# Combating terrorist financing with artificial intelligence systems

Javier Valls-Prieto

## Introduction

Terrorism is a phenomenon that changes very quickly with time. One of the key factors to survey and evaluate its success is its flexibility and the ease with which it mutates into new forms that adapt its actions depending on their goals and their facility to get funding. International terrorism uses international corporations' structure and management methods adapted to new technologies to produce a new form of decentralized terrorism that is complicated to fight with only the classical tools of legal enforcement agencie, as at present.

One of the first problems to face is the definition of terrorism, which it is not easy although there are attempts to do so. One of the difficulties is that terrorism changes depending on its political goals, the state where its activities are carried out and the way it is funded.

The European norms have made a considerable effort to define it, but because of the ability of terrorist groups to adapt to new situations, to have a full definition of this concept is complicated. For this reason we need to look for non-normative definitions (economic, political, criminologist or sociologic ones).

The regulation of money laundering and terrorist financing is different and a good system of money tracking and information sharing has been introduced, hindering the possibilities of financing criminal activities. Although money laundering and terrorist actions have different aims, one being economic and the other to have political impact, the modus operandi is quite similar. In the end the economic benefit of the operation is not personal profit but for the final success of the terrorist attack. The duties implemented by the update of the European norm, Council Framework Decision 2002/475/JHA of 13 June 2002 on combating terrorism, on the transfer of information between the private sector, in particular, the financial and banking system, and the law enforcement agencies is a big step in the fight against terrorism. As we will see later, terrorist organizations need large sums of money to operate, not only for the attack, but for the basic infrastructure. However, as with all criminal activities, terrorist groups change their financial methods to avoid establishing institutions to move the money by using new practices based on new technologies.

The new strategy of information-sharing between institutions and the free movement of capital throughout the world creates a new need for states to obtain the economic evidence to fight terrorism. The European investigation order has provided a new criminal prosecuting cooperation system for requesting evidence from other member states based on the trust between them. For our study, the financial and economic information exchange is a key factor in the fight against terrorism.

But this legal change has produced an evolution in the terrorist groups. Islamic terrorism has developed methods similar to international corporations in its use of international financing systems and the use of new technologies that have helped in the proselytism of terrorism and terrorist financing. But this applies not only to Islamic terrorism but also to far right terrorism, as shown in the Christchurch attack which has developed similar tactics with new technologies for proselytism, financing and obtaining material supplies to perpetrate their attacks.

This changing of the place of action to Internet facilitates terrorist activities due to its anonymity and lack of guardians. That is why the development of artificial intelligence to fight terrorism enables legal enforcement agencies to develop new techniques in two important areas: surveillance and money-tracking. But it is not free from other risks. This massive surveillance and tracking of financial transactions can be dangerous for human rights in a democratic society. One of the challenges is the international legitimation system of the use of this computer technology by intelligence service and law enforcement agencies. The balance between citizen's freedom and security is again on the table when we deal with complicated criminality such as terrorism. That is the aim of this work.

**Definition of terrorism**

For the propose of this paper we define terrorism as "acts of violence that target civilians in the pursuit of political or ideological aims"[1] although the international legal definition, set out by the General Assembly in its resolution 49/60, considers terrorism as criminal acts intended or calculated to provoke a state of terror in the general public, a group of persons or particular persons for political purposes[2]. After the terrorist attack of 11 September 2001, the Security Council gave a new definition that referred to criminal acts, including against civilians, committed with the intent to cause death or serious bodily injury, or the taking of hostages, with the purpose of provoking a state of terror in the general public or in a group of persons or particular persons, to intimidate a population or compel a Government or an international organization to do or to abstain from doing any act[3]. The most current definition is provided by NATO and it defines terrorism as the unlawful use or threatened use of force or violence, instilling fear and terror, against individuals or property in an attempt to coerce or intimidate governments or societies, or to gain control over a population, to achieve political, religious or ideological objectives[4].

