The new EU counter-terrorism directive: closing all the gaps in the EU legal framework?

Maria O'Neill

This is an Accepted Manuscript of a book chapter published by Routledge in The development of transnational policing: past, present and future on 15th October 2019, available online: https://www.routledge.com/The-Development-of-Transnational-Policing-Past-Present-and-Future-1st/McDaniel-Stonard-Cox/p/book/9781138488779

The new EU counter-terrorism directive: closing all the gaps in the EU legal framework?

Dr Maria O'Neill

Abstract

The EU has tightened its definition of terrorism, yet gaps still remain. The nexus between public (national security and law enforcement) services and private commercial operators needs further examination. This contribution proposes a global nodal governance of security, focusing on this public/private security nexus. This should be developed through the use of reflexive law-based mechanisms, supported by and working with traditional criminal law, to comply with the principle of legality. This would enable state security and law enforcement to benefit from the expertise and knowledge based in financial and technology commercial operators for the benefit of terrorism prevention.

1. Introduction

The European Union (EU) has recently updated its provisions on terrorism through the passing of Directive (EU) 2017/541 on combatting terrorism, replacing the earlier Council Framework Decision 2002/475/JHA. A directive is an order to member states to pass law. Post-Lisbon (and pre-Brexit) these new counter-terrorism provisions needed to have been enacted in 24 individual EU member states' legislation by the 8th September 2018. The Commission will undertake a full review of its implementation, and its effectiveness, in due course. The UK, Ireland and Denmark are maintaining opt-out positions on this directive. This directive provides for ten distinct terrorist offences (Article 3), seven offences related to terrorism, and three further "other offences related to terrorism". While much of the earlier framework decision is replicated, there are some substantial new offences, in particular the other "offences related to terrorism". Many arise at the nexus between security and private commerce, for example financial or IT companies hereinafter "commercial operators". They include "public provocation to commit a terrorist offence" (Article 5), "recruitment for terrorism" (Article 6), "providing training for terrorism" (Article 7), "organising or otherwise facilitating travelling for the purpose of terrorism" (Article 10) and terrorist financing, (Article 11). This could have major ramifications for commercial operators, who are involved in publishing material on social media, (or providing the means to publish, depending on how a particular law is interpreted), which could lead to training, incitement or recruitment for terrorism. Others could be involved in providing travel packages which are used by terrorist organisations for the purpose of travelling for terrorism. Other commercial operators may be in the business of providing or maintaining financial mechanisms which end up being used for the purpose of collecting or transferring funds to pay for terrorist activities. The relevant commercial operators are not in the business of security provision, and therefore cannot be classified as private security providers. The term, "private security providers" has been adopted in the literature to mean those whose primary commercial focus is the provision of security or security related services (Bures and Carapicio, 2017, Stenning, 2000).

This chapter will examine the provisions of the 2017 counter-terrorism directive, focusing on the issues which arise with regard to the regulation of the private/public security nexus. In particular many of the commercial operators relevant to this analysis, such as internet service providers, operate in a transnational context. The traditional command (you will not do this) and control (and if you do we will punish you) approach to the drafting of criminal law legislation shows its limitations in two contexts. The first of these limitations arise in the regulation of constantly changing complex situations. These would include newly developed banking services and the rapidly evolving world of technology. Also of interest to this paper is the way that technology, to include the internet, is being used by, *inter alia*, criminals and terrorist organisations, and those who inspire individual terrorists. Traditionally drafted legislation, with its requirement under the principle of legality, to be precise and focused, has a problem keeping up with rapidly evolving situations. The second weakness arises when the laws of an individual jurisdiction try to influence individuals and companies which operate transnationally, and which are not based in that particular jurisdiction.

A late 20th century concept of reflexive law is worth examining in the context of the public/ private security nexus, to include its transnational context. As stated by Kennedy (2015, p.129), reflexive law is a concept of law which is based on "renouncing standards and targets in favour of communication and structural supports for contemplation". The practice of using the ideas which underpin reflexive law which is now emerging, has built on Teubner's (1983) original concept, which itself was a development of earlier responsive law theories. It requires the "fusion of public and private governance regimes" (Janczuk-Gorywoda, 2012, p.1439), such as, in the context of this contribution, those of technology companies and national security and law enforcement agencies. Rather than relying exclusively on the traditional "'vertical' subordination of citizens to their sovereigns" there is a focus on "'horizontal' relations between equally situated market actors" (Caruso, 2002, p.3), in public-private governance regimes. The motivation for states is that with the shift from "government to governance" across a range of sectors, law, as traditionally designed and operated, begins to show its limitations and "appears to have become a fragile project" (Zumbansen, 2008, p.771). Businesses' motivation to engage with mechanisms based on reflexive law is that they are "seeking to move 'beyond compliance'" focusing, for example in the environmental sector, on "voluntary performance of targets and internal environmental management systems", thereby avoiding what would otherwise be very expensive environmental litigation (Kennedy, 2015, p.129). In addition, the relevant environmental commercial operators would be avoiding very poor public and customer relations. In this process business can contribute to the development of collaborative solutions to evolving complex problems, leading to benefit for themselves, government, and the subject matter of their concerns, such as the environment.

If deployed carefully, regulation based on the reflexive law concept should prove to be an additional tool to bring about a change in behaviour in the market. All the underpinning criminal offences would still have to be legislated for in accompanying traditional command and control legislation in order to comply with the principle of legality. Regulation based on reflexive law has the greatest impact on the global market place if enacted by key jurisdictions, those with the largest revenue generating power for commercial operators. These would typically be the US, EU and UK. Together these jurisdictions could enact corporate governance standards, requiring reflexive law mechanisms to be used to ensure that commercial operators do not undermine the law enforcement and security requirements of states. Commercial operators, in order to operate efficiently, usually align their internal

operations and standards to those of their largest export markets, and where these have differing standards, to the export market with the highest standards.

