DRAFT Version 9 May 2016
Strasbourg, France

T-CY (2016)17

Cybercrime Convention Committee (T-CY)

Implementation of Article 13 Budapest Convention by Parties and Observers:

A Comparative Study

DRAFT

prepared by professor Ian Walden
Centre for Commercial Law Studies, Queen Mary, University of London

www.coe.int/TCY

Contents

Contact

Alexander Seger
Executive Secretary of the Cybercrime Convention Committee (T-CY)
Directorate General of Human Rights and Rule of Law
Council of Europe, Strasbourg, France

Tel +33-3-9021-4506
Fax +33-3-9021-5650
Email: alexander.seger@coe.int

1 Introduction

This report is concerned with Article 13 of the Budapest Convention ('Convention') on 'Sanctions and measures':

> 1 Each Party shall adopt such legislative and other measures as may be necessary to ensure that the criminal offences established in accordance with Articles 2 through 11 are punishable by effective, proportionate and dissuasive sanctions, which include deprivation of liberty.
> 2 Each Party shall ensure that legal persons held liable in accordance with Article 12 shall be subject to effective, proportionate and dissuasive criminal or non-criminal sanctions or measures, including monetary sanctions.

The study is based on the responses to a questionnaire submitted by the Parties and observers.[1] The purpose of this study is three-fold. First, to examine the practice of the Parties in implementing Article 13, to enable a better understanding of the extent to which the Convention's key objectives, harmonisation and international co-operation, are either reinforced or undermined by the approach of the Parties to sanctions. Second, to provide guidance to any country reviewing its current sanctions regime in respect of specific offences under the Convention, as well as prospective signatories and other observing jurisdictions about the factors that should be considered when adopting sanctions in the cybercrime area. Third, the study provides some tentative recommendations to the T-CY about future work and potential activities, were such an opportunity to arise at some point in the future.

2 Understanding the obligation

Article 13 requires that sanctions be 'effective, proportionate and dissuasive'. While the offences are 'criminal' in nature,[2] the sanctions could include civil or administrative measures. This is made explicit in respect of legal persons, at 13(2), but it does not preclude a similarly broad interpretation of sanctions under the previous paragraph.

As with other provisions of the Convention, this phrase must be interpreted in accordance with Article 15 regarding conditions and safeguards, specifically the requirement to comply with the principle of proportionality. In terms of assessment, due consideration to the obligation to have 'effective, proportionate and dissuasive' sanctions may need to occur not only at the legislative phase, but also at the various points in the criminal justice system where policy and practice can impact the resultant treatment of a perpetrator of cybercrime, from the investigation by the police, to decisions whether to prosecute, to the exercise of discretion by the court at sentencing.

In most legal systems, the maximum level of sanction, and hence the degree of seriousness with which a particular form of criminal conduct is viewed, is determined by legislators, and is laid down in the criminal code. The sentencing phase lies within the discretion of the judiciary, although often subject to guidance designed to facilitate consistency and certainly across the criminal justice system. However, in some jurisdictions, the legislature may further constrain such judicial discretion through the imposition of statutory minimum sentences. Proportionality concerns have been raised against certain forms of minimum sentencing policy, such as the 'three-strikes' rule.[3]

[1] T-CY(2015)18, Assessing implementation of Article 13 Budapest Convention on Sanctions and Measures: Compilation of replies to the questionnaire, 16 February 2015 ('Replies').
2 See Engels and Others v the Netherlands judgment of 8 June 1976, Series A no. 22, § 82.
[3] E.g. under US federal criminal law, mandatory life imprisonment for a serious violent felony (18 USC § 3559(c)).

While this study is primarily focused on state practice, it is also worth noting briefly the differing theoretical approaches to punishment, since the extent to which a Party explicitly or implicitly embraces one approach in preference to another could impact on how they have met their obligation to implement an 'effective, proportionate and dissuasive' sanctions regime.

The academic literature recognises two broad categories of approach to punishment, retributive and consequential.[4] The former is sometimes seen as backward-looking, since the primary focus is concerned with ensuring an appropriate punishment for the wrong committed: 'Let the punishment fit the crime'. The latter is more concerned to achieve an objective in the future, such as the prevention of reoffending or compensating the victim. The wording used in Article 13 can be seen as embracing both approaches, since the principle of 'proportionality' is central to retributive justice, while 'effective' and 'dissuasive' can be seen as more consequential in nature.

The relationship between the three words, 'effective, proportionate and dissuasive', can itself be disputed.[5] For example, should proportionality and dissuasion simply be seen as elements of 'effectiveness', rather than separate criteria? Alternatively, should proportionality always be seen as the preeminent criterion, since it is a foundational principle within the European Convention on Human Rights ('ECHR') and the European Court of Human Right's ('ECtHR') jurisprudence? The study proceeds on the presumption that all three words have distinct meaning and significance.

The European Commission has defined the terms in the following manner:

> "*Effective* requires that the sanction is suitable to achieve the desired goal, i.e. observance of the rules; *proportionality* requires that the sanction must be commensurate with the gravity of the conduct and its effects and must no exceed what is necessary to achieve the aim; and *dissuasiveness* requires that the sanctions constitute an adequate deterrent for potential future perpetrators."[6]

The notion of an 'effective' sanction under the Convention, however, demands a more complex answer than simply ensuring 'observance of the rules', since the objectives being sought by the Convention, as an instrument of public international law, differ from national legislation. Achieving harmonisation and enhancing international co-operation obliges the Parties to give consideration to the needs of the other Parties, as well as purely domestic concerns about tackling cybercrime.

Assessing 'effectiveness' also has a dual perspective, which can entail both a theoretical *ex ante* evaluation of the sanction regime 'on-the books' in terms of meeting its objectives, and an empirical examination, *ex post*, as to whether the sanction regime has worked in practice.[7] The former is primarily a matter of substantive law, while the latter is concerned with issues of procedural law, although the obligation of the Parties under Article 13 is applicable to both.[8] This study, however, focuses solely on the former.

While 'effective' enforcement clearly does not require the Parties to pursue prosecutions in all cases of cybercrime; conversely, a failure to have some *di minimis* enforcement strategy and associated resource to tackle cybercrimes could be viewed as a breach of a Party's obligation

[4] Walker, N., *Why punish?* Oxford University Press, 1991.
[5] Harding, C., "Member State Enforcement of European Community Measures: The Chimera of 'Effective' Enforcement, 4 *Maastricht J. Eur. & Comp. L.* 5 1997.
[6] Commission Communication, Towards an EU Criminal Policy: Ensuring the effective implementation of EU policies through criminal law, COM(2011) 573 final, 20.9.2011, at p.9.
[7] Faure, M., "Effective, proportional and dissuasive penalties in the implementation of the environmental crime and ship-source pollution directives: Questions and challenges", *European Energy and Environmental Law Review*, December 2010, 256.
[8] By analogy, the European Court of Justice has noted: "whilst the choice of penalties remains within their discretion, they must ensure in particular that infringements…are penalized under conditions, both procedural and substantive,…which, in any event, make the penalty effective, proportionate and dissuasive." Case C-68/88, *Commission v Greece* [1991] 1. C.M.L.R. 31, at 24.

under Article 13, irrelevant of what is prescribed in the criminal code.[9] Indeed, by virtue of Article 26(4), a Party has a specific obligation to submit a case to its competent authorities where it refuses to extradite a national and has jurisdiction over the offence. It should also be noted that while prosecution statistics may be low for certain categories of cybercrime, this may not always be indicative of a regime's effectiveness, where an enforcement strategy targets limited but high profile cases that can have a disproportionately dissuasive impact on potential offenders.

