

## I. The renewed EU internal security strategy

IAN ANTHONY

In June 2015 the European Union (EU) adopted a renewed internal security strategy that established priority work areas for the five-year policy cycle 2015–20.<sup>1</sup> The new document built on its predecessor, *Towards a European Security Model*, adopted in 2010—which was the first document of its kind.<sup>2</sup>

It could be argued that the issue of internal security has been on the EU's table ever since it was established by the 1992 Treaty on European Union (TEU).<sup>3</sup> The TEU created EU citizenship, and established police and judicial cooperation on criminal matters within the pillar on justice and home affairs to offer all citizens a common level of protection against crime. The amendments to the TEU in the 1997 Treaty of Amsterdam included a commitment to 'maintain and develop the Union as an area of freedom, security and justice, in which the free movement of persons is assured in conjunction with appropriate measures with respect to external border controls, asylum, immigration and the prevention and combating of crime'.<sup>4</sup>

The 1997 amendments mandated closer cooperation between police forces, customs authorities and other competent authorities in the EU member states, both directly and through the European Police Office (Europol), and established procedures to promote that cooperation. The offences that closer cooperation was intended to tackle were terrorism, trafficking in persons and offences against children, illicit drug and arms trafficking, corruption and fraud.

The mass impact terrorist attacks on the United States on 11 September 2001 fed into further discussion of whether new mechanisms were needed to strengthen and protect the EU. Many elements in the response package defined by EU leaders after September 2001 depended on action in functional areas such as trade, external assistance, civil protection, the regulation of air and sea transport, information security and data protection, where legislation was already established to a significant degree at the EU level.<sup>5</sup> The response also highlighted areas where greater coordination and

<sup>1</sup> Council of the European Union, *The Renewed European Union Internal Security Strategy, 2015–2020*, 9798/15, Brussels, 10 June 2015. If the relevant document number is quoted, EU documents can be obtained from <<http://europa.eu/documents/>>.

<sup>2</sup> Council of the European Union, *Towards a European Security Model*, 7120/10, Brussels, 8 Mar. 2010 (endorsed by the European Council, 25–26 Mar. 2010).

<sup>3</sup> Treaty on European Union (Maastricht Treaty), signed 7 Feb. 1992, entered into force 1 Nov. 1993.

<sup>4</sup> Treaty of Amsterdam, Amending the Treaty on European Union, the Treaties Establishing the European Communities and Certain Related Acts, 2 Oct. 1997.

<sup>5</sup> See Burgess, N. and Spence, D., 'The European Union: new threats and the problem of coherence', eds A. J. K. Bayles and I. Frommelt, *Business and Security: Public-Private Sector Relationships in a New Security Environment*, SIPRI (Oxford University Press: Oxford, 2004).

cooperation between states were needed. While the North Atlantic Treaty Organization (NATO) provided an alternative framework for coordinating military responses, the EU provided the most convenient and efficient way of organizing discussions between national law enforcement agencies.<sup>6</sup>

Thinking about internal security, and the architecture needed to promote it, evolved and developed within the EU during the preparation of the Lisbon Treaty.<sup>7</sup> The Treaty established that the area of freedom, security and justice was a shared competence and, in its Chapter on judicial cooperation on criminal matters, extended the scope of European criminal law to offences that were particularly serious and had a cross-border dimension, most notably terrorism, transnational organized crime and money laundering. The Treaty also created the Standing Committee on Operational Cooperation on Internal Security (Comité permanent de coopération opérationnelle en matière de sécurité intérieure, COSI).<sup>8</sup>

### **Is there an emerging EU security model?**

Security has traditionally been thought of as the responsibility of states. The main focus of national security is protecting the state, while international security has traditionally focused on protecting states from each other. However, the evolving security discourse inside the EU increasingly emphasizes the need to protect citizens, not just territory, in highly integrated societies that depend on a shared social and cultural base, as well as economic and technological interdependence.<sup>9</sup> The EU's 2010 internal security strategy underlined that 'the concept of internal security must be understood as a wide and comprehensive concept which straddles multiple sectors in order to address these major threats and others which have a direct impact on the lives, safety, and well-being of citizens'.<sup>10</sup>

The five-year EU policy cycles used to plan various functional aspects of internal security began to reflect the need for integrated, multidisciplinary and intelligence-led efforts to address different threats—whether from states, terrorists or organized criminal groups. The need to approach internal and external security in a more integrated way was also underlined in

<sup>6</sup> NATO quickly determined that the attacks were an action covered by Article 5 of the 1949 North Atlantic Treaty (Washington Treaty).

