtedness checks) applied to people who want to work in the financial services sector, largely on the grounds that the latter can directly steal funds from the public. It is important to understand such restrictions in a global context rather than the traditional nation-state perspective of regulation and criminal justice. The Committee might want to consider whether CoE cooperation is good enough to deal with these issues, and with the laundering of the proceeds from corruption, drugs, fraud, people smuggling/trafficking, et cetera. This includes delicate issues such as the relative prioritisation of domestic and transnational demands upon scarce policing resources.

Committee Priorities

Prioritising crimes

The issue of how we reach rational priorities of what crimes to focus on may be contentious. The easiest thing to do is to select the most harmful and the most politically unacceptable crimes as our priorities. However if one wishes to critique the often media-led populist campaigns on harm and/or to focus also on what we can readily achieve the position becomes more complicated. How, for example, can we and should we weight MTIC fraud against identity fraud, or identity fraud (which mostly affects individuals) against IP violations, or any of the above against drugs trafficking? Should we treat 'legal highs' as primarily a public health issue and try to persuade people not to use them if they are unsafe (even if pleasurable), or should we add them to the long list of drug offences against which we have mostly been unsuccessful? The EU SOCTA 2013 identifies a number of key priorities, which, in Europol's view, require the greatest concerted action by EU Member States and other actors to ensure the most effective impact on the general threat. Facilitated illegal immigration, trafficking in human beings, synthetic drugs and poly-drug trafficking, Missing Trader Intra-Community (MTIC) fraud, the production and distribution of counterfeit goods, cybercrime and money laundering are the particular crime areas listed in this category. The Committee may wish to consider whether it shares these priorities, and what difference this prioritisation makes to MS actions, including their Mutual Legal Assistance processes. The Joint Investigation Teams of the EU have been under-utilised in the past: is there a need for or benefit from such measures in the Council of Europe and is this politically plausible enough to consider?

The Criminal Law focus

There remain issues arising from the intersection between criminal and regulatory controls, as some of the newer methods of administrative approaches to the control of organised crime (e.g. Dutch BIBOB 2002 legislation, some UK and Swedish strategies of administrative as well as police action) raise problems of cross-border and even of domestic data protection and accessibility which may not have been taken on board in CoE legal instruments or practices.¹⁰ There remain issues for debate about the 'specialness' of criminal law as an instrument of social control, and these are implicit in this Committee's mandate to look at issues that 'require a criminal law response'. These could require both criminal law *and* other responses, and the Committee might look at the issue of the 'mixed economy' of enforcement measures and how well prepared the CoE MS are to operate this mix domestically and in terms of cooperation instruments. For this, we might find helpful some data about the demand for and supply of mutual legal assistance between CoE MS, supplemented by some analysis of the untapped demand for such cooperation, given that many bodies do not ask if they expect to be refused, since this is a waste of their time.

¹⁰ See 'Reducing and preventing organised crime: An evidence-based critique', Levi, M. and Maguire, M., *Crime, Law and Social Change*, 41 (5), pp. 397-469; *Incapacitation: Trends and New Perspectives*, Malsch, M. and Duker, M. (eds.), Ashgate.