It has been noted that a proportionate response can be seen "as one which achieves a balance between the nature of the interest to be enforced on the one hand, and an appropriate choice of judicial means and investment of resources on the other hand".[10] In terms of public resource, for example, imprisonment is considerably more costly than the imposition of fines or other non-custodial sentences; a fact that would appear to be reflected in the sentencing practices of the Parties (see further section 6.1 below).

The basis of dissuasion is the idea that a person, being aware that a certain form of conduct will result in a sanction, should be motivated to avoid such conduct and comply with the law. Whether that motivation is based purely on a rationalist cost-benefit analysis,[11] or some other more nuanced causation, it is broadly recognised that the sanction provided for in the statute is only one factor in an evaluation of dissuasive effect. Another key factor is the perpetrator's perception of the probability of apprehension, prosecution and conviction. It is widely acknowledged that an improvement in levels of detection has a greater deterrent impact than increasing the level of sanction.[12] Such detection will of course depend on a range of domestic factors, such as law enforcement resources, but also the uniquely transnational nature of much cybercrime can further dampen the dissuasive effect of a nation's sanctions regime.

3 Assessment criteria

The phrase 'effective, proportionate and dissuasive' can be assessed from at least four different perspectives: the perpetrator, the victim, procedurally and in terms of international co-operation.

3.1 Perpetrator

Sanctions are designed to deter both the perpetrator from engaging in further criminal conduct, as well as other persons from engaging in the same conduct.[13] The sanction may target a person's liberty to act, through imprisonment or prohibitions, or the economic benefits that his conduct generated, through forfeiture or confiscation orders. Economic sanctions may be designed to deprive the perpetrator as well as compensate the victim, in terms of compensation orders.

When a perpetrator has been tried and found guilty, considerations at sentencing may address two distinct audiences. First, and always, the individual perpetrator, for whom the sentence must be effective and dissuasive in respect of future conduct, i.e. repeat crimes, but proportionate in respect of the criminal conduct of which the perpetrator has been found guilty. Second, the sanction can act as a signal to others that may be tempted to engage in such conduct, i.e. potential perpetrators. Here issues of proportionality become subordinate to the deterrent effect of the message conveyed by the sentence.

In a significant number of jurisdictions, the applicable tariff may vary in accordance with certain aggravated circumstances; the most common being the concept of a 'protected computer' in computer integrity offences. A 'protected computer' is generally either defined on the face of the

[9] See C-265/95, *Commission v France* [1997] E.C.R. I-6959.
[10] Harding, supra n.5, at 16.
[11] Becker, G.S., "Irrational behaviour and economic theory", *The Journal of Political Economy*, vol. 70, no. 1 (Feb. 1962), 1-13.
[12] Smith, Grabosky and Urbas, *Cyber Criminals on Trial*, Cambridge University Press, 2004, at 112.
[13] Referred to respectively as 'special' and 'general' deterrence.

legislative instrument itself or is designated through secondary regulations or other executive order making power. A 'protected computer' identifies a target or 'victim' computer as requiring greater protection from attacks than others, usually because of the nature of the processing being carried out by the system, such as critical national infrastructure. Where a perpetrator engages in unauthorised conduct against such computers the tariff is usually significantly higher, which is designed to act as a greater deterrent against such attacks. In terms of Article 13, considerations of proportionality may arise with regard to the severity of the enhanced tariff, or concerning the range of systems that fall within the defined scope of a 'protected computer'. Other aggravated circumstances in sanction regimes include whether the person is part of a criminal organisation or where the defendant is a repeat offender.[14]

For all of the Convention offences, the person must have the *mens rea* of intention and be acting 'without right', which will also generally require knowledge where the conduct is 'undertaken without authority'. However, Parties could obviously go beyond these requirements and impose liability for differing forms of fault, such as recklessness and negligence, or adopt a non-fault or strict liability approach. In such cases, an assessment of 'effective, proportionate and dissuasive' may need to be different, on the basis that these involve different degrees of guilt on behalf of the offender. Such considerations are beyond the scope of this study, but should form part of any general review of a sanctions regime.

Where the perpetrator is a legal person, such as a company, different considerations about sanctions and measures will arise and may encompass criminal, civil and administrative law.[15] For example, requiring a legal person to give publicity to their infringing conduct may be sufficient sanction in terms of the reputational impact.[16]

In terms of ancillary offences, at Article 11, the Explanatory Report notes that some states do not criminalise attempts. Where a person is found guilty of aiding and abetting, often referred to as 'secondary liability', most legal systems impose the same sanction regime as that for the perpetrator; although the person's ancillary role may be a factor for consideration at sentencing.

Where a person pleads guilty to an offence, thereby avoiding the need for a full trial, most sentencing systems will give favourable recognition to the person's plea, with a consequent reduction in sentence. The reduction is effectively taking account of the benefit to the administration of justice, including those involved (from victim to expert witness), from the swift disposal of the case.

3.2 Victims

The place of victims in the criminal justice system has evolved over recent years, as it has been increasingly required to give greater attention to the needs and interests of victims. In terms of sanctions and measures, victims may either be given express recognition within the sentencing process, through some form of restitution process (a top-down perspective), or may be granted rights of standing to commence separate civil proceedings against the perpetrator (a bottom-up perspective).[17] In terms of the former, the court may give the victim an opportunity to reveal the nature and scale of harm suffered, during the course of the court's deliberations as to the appropriate sentence to impose. In addition, in many jurisdictions the statutory framework will grant the court the power to award compensation to the victim against the perpetrator.[18] In terms

[14] E.g. Belgium and the US.
[15] Explanatory Report, para. 129.
[16] Such measures have been deployed in cases of intellectual property infringement (see Directive 2004/48/EC 'on the enforcement of intellectual property rights' (OJ L 195/16, 2.6.2004), at art. 15) and discrimination (Case C-54/07 *Feryn* [2008] ECR I-5187, at para. 68).
[17] E.g. in the US, the 18 USC § 1030 (g) (re: illegal access and interference); 18 USC § 2520 (re: illegal interception).
[18] E.g. Singapore, Computer Misuse and Cybersecurity Act, s. 13.

of the latter, the interests of the victim, whether as claimant or beneficiary, are more properly an issue of remedies, rather than sanctions, which is the scope of Article 13.