<sup>7</sup> Horgby, A. and Rhinard, M., *The EU's Internal Security Strategy: Living in the Shadow of its Past* (Swedish Institute for International Affairs: Stockholm, Dec. 2013).

<sup>8</sup> Treaty on the Functioning of the European Union (Lisbon Treaty) amending the Treaty on European Union and the Treaty establishing the European Community, signed 13 Dec. 2007, entered into force 1 Dec. 2009.

<sup>9</sup> European Commission, *Research for a Secure Europe: Report of the Group of Personalities in the field of Security Research* (European Communities: Luxembourg, 2004).

<sup>10</sup> Council of the European Union, *Towards a European Security Model*, 7120/10, Brussels, 8 Mar. 2010.

December 2005, when the EU adopted a strategy to facilitate working with external partners to address internal security problems.<sup>11</sup>

Recent proposals by the European Commission for counterterrorism measures and measures to address the risks posed by foreign fighters extend beyond EU boundaries. For example, the March 2015 EU regional strategy for Syria and Iraq also addresses the threat from Islamic State (IS), while the April 2015 Sahel regional action plan discusses the measures needed to reduce the security threat to the EU from terrorist activity by al-Qaeda in the Islamic Maghreb (AQIM), operating from northern Mali.<sup>12</sup>

In emphasizing the need to protect people in Europe within a global society, the 2010 internal security strategy mirrored the approach in the 2003 external security strategy, *A Secure Europe in a Better World*. The 2003 document noted that increasingly open borders would make it difficult to separate the internal and external aspects of EU security, while growing dependence on an interconnected infrastructure in transport, energy, information and other fields would create new vulnerabilities.<sup>13</sup> In June 2015 the High Representative of the European Union for Foreign Affairs and Security Policy and Vice-President of the European Commission (HR/VP) described the increasing concurrence, intensity, frequency and complexity of conflicts and crises in the direct neighbourhood of the EU, and presented the results of a strategic review of EU foreign and security policy to the European Council.<sup>14</sup> The review emphasized the interconnected nature of security and the need to ensure coherence between internal and external dimensions. She was subsequently asked by the member states to prepare a global strategy for foreign and security policy by June 2016.

*Security priorities: protecting the union—its member states or its citizens?*

Finding the balance between national and collective efforts to strengthen security has been an important component of the EU discussion on internal security. The TEU and the Treaty on the Functioning of the European Union (the EU's two most important treaties) underline that maintaining law and order and safeguarding national security are state functions, and that national security remains the sole responsibility of each member state.

<sup>11</sup> Council of the European Union, *A Strategy for the External Dimension of JHA: Global Freedom, Security and Justice*, 15446/05, Brussels, 6 Dec. 2005.

<sup>12</sup> Council of the European Union, Council conclusions on the EU Regional Strategy for Syria and Iraq as well as the ISIL/Da'esh threat, 7267/15, Brussels, 16 Mar. 2015; and Council of the European Union, Council conclusions on the Sahel Regional Action Plan 2015–20, 7823/15, Brussels, 20 Apr. 2015.

<sup>13</sup> European Council, 'A secure Europe in a better world: European Security Strategy', Brussels, 12 Dec. 2003, <<https://www.consilium.europa.eu/uedocs/cmsUpload/78367.pdf>>.

<sup>14</sup> European External Action Service (EEAS), 'The European Union in a changing global environment: a more connected, contested and complex world, executive summary', EEAS Strategic planning, 25 June 2015.

However, the treaties also recognize that some security problems require systemic responses, and that solutions need to be found at the EU level. Common action among the member states has been agreed to be the best way to provide citizens with a high level of safety and security.