Annex A

Crimes of Globalisation: some Measurement Issues

Any set of statistics that relates to crime categories contains an element of social construction. Unless one is to define 'crime' as coterminous with (far from objective) 'social harm', the decision by any polity to treat a harm as a 'crime' rather than, for example, a matter for 'regulation' or administrative law or even social disapproval represents a moral as well as political decision (whether intended or not). The traditional legal distinction between *mala in se* (wrongs in themselves) and *mala prohibita* (wrongs that are forbidden) reflects not just process differences in terms of whether evil intent has to be proven but conscious or unselfconscious ideological valuations of relative harm. Sometimes this is combined with a judgement about how economic interests might be affected by taking these wrongs seriouslyⁱ. A good example would be the length of time it has taken the US to get the rest of the world to criminalize transnational bribery of public officials overseas (via the 1997 OECD Convention and the UNCAC 2005) since they first passed the Foreign Corrupt Practices Act 1977. The question of whether criminal sanctions actually have to have been applied for the conduct to be included in an empirical review of the costs of crime applies to all areas of crime, but has been a particular issue for white-collar crimes because of their contested and relatively under-policed nature. Given the tiny number of transnational bribery prosecutions, even in the US (and none in the UK), this would have a huge impact on the analysis of costs, incidence and prevalence. Thus, if we are to include unprosecuted cases, this inevitably involves making assumptions about levels of intention and recklessness that would be highly contentious in criminal cases. Some critical criminologists would contend that one should go beyond this and include social harms that have been 'politicked out' of the criminal law and the criminal process: in this paper, I will draw the line at recasting the criminal law but if one were to take no account of unprosecuted cases, then the notion of the 'dark figure of crime' would make no sense. It is important to take account of the growing significance of the private sector and 'its' actionsⁱⁱ in policing fraud and acting as gatekeepers of the criminal process.

There are a number of questions we might ask of such crimes.

1. **What do we want data for, and how serious are we?**
2. **What do we count, whom do we count and where do we count them?**
 - The expansion of transnational/human rights crimes
 - Counting victimisations; and counting consensual illicit acts such as illegal drug-taking, (in some jurisdictions) gambling and prostitution.
3. **Are there any crimes that are *only* transnational?**
4. **What are the mechanisms of transnational crime delivery and how do these affect the counting challenge?**
 - Separation of place of offending from offender residence *in different jurisdictions*
 - Most serious offenders in the supply chain may never set foot in the jurisdiction where the victimisation or where the consensual purchase takes place.

We sometimes also count 'organised crime groups' – nationally plus references to foreign countries or 'hubs'. However, quite apart from the epistemological problem of knowing (and justifying) when crime networks begin and end, there remain some practical questions:

1. Do we multiply count trafficking crimes in every country the drugs or people pass through?
2. Do we multiply count proceeds of crime in every country the funds pass through?
3. How do we evaluate the harmfulness of crimes or harms arising in a third party country?

Although offences connected with trade might be the earliest forms of globalisation-connected offences – the transfer of people and products, whether *per se* licit or illicit – I will focus primarily on financial crimes. Let us take an example. From UK cases examined, boiler room frauds are commonly based abroad (e.g. in Spain, where police interest is low), have never sought authorisation by the Financial Conduct Authority (FCA) – which is a legal requirement to sell securities - and use high pressure sales and telemarketing. If the fraudsters have sufficient nerve, they can seek to become regulated in one EU country and obtain a ‘passport’ to operate in another under EU single market regulations, using that as a base for fraud and making it difficult for regulators to intervene to close them down. In all of these cases, what the boiler room is really selling is deceptive and worthless expectations. Clearly, non-EU Council of Europe MS do not have all of these ‘benefits’ for fraudsters, but some of the same principles apply.

From a crime-recording viewpoint, it might be sensible to develop an international protocol about where the crime should be recorded in cross-border crimes. This is even more important where cybercrimes are committed against individuals globally from a jurisdiction – if identified at all – that is hard to reach by mutual legal assistance. If the scams are recorded separately where the victims live, this might inhibit the collation of collective data identifying the origins of the scam and thus reduce prevention possibilities, including cross-border enforcement interventions.

Furthermore, we are used to working out metrics for measuring harm. Traditionally we have merely counted crimes. But the burgeoning interest in the impact of crime has led to work on the cost of crime (Cohen, 2005). To date, only applied to substance misuse, household crimes, street crimes & those illicitly sexually exploited women who have escaped – from which questionable extrapolations are made about harm to trafficked/smuggled women generally. Hitherto, this has been calculated only in a national context, in terms of:

- o **Productivity losses**
- o **Medical and mental health care**
- o **Direct property losses**
- o **Indirect costs of victimization**

There are some paradoxes. Using court settlements or negotiated ones in the shadow of the court, Injuries to wealthy may be valued higher if not ‘normalised’ against income or wealth. Can it be applied to fraud and to e-crimes?