This chapter proposes a nodal governance of security based on reflexive law concepts adopted by the above key jurisdictions. This should be deployed when tackling transnational threats which arise at the point where global business interacts with counter-terrorism operations. Different states' national security and law enforcement agencies would be key nodes in the proposed framework. Market leaders from the commercial world would also have to be included in the nodal framework, as there would be a need to harness the abilities of highly trained knowledge makers, such as the leading computer programmers and software developers, or the commercially based developers of new financial products, to assist in designing and maintaining compliance and reporting mechanisms. This chapter will first take an overview of key new provisions of the 2017 counter-terrorism directive. It will then go on to focus on the public-private security nexus, the point where commercial operators, in their day to day business activities bisect the work of national security and law enforcement agencies. The use of reflexive law-based mechanisms in the governance of security will then be examined. The chapter will go on to examine possible use of a nodal governance of security and will then sketch out some of the issues around one such security nexus under the counter-terrorism directive, that of technology companies.

2. **The 2017 directive on Counter-terrorism**

The new EU counter-terrorism directive (Directive (EU) 2017/541) recognises that "the terrorist threat has grown and rapidly evolved in recent years" (paragraph 4, Preamble). Closely allied is the four pillared (prevent, protect, pursue, respond) EU Counter-Terrorism Strategy (2005), which was further developed and revised in 2014. These have been closely monitored in light of recent terrorist developments. This contribution feeds into the evolving "prevent" pillar of the EU's Counter-Terrorism Strategy, an issue also explored elsewhere in this book by Silva and Deflem. While the intelligence services of the EU member states are not formally coordinated at an EU level, the role of all other actors, to include police, prosecutors, banks, etc. is reflected in EU legal and policy provisions. For example, provisions have been put in place providing for transnational cooperation for national law enforcement and prosecutors, while coordination of responses are provided for in the context of counter-terrorism for customs, border forces, military etc. Recognising that the term "police" is used more narrowly in many EU countries, particularly those with gendarmerie, than in the English-speaking world, the terms police and law enforcement are used interchangeably in this contribution.

Reflecting the evolving nature of the terrorist threat, and the need for all jurisdictions to be able to effectively prosecute and imprison, the range of offences under the directive, as enumerated above, is broader than under the earlier framework decision. The 2002 framework decision on counter-terrorism did legislate for directing a terrorist group, or participating in terrorist activities, however the new directive (Article 13) provides that "it shall not be necessary that a terrorist offence be actually committed" for an offence under the directive to occur. It could just as easily read that it is not necessary for a terrorist attack be actually committed. The emphasis of the EU counter terrorism strategy, and intelligence led policing more generally, is as much "prevent" and "protect" before an attack, as "pursue" and

"respond" after the event. This is to be welcomed as it should therefore be easier to convict across the EU after an intelligence-led disruption of a planned terrorist attack.

Many of the offences new to this directive, (public provocation, recruitment, training, travelling etc. Articles 5-11) could easily involve both national and transnational private commercial operators. Travel companies, social media platforms or other internet-based businesses will need to ensure that they are not facilitating any of these additional offences. particularly as the liability of legal persons continues to be covered by the directive (Article 17). In particular, aiding and abetting of any of these offences, to include the new offences, with the exception of travel, and inciting in the case of travel, are also to be treated as an offence (Article 14). From a perusal of the available literature, it is not clear why travel is being treated differently.

Some EU jurisdictions, unfortunately, encounter terrorism situations on a much more frequent basis than others and would therefore be more experienced in tackling different types of terrorist activities. For example, Europol's Terrorism Situation and Trend Report 2018, reporting on the situation in 2017 in 28 EU member states, reported on 205 foiled, failed or completed attacks, with over half of those being in the UK. Over a quarter of the attacks were reported by France, with a further seven EU member states reporting one or more attacks in 2017. This left 19 EU member states in the position of having had no terrorist attacks to report in 2017. A larger number of EU countries (19) were however reporting on terrorism arrests made during the year. Therefore, the EU, in adopting a broad and muti-faceted definition of terrorism, will be spreading a comprehensive approach to legislating for terrorism offences among its member states. There will still, however, be some disparity across EU jurisdictions in tacking terrorism due to some of the legal provisions in the EU directive being mandatory, while others are optional. Mandatory provisions provide a base line definition of terrorism, so that other cross border law enforcement mechanisms, such as Joint Investigation Teams and European Arrest Warrants can operate. Optional provisions are recommendations to legislate, however, national legal or practical considerations may affect uptake of these recommendations. New in the directive, an EU member state may extend its jurisdiction for Article 7 offences (providing training for terrorism) to cover "providing training for terrorism where the offender provides training to its nationals or residents" (Article 19.1.c). There is no requirement that that training be provided in either that state or any other EU member state. In addition, each member state can "extend its jurisdiction if the offence is committed in the territory of another member state" (Article 19.1). As the directive was to be implemented by the 8th September 2018, it is as yet too early to say what the likely uptake of this provision will be across the EU. The EU Commission will conduct an analysis of the implementation of the directive in due course. Uptake of these provisions will depend on how a particular jurisdiction reacts to extra-territorial effect of its laws, with some being more enthusiastic in its use, such as England & Wales, than others.

Expressly provided in the directive but implied in the framework decision (Article 20.1), effective investigative tools "such as those which are used in organised crime or other serious crime cases" need to be available for combatting terrorism offences. Some jurisdictions have seen a clear dividing line between organised crime (low policing) and counter-terrorism (high policing) and allocated relevant forces different powers and capabilities. The EU is aiming to see all agencies (other than specialised intelligence services, such as the UK intelligence services, over which it has no jurisdiction) have all legal tools available to them, to include those originally developed by organised crime and drug trafficking officers, in order to effectively combat both national and transnational terrorism. In addition, those working on a

counter-terrorism operation should ideally be able to engage with their counterparts in the next jurisdiction, even if one or other force is not a specialist counter-terrorism unit (as long as all officers have the necessary security clearances). In addition, police in one jurisdiction may need to interact with customs, border force etc. in another jurisdiction.

With a specific focus on the issue of on-line content which would assist with either radicalising or training potential terrorists, taking a command and control approach to regulation Article 21 of the new directive provides that "member states shall take necessary measures to ensure the prompt removal of online content constituting public provocation to commit terrorist offences… hosted in their territory". In addition, "they shall endeavour to obtain the removal of such content hosted outside their territory". The directive does not provide how this objective is to be achieved. If the removal of content is "not feasible", then the directive goes on to provide (Article 21.2) that the member state shall "take measures to block access to such content towards the internet users within their territory". Article 21.3 sets out the parameters for national measures for removal and blocking of relevant online content.