Promoting the security of the EU, its member states and its citizens is consistent because the EU identifies itself as a community of shared values that are listed in its founding documents: respect for human dignity, freedom, democracy, equality, the rule of law and human rights, including the rights of persons belonging to minorities in societies where pluralism, non-discrimination, tolerance, justice, solidarity and equality between women and men prevail. However, in a worsening security environment, unity has been put under severe strain, as reflected in public attitudes to issues such as migration and territorial defence in an EU that has been transformed by the enlargement of its membership.

The EU does not have a specific definition of security that is systematically applied. In its regular *Eurobarometer* opinion surveys, the EU asks citizens about their fears and concerns, and respondents normally rank the national economy and personal finances as their main priorities. In the survey at the end of 2015 immigration and terrorism were considered to be the two most important issues facing the EU—the first time that non-economic issues have occupied the top two places since polling began in 1974.<sup>15</sup>

Concern about terrorism in public opinion polls has been growing year-on-year for some time, and the proportion of survey respondents who link terrorism and religious extremism has increased substantially since 2011. Concern about immigration reflects a major change in opinion during 2015. Immigration was considered to be the most important issue facing the EU by those surveyed in every member state except Portugal (where it was ranked second), which is also an unprecedented result.<sup>16</sup>

During the 1990s relatively few of those surveyed (typically around 15 per cent) considered immigration to be an important issue, and most were positively disposed towards it. In 1998, in the framework of the European Year against Racism, *Eurobarometer* included a specific question: 'If people from different countries of the South of the Mediterranean wish to work here in the European Union, do you think that they should be accepted without restrictions, be accepted but with restrictions or not be accepted?' At that time, 60 per cent of respondents believed that such people should be accepted with restrictions, 13 per cent felt that they should be accepted without any restrictions, and 21 per cent felt that they should not be accepted

<sup>15</sup> European Commission, Directorate General for Communication, 'Public opinion in the European Union', Standard Eurobarometer Report no. 84, Brussels, Dec. 2015; 90% of the survey had already been completed before coordinated terrorist attacks took place in Paris in Nov. 2015.

<sup>16</sup> European Commission (note 15).

at all.<sup>17</sup> By 2015, almost 60 per cent of those surveyed had a negative view of immigration by people from outside the EU.<sup>18</sup> The attitude to migration from other EU member states, however, was still positive.

The 1998 survey reflected the views of citizens in the 15 countries that were members of the EU at the time, while the 2015 survey reflected the views of an EU that has incorporated 11 countries from central and eastern Europe: Bulgaria, Croatia, the Czech Republic, Estonia, Hungary, Latvia, Lithuania, Poland, Romania, Slovakia and Slovenia; as well as two Mediterranean countries—Cyprus and Malta.

In a benign European security environment the evolving EU discourse decreased the emphasis on traditional threat analysis, based on countering the military capabilities of identified adversary states. However, compared to the situation when the European security strategy was framed in 2003, EU citizens and member states are now paying more attention to the potential risks associated with the systematic modernization of Russia's armed forces.

In 2015 the European Council called on member states to allocate a sufficient level of expenditure for defence and to improve cooperation to deliver key defence capabilities. Moreover, since any threat from an adversary state is now expected to include non-military forms of attack, the Council also called for better mobilization of EU instruments to help counter hybrid threats.<sup>19</sup> However, many EU member states see NATO as the main framework for their collective defence, and support for EU engagement in defence matters differs.

The evolving thinking gradually defined the need for what has been labelled an 'internal-external hybrid of societal security', which began to be reflected in official circles more than a decade ago.<sup>20</sup> The challenges that confront the EU demonstrate the need for effectively embedded societal security instruments, and also highlight the formidable challenge of creating them. Working with external partners to address internal EU security problems remains a challenge, and developing a common approach to internal security is also difficult given the diversity in national, regional and local governance across the EU, and because the responsibilities and organizational structures of the different security services—such as the police, judicial and customs services, and the intelligence and civil protection agencies—also vary across member states.

<sup>17</sup> European Commission, Directorate-General for Information, Communication, Culture, Audiovisual, 'Public opinion in the European Union', Standard Eurobarometer Report no. 48, Brussels, Mar. 1998, p. 68.

<sup>18</sup> European Commission (note 15), p. 27.

<sup>19</sup> European Council, Conclusions, 25–26 June 2015, EUCO 22/15, Brussels, 26 June 2015.