- In UK, 2005, a minimum of £12.9 billion, plus income tax + share of EU fraud (Levi et al., 2007; Levi and Burrows, 2008)
- By 2013, the cost of frauds identified rose to £52 bn (National Fraud Authority, 2013).

There has been a rise in the number of corporate victimisation surveys conducted by international accounting and consulting firms. However although (for sound marketing reasons), they break up their global totals on a country basis, presumably based on where the company is headquartered, this does not resolve the question of where the crimes occurred, since any of these companies can

operate in a number of jurisdictions and occur losses there. Partly because individuals are not targets for expensive consultancy services, there are very few studies of fraud/e-crime against individuals, except for those based around the International victimisation surveys, that ask only about consumer fraud and local corruption (van Dijk, 2007a, 2007b, 2008; van Dijk et al., 2008).

One can express data about the risks and impact of fraud on business activities in a number of different ways:

1. Absolute numbers of incidents, e.g. stolen credit and debit cards (not always reliably differentiated from lost ones by victims or in issuer or police records – the fewer defined as stolen rather than lost, the lower the recorded crime rate);
2. Absolute fraud loss figures (with a grey area of bad debt that may in fact be fraud by debtors such as cardholders but is seldom given out when ‘fraud statistics’ are presented);
3. Fraud to turnover (in some respects a better measure because it takes into account rising expenditure patterns) or fraud per financial instrument, e.g. per credit, charge or debit card; per internet transaction by number and/or value;
4. Fraud to profit (which replenishability factor – if better data were available - would measure how much business has to be done to make up for the losses); and
5. Fear of fraud (e.g. as experienced by cardholders, potential cardholders, retailers and bankers), which can have a chilling effect on commercial activity such as e-commerce or, conversely, can lead to inappropriate decisions by those who have insufficient awareness of the true risks they are taking or creating.

Each of these methods has its advantages and disadvantages, and organisations may wish to deploy them tactically to suit their interests. In media terms (as with crime statistics generally), the preference may be for bald data that can be used for simple headlines. The ratio per transaction or per turnover may be as unattractive to the tabloid press or television as would be the number of offences per male or female juvenile in vandalism or homicides per released violent offender in other criminological spheres. For *individual* victims, on the other hand, there is less variation, though one could still analyse the different impact in terms of whether the funds were compensated by some government or private scheme - normally restricted to financial services investments up to a moderate limit, though even these do not exist in many parts of Central or Eastern Europe, or Third World countries; how much work it would take to make up the losses (expressed, say, in days); or indeed, in the case of retired/involuntarily unemployed persons, whether they could recover the losses at all; the emotional and health impact on victims; or indeed the general effects on consumer/investor confidence.

There are broader questions about international statistics. How do we compare financial crime harms with harms from other crimes and from ‘natural disasters’ and from the global financial crisis, in connection with which almost no senior banker and certainly no regulator has been prosecuted anywhere in the world? This is despite the transnational impact of US mortgage origination fraud.

The Future: Harm and Risk

There are three dimensions of harm and risk:

1. Economic costs (present/future) & impact upon victims and upon third parties who fear being defrauded

What difference does it make to us if victims are non-citizens?

2. What the media represent the risks to be – this is a key driver of political reactions to crime.
3. Continuing risks arising from the kind of people who are committing financial crimes. These consist of
 - ‘Organised criminals’ with no stake in social respectability to constrain them and growing access to corruptible/pressurisable staff, especially in recession
 - what they spend their money on (terrorism, political corruption, business) - though mostly on party-going

So do we need to combine victim surveys with offender location studies, & how do we do that for offences with low-clear ups? We need ‘sentinel’ trend data, not precise numbers, which anyway are bound to be imprecise: the more precise that numbers are, the more suspicious we should be of them.