Now that there is a requirement in the directive to legislate for terrorism offences which involves commercial operators, there is a need to develop a governance framework involving both key national security and law enforcement agencies and relevant commercial operators. The 2017 counter-terrorism directive did not however address the issue of how such a framework would be developed. This paper proposes the development of a governance framework using a nodal governance of security based on reflexive law. Rather than using territorially based command and control legislation, or piecemeal negotiated solutions with one or more of the current commercial operators in one or more national jurisdiction, this should assist in developing long term mutually beneficial relationships between the relevant commercial operators and key national security and law enforcement agencies. The arising public-private security nexus and the possibility to develop a nodal form of governance to address that nexus will now be examined.

3. **Public-Private security nexus**

Many academics, such as Stenning (2000) and Wakefield (2016), have been examining the role of the police, and concepts underpinning both policing and the provision of security in recent years, to include the role of private security providers and their interaction with the police. Less emphasis to date has been put on the current or potential role of the non-security providing corporate world in assisting law enforcement and counter-terrorism, through the provision of information which has the potential to be developed by national security and law enforcement agencies into intelligence. Intelligence-led policing is a style of policing initially developed in the UK (Radcliffe, 2016), and has now, at least for transnational law enforcement, been adopted by EU member states. The processing of intelligence for intelligence led policing is also the key function of Europol. Brodeur (2010, p.309), in his attempts to map those involved in policing, developed a concept of the "outer edges of policing". Brodeur's concept of policing, to include its outer edges, does not involve either "intelligence led policing", or the feeding of intelligence from the outer edges of policing to the state forces or agencies. Brodeur (2010) does address "private policing" in the context of the "outer edges of policing", adopting this term in the context of private security providers. Of more direct relevance to the outer edges of intelligence policing, Gottschalk (2016)

examines the role of fraud examiners in private policing, establishing that they operate in parallel with state law enforcement, with little interaction between the two. This lack of interaction is highly problematic. If there is no mechanism or practice for those such as fraud examiners to feed intelligence to state agencies or forces, then they cannot be contributing to the outer edges of intelligence led policing by state forces or agencies. There would appear to be a breakdown in intelligence sharing by those engaged in private policing roles, presumably tasked with narrow corporate interest roles, with the state forces and agencies which have been tasked with general public security. The term "private policing" has not been used in the literature to address the involvement of commercial operators which, as a result of their primary commercial operations, can, as a secondary product, acquire information which is of use to state security and law enforcement services, as the ingredient for developing actionable intelligence, either to combat organised crime, or to counter terrorism. It is for that reason that the term commercial operators is being used in this chapter to refer to those which could fulfil this role.

A further issue in the context of commercial operators which operate transnationally is that traditional security and law enforcement structures have been designed to secure the post-Westphalian state. Protecting one's own state is not always aligned with taking action to protect another state, or stateless persons, or even human beings generally. State structures need to be further developed in order to combat the increasing phenomenon of transnational serious and organised crime, or transnational terrorism. Criminal law as usually devised and operated falls into command and control regulatory frameworks, as does the design and operation of their associated policing frameworks. With traditional legal frameworks the issue of "the application of domestic law to international actors" arises, as "the power of command-and-control regulation largely [stopping] at the border" (Girard, 2014. p.321, 2). States regularly encounter problems regulating behaviour which occurs beyond its borders, even if the effect of that behaviour is felt within its territory. In particular, it is very difficult for a state criminal law structure to punish those outside its borders. Only in exceptional cases will another state assist in prosecution or extradition proceedings. Some new mechanism need to be developed to cover the increasing level of threat arising from globalisation. In addition, traditional "command-and-control is too static" (Orts, 1995, p.782). Writing in the context of environmental regulation, Orts (1995) points out that "command-and-control establishes performance and technological standards" (p.782), but by the time the law has been passed or adopted, technology has moved on, and knowledge has changed (p.782). The same can be said for the transnational terrorist threat.

In addressing the twin issues of developing a workable extra territorial effect of domestic law and the regulating of rapidly evolving areas such as technology, it is necessary to refocus and broaden the debate on law enforcement. The change in focus from "police" to "policing" has already happened (Shearing 2001). Brodeur (2010) has moved from "policing" to the "governance of security". Governance of security sets frameworks within which commercial operators and national security and law enforcement agencies can operate and interact. Commercial operators can both combat the publication of radicalisation material on their own platforms and report information to the relevant authorities. This would protect them from possible prosecution, from exploitation by organised crime or terrorist groups, protect their consumer base, and be good public relations and corporate governance behaviour. The communicated information could then be developed into actionable intelligence, leading to more focused traditional policing or counter-terrorism operations. The involvement of commercial operators in the design of laws would not necessarily be a radical departure from the current situation, as national and transnational commercial operators, such as internet

service providers, have already engaged in processes involving the shaping of regulation (Bures and Carapicio, 2017, p.234).

Shifting focus to the "governance of security" from "policing" allows for the development of the concept of "a regulated network of participatory 'nodes'" (Shearing, 2001, p.261) in a transnational public/private commercial operator context. As Shearing (2001) has stated, each of these nodes can then be designed to have the "authority, capacity and knowledge that together provide for the governance [of] security". Nodal governance means that all parties in the network have the ability and opportunity to influence the other. It is in this context that the nodal governance of security becomes relevant, with Shearing (2001, p.261) advocating that "effective and efficient governance requires the mobilisation of a network of capacities and knowledges located within a variety of institutional nodes" to include the leading developers of relevant technology.

New and emerging commercial operators would have to be welcomed into this nodal governance framework in order to achieve maximum market coverage, and also, from a commercial point of view, ensure that the cost of compliance is borne by all players in the market. Commercial operators would bear their share of the costs of compliance through the requirement to internalise their obligations under the governance of security framework into their own corporate governance structures and processes. Their own auditors would be required to investigate and report on compliance, possibly with reports being sent to regulatory authorities as part of the usual corporate reporting cycles. Even if this is not required in the home jurisdiction of the relevant corporate structure, a licence to operate within, say the EU, UK or US could be withheld if these reports are not made, either in the company's home jurisdiction, or where this is not possible reports could be made to their counterparts within the nodal governance framework. The sharing of best practice between commercial operators, or between leading IT based national security agencies and commercial operators, to include the most effective approaches and technological responses, might also be encouraged.