<sup>20</sup> Sundelius, B., 'A brief on embedded societal security', eds P. Faber and V. Ratchev, *Information & Security: An International Journal* (Procon: Sofia, 2005), pp. 23–37.

Finally, to achieve an integrated approach, new kinds of partnership would be needed with private sector actors that have only recently begun to see themselves as part of the security discourse.<sup>21</sup>

### **Priorities for the EU internal security strategy**

The 2015 Renewed European Union Internal Security Strategy incorporated the recommendations put forward by the European Commission on 28 April 2015 in a communication on the European Agenda on Security. The three main priorities for the internal security strategy in the period 2015–20 are tackling terrorism and preventing radicalization, disrupting organized crime and fighting cybercrime.<sup>22</sup>

The main priorities display continuity with most of the elements of the previous internal security strategy, which grouped strategic objectives under five headings: disruption of international criminal networks; prevention of terrorism and addressing radicalization and recruitment; raising levels of security for citizens and businesses in cyberspace; strengthening security through border management; and increasing Europe's resilience to crises and disasters. Far from improving, however, the situation in most of these areas inside the EU has deteriorated in the past five years.

#### *Resilience against the impact of crises and natural or human-made disasters*

While the 2010 internal security strategy set out the challenges, principles and guidelines for dealing with natural and human-made disasters, the successor document contains only a single reference to this issue: the preamble underlines the need to strengthen protection of critical infrastructures and ensure resilience, and enhance operational preparedness and political coordination to react to, deal with and mitigate crises and natural or human-made disasters.

In the EU context, the concept of resilience has been borrowed from material science, where it refers to the capacity of a material to resume its original shape after being exposed to extreme conditions. In the field of security, resilience combines the inherent strength of an entity to resist stresses and shocks with the capacity to bounce back rapidly from the impact. Increased resilience (and thus reduced vulnerability) can be achieved 'either by

<sup>21</sup> Burgess and Spence (note 5).

<sup>22</sup> European Commission, The European Agenda on Security, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, COM (2015) 185 final, 28 Apr. 2015; and Council of the European Union (note 1).

enhancing the entity's strength, or by reducing the intensity of the impact, or both'.<sup>23</sup>

The Lisbon Treaty established that the EU should undertake actions to support, coordinate or supplement the actions of member states in the area of civil protection. Many aspects of resilience are best dealt with by states or at the more local, sub-state level. However, planning for critical infrastructure protection with a focus on EU-wide elements was part of the preparation of the 2010 internal security strategy after the Lisbon Treaty entered into force. The EU promoted discussion at the expert level among member states to increase preparedness and think through coping and adaptation mechanisms at the national, regional and local levels. These efforts are continuing to enhance the resilience of specific trans-border infrastructure that has been designated critical to the EU as a whole. Four areas were designated for pilot projects to enhance resilience: the system for air traffic control over EU airspace, the Galileo geo-location satellite system, the electricity transmission grid and the gas transmission network.<sup>24</sup> Following a review in 2012, a reshaped policy on critical infrastructure protection is being managed by the Directorate-General for Migration and Home Affairs, supported by the Joint Research Centre, outside the framework of the internal security strategy.<sup>25</sup>

### *Cybersecurity*

The way in which the EU approaches the disruption of organized criminal networks is another issue that has been modified in line with the changing nature of criminal behaviour. The creation and expansion of the digital economy has provided organized criminals with what could be seen as a lower risk alternative to physical robbery. In 2015 citizen concern about organized crime remained a factor among those responding to *Eurobarometer* surveys, but concern about cybercrime now registers significantly among poll respondents too.<sup>26</sup>

Increasing levels of security for citizens and businesses in cyberspace is a priority of the internal security strategy, but it is one that must take account of other EU public policy initiatives. In February 2013, recognizing security in cyberspace as an increasingly important international issue, the Euro-

<sup>23</sup> European Commission, *The EU Approach to Resilience: Learning from Food Security Crises*, Communication from the Commission to the European Parliament and the Council, COM (2012) 586 final, 3 Oct. 2012, p. 4.

<sup>24</sup> European Commission, *Staff Working Document on a new approach to the European Programme for Critical Infrastructure Protection: Making European Critical Infrastructures more secure*, SWD (2013) 318 final, 28 Aug. 2013.