Where a victim is granted explicit recognition by a sentencing court, he should be better placed to bring a claim if the procedural framework enables the civil courts to base its determinations on the findings of the criminal court. The imposition of a limitation period for the bringing of any such claim by a victim could effectively deter such claims, which could in itself represent a failure to impose 'effective, proportionate and dissuasive' sanctions.[19] However, when assessing whether a criminal sanction regime is 'effective, proportionate and dissuasive', consideration should not be given to any hypothetical non-criminal measure, such as civil compensation, which may be available against the perpetrator.[20]

3.3 Procedures

From a procedural perspective, the use of certain coercive and covert investigative techniques, such as interception, may only be deployed where the conduct under investigation is considered to meet a minimum threshold, such as 'serious crime', which is usually defined by reference to the applicable sanction. As such, a Party needs to give appropriate consideration to the proportionality of any such triggering thresholds, such that highly intrusive investigative techniques are only deployed against the more egregious forms of criminal conduct.

Criminal procedures may also contain offences for non-compliance by the person against whom a power is exercised. As such, a Party should consider whether the applicable sanctions are 'effective, proportionate and dissuasive' with respect to such procedural offences, especially as the person against whom the power is exercised may be an innocent third party, such as a service provider,[21] rather than a suspected perpetrator. Although in both cases non-compliance is an offence against the administration of justice, any sanction should likely reflect the differing positions of the defendants. So, for example, under Article 19(4), a person can be compelled to provide information about measures used to protect data, such as a cryptographic key. Failure to assist will generally be an offence, but the maximum applicable tariff may inevitably be lower than that which would potentially arise were the perpetrator to comply with the request.

Compared to the substantive offences, assessing whether a procedural offence is 'effective, proportionate and dissuasive' is likely to be easier to evidence in terms of actual data, because the offences are deployed against a clearly defined set of persons, i.e. the recipient of the order, rather than a theoretical class of potential actors, i.e. those minded to engage in criminal conduct. Over time, therefore, legislators and the judiciary should be better placed to determine the appropriate sanction or measures.

It should also be noted that in some legal systems, the hierarchical structure of the judicial system may impact the sanctions regime, with lower courts being constrained as to the scope and scale of sanction that may be imposed compared to the higher courts.[22]

Finally, it should be recalled that Article 13 is only applicable to the offences detailed in Articles 2-11, so does not establish obligations concerning offences arising from the operation of the criminal procedures detailed in Section 2 of the Convention. For example, any sanctions applicable to an offence of obstruction by a suspect or a failure to disclose subscriber information by a service provider, do fall within the remit of Article 13, but would instead be evaluated in terms of the necessity for conditions and safeguards under Article 15. A disproportionate penalty for a failure to

[19] See Case C-81/12, *Asociaţia Accept* (2013), at paras. 65-67.
[20] See Case C-45/08, *Spector Photo Group NV* (2009), at para. 74-77.
[21] E.g. in the Yahoo! case in Belgium, the court at first instance imposed a €55k fine, with an additional €10k for every day they continue to refuse to comply (Court of Dendermonde, Not. nr. DE 20.95.16/08/26, 2 March 2009).
[22] E.g. in the UK, the distinction between summary conviction and conviction on indictment.

comply with a procedural obligation could constitute an unwarranted interference in an individuals rights and liberties, such as the right to a fair trial under Article 6 of the ECHR.

3.4 International co-operation

When assessing if a sanctions regime is 'effective', consideration should not only focus on a domestic perspective, but should also be assessed in terms of the Convention's key objectives to establish a 'common criminal policy' or harmonization and of promoting enhanced international co-operation.

Substantial divergent approaches to sanctioning between the Parties could create distortions, with perpetrators choosing to locate their offending in jurisdictions considered 'soft' on sanctioning or, indeed, enforcement. This could obviously undermine the objective of harmonisation.

Sanctions are critical in international co-operation. Too low and the conduct will not meet the minimal threshold required to trigger obligations. Under Article 24, for example, extradition is conditional on the offence being punishable under the laws of both Parties to a common level:

> "deprivation of liberty for a maximum period of at least one year, or by a more severe penalty"

Conversely, too severe and co-operation may also not be possible. So, for example, the possibility of imposing the death penalty will usually mean that countries that reject such sanctions will be unwilling to co-operate.

Issues of 'proportionality' can also arise in the context of sanctions, not least in the minds of the general public. In UK extradition case, *McKinnon*, for example, the US indictment listed seven counts of computer fraud and related activity, each of which carried a maximum sentence of 10 years.[23] These sentences could run consecutively, depending on the decision of the federal judge, giving a possible total of 70 years. The reality was that such an outcome was extremely unlikely. However, in terms of generating support for McKinnon's campaign against extradition, such differential sentencing regimes provided fuel for claims of disproportionality and unfairness in the extradition process.

4 Other cybercrime instruments

For Parties to the Convention that are Member States of the European Union, the Directive 'on attacks against information systems'[24] utilises the same phrase, 'effective, proportionate and dissuasive', in respect of the general obligation on penalties, but then details minimum sanctions that should be imposed or lists the types of sanction that should be considered. This represents a more enhanced form of harmonisation than possible under the Convention.

The Directive first specifies maximum terms of imprisonment for the commission of the offences, a period of two years "at least for cases which are not minor" (art. 9(2)). For intentional system or data interference, where a significant number of systems have been affected through the use of a tool designed or adapted specifically for that purpose, the maximum term of imprisonment should be at least three years (art. 9(3)); while the minimum should be at least five years where such interference is committed by a criminal organisation, causes serious damage or has been committed against a 'critical infrastructure information system' (art. 9(4)). Similar provisions were

[23] US Department of Justice Press Release, 12 November 2002, available at < http://www.justice.gov/criminal/cybercrime/press-releases/2002/mckinnonIndict.htm>.
[24] OJ L 218/8, 14.8.2013.

present in Decision (2005) that preceded the Directive,[25] and it is worth noting that there has been no sanction inflation in the intervening period.

Where legal persons are involved in the criminality, the sanctions may include the following: exclusion from entitlement to public benefits or aids; disqualification; judicial supervision, the entity may be wound-up or offices may be closed (art. 11(1)). Such matters are considered further below at section 5.2.

Similarly, the Directive addressing child pornography [26] also prescribes minimum terms of imprisonment:

- Acquisition or possession: 1 year;
- Knowingly obtaining access by ICTs: 1 year;
- Distribution, dissemination or transmission: 2 years;
- Offering, supplying or making available: 2 years;
- Production: 3 years[27]

However, Member States are granted certain discretion over the application of these minimums in certain circumstances, e.g. where the person depicted is in fact over 18 years at the time, although appearing to be a child.

The African Union Convention on Cyber Security and Data Protection (2014)[28] adopts the same phrase, 'effective, proportionate and dissuasive criminal sanctions' (art. 31). Where crimes are committed through a 'digital communication medium', it calls for the competent courts to be given the power to impose 'additional sanctions', but it does not further specify what those may be (art. 31(2)(a)); although in the following provision reference is made to the possibility of imposing on the convicted person a requirement to publicise any decision, including through the same medium (art. 31(2)(b)).