Commercial operators often have highly skilled knowledge workers who can, while still focused on the business plans of their employers, if properly harnessed, add value to national security and law enforcement activities. Brodeur (2010) refers to "smart crime", where crime is "increasingly defined as knowledge-based" and where public policing, on its own, is "minimally effective" (p.254). Only the knowledge makers of the commercial operators, based in financial and IT companies can keep up with the fast-changing pace of developments in some sectors of society. Commercial operators are therefore needed to assist in designing and maintaining compliance and reporting mechanisms. Transnational commercial operators are also often operating beyond national command and control legal frameworks. As a result, new forms of conceptualising governance of security frameworks and new forms of regulating these frameworks are necessary.

The limits of national criminal law and law enforcement have been recognised for many years. There has been an allied recognition of the need to develop transnational law enforcement networks. As well as developing such networks within the EU, the EU has been developing similar provisions with non-EU member states, such as Europol operational agreements with the US, Australia, Canada and a number of countries directly neighbouring the EU, and Eurojust's variety of agreements with third states and organisations involving cooperation agreements, liaison prosecutors and contact points. These can provide models for

state to state cooperation globally. They do, however, need to be further developed in order to encompass the transnational corporate world, as suggested in this chapter.

A nodal governance of security structure, designed and implemented by earlier adopter jurisdictions and commercial operators, operating under relevant regulatory frameworks, could be further developed and added to as more jurisdictions enact the relevant legislation. Information being passed to state security or law enforcement agencies, as appropriate for the relevant jurisdiction, can then be disseminated, in accordance with relevant national laws, and, in the context of the EU, data protection and data security rules, to other state law enforcement and security agencies. This would involve using either already developed, or developing, transnational law enforcement or security networks.

A nodal governance framework, building on earlier concepts of the "governance of security" (Brodeur, 2010, p.9) would therefore have to be developed, involving multiple jurisdictions, their national security and law enforcement agencies, and relevant commercial operators. As Burris, Drahos & Shearing (2005, p.33) point out, nodal governance is based on "contemporary network theory", which "explains how a variety of actors operating within social systems interact along networks to govern the systems they inhabit". In this way, these nodes "mobilize the knowledge and capacity of members to manage the course of events" (ibid.). Each of the members of the network are nodes, with the nodes, some more so, some less, exerting influence on the other nodes through the network (p.39).

Financial firms

The development of the governance of security frameworks to address a similar private/public security nexus in the area of anti-money laundering and counter-terrorism financing is instructive. These originate from the G7's Financial Action Task Force (FATF) recommendations (FATF web site), which have been adopted globally. Adoption has been encouraged or required by regional anti-money laundering organisations, such as the Asia/Pacific Group on Money Laundering, as is the case for the US and China, or through regional integration organisations, such as the EU. A combination of active adoption by states of the FATF standards, together with peer to peer pressure to adopt the standards in order to access inter-bank clearing systems etc., without which financial institutions have problems operating, and a system of black listing of non-compliant jurisdictions has led to substantial global adoption of these standards.

A framework for the governance of new and emerging security threats with a public/private nexus can therefore be developed, building on the FATF approach. This could include a peer to peer pressure system, to ensure that those commercial operators not directly effectively regulated in this context by their own states, are still required to comply with agreed global norms, in order to be able to effectively interact with their required service providers, advertisers, or their peers. In addition, the commercial operator could be prohibited from operating within individual jurisdictions if there is a failure to comply. Implementing provisions to meet the requirements of dominant jurisdictions, such as the EU, US and the UK would lead, in all likelihood, to new internal governance structures affecting the entirety of the commercial operators' global business, thereby spreading good practice to less regulated jurisdictions. When this happens in the context of EU regulation, which often sets the highest norms globally for other aspects of commercial transactions, this is known as the "Brussels effect" (Bradford, 2012).

Bradford's (2012, p.9) "Brussels effect" relies on neither cooperation nor coercion. When the EU imposes its standards "equally on domestic and foreign players" (p.36), the foreign companies need to decide whether to produce products or services following a number of different regulatory standards, or to the highest set of standards. A commercial entity usually decides to adopt the highest set of standards for cost reasons. An example that Bradford (2012) used in her writings to evidence the Brussels effect is internet companies, which "find it difficult to create different programmes for different markets", and therefore apply the "strictest international standards across the board" (p.25). She cites both Google and General Motors amending their global privacy policies to the EU standards (p.6). Google still expressly refers to EU standards in its privacy policy for all its customers.

Social media platforms

A similar approach to FATF could be adopted for other public/private security nexuses, such as countering radicalisation on social media platforms. Just as the banks know the area of financial services better than national law enforcement and security services, so too technology commercial operators know social media best, and what solutions would be most effective to tackle the security threat. In addition, leading companies in this market are and will be continually changing. Holding one company, in one jurisdiction, to task for its activities will not lead to a general adoption of standards across the relevant industry. It should be remembered that future commercial operators could be legally based in any jurisdiction across the globe.

While actual law enforcement and counter-terrorism operations would remain the remit of individual states, following their internal legal frameworks, the nodal governance framework would operate in two distinct ways; 1. ensuring common standards were maintained by commercial operators through their corporate governance framework, and 2. ensuring structures and procedures were provided so that information could be reported by the commercial operators to the relevant national security and law enforcement agencies, with a view to the development of actionable intelligence. As stated by Grabosky (1994, p.196) in a wider context, "corporate criminology for the twenty first century will focus on a wider regulatory space, and will seek to devise an ordering to harness the interest of third parties in developing a new culture of compliance". Grabosky's view is becoming increasingly relevant in the current age. As Burris, Drahos & Shearing (2005, p.58) point out, the effectiveness of a nodal governance framework "depends on how nodal governance is constituted". Initial designs may have to be revised or amended to ensure that the governance of security at a public/private security nexus operates effectively.