<sup>25</sup> European Commission, *Staff working document on the review of the European Programme for Critical Infrastructure Protection (EPCIP)*, SWD (2012) 190 final, Brussels 22 June 2012.

<sup>26</sup> On the nexus between access to information and communications technologies, cybersecurity and human development more generally see chapter 10 in this volume.



pean Commission and the HR/VP published a joint communication proposing an EU cybersecurity strategy.<sup>27</sup> It is an objective of the EU to become a world leader in the digital economy. Bringing e-commerce within the single market is expected to promote that goal by helping EU companies compete globally.<sup>28</sup> Enhancing cybersecurity is an important part of creating the conditions in which online services can develop.

An important outcome of the 2013 discussion on cybersecurity was a directive on attacks against information that requires all member states to criminalize the use of malicious software and strengthens the framework for information exchange on attacks.<sup>29</sup> Implementation of the cybercrime directive should have been completed by April 2015, but by that date only 10 of the 28 member states had confirmed its full incorporation into their national legislation, while two countries reported partial incorporation.<sup>30</sup> The 2015 internal security strategy underlines the need to ensure full implementation of the 2013 directive by member states.

Another of the package of measures put forward in 2013 was a draft directive concerning measures to ensure a high common level of network and information security across the EU. The directive was agreed at the political level in December 2015. Once it enters into force operators of essential services in the energy, transport, banking and health care sectors, as well as providers of key digital services such as search engines and cloud computing, will be obliged to take appropriate security measures and report suspicious and malicious incidents to the national authorities.<sup>31</sup>

### **The renewed European Union Internal Security Strategy, 2015–20**

The renewed internal security strategy rests on five main principles. First, that fighting crime and reducing radical extremist violence should not degrade respect for the fundamental rights of citizens. Second, that the public should be kept informed about how the strategy is being implemented, including through a specific role for national parliaments in EU member

<sup>27</sup> European Commission and High Representative of the EU for Foreign Affairs and Security Policy, 'Cybersecurity strategy of the European Union: An open, safe and secure cyberspace', Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, JOIN (2013) 1 final, Brussels, 7 Feb. 2013.

<sup>28</sup> Creating a connected digital single market is one of the highest political priorities for the current Commission. Juncker, J-C., *A New Start for Europe: My Agenda for Jobs, Growth, Fairness and Democratic Change*, Political guidelines for the next European Commission, 15 July 2014.

<sup>29</sup> Council of the European Union, Directive 2013/40/EU of the European Parliament and of the Council on attacks against information systems and replacing Council Framework Decision 2005/222/JHA, 12 Aug. 2013.

<sup>30</sup> European Commission, DG Migration and Home Affairs, 'Combating cybercrime: EU-wide rules against cyber attacks come into force', 4 Apr. 2015.

<sup>31</sup> European Commission 'Commission welcomes agreement to make EU online environment more secure', Press release IP/15/6270, Brussels, 8 Dec. 2015.



states and a wider Security Consultative Forum with broad cross-sectoral participation. Third, that the main priority should be the most efficient use of the many existing regulations, tools and instruments that the EU has already created, rather than the development of new ones. Fourth, that a more ‘joined-up’ inter-agency and a cross-sectoral approach to internal security is needed in order to use existing instruments more efficiently. Fifth, because threats are not confined to the borders of the EU, there is a need to bring the internal and external dimensions of security together as part of a uniform approach.<sup>32</sup>

The renewed internal security strategy is not intended to bring all parts of the wider security acquis into a single framework. As indicated above, some issues that were part of the 2010 strategy are now dealt with elsewhere in the EU system, and other public policy frameworks also address aspects of issues that remain within the internal security strategy.

To implement the European Agenda on Security, the European Commission work programme for 2016 identifies three main priority actions: updating the EU rules on terrorist offences and related penalties contained in the Framework decisions agreed in 2002 and 2008; introducing improved rules on firearms; and developing a proposal on combatting fraud and counterfeiting in non-cash means of payment.<sup>33</sup>

#### *Implementing framework decisions on terrorism*

The 2002 and 2008 framework decisions require member states to define terrorist offences in national criminal law and introduce minimum penalties.<sup>34</sup> A 2014 report on the way in which member states had implemented the framework decisions pinpointed two issues where additional clarification was needed: how to address indirect provocation or incitement to carry out terrorist acts, and how to address offences by ‘lone wolves’—individuals without an affiliation to any larger group who carry out acts of terrorism.<sup>35</sup> In December 2015 the European Commission put forward proposals on updating the framework decisions for consideration by member states.<sup>36</sup>

<sup>32</sup> Council of the European Union (note 1).