The League of Arab States Convention 'on combating Information Technology Offences' (2010)('Arab Convention') does not contain a general provision on sanctions, but does call upon the parties to impose criminal liability on legal persons, where appropriate (art. 20), as well as increase penalties where traditional crimes are committed by means of information technology (art. 21). The Convention also refers to the need for offences to have a minimum term of one-year imprisonment to be considered extraditable (art. 31(1)(a)).

Imposing increased penalties where information and communication technologies ('ICTs') are involved is an approach also adopted in the ECOWAS Directive 'on fighting Cyber Crime',[29] which states the following:

'Under this Directive, the use of ICTs to commit common law offences such as theft, fraud, possession of stolen goods, breach of trust, extortion, terrorism, and money laundering or organised crimes shall constitute a higher degree of offence that the common law offences' (art. 24)

Such provisions can be seen as problematic in two respects. First, they fail to address the treatment of the 'new' computer integrity offences, i.e. non-traditional crimes. Second, it may be argued that a harsher penalty imposed for an offence simply because of the means involved, i.e. the use of ICTs, could itself be viewed as disproportionate. While the targeting of 'protected

[25] OJ L 69/67, 16.3.2005.
[26] Directive 'on combating the sexual abuse and sexual exploitation of children and child pornography' OJ L 335/1, 17.12.2011.
[27] Articles 5(2)-(6).
[28] EX.CL/846(XXV).
[29] C/DIR. 1/08/11.

systems' may be a valid aggravating circumstance, rendering any involvement of ICTs in the commission of a crime a pertinent factor in sentencing will become increasingly meaningless and the norm rather than deserving of special consideration.

The ECOWAS Directive calls upon states to implement 'proportionate and dissuasive sanctions' (art. 28). It also refers to 'supplementary sanctions', specifically confiscation and publicity obligations (art. 29).

Finally, model laws, such as those promulgated by the Commonwealth, the Southern African Development Community ('SADC') and in the Caribbean ('HIPCAR'), refer to the possibility of imprisonment and fines, but leave those sections blank for the implementing jurisdiction to determine.

5 Legal framework

Of the 52 countries approached, only 3 were not in a position to respond.[30] The results presented below are based solely on the national responses, as the study team was not asked to engage in primary research and gather material on any country independently. The level of detail provided by respondents also varied significantly. Where responses were provided in a language other than English, the research team used Google Translate to produce a rough translation, so mistakes may have arisen from this process.

5.1 Offences under Arts 2-10 committed by natural persons

While the vast majority of respondents had criminal measures matching each of the Convention offences, there were some countries that did not, especially in respect of the possession of devices (e.g. Albania) and child pornography (e.g. Panama).

The table below indicates the range of different sanctions applicable to the Convention offences. In each case, the stated sanction is the maximum available under the legislative provision, absent any aggravating factors (discussed further below). Both the 'lowest tariff' and 'highest tariff' columns therefore indicate the maximum sanction available for the basic offence, *not* the minimum that may be imposed.

Offence	Lowest tariff	Respondent	Highest tariff	Respondent[31]
Access	Fine	Bulgaria	10 years	Australia, Canada
Interception	6 months	Austria	10 years	Canada, Mauritius
Data Interference	Fine	Armenia	10 years	Australia, Mauritius
System Interference	Fine	Bulgaria	10 years	Mauritius
Devices (Supply)	6 months	Austria	10 years	United States
Devices (Possession)	6 months	Austria	10 years	United States

[30] Sri Lanka, Ukraine and Senegal.
[31] The listed jurisdictions are examples, rather than a complete list.

Forgery	1 year	Austria	10 years	Italy
Fraud	6 years	Spain	10 years	Mauritius
Child porn (Supply)	2 years	Albania	30 years	United States
Child porn (Possession)	1 year	Switzerland	20 years	United States
Copyright	Community service	Moldova, Morocco	7 years	Romania

The table is illustrative of the differing attitudes between respondent countries as to the relative seriousness of the Convention offences. While there is considerable harmonisation at the top-end, especially between the computer integrity and computer-related crimes, this becomes less apparent at the bottom end, where some countries clearly view the integrity offences at the lower end of seriousness. Given the impact that lower sentences have on international co-operation, this is a matter of some concern in terms of achieving a key objective of the Convention. For the content-related offences, while child pornography is being viewed with ever-greater seriousness, criminal copyright infringement has remained relatively stable, with the majority of countries imposing maximum tariffs in the 2-5 year range.

The majority of Parties provide for enhanced penalties in a wide range of different aggravating circumstances. These can be divided into two broad categories: those focused on the 'victim', whether system, data or the resultant harm caused, or focused on the 'perpetrator':

Victim	
Nature of the target	e.g. 'computers systems of public importance' (Albania, Azerbaijan, Bosnia, Croatia, Estonia, France, Germany, Italy, Latvia, Lithuania, Montenegro, Portugal, South Africa, Philippines, Macedonia)
Nature of the information accessed	e.g. 'protected' or 'secret' information (Bulgaria, Denmark, Estonia, Portugal, South Africa, Morocco)
Harm caused by the conduct	e.g. 'grave consequences' (Albania, Bulgaria, Estonia, Montenegro, Serbia)
Perpetrator	
Conduct of the perpetrator	e.g. repeat offenders (Azerbaijan, Belgium, Georgia, Norway) and concealing identity (Croatia)
Nature of the perpetrator	e.g. involved in a criminal organisation (Azerbaijan, Finland, France, Germany, Latvia, Moldova)
Position of the perpetrator	e.g. those considered 'insiders' within the victim organisation (Belgium, South Africa, Panama)

Express recognition of specified aggravating circumstances enables substantive criminal law to be more nuanced in its treatment of certain forms of conduct and, in the context of cybercrime, can be viewed as particularly valuable for the integrity offences, where the breadth of conduct covered can lead to concerns about 'vagueness'[32] and over-criminalization.

Critically, the range of aggravating circumstances also serve to mitigate the discrepancies identified above between respondents in respect of the treatment of offences. The following table illustrates the position of the 'lowest tariff' countries if aggravating circumstances are present.

Offence	Basic maximum	Aggravated maximum	Respondent
Access	Fine	1-8 years	Bulgaria
Interception	6 months	2-3 years	Austria
Data Interference	Fine	2 years	Armenia
System Interference	Fine	3 years	Bulgaria
Devices (Supply)	6 months	2-3 years	Austria
Devices (Possession)	6 months	2-3 years	Austria
Forgery	1	1-10 years	Austria
Fraud	6	8 years	Spain
Child porn (Supply)	2	5 years	Albania
Child porn (Possession)	1	3 years	Switzerland
Copyright	Community service	5 years	Moldova

The respondent Parties have only provided information about currently applicable sanctions, not about whether and how these may have changed over time. However, where available, such longitudinal trends can provide an interesting and valuable insight into the changing perception of cybercrime amongst policy makers and legislators.