4. The use of Reflexive law-based mechanisms in the governance of security

The approach of reflexive law, discussed above, could be taken in the area of the governance of security, particularly where a security issue arises at both a transnational level, beyond the usual regulatory enforcement space of an individual state, and at a nexus between public (security and law enforcement) and private commercial (technology) operators. The underlying criminal offences and obligations would have to be clearly legislated for in domestic legislation, thereby maintaining the principle of legality. The additionality of an approach based on reflexive law is in ensuring that transnational commercial operators

manage their businesses in a way that does not undermine national and transnational security. In addition, the legal obligation on the private commercial operators should also be covered by both criminal and corporate law provisions. Many corporate law provisions already cover areas of white collar crime leading to heavy fines and imprisonment. For example insider dealing, in the UK, under s.52 of the Criminal Justice Act 1993, leads to a fine or imprisonment for up to seven years, or both, under s.61. Offences relating to cartels under competition law, in the UK, are covered by s.188 of the Enterprise Act 2002, as amended, leading to, under s.190 a maximum of five years imprisonment or a fine, or both. This would not, therefore, be a completely new development in corporate law.

Corporate governance law could easily accommodate new objectives. For example in the UK, the Companies Act 2006 (Strategic Report and Directors' Report) Regulations 2013 requires the reporting of "social, community and human rights issues… including information about any policies of the company in relation to those matters and effectiveness of those policies" (Section 3, inserting a new Section 414C.7.b.(iii) into the Companies Act 2006), with failure to do so leading to a criminal offence under which an individual can be fined (Companies Act 2006, Section 414A.). An obligation could be placed on private commercial operators to report information that they become aware of to relevant public security and law enforcement agencies. The counter-terrorism directive could be amended to require member states to legislate in this area, and to set up law enforcement and counter-terrorism frameworks to receive this information from the corporate world. Relevant domestic company law provisions should also set out clear legal requirements to report that security governance internal corporate processes are being undertaken, to include the form that it is taking. This would avoid any claims that the proposed reflexive law-based mechanisms breached the principle of legality.

Reports on internal processes would typically be made by companies to relevant regulatory authorities, shareholders and the public in their annual reports. Traditionally a company registered (or have its real seat, depending on the jurisdiction), in, for example, China, would have to comply with Chinese corporate law. However, if that Chinese private commercial operator was doing business in say, the UK, it would, for the purposes of the subject matter of this paper, also have to comply with these specific corporate governance and reporting provisions under UK law, and to also report to UK company regulators. This would arise if the Chinese reporting structures did not allow or permit this type of reporting in China, or if those reporting mechanisms were not considered to be of equivalent standard to those in the UK. In addition, the Chinese private commercial operators would have to report relevant national security sensitive information that it obtained while doing business in the UK, to the UK security and law enforcement agencies, if the Chinese security and law enforcement agencies were not also in the transnational nodal security governance framework proposed in this paper. If the Chinese security and law enforcement agencies were full members of the proposed nodal framework on security, then they would be automatically sharing relevant information and intelligence with their counterparts in the UK.

The ideas underpinning reflexive law, as conceived in a non-security environment, such as in the context of employment or environmental regulation, is legislated for in a manner which does not give "specific orders or commands", but rather by way of establishing "incentives and procedures that encourage institutions to think critically, creatively, and [importantly in the context of the fast moving technology world,] continually about …their activities" (Orts, 1995, p.280). This would still be relevant when considering how those activities would affect the technological commercial operator/ national security - law enforcement nexus. Constant

reflection is therefore required, and reflexive processes set up, in order for law to be continuously responsive to evolving situations (Teubner, 1983, p.275). Corporate regulators and national security and law enforcement agencies would have to be involved in this process of constant reflection on how the evolving legal framework was operating. This could be provided for in amendments to the counter-terrorism directive. As Teubner (1983, p.277) has stated, the role of the legal system is "to guarantee coordination processes and to compel agreement".

In some policy areas where concepts based on reflexive law have already been deployed, it is thought that the shift of responsibility from the State to the market might be sufficient to meet the objectives set, such as better environmental or employment regulation, leading to the creations of "new public-private hybrid models of governance" (Shaffer, 2011, p.244). This is not what is being proposed here. Those responsible for national security and law enforcement will not be interested in the State ceding power to the market. Nevertheless new, or at least, additional modes of governance are required in order to effectively tackle transnational threats. The spreading of the responsibility to provide security, or to support those already tasked with the provision of security, is already moving beyond the traditional national security and law enforcement agencies, with Bures and Carapicio (2017, p.237) writing about the "responsibilization of all sectors of society for collective security". This responsibilisation would include not only the private provision of security services, such as at airports, commercial premises, the operation of CCTV etc. but also the tasking of non-security providers with security related tasks. For example, the provisions of the Prevent pillar of the EU Counter-Terrorism Strategy (2005), as developed and implemented, on terrorism finance tracking provisions, the security of explosives, and ensuring that chemicals are not diverted from commercial supply chains are all relevant.

It is difficult for legislation to provide a design for the necessary "formal and institutional architecture", given "the multi-layered forms of societal rationalities" which the law needs to interact with (Wen, 2016, p.351). It is expected that the relevant sectors would assist in designing the necessary frameworks for their particular sector, and then constantly reflect on whether the process is working or needs redesign. As pointed out by Zumbanzen (2008, p.793), reflexive law-based regulation needs to be "tentative, experimental, and learning". The law itself, and the structures and mechanisms that it aims to develop, requires constant self-critical review of the relevant social institutions and their processes (Orts, 1995, p.780). The complexity at which any sub-set of society operates, to include both the national security and law enforcement agencies, and their potential engagement with the rapidly evolving technology sector, precludes the legal framework expressly setting out how internal and intra-nodal procedures and processes are to be managed. All the law can state is that they have to be managed effectively. The complexity of this potential relationship means that a traditional command and control legal framework is "bound to fail" (Dorf, 2003, p.395).

Reflexive law-based regulation does also attempt to address the "application of domestic law to international actors" (Girard, 2014, p.321). The approach of "reflexive regulation" is to set the required objective by way of law, which is mandatory on the legal entities operating within a particular jurisdiction but leaving it to the market operators to "determine the most efficient and effective ways to achieve [the] desired results" (Girard, 2014, p.338). In designing "horizontal" relations, which can extend outside the territorial boundary of an individual state, regulation based on reflexive law concepts "seeks to design self-regulating social systems through norms of organization and procedure" (Teubner, 1983, p.254-255).