Gradually, via the impact of routine activities theory, criminologists have begun to see ‘the causes of crime’ as including an analysis of how crime is organized socially and technically. To understand how this is possible, we need to examine crime as a business process, requiring funding, technical skills, distribution mechanisms, and money-handling facilities. This is an area in which the interests of several components of our Committee interact. The larger the criminal business, the more likely all these elements will be required. On the other hand, those persons who commit acts defined as ‘not really criminal’ by their reference groups and by policing agencies, and where technological means of detection are not very powerful, are enabled thereby to commit offences with relative impunity. One method of improving one’s chances of remaining unprosecuted and with assets available is to use the ‘offshore secrecy’ paraphernalia of modern commerce, though anti-money laundering legislation and evaluation has made the world shrink in terms of opportunities for concealment *once a well-resourced investigation happens*. Even the attempt to combat ‘harmful tax competition’ and control the more abusive aspects of offshore finance centers/tax havens has had some successes, and in 2012, the Financial Action Task Force (2012) included tax evasion as a predicate offence in its new set of guidance. This could be characterized as risk-managing financial globalization, but by the nature of many frauds, they will not be picked up by the system until they become substantial: the logical result may be that there may be the same number of frauds, but the larger ones will be smaller than they would otherwise be. It is the *systemic* protection that is the principal objective.

There are barriers of distrust, of language and culture, and of modesty of ambitions and skills, that inhibit the transnationalization of all forms of crime, including fraud and corruption, and one must question any assumption that transnational crime will somehow replace ordinary, local crime. But when one can set up an Internet site from the privacy of one’s home, get registered to process credit card transactions for one’s pornography site, and then send modest extra invoices for non-existent transactions to thousands of people who *have* purchased from one’s site, the possibilities for transnational fraud are readily visible and fairly open to many existing criminals. (Even dull thieves and robbers can obtain coerced assistance from those fraudsters unlucky enough to be sent to jail.)

Transnational functions are an inherent part of many financial fraud schemes, to lend plausibility and evade authorization mechanisms, and to frustrate civil and criminal investigations and asset recovery. However, in the financing and laundering aspects – as well as the physical transportation of legal and illegal goods and services – the transnational component applies to many other crimes as well. In the final analysis, the globalization offered to the international corporate world creates

possibilities for illegal financial entrepreneurs that are both technically and economically difficult to police, even absent corruption on the part of political elites and law enforcement agencies.

References

Cohen, M. (2005) *The Costs of Crime and Criminal Justice*, London, Routledge.

Van Dijk, J.J.M. (2007a). The International Crime Victims Survey and Complementary Measures of Corruption and Organised Crime. In: Hough, M. & Maxfield, M. (Eds.) *Surveying Crime in the 21st Century*. Crime Prevention Studies, volume 22. Cullompton, Willan Publishing.

Van Dijk, J.J.M. (2007b) The ICVS and Beyond: Developing a Comprehensive Set of Crime Indicators. In: Aromaa, K. & Viljanen, T. (Eds.) *International Key Issues in Crime Prevention and Criminal Justice, Papers in celebration of 25 years of HEUNI*. Helsinki, HEUNI.

Van Dijk, J.J.M. (2008). *The World of crime; breaking the silence on problems of crime, justice and development*. Thousand Oaks: Sage Publications

Van Dijk, J.J.M., van Kesteren, J.N. & Smit, P. (2008). Criminal Victimization in International Perspective, Key findings from the 2004-2005 ICVS and EU ICS. The Hague, Boom Legal Publishers.

M. Levi and J. Burrows, (2008) 'Measuring the impact of fraud: a conceptual and empirical journey', *British Journal of Criminology*, 48(3): 293-318.

Levi, M., Burrows, J., Fleming, M. and Hopkins, M. (with the assistance of Matthews, K.). 2007. *The Nature, Extent and Economic Impact of Fraud in the UK*. London: Association of Chief Police Officers. <http://www.cardiff.ac.uk/socsi/resources/ACPO%20final%20nature%20extent%20and%20economic%20impact%20of%20fraud.pdf>.

National Fraud Authority (2013) *Annual Fraud Indicator, 2013*, London: Home Office.

ⁱ Though even if one thought something very harmful and intended, one might choose to deal with it pragmatically by other than criminal law or penal sanction means: see the restorative justice model developed by Braithwaite, 1987 et seq.

ⁱⁱ The quotation marks are intentional: the extent to which the private sector acts homogeneously and/or has objective and subjective homogeneous interests might repay some attention.