Based on the experience of the authors, the level of sanction for the computer-related crimes, i.e. fraud and forgery, do not appear to evidence any significant divergence from that applicable to the traditional offences. This is not surprising given that ICTs are simply tools for committing the same underlying offence. Indeed, for many Parties, Articles 7 and 8 of the Convention have been implemented through amendments to existing criminal provisions, rather than stand-alone offences (e.g. UK, Germany). For the content-related offences, i.e. child pornography and copyright infringement, there appears to have been a significant increase in the applicable tariff over recent years, which reflects the fact that the volume of such crimes has grown rapidly in a cyber environment, where the ease of copying and distribution are of a qualitatively different nature to traditional practices. In the UK, for example, the maximum tariff for making indecent images has risen from 3 to 10 years, over recent decades, while the corresponding tariff for

[32] See *US v Drew*, 259 FRD 449 (CD Cal 2009).

possession has risen from 6 months to 5 years.[33] For the computer-integrity offences, there has also been a noticeable trend to increase the level of sanction over time, as the centrality of ICTs to the functioning of modern economics and society has been recognised.

While these trends may be apparent from the evolving statutory treatment of the Convention offences, and reflect changing public policy priorities, they are not necessarily reflected in the practice of the courts at the point of sentencing. Such divergences may represent an inevitable lag between the attitudes of legislators and the judiciary, with the latter playing catch-up. Alternatively, it may reflect a more stubborn cultural perception that certain types of 'white-collar' crime, such as copyright infringement, are not as serious as others.[34]

5.2 Offences under Arts 2-10 committed by legal persons

Extending criminal conduct to legal persons as well as natural persons is recognition that much cybercrime is simply one strand of organised crime. While the Convention obliges the Parties to impose sanctions on legal persons, the nature of those sanctions is left to the Parties to decide, whether criminal, civil or administrative. This reflects the fact that in some Parties the criminal law is not generally applicable to legal persons (e.g. Germany).[35] However, it is also worth noting that studies indicate that the imposition of administrative fines, rather than criminal, is less costly to impose, due to the lower evidential threshold and simpler procedures, which means they can be seen as more 'effective'.[36]

The primary form of sanction, as implied by article 13(2) of the Convention, is monetary, which could include a fine, restitution or an account of profits[37] or an award of damages or compensation to the victim (as remedies). Imposing fines on legal persons is less likely to lead to an 'insolvency problem',[38] which often results in the need to impose non-monetary sanctions on individuals, such as imprisonment, with associated increased costs to the state.

Among the respondents, the level of fine may be prescribed as a maximum, but it is calculated in accordance with varying criteria:

- As a percentage of the legal entity's revenues (e.g. Poland, 3% of annual revenue in the year the offence was committed is the maximum allowable fine);
- Some multiple of the financial gain accrued from the offence (e.g. Hungary, three times the financial gain);
- Some multiple of the damage caused by the offence (e.g. Montenegro, between two and a hundred times);
- Some multiple of the fine that could imposed on a natural person (e.g. Australia, Dominican Republic and France);
- Some multiple of a specified daily rate (e.g. Austria).

The level of the fine may also be enhanced for specified offences, such as drug trafficking (e.g. Luxembourg). In some jurisdictions, a fine may take the form of suspended sentence, not becoming payable unless and until the legal person has been found liable for other criminal offences within a set period of time, e.g. between one and five years (e.g. Bosnia Herzegovina and Croatia).

[33] See Protection of Children Act 1978, s. 6(2) and Criminal Justice Act 1988, s. 160, respectively.
[34] Smith, supra n.12, at 10.
[35] See generally Vermeulen, G., De Bondt, W., and Ryckman, C., *Liability of legal persons for offences in the EU*, Maklu, 2012.
[36] See Faure, M., Ogus, A. and Philipsen, N., "Curbing consumer financial losses: The economics of regulatory enforcement", *Law and Policy,* 2009, vol. 31, 174.
[37] Commonly used for copyright infringements.
[38] Faure, supra n.7, at 5.1.

In addition to monetary penalties, the parties have also provided a range of supplemental sanctions. At one extreme, the legal entity itself may be liquidated or dissolved (e.g. Azerbaijan, Belgium, Moldova, Portugal and Spain); the corporate equivalent of the death penalty. More commonly, the legal person may have its licence or authorisation to engage in an activity revoked (e.g. Norway). Such a ban may be imposed either on a temporary or permanent basis (e.g. Belgium). This sanction is obviously only available where the activity is subject to some form of prior licensing or authorisation regime, which will vary considerably between the parties. In some parties, general commercial activity can require authorisation, while in most parties, only specific sectors are subject to such controls, such as telecommunications or the professions (e.g. lawyers and accountants). Another option is to intervene at the level of corporate governance, imposing judicial supervision over the activities of the legal person for a period of time (e.g. Dominican Republic, Malta, US), effectively imposing a prior restraint on the legal person, akin to an authorisation or licensing regime, although potentially costly to implement.

The seizure or confiscation of property may also be imposed, which is likely where the property had some direct involvement in the criminal conduct, such as machines used in commercial scale copyright infringement (e.g. Bosnia Herzegovina), or the seizure is a form of crime prevention (e.g. Czech Republic).

Another grouping of sanctions relate to legal persons as beneficiaries of the state and the possibility of their withdrawal or deprivation. These benefits may include entitlements to favourable tax treatment (e.g. Panama), or financial subsidies or grants (e.g. Portugal), or exclusion from the right to offer goods and services to the state under public procurement procedures (e.g. Luxembourg, Poland).

A final sanction concerns publicity obligations, requiring the legal entity to publish an adverse decision (e.g. Albania, Dominican Republic, Poland). Traditionally, public denunciation of a crime through sentencing remarks can be viewed as a symbolic statement about societal attitudes towards, and toleration of, particular criminal behaviours.[39] However, the coverage given to judicial comments is inevitably generally limited in most countries. As a consequence there have been legislative moves to enhance denunciation as a sanction by requiring offenders to take steps to publicise their own offending, including paying for 'prominent advertising' in cases of copyright infringement.[40] Such publicity is designed to 'name and shame' and thereby tarnish the reputation of the entity, with (hopefully) resultant economic consequences.

In some respondents, the sanctions available against legal persons may not be levied on certain categories of legal person, generally local and public authorities, as well as international organisations (e.g. Bulgaria).

Legislation can provide that a director, manager or similar officer of the legal person may be held personally liable for the actions of the legal entity, where that person is held to have the requisite fault, such as consenting to the illegal conduct or a negligent failure to supervise or exercise effective control (e.g. Malta, Netherlands, Philippines). In Japan, an advertising company installed a virus on the smartphones of victims to enable them to obtain personal data from contact lists for the purpose of sending unsolicited marketing messages. The company was fined and given a suspended sentence, as well as a 'representative director'.[41] The imposition of imprisonment on an individual concurrent with any monetary penalty imposed on the corporate entity is likely to heighten both the effective and dissuasive impact of the sanctions regime.