The intention behind the use of regulation based on reflexive law is to regulate by creating "a level playing field for all businesses" (Wen, 2016, p.21). However, it has been noted that larger operators often succeed in having their interpretation adopted by other players in the market (Wen, 2016, p.22). Jurisdictions could gain legal leverage over other extra-territorial companies whose jurisdictions are not fully integrated into the evolving nodal public/ private governance of security framework on the basis of their turn over or effect on the domestic market, a tactic that has been effectively deployed to underpin EU Competition law for decades (Fox, 1999).

Provisions modelled on reflexive law have already been deployed in particular in environmental law, such as the US's Pollution Prevention Act 1990, and in employment law, the EU's provision on the improvement of health and safety at work (Council Directive 89/391/EEC), with public disclosure requirements being a key focus of those reflexive law-based frameworks. This is from where much of the legal academic commentary derives. Latterly provisions modelled on some of the aspects of reflexive law have also been deployed in the UK (Modern Slavery Act 2015, Section 54) and the US State of California (Transparency in Supply Chains Act 2010) when dealing with human trafficking. Within the EU, provisions modelled on some of the aspects of reflexive law have also been recently enacted in Directive 2014/95/EU which addresses the issue of disclosure of non-financial and diversity information by certain large undertakings and groups.

Lessons can be learnt from the use of reflexive law in environmental and employment law. Alders and Wilthagen (1997, p.436) point out that effective functioning of a system based on reflexive law concepts requires "(1) systems monitoring, (2) intermediary structures and networks (echoed by Deakin and McLoughlin (2011, p.21)), (3) corporate social responsibility, and (4) other market-oriented regulatory tools." To this could be added, in the context of this paper, traditional command and control legislation, specifying supporting criminal offences and relevant criminal sanctions, against both individuals and companies, in compliance with the principle of legality.

As stated by Alders and Wilthagen (1997 p.436), an effective "reflexive, negotiating government does keep (and does need)… certain teeth and claws" when operating a system based on reflexive law concepts. In addition, peer to peer pressure could be deployed, as was effectively used by the FATF. As pointed out by Deakin and McLoughlin (2011, p.21-22), "a reflexive approach does not imply the absence of 'hard law'". Rather, they say, "the legal framework has a number of roles to play: inducing efficient disclosure, setting default rules and encouraging bargaining in the shadow of the law" (p.21-22).

The mechanisms by which a framework based on reflexive law concepts will operate need to be "identified, and once identified, must be affirmatively created" (Deakin & McLoughlin, 2011, p.5). In the context of engagement with the corporate world, the "managerialisation" of law is also key, whereby in-house corporate lawyers gain leverage over their internal governance structures, and can "use the threat of litigation, with the potential for substantial liabilities and wider reputational losses, to persuade employers", to alter their course (Deakin & McLoughlin, 2011, p.6).

5. Nodal governance of security

Moving on to the issue of how to develop the proposed nodal governance of security framework, there is a need to examine which entities would be involved in the development and operation of such a nodal governance. The concepts underpinning this develop come from another area of debate. In this context it is worth noting that there is an ongoing shift in emphasis from state security to global or human security concerns. The focus of the security debate is now on protecting all individuals (or in some cases the environment/ the planet) whatever the individual's nationality and where ever they are located. The UN's Human Development Report (UNDP, 1994, p.24) has called for a move away "from an exclusive stress on territorial security to a much greater stress on people's security". The UN concept of human security originates from this UN report (Kaldor, 2008, p.35), but was also developed on in the UN Millennium Declaration of the General Assembly of the 8th September 2000. This declaration speaks, inter alia, about the need to "take concerted action against international terrorism" (p.9, fifth indent), as well as the need to "intensify our efforts to fight transnational crime in all its dimensions, including trafficking as well as smuggling in human beings and money laundering" (p.9, seventh indent).

The UN's Commission on Human Security (2003, p.130) has stated that the human security approach recognises "the interdependence and interlinkages among the world's people", as it is no longer possible to isolate one population from another in the context of globalisation. Therefore, there is a need to "forge alliances that can yield much greater force together than alone" (Commission on Human Security, 2003, p.130). Rather than leading to the disappearance of boundaries between states, this is leading to what Kaldor (2008, p.36) refers to as the blurring of boundaries between inside and outside the State. This has meant that national security agencies, while still tasked with securing a particular state, are now also assuming the task of securing human beings in the context of human security, by transmitting intelligence to their counterparts in other states in a timely manner and assisting the development of their counterparts in other states.

Just as both new technology and increased mobility "have infused the transnationalisation of criminal activity" (den Boer, 2008, p.71), the same can be said about terrorism. The human security concept is "peopled centred" (UNDP, 1994, p.23), with human beings having a right to personal security, not just as protection from "agents of the state", but also "safety against physical assault by private actors" (Donnelly, 2013, p.35). A human security approach provides that "all lives ought to weigh the same" (de Wilde, 2008, p.237). This means that "nation-states can no longer privilege the lives of their own nationals" (Glasius & Kaldor, 2006, p.15), requiring states to intervene to protect those individuals that come within their sphere of influence, and who are not being adequately protected, whether it is due to war, or in the case of failed or weak states, by their own states (Glasius & Kaldor, 2006, p.15). The human security concept, therefore, requires states to act together. The human security focus to the emerging analysis, as Wood and Dupont (2006, p.9) point out, requires security to "become an all-encompassing condition in which individual citizens [or human beings whatever their nationality] live in freedom, peace and safety and participate fully in the process of governance".

In the academic analysis of the privatisation of security, where private companies provide security services, (a separate category of private business to the commercial operators focused on in this contribution,) it has been pointed out that there has been "significant pluralization" of security governance (Johnson, 2006, p.33). In the context of public-private security provision partnerships there has been a "growing literature on new security arrangements" (Bures and Carapicio, 2017, p.235), with a clear indication being made that

"the market logic has spilled over the security one" (p.234). Writing about the public/private partnerships in the context of military security, Bures and Carrapico (2017, p.236) have written about "the relative decline of political and socio-economic steering capacities of Westphalian territorially-bound nation-states vis-à-vis the (global) business actors," and the resulting "blurring of traditional boundaries between the political, economic and civil spheres of society". They also speak about the "commodification of security" and the increasing use of experts, leading to the view that the private sector can best "deal with security threats and risks given its high degree of efficiency" (p.237).