<sup>33</sup> European Commission, Work programme 2016: No time for business as usual, Annex to the Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, COM (2015) 610 final, 27 Oct. 2015, p. 5.

<sup>34</sup> Council of the European Union, Framework Decision of 13 June 2002 on combating terrorism, 2002/475/JHA, *Official Journal of the European Communities*, L164/3, 22 June 2002; and Council of the European Union, Framework Decision amending Framework Decision 2002/475/JHA on combating terrorism, 6561/08, Brussels, 15 Feb. 2008.

<sup>35</sup> European Commission, Report from the Commission to the European Parliament and the Council on the implementation of Council Framework Decision 2008/919/JHA of 28 November 2008 amending Framework Decision 2002/475/JHA on combating terrorism (SWD (2014) 270 final), COM (2014) 554 final, 5 Sep. 2014.

<sup>36</sup> European Commission, Proposal for a directive of the European Parliament and of the Council on combating terrorism and replacing Council Framework Decision 2002/475/JHA on combating

*Regulating firearms*

Trafficking in firearms has been described as a core business of organized crime, and the European Agenda on Security highlights the risk that organized criminals may now be able to source and trade more lethal firearms in Europe and in larger numbers.<sup>37</sup> The potential risks posed by the spillover effects of armed conflict were illustrated by the significant increase in the seizures of illegal weapons and live ammunition crossing the border from Ukraine into Poland.<sup>38</sup>

In November 2015 the European Commission put forward proposals aimed at tightening controls on the legal acquisition and possession of firearms and implementing common minimum standards on the deactivation of firearms.<sup>39</sup> In December 2015 the Commission issued a complementary Action Plan on the illicit trafficking of firearms and the use of explosives, which proposes measures to assist in the detection, investigation and seizure of firearms, explosives and explosives precursors to be used for criminal and terrorist purposes.<sup>40</sup>

**Disrupting organized crime and fighting cybercrime**

The UN Office for Drugs and Crime has documented the increasingly transnational nature of certain types of organized crime.<sup>41</sup> A transnational crime could be a crime committed in more than one state by the same group, a crime committed in one state but planned or controlled from another, or a crime committed in one state but that has substantial effects in other states.

The EU first introduced major legislation to prevent the use of the financial system for money laundering in its initial anti-money laundering directive in 1991, and has updated the legislation as the nature of the problem has evolved. In May 2015 the EU adopted a fourth anti-money laundering directive, partly to ensure that recent recommendations by the Financial Action

terrorism, COM (2015) 625 final, 2 Dec. 2015.

<sup>37</sup> European Commission (note 22), p. 17.

<sup>38</sup> Porter, T., 'Poland: Weapon smuggling following Ukraine war arming organised crime and terrorists in western Europe', *International Business Times*, 25 Jan. 2016.

<sup>39</sup> European Commission, Remarks of Commissioner Elżbieta Bieńkowska at the press conference on the preparation of the 20 November Justice and Home Affairs Council and the firearms package, SPEECH/15/6126, 18 Nov. 2015.

<sup>40</sup> European Commission, Implementing the European Agenda on Security: EU action plan against illicit trafficking in and use of firearms and explosives, Communication from the Commission to the European Parliament and the Council, COM (2015) 624 final, 2 Dec. 2015.

<sup>41</sup> The UN Convention against Transnational Organized Crime defines an organized criminal group as a group of three or more persons that was not randomly formed, that exists over a period of time, and that acts in concert with the aim of committing at least one crime punishable by at least four years incarceration. United Nations Convention against Transnational Organized Crime, UN General Assembly resolution 55/25, 15 Nov. 2000.