[39] Smith, supra n.12, at 109.
[40] E.g. Directive 2004/48/EC 'on the enforcement of intellectual property rights' (OJ L 195/16, 2.6.2004), at art. 15 'Publication of judicial decisions'.
[41] Replies, at 497.

5.3 Offences for aiding and abetting offences under Arts. 2-10

Article 11 of the Convention refers to 'ancillary liability', distinguishing between aiding and abetting (para. 1), also known as 'accessory liability', and attempts (para. 2). In the vast majority of Parties, the scale of liability is identical as between the principal and an accessory. Not surprisingly, where the sanction does differ, it is lower for the accessory (e.g. Dominican Republic, Tonga). In Iceland, for example, a more lenient penalty may be imposed if the contribution is minor; if the contribution simply strengthens an already existing resolve to commit the crime; if the crime is not completed or the contribution is unsuccessful.[42]

While the data is unclear, most Parties do not appear to have legislated specifically for accessory liability in respect of the Convention offences, but rather apply general principles of law, whether detailed in the penal code (e.g. Albania) or otherwise (e.g. United Kingdom).

Finally, it worth noting that while the sanction is usually identical, the fault element, or *mens rea*, for an accessory is generally different. Accessory is both more limited, generally requiring knowledge or intent, rather than recklessness or negligence, as well as being dual in nature, requiring intent in respect of the aiding and abetting, and knowledge in respect of the essential matters that comprise the offence.

5.4 Offences for attempting to commit offences under Arts. 2-10

Some Parties provide for more lenient punishment for attempts than commission (e.g. Philippines). Alternatively, some Parties provide for leniency if the attempt could not have led to the commission of the offence, for whatever reason (e.g. Hungary, Iceland, Switzerland). Others provide for more lenient penalties for attempt than for aiding and abetting (e.g. Germany, Iceland). Such a distinction could be justified on the grounds in an attempt no actual offence is committed, while in the latter it has, partly due to the assistance.

5.5 Characterising 'serious offences'

Some jurisdictions recognise a statutory distinction between an offence and a 'serious' criminal offence, based on the level of applicable sanction (e.g. Australia, UK). In other Parties, an offence is 'serious' if it is specified as such in the substantive provision itself (e.g. Netherlands). Meeting the threshold may have a range of consequences under the domestic legal system, including in which court the case will be heard (e.g. South Africa); procedural implications in terms of the use of certain covert or coercive investigative techniques (e.g. UK) and the imposition of supplementary sanction measures (e.g. Tonga). The Convention requires the Parties to determine 'a range of serious offences' for which the competent authorities may engage in the interception of communications.[43]

In Australia a 'serious offence' is punishable by imprisonment for 2 years or more and is distinguished from a 'serious terrorism offence'.[44] For the purpose of determining the deployment of certain investigative techniques, UK law defines 'serious crime' in the following terms:

(a) that the offence or one of the offences that is or would be constituted by the conduct is an offence for which a person who has attained the age of twenty-one and has no previous convictions could reasonably be expected to be sentenced to imprisonment for a term of three years or more;
(b) that the conduct involves the use of violence, results in substantial financial gain or is conduct by a large number of persons in pursuit of a common purpose.[45]

[42] General Criminal Code, s. 22.
[43] Article 21(1).
[44] Crimes Act 1914, s. 3C.
[45] Regulation of Investigatory Powers Act 2000, s. 81(3).

Under EU procedural law, the offences in respect of which a Member State has an obligation to assist another Member State are listed by category, which includes 'computer-related crime', as well as requiring a "custodial sentence or a detention order for a maximum period of at least three years".[46]

5.6 Confiscation of instruments and proceeds

The Parties were asked about two forms of confiscation as sanction. The first, often referred to as forfeiture, involves the instruments or tools used for the commission of a crime, such as computers, mobile phones, SIM cards and USB sticks. The object is to remove the offender's ability to reoffend. The second involves confiscation of any items or proceeds from the commission of an offence, such as copyright infringing DVDs or monies. Here, the object is to seize the economic benefits accrued by an offender, undermining any incentive to engage in the criminal conduct.

As with the 'ancillary offences', most Parties have general legal provisions governing both forms of confiscation, rather than provisions specific to the Convention offences. In some Parties, the courts may order the destruction of the instruments or proceeds as an alternative to confiscation (e.g. Tonga).

Limits may be placed on the confiscation of items or proceeds where they have made their way into the hands of an innocent third-party (e.g. Philippines, Morocco, Switzerland).

Finally, in Panama, confiscation as a sanction was ruled to be unconstitutional, because it breached Article 30 of the Constitution, which states: "There's no death sentence, expatriation, or confiscation of property".

5.7 Alternative or cumulative sanctions for offences under Arts 2-10

Over the years, criminal justice systems have developed a range of alternatives to the traditional sanctions of imprisonment and fines. The Parties were asked to indicate what available sanctions existed that could either be imposed as an alternative to the standard tariff or as an additional form of sanction. These sanctions lie along a spectrum in terms of severity, formality and by whom they are determined.

At the least severe end of the spectrum, an offender may be issued with a warning or caution, putting them on notice that future conduct will result in criminal proceedings. The level of formality attached to a warning will generally vary according to where within the criminal justice system the warning is issued. The police may be empowered to issue a formal warning (e.g. UK), a prosecutor (e.g. Hungary) or a court (e.g. Serbia).

Further to criminal proceedings, the offender may be placed under supervision, generally referred to as probation. This may also involve the individual undergoing treatment or education designed to prevent reoccurrence of the behaviours (e.g. Slovakia).

Various forms of public shaming may be used, where the emphasis is on altering the offender's position with society. These include the stripping of decorations and honorary titles (e.g. Albania, Azerbaijan) and removal from elected public office (e.g. Spain).

Alternatively, a community service order may be served, requiring the offender to engage in unpaid work under the direction of the state (e.g. Estonia, Finland, Latvia). This is designed both

[46] Directive 2014/41/EU 'regarding the European Investigation Order in criminal matters' (OJ L 130/1, 1.5.2014), at Art. 11(1)(g).

to punish the individual, through the loss of productive time, as well as enable society to symbolically 'recover' some of the loss suffered as a result of the criminal conduct.