There are already examples in the area of counter-terrorism where "prevention, detection and reporting are carried out by private partners" with public agencies having the "analytic and repressive" role (Bures and Carrapico, 2017, p.235), for example in aviation, where a variety of passenger name recognition schemes operate. In the privatisation of security debate, Johnson has stated that "it is necessary to consider how, in a market economy, mechanisms can be established to ensure that the collective good is protected in security networks made up partly of commercial elements" (Johnson, 2006, p.34). He goes on to point out that the "process has been far more complex" than a steering versus rowing analogy would suggest (p.33).

The nodal governance model, discussed above, has already been adopted in the context of the relationships between public and private security providers operating in a transnational context (Johnson, 2006, p.35), with emphasis having been put "on the state's meta-authoritative role" (p.50). Lessons can be learnt here which can transfer to the public - security/private - commercial operator nexus. As Brodeur (2006, p.ix) has pointed out, nodal governance "implies that power flows from a nexus of connected – but not necessarily co-ordinated – agents rather than from a single well". Nodal governance is already operating well when "professional bodies, trade associations and insurance companies carry out regulatory functions" (Johnson, 2006, p.51). A variety of actors similarly operate at a transnational level, for example in the context of implementing the FATF provisions where it has long been the case that, "private financial institutions are in effect, authorized to make security decisions" (Bures and Carapicio, 2017, p.235). This places the State as being a key player in security governance, amongst a "network of governing agencies" (Johnson, 2006, p.34). Therefore the State, or in the context of the above argument, groups of states, to paraphrase Orts (1995, p.280), need to deploy mechanisms based on reflexive law concepts in order to "establish incentives and procedures that encourage institutions to think critically, creatively, and continually about how their activities affect [human security] and how they may improve their [security] performance".

6. Involving the technology companies

The current EU legal provisions on data protection would have little negative impact on the above proposals. Importantly the above proposals do not involve the storage of data by commercial operators. The recent General Data Protection Regulation (EU) 2016/679, (GDPR) does not apply to law enforcement or counter terrorism activities of competent authorities, such as national law enforcement (Article 2.d). Legislation requiring commercial operators to notify domestic law enforcement once material of relevance to law enforcement or counter-terrorism activities is encountered would be a lawful processing of data under Article 6.3 GDPR. This obligation to notify should be set out in domestic legislation, or in the

case of the EU, also in EU legislation, and be clear and unambiguous, thereby upholding the principle of legality.

The regulatory gaps in the 2017 directive on counter-terrorism discussed in this contribution appear to have already been identified by the EU Commission, as evidenced by Commission Recommendation of 1st March 2018. The European Commission press release (2018), entitled "A Europe that Protects: Commission reinforced EU response to illegal content on line" talks about "recommending a set of operational measures – accompanied by the necessary safeguards – to be taken by companies and Member States", while it considers whether further legislation is required in order to address the issue of illegal online content. However, the Commission does state that it "will monitor actions taken in response to this Recommendation and determine whether additional steps, including, if necessary legislation, are required". The press release calls for "operational measures to ensure faster detection and removal of illegal content online", to include "clearer 'notice and action' procedures", "more efficient tools and proactive technologies", "stronger safeguards to protect fundamental rights", which are set out in the EU Charter of Fundamental Rights 2000, "special attention to small companies" and "closer cooperation with authorities". It goes on to call for "increased protection against terrorist content online", to include a "one-hour rule", "faster detection and effective removal", an "improved referral system" and "regular reporting". Similar provisions to those set out in the EU's recommendation could also be adopted in other global standard setting economies, such as the US and the UK, which have a proven effect on standards of transnationally operating commercial operators, availing of similar transnational reach such as the previously discussed "Brussels effect". It is hoped that an approach based on reflexive law concepts is seriously considered when addressing the remaining gaps at the public/private security nexus in the 2017 directive in counter-terrorism at an EU level, and that similar provisions will also appear in the US and UK-post Brexit regulatory framework addressing emerging terrorist related security threats. The involvement of commercial operators in the design of laws would not necessarily be a radical departure from the current situation, as national and transnational commercial operators, such as internet service providers, have already engaged in processes involving the shaping of regulation (Bures and Carapicio, 2017, p.234).

Conclusion

With the enactment of Directive (EU) 2017/541 this contribution addresses the security issues which arise at the nexus between public (national security and law enforcement) services and private commercial operators, such as financial or technology companies. Building on the experience of the implementation of the FATF provisions, this contribution recommends the development of a nodal governance of security framework, allied with the deployment of corporate governance requirements, at least in key economies which have substantial leverage over global business, such as the USA, the EU and the UK. While traditional command and control legislation used for criminal law has shown its limitations in addressing issues arising from rapidly evolving sectors such as novel financial products and services, or new ways of using technology, it would still be required to implement related criminal law offences, in order to ensure compliance with the principle of legality. For its part, corporate governance regulation based on reflexive law principles would be an additional tool for national security and law enforcement agencies, if deployed within a nodal framework for security. Regulation based on reflexive law should enable national security

and law enforcement agencies to benefit from the expertise based in financial services or technology-focused commercial operators. A gap clearly exists when considering recent developments in transnational terrorism, and this contribution is an attempt to plug that gap.

Bibliography

Aladers M. and Wilthagen, T. (1997) Moving Beyond Command-and-Control: Reflexivity in the Regulation of Occupational Safety and Health and the Environment, Law & Policy 19(4), 415-443.

Bradford, A. (2012). The Brussels Effect. *Northwestern University Law Review*, 107(1), 1-68.

Bradley G. (2014) Corporate Transparency through the SEC as an Antidote to Substandard working Conditions in the Global Supply Chain. *Georgetown Journal on Poverty Law & Policy* XXI(2), 317- 339.

Brodeur, J.M. (2006) Forward. In: Wood, J. & Dupont, B. (eds.) *Democracy, society and Governance of security*. Cambridge, UK, Cambridge University Press, pp. ix-x.

Brodeur, J-P. (2010) *The Policing Web*. Oxford, UK, Oxford University Press.

Bures O. & Carrapico H. (2017) Private security beyond private military and security companies: exploring diversity within private-public collaborations and its consequences for security governance. *Crime, Law and Social Change* 67, 229-243.