Task Force were incorporated into EU legislation, but also to address some newly identified risks.<sup>42</sup>

One of the most important developments has been the growth in e-commerce, and the associated use of digital banking and online payment systems. Digital banking is growing rapidly and banks that do not become ‘digitally proficient’ are considered likely to fail as their customers move to competitors that offer more up-to-date banking services.<sup>43</sup>

The original legislation focused on the criminal proceeds from drug trafficking,<sup>44</sup> However, over time, the legislation has been amended to reduce the risk that the financial system will be exploited to finance other types of crime, such as corruption, fraud, terrorism and the proliferation of weapons of mass destruction. Moreover, while the legislation was originally applied in the traditional banking sector, its coverage has progressively been expanded to bring other actors within its scope.

### *EU directives on anti-money laundering*

Generally speaking, private sector financial institutions must apply anti-money laundering and counterterrorism rules. The directives that updated the EU legislation on anti-money laundering before 2015 banned anonymous bank accounts, set out rules for customer identification in financial transactions and payments, defined verification requirements for payments and required financial institutions to make a risk assessment before issuing credit or making a payment.

The 2015 Directive expands the scope of application of existing rules to include providers of gambling services, and risk assessments of ‘virtual currencies’, such as Bitcoin, as well as digital payment instruments, such as mobile phone banking.<sup>45</sup> The directive also clarified that there should not be

<sup>42</sup> Council of the European Union, Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC, *Official Journal of the European Union*, L 141, 5 June 2015.

<sup>43</sup> Broeders, H. and Khanna, S., ‘Strategic choices for banks in the digital age’, McKinsey & Company, Jan. 2015.

<sup>44</sup> Organized crime, and in particular drug-related crime, was a consistent focus of public concern throughout the 1990s. A steady increase over time meant that by 2000, one in five citizens who provided survey responses reported being personally affected by drug-related crime. European Commission, Directorate General for Justice and Home Affairs, Drugs Coordination Unit, *Drugs and Security: Public Opinion Regarding Security and Victimization in the EU*, Sep. 2002.

<sup>45</sup> In 2013 the case of the Silk Road website, which was an online marketplace for drugs and other illegal goods, and the collapse of the MtGox bitcoin exchange highlighted the potential risks posed by virtual currencies. When the FBI closed the Silk Road website, it seized more than \$33.6 million worth of bitcoins, while the MtGox exchange collapsed after losing over \$400 million of bitcoins belonging to its customers following a breach of security. Kien-Meng Ly, M., ‘Coining bitcoin’s “legal bits”’: examining the regulatory framework for bitcoin and virtual currencies’, *Harvard Journal of Law & Technology*, vol. 27, no. 2 (Spring 2014).

any differentiation in the treatment of politically exposed persons who hold or have held prominent positions domestically and those who hold or have held such functions abroad. Therefore, financial institutions are required to exercise vigilance regarding evidence of money laundering undertaken for political purposes, which is essentially an anti-corruption measure.

The 2005 (Third) Anti-Money Laundering Directive required EU member states to establish national Financial Intelligence Units (FIUs), which play a central role in identifying and investigating suspicious money transfers.<sup>46</sup> Once they have established a risk assessment procedure, and applied it as part of customer due diligence, a financial institution is obliged to file a suspicious activity report (SAR) with its national FIU if it identifies financial transactions that pass a certain risk threshold.

Over time, SARs filed with national FIUs can build a valuable set of data for law enforcement. In the UK, for example, cross-referencing a sample of SARs with other information suggested that more than 30 per cent of SARs name individuals known to the police for other reasons, while around 40 per cent were linked in other ways, such as through common addresses. Financial intelligence can add to the overall criminal intelligence picture and has been credited with a specific role in counterterrorism. In 2006, after the police arrested a number of suspects in connection with an alleged plot to blow up aircraft leaving the UK, the Treasury was able to freeze the assets of 19 individuals before they could be moved.<sup>47</sup>

Developing and applying the risk-based approach required by anti-money laundering directives was a challenge for financial institutions when transactions were recorded on paper. While electronic screening is quick enough that it does not damage regular business, screening paper records caused serious disruption to payments and transfers. Advances in technology allow electronic transactions to pass through a series of databases that screen for known 'red flags' and block suspicious transactions for further scrutiny. However, electronic screening is only possible if there are agreed risk indicators, and if the right information is captured in databases. The person who has signature authority or legal title to the funds in an account may not be the person who ultimately controls how the money is used. Anti-money laundering and counterterrorist legislation is concerned with the ultimate level of control, rather than proxies or intermediaries.