Another means of trying to prevent reoccurrence of the offending conduct is to supplement any custodial or financial sanction with a prohibition (or confiscation) order, removing the object or means of engaging in the criminal behaviour. In a cybercrime environment, an inevitable target of such prohibitions is the ICT devices and Internet services used by the perpetrator (e.g. Canada, Croatia, Spain and UK). While such techniques are available in most Parties, the implementation of prohibitions is becoming increasingly complex in a modern environment where devices and communication services are ubiquitous, at the centre of social and economic life and often shared resources (e.g. a family).[47] In Hungary, the prohibition may extend to certain data, with the courts being given the power to issue an order for "irreversibly rendering electronic information inaccessible".[48] While in Luxembourg, a court may require data to be deleted if it is considered dangerous to persons or property, irrespective of any judgment on the merits of the data.[49] In Estonia, a court ordered the police to delete illegal content on an offender's hard drive, before returing the equipment to the person.[50]

Rather than targeting devices and services, the prohibition may relate to the offender's profession or business (e.g. Denmark, France, Norway, Macedonia, Spain) or his right to stand for or hold public office (e.g. Albania, Iceland, Morocco). Restricting or monitoring a person's movements may also provide an alternative to custody, using some form of electronic surveillance technique, such as tagging (e.g. Estonia).

A final supplemental or cumulative measure involves a requirement to pay compensation to the victim(s) of the criminal conduct (e.g. Italy, Lithuania, Netherlands and the United States), as a form of restitution. In the US, for example, two perpetrators of identity theft and credit card fraud, operating through a ring known as 'carder.su' were sentenced to between 9 and 12 years imprisonment, as well as being ordered to pay restitution to the value of $50.8m.[51] In Slovakia, such compensation would rank above any requirement for forfeiture of property or proceeds of crime in favour of the state.[52] The viability of compensatory sanctions will obviously depend on the offender's ability to pay, which itself can be dependent on the number of victims. For some cybercrimes, such as the dissemination of malware, the industrial scale of harm caused will often mean compensation would only be realistically available if legal entities were involved in the commission.

6 Sanctions in practice

As noted already, whether a sanctions regime can be considered 'effective, proportionate and dissuasive' depends not only on what is stated on the face of the statute, but also actual practice within the jurisdiction in terms of enforcement activity by the investigative authorities; prosecutorial policy and the type, severity and consistency of sanctions handed down by the courts.

While this section reports on the statistics provided on sanctions imposed for cybercrimes, as well as national sentencing guidelines specifically relating to cybercrime, it does not examine the sentencing process itself, which is its own distinct area of study and beyond the scope of this report.

[47] See further Walden, I., and M. Wasik, 'The Internet: Access ~~Denied~~ Controlled!', pp. 377-387, [2011] *Crim. L.R.*
[48] Hungarian Criminal Code, s. 77.
[49] Italian Code of Criminal Procedure, Art. 66. See also the Philippines.
[50] Replies, at 322.
[51] Ibid, at 912.
[52] Slovakia Criminal Code, s. 59.

Respondents were also asked to give examples of 'typical' cases concerning individuals, legal persons and confiscation. These case studies can offer a qualitative insight into a sanctions regime and identify broader issues of interest and concern. While a minority of respondents were able to provide such examples, those that did have been referred to throughout the study.

6.1 Statistics

Respondents were asked to provide available data or statistics about prosecutions. While these statistics provide some empirical basis for assessing the extent to which the domestic criminal justice system reflects the statutory provisions, they do not enable us to assess whether the sanctions regime as a whole meets the objectives of the Convention, in terms of improving international co-operation.

Only 19 countries were able to supply any information and these contributions varied significantly in terms of the range of offences covered, the level of detail and the periods of time covered. In particular, very little data was provided on the actual level of sanction imposed on offenders (e.g. term of imprisonment), to enable a comparison with the available statutory range. While such paucity of information has been widely recognised in previous studies,[53] it remains a problematic issue for policy-making in the area of cybercrime and, in terms of the Convention, when assessing whether a Party's sanction regime is 'effective, proportionate and dissuasive'.

The following briefly details some of the key findings from the data supplied:

- *Albania*: The data indicates that computer-related forgery and fraud were the overwhelming forms of criminal conduct (about 85%), resulting in prison terms in the majority of cases.[54]

- *Bosnia and Herzegovina*: Figures supplied are for 2013-2014 in respect of integrity offences and child pornography. What is of particular interest is the breakdown of figures into the various stages of the criminal justice process; from an order to investigate (and not initiated), to an indictment filed (and confirmed), to acquittal or conviction with applicable sentence. These stages illustrate the complexity and leakages that can occur within a system. In addition, over the two-year period, there were only 4 prison sentences given.[55]

- *Canada*: Statistics were provided in respect of 4 offences over a three-year period (2011-2014), where the charge was considered the 'most serious offence' and was classified as a 'cybercrime' (i.e. child pornography, unauthorized use of a computer, possession of a device and mischief in relation to a computer). In terms of relative volumes, child pornography was 10 times that of unauthorized use, which was itself 10 times that of the other two offences. In terms of trends, there is no significant rise during the reporting period. In terms of sentencing decisions, the child pornography cases split evenly between imprisonment and probation; while the unauthorized use cases more often resulted in probation rather than custody. The other charges did not result in custodial sentences.[56]

- *Czech Republic*: The data indicates the fraud was by far the most common form of cybercrime. Unauthorised access was the second by volume, followed by child

[53] E.g. See UNODC, *Comprehensive Study on Cybercrime*, (February 2013), at Annex Two: Measuring Cybercrime. Available at <http://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf>.
[54] Replies, at 17.
[55] Ibid, at 143.
[56] Ibid, at 210.

pornography and copyright infringement. However, no data was provided on the sanctions.[57]

- *Denmark*: It was not possible to provide data on some crimes, because the statistics do not distinguish between cyber and non-cyber instances. With regard to computer-integrity and content-related offences, data was provided for the period 2001-2015. Both child pornography and illegal access evidence a slight rise across the period, but marked by peaks and troughs. The only area of very substantial and consistent rise over the period was in relation to data fraud.[58]

- *Germany*: Conviction numbers were supplied in respect of the computer-integrity offences, computer-related and copyright infringement, over a period from 2007-2013. By volumes, fraud and forgery were by far the most common, although fraud saw a slight fall during the period, while forgery rose significantly. Data espionage and tampering were the most common integrity crimes, but remaining relatively constant over the period. Copyright infringement saw a significant fall.[59]

- *Hungary*: Data was provided on volumes and average length of imprisonment from 2013 until the first half of 2015. By volume, fraud was the most common, followed by copyright infringement. In relation to fraud, while the maximum penalty is 10 years imprisonment, the average term imposed was around 2 years; while for copyright infringement, the average was 1 year, from a possible maximum of 10. For unauthorised access, the maximum is 8 years, but the average was 1 year.[60]

- *Italy*: The data supplied covered the period 2010-2015 and all the Convention offences. The two most common offences, child pornography and copyright infringement, both evidenced a significant decline over the period, a trend that was echoed across the other categories to a lesser degree. In terms of sanctions, various types of confiscation were by far the most prevalent, with only one apparent custodial sentence out of some 6700 recorded offences. The number of prosecutions of legal persons for cybercrime offences has been recorded, but totalled only 48 during the period.[61]

- *Poland*: Data was supplied on the integrity offences and copyright infringement from 2010-2014. While copyright comprised the majority, the numbers were declining over the period, while numbers were steady for the integrity offences.[62]

- *Romania*: Data is only available for 2015, but records whether the Convention offence was the primary or secondary charge and the prosecution of legal persons. In respect of the integrity offences, the charge is more likely to be secondary, which suggests that integrity offences can often be preliminary offences, facilitating the commission of other offences.[63]

- *Serbia*: The Special Prosecutors Office for High-Tech Crime has supplied Statistics for 2014. The two main categories of offence are the content-related crimes, child pornography and copyright infringement, with prison sentences in about a quarter of cases, the remainder being given probation.[64]

[57] Ibid, at 278.
[58] Ibid, at 296.
[59] Ibid, at 410.
[60] Ibid, at 452.
[61] Ibid, at 472.
[62] Ibid, at 698.
[63] Ibid, at 698.
[64] Ibid, at 762.