Burris, S., Drahos, P. & Shearing, C. (2005) Nodal Governance. *Australian Journal of Legal Philosophy*, 30, 30-58.

Caruso D. (2002), Private Law and State-Making in the age of Globalization. *International Law and Politic*s, 39(1), 1-74.

Commission on Human Security, Human Security Now, New York, 2003.

Commission Recommendation of 1.3.2018 on measures to effectively tackle illegal content online (C (2018) 1177 final).

Council of the European Union, EU Counter Terrorism Strategy 2005, 14469/4/05 REV 4.

Deakin, S. &. McLaughlin C. (2011) Gender inequality and reflexive law: the potential for different regulatory mechanisms for making employment rights effective. *Centre for Business Research, University of Cambridge Working Paper No. 426, September 2011*. Available from https://www.cbr.cam.ac.uk/fileadmin/user_upload/centre-for-business-research/downloads/working-papers/wp426.pdf, [Accessed 16th of May 2018].

de Wilde, J. (2008) Speaking or Doing Human Security? In: den Boer, M. & de Wilde, J. (eds.) *The Viability of Human Security*. Amsterdam, Netherlands, Amsterdam University Press, pp. 225 -254.

den Boer, M. (2008) Governing Transnational Law Enforcement in the EU: Accountability after Fusing Internal and External Security. In: den Boer, M. & de Wilde, J. (eds.) *The Viability of Human Security*. Amsterdam, Netherlands, Amsterdam University Press, pp. 71-96.

Donnelly, J. (2013) *Universal Human Rights in Theory and Practice*. Chapel Hill, NC, USA, Cornell University Press.

Dorf, M. (2003) The Domain of Reflexive law. *Columbia Law Review* 103(2), 384-401.

European Commission – Commission Recommendation on measures to effectively tackle illegal content on line (C(2018) 1177 final, Brussels, 1st March 2018. https://ec.europa.eu/digital-single-market/en/news/commission-recommendation-measures-effectively-tackle-illegal-content-online [Accessed 16th of May 2018].

European Commission – Press release A Europe that protects: Commission reinforced EU response to illegal content on line, Brussels, 1 March 2018. http://europa.eu/rapid/press-release_IP-18-1169_en.htm [Accessed 16th of May 2018].
FATF (2012) The FATF Recommendations; International Standards of Combating Money Laundering and the Financing of Terrorism & Proliferation, FATF, February 2012. http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF_Recommendations.pdf [Accessed 16th of May 2018].
Feasley, A. (2016) Eliminating Corporate Exploitation: Examining Accountability Regimes as Means to Eradicate Forced Labor from Supply Chains, *Journal of Human Trafficking* 2(1), 15-31.
Fox, E.M. (1999) The Merger Regulation and its Territorial Reach. *European Competition Law Review* 20 (6), 334-336.
Glasius M. & Kaldor, M. (2006) A human security vision for Europe and beyond. In: Glasius, M. & Kaldor, M. (eds.) *A Human Security Doctrine for Europe: Project, Principles, Practicalities*. London, UK, Routledge, pp. 3-19.
Gottschalk, P. (2016) Private policing of financial crime: Fraud examiners in white-collar crime investigations. *International Journal of Police Science & Management*, September 18(3), 73-183.
Grabosky, P .N. (1994) Beyond the Regulatory State. *The Australian and New Zealand Journal of Criminology*, 27, 192-197.
Janczuk-Gorywoda, A. (2012) Public-Private Hybrid Governance for Electronic Payments in the European Union. 13 *German Law Journal* 13(12), 1438-1458.
Johnson, L. (2006) Transnational security governance. In: Wood, J. & Dupont, B. (eds.) *Democracy, society and Governance of security*. Cambridge, UK, Cambridge University Press, pp. 33-51.
Kaldor, M. (2008) From Just War to Just Peace. In: den Boer, M. and de Wilde, J. (eds.) *The Viability of Human Security*. Amsterdam, Netherlands, Amsterdam University Press, pp.21-46.
Kennedy, R. (2015) Rethinking Reflexive Law for the Information Age: Hybrid and Flexible Regulation by Disclosure. *George Washington Journal of Energy & Environmental Law*. 7 (2), 124 – 139.
Orts, E.W. (1995) A Reflexive Model of Environmental Regulation. *Business Ethics Quarterly*, 5 (4) 779-794.
Ratcliffe, J.H. (2016) *Intelligence-Led Policing* (2nd edition). London, UK, Routledge.
Report from the Commission to the Council and the European Parliament - Evaluation report on the Data Retention Directive (Directive 2006/24/EC), COM (2011) 225.
Shaffer, G. (2011) Transnational Legal Process and State Change. *Law & Social Inquiry* 37(2), 229-264.
Shearing, C. (2001) A nodal conception of governance: Thoughts on a policing commission. *Policing and Society*, 11:3-4, 259-272.
Stenning, P.C. (2000) Powers and Accountability of Private Police, European Journal on Criminal Policy and Research, 8, 325-352.
Teubner, G. (1983) Substantive and Reflexive Elements in Modern Law. *Law & Society Review*. 17(2) 239-286.
UNDP, Human Development Report 1994, New York, 1994.
UN GA, UN Millennium Declaration of the General Assembly, 8th September 2000.
Wakfield, A. (2016) Conceptualising private policing. In: Brunger M. Tong S. & Martin D. (eds.)' Introduction to Policing Research –Taking lessons from practice. London, UK, Routledge, 43-56.

Wen, S. (2016) The Cogs and Wheels of Reflexive Law – Business Disclosure under the Modern Slavery Act. *Journal of Law and Society*, 43(3), 327-359.
Wood J. & Dupont, B. (2006) Introduction: Understanding the governance of security. In: Wood J. & Dupont, B. (eds.); *Democracy, society and Governance of security*. Cambridge, UK, Cambridge University Press, pp. 1-10.
Zumbansen P. (2008) Law after the welfare state: Formalism, Functionalism and the Ironic Turn of Reflexive Law. *The American Journal of Comparative Law*, 56, 769-808.

Case law

Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland Ltd.* v *Minister for Communications, Marine and Natural Resources*. [2014] ECR page 00000.