One key piece of information that financial institutions have lacked is knowledge of beneficial ownership, which makes it difficult for screening to detect the use of so-called front companies. The 2015 Directive requires

<sup>46</sup> Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing, *Official Journal of the European Union*, L309/15, 25 Nov. 2015.

<sup>47</sup> British Treasury, Home Office, Serious Organized Crime Agency, and Foreign and Commonwealth Office, *The Financial Challenge to Crime and Terrorism* (Stationery Office: London, Feb. 2007).

member states to establish a central register of beneficial ownership information that will be accessible to the competent authorities, financial intelligence units and, within the framework of the conduct of customer due diligence, private sector financial institutions. This information should make it more likely that screening processes will identify the true beneficiaries of a payment or financial transfer as part of a risk assessment.

Over time, EU legislation has promoted the traceability of finance to help with risk assessment and subsequent investigations of money laundering or terrorist financing. EU legislation establishes minimum standards for information that must accompany a payment or transfer, rules on the collection and storage of information, and the conditions on which it must be supplied to others. In May 2015 the EU enacted a new regulation on information accompanying transfers of funds.<sup>48</sup>

In 2007 the EU decided that each member state should create a national focal point to facilitate the EU-wide tracing of assets derived from crime.<sup>49</sup> Once the 2015 Directive has been transposed into national law, FIUs and national Asset Recovery Offices should be able to promote a common approach to the confiscation of assets. The national authorities of EU member states should recognize the asset freezing and confiscation orders issued in other member states, including in cases where there has not been a criminal conviction.

#### *Transatlantic cooperation*

Since August 2010 the EU and the USA have had an agreement on the processing and transfer of financial messaging data from the EU to the USA to support the Terrorist Finance Tracking Program (TFTP).<sup>50</sup> The TFTP is a national programme administered by the US Treasury to track financial flows associated with terrorist groups. One important source of information for the TFTP is the Society for Worldwide Interbank Financial Telecommunication (SWIFT), a worldwide messaging system used to transmit financial transaction information.

While SWIFT is a private company registered in Belgium, until 2009 it stored data on intra-EU financial transfers on computer servers in the USA, making the data accessible to US government agencies in possession of a subpoena issued under US law. While data managed at SWIFT's US Operating Centre is still under US jurisdiction, as part of a reconfigu-

<sup>48</sup> Regulation (EU) 2015/847 of the European Parliament and of the Council of 20 May 2015 on information accompanying transfers of funds and repealing Regulation (EC) 1781/2006, *Journal of the European Union*, L141, 5 June 2015.

<sup>49</sup> Council Decision 2007/845/JHA of 6 Dec. 2007 concerning cooperation between Asset Recovery Offices of the Member States in the field of tracing and identification of proceeds from, or other property related to, crime, *Official Journal of the European Union*, L332, 18 Dec. 2007.

<sup>50</sup> On the Terrorist Finance Tracking Programme see <<https://www.swift.com/about-us/legal/compliance/tftp>>.

ration of its information and communications architecture, the company data on intra-EU transfers was moved to servers in the EU in 2009. Under an agreement between the EU and the USA, the US Government can make targeted searches of a subset of European data provided by SWIFT.<sup>51</sup>

In 2015 France proposed a European system to use SWIFT's international bank transfer database during the discussion on the renewed internal security strategy. The proposal was not adopted but French authorities continue to seek its inclusion in future decisions.<sup>52</sup>

## Conclusions

Although the EU has established itself as an actor in the field of internal security, describing and categorizing the security acquis in more specific terms is extremely difficult. At the working level within EU institutions there is an ambition to promote a more 'joined-up', inter-agency and cross-sectoral approach to security. However, in 2015 the EU continued to take actions related to internal security in many different public policy fields, not only in the framework of its internal security strategy.

<sup>51</sup> Agreement between the European Union and the United States of America on the processing and transfer of financial messaging data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program, *Official Journal of the European Union*, L195, 27 July 2010.

<sup>52</sup> Ministry of Finance and Public Accounts, French Republic, Countering terrorist financing, Press kit, Nov. 2015.