- *Slovakia*: Prosecution numbers between 2012-2014 indicate a clear prevalence of fraud and payment card fraud. With regard to the integrity offences, the respondent notes that "police officers do not identify cases in terms of Section 247 of the Code of Criminal Procedure" (the relevant offences), which results in under-reporting. The statistics on child pornography cases focus on 'clear up rates', which is also indicative of what drives statistical reporting.[65]

- *United Kingdom*: There are various sources of data generated through a range of different methodologies. Data from the Ministry of Justice is available between 2004-2014. With respect to the integrity offences, there has been a rise in prosecutions for access offences, but a fall in respect of interference offences. In both cases, however, there has been a greater reliance on suspended sentences, rather than custody. Fraud, forgery, indecent images (i.e. child pornography) and copyright infringement all occur in much larger numbers, but have all experienced a fall in recent years.[66]

- *United States*: Data has only been provided in respect of the integrity offences under the Computer Fraud and Abuse Act. The average term of imprisonment has been recorded between 2003-2012. This average has risen from 10 to 29 months during this period, a near three-fold increase. However, this must be compared against the potential terms of between 1 year (for a misdemeanour) and 10 years (for a felony as a first offence).[67]

Given the nature of the questionnaire, it is inevitable that the statistics do provide a comprehensive picture of the sanction regimes of the Parties. However, the data does enable us to offer some tentative observations about the experience and practices of the Parties. First, fraud is the most common category of cybercrime, occurring in substantially greater numbers than the integrity offences. Part of an explanation for the low numbers may be because integrity offences are often only a stage within a broader chain of criminal conduct and therefore represent a minor component of the eventual potential charges available to prosecutors. Second, custodial sentences appear to be more often the exception rather than the rule, with probation or suspended sentences as the preference. Even where imprisonment is used, there exists a large discrepancy between the statutory maximum available and that imposed. This may reflect concerns about the effectiveness of prison, whether as a means of punishment or rehabilitation. It may also reflect concerns about the relative public costs of prison compared with other modes of punishment. Alternatively, it may be represent a disjuncture between the attitudes of the legislators and the judiciary towards cybercrime. Finally, while the need to address the role of legal persons has been increasingly recognised within the substantive criminal law of the Parties, successfully prosecuting them through the criminal justice system remains a complex and uncommon practice.

6.2 Sentencing guidelines

As noted previously, while domestic statutory frameworks lay down a maximum (and possibly minimum) applicable tariff for each and every form of Convention offence, standard practice in the legal systems of the Parties is for the type and level of sanction imposed on an offender to be determined through an exercise of discretion by the courts. The inevitable variance that results from this approach can either be viewed as necessary feature of an individual's right to a fair trial and recognition that the judge is best placed to consider all the relevant facts and circumstances of the case, or as undermining legal certainty and the primacy of legislative decisions about the scale of sanction appropriate for certain forms of criminal conduct.[68] One means of attempting to reconcile the two perspectives is through the promulgation of sentencing guidelines. Sentencing

[65] Ibid, at 781.
[66] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/428937/outcomes-by-offence-tables.xlsx
[67] Replies, at 910.
[68] Faure, at 6.2.

guidelines are directed at the judiciary and detail those factors considered relevant to sentencing decisions in respect of particular crimes and (sometimes) those factors considered irrelevant. A body considered independent of both government and the judiciary, such as the UK's Sentencing Council and the US Sentencing Commission,[69] often develops the guidelines.

With regard to sentencing guidelines for the Convention crimes, the majority of respondents either appear to have no guidelines at all (e.g. Bulgaria) or have generic guidelines applicable to all categories of offence rather than tailored to the cybercrime offences (e.g. Slovakia in respect of custodial offences, Lithuania). Only a small number of Parties have specific written guidelines in respect of cybercrime, covering all the Convention offences or for a subset (e.g. Albania, some Canadian states, Montenegro, UK, Philippines and the US), or are currently in preparation (e.g. Denmark). In some common law countries, which operate on the basis of precedent, court decisions can establish sentencing principles that then become guidelines (e.g. Australia, Canada).

7 Concluding remarks and recommendations

This study has carried out a comparative examination of the sanction regimes applicable to the Convention offences. For respondents that are a Party to the Convention, there is obligation to implement an 'effective, proportionate and dissuasive' sanctions regime, at Article 13. This study has examined various interpretations and the constituent parts of this obligation, as well as state practice in terms of substantive and procedural criminal law, and recorded case law.

7.1 The key findings of the study are as follows:

1. Some respondents have sharply differing attitudes to how seriously computer-integrity offences should be treated under a sanctions regime. This differential has the clear potential to undermine the Convention's objective of enhancing international co-operation.

2. Statutory recognition of a range of aggravated circumstances can serve both to significantly reduce the differences between respondents' sanction regimes, as well as the danger of over-criminalization.

3. There is a stark disparity between the maximum level of sanction prescribed in statute and judicial practice, where imprisonment appears to be the exception rather than rule, while suspended or conditional sentences are favoured over actual jail time.

4. Most respondents have a comprehensive and diverse range of sanctions available against legal persons involved in the commission of cybercrime. However, the evidence suggests that cases involving legal persons comprise a small minority of current case law.

5. The ancillary offences of attempt and aiding and abetting are generally available under general criminal law provisions. No evidence was supplied about the volume of prosecutions for such offences.

6. Distinctions between ordinary and 'serious' criminal offences are expressly recognised in the criminal law of some respondents. To date, harmonisation only exists under EU procedural law.

7. Alternative and cumulative sanctions constitute an essential part of an 'effective, proportionate and dissuasive' sanctions regimes, especially alternatives to imprisonment.

7.2 Recommendations

[69] See https://www.sentencingcouncil.org.uk and http://www.ussc.gov respectively.

The following recommendations are made to the T-CY for consideration:

1. Consider the possibility of developing a guidance note for the Parties on a sanctions regime for the Convention offences, including addressing the issue of 'serious offences'.

2. Consider the possibility of developing model sentencing guidelines for the Convention offences, which would elaborate potential relevant and irrelevant factors for consideration.

3. Future research should include an empirical study of the extent to which a Party's sanction regime has facilitated or hindered international co-operation in the fight against cybercrime.