At the regional level the European Union has defined terrorism setting out a list of crimes that have the aim of causing serious damage to a country or an international organization by intimidating the population or unduly compelling a Government or international organization to perform or abstain from performing any act, or seriously destabilizing or destroying the fundamental political, constitutional, economic or social structures of a country or an international organization. The list of crimes are: attacks upon a person's life which may cause death; attacks upon the physical integrity of a person; kidnapping or hostage taking; causing extensive destruction to a Government or public facility, a transport system, an infrastructure facility, including an information system, a fixed platform located on the continental shelf, a public place or private property likely to endanger human life or result in major economic loss; seizure of aircraft, ships or other means of public or goods transport; manufacture, possession, acquisition, transport, supply or use of weapons, explosives or of nuclear, biological or chemical weapons, as well as research into, and development of, biological and chemical weapons; release of dangerous substances, or causing fires, floods or explosions the effect of which is to endanger human life; interfering with or disrupting the supply of water, power or any other fundamental natural resource the effect of which is to endanger human life; threatening to commit any of the acts listed above[5]. The Framework Decision follows with the definition of a

[1] OHCHR, "Human Rights, Terrorism and Counter-terrorism", United Nations, 2008, p. 5.
[2] General Assembly, "Measures to eliminate international terrorism", United Nations, 1995, p. 4.
[3] Security Council, Resolution 1566 (2004) p. 2.
[4] NATO, AAP-06. NATO Glossary of Terms and Definitions, 2018.
[5] Article 1 of the Council Framework Decision of 13 June 2002 on combating terrorism (2002/475/JHA)

terrorist group as: a structured group of more than two persons, established over a period of time and acting in concert to commit terrorist offences. 'Structured group' shall mean a group that is not randomly formed for the immediate commission of an offence and that does not need to have formally defined roles for its members, continuity of its membership or a developed structure. Within this definition, terrorist crime can be committed by: directing one of them and participating in one of them by suppling information or material, or funding its activities. These last activities as set out in Article 3 of the Framework Decision are aggravated theft, extortion and drawing up false documents, these three activities being linked to the crimes above. In 2008, the Framework Decision 2008/919/JHA of 28 November 2008, which amends the Framework Decision of 2002, adds three new forms of terrorism: public provocation to commit a terrorist offence, recruitment and training for terrorism. The last update of the European definition of terrorism reorganizes both the Framework in the new Directive of 2017 and adds new crimes: receiving training for terrorism, travelling for the purpose of terrorism and organizing or otherwise facilitating travelling for the purpose of terrorism. Finally, there is a development of the crimes related to terrorist financing, punishing providing or collecting funds, directly or indirectly, to commit or to contribute to the commission of a terrorist attack.

Outside the European Union there are other definitions of terrorism. In the 1980s the CIA defined terrorism as "Terrorism is the threat or use of violence for political purposes by individuals or groups, whether acting for or in opposition to established governmental authority, when such actions are intended to shock, stun or intimidate victims. Terrorism, has involved groups seeking to overthrow specific regimes, to rectify perceived national or group grievances, or to undermine international order as an end in itself"[6]. It is true that this definition does not involve all possibilities of terrorism and, moreover, some rebel groups could be included in the definition such as the French resistance in the Second World War. A more modern and narrower definition is provided by Fortna, Lotito and Rubin. They consider terrorism as the systematic use of intentionally indiscriminate violence against public civilian targets… to send a political massage to a wider audience[7].

Regardless of any particular definition, specifically because the phenomenon is so difficult to define because of its evolution and its subjectivity, Cronin gives some key point of terrorism. For her, terrorism always has a political nature; it tries to bring about political change with its actions to balance an injustice done. The use of violence has a non-state character, even when it has military support from states. The third key point is that terrorism deliberately targets the innocent. That is the difference from state violence that could kill the innocent as well, but not as a strategic target. Finally, terrorist groups are not under the enforcement of international laws or norm in their activities and that is to maximize the psychological effect of the attack[8].

For the purpose of this work the definition of cyberterrorism is also important. It can be defined as attacks against computer networks with a political, religious or ideological motivation. Most of the state infrastructure, such as water and energy supply, hospitals, financial markets, emergency services, air/shipping control and similar[9]. Over time, and similar to the classical

[6]Ruwantissa Abeyratne, 'Suppression of the financing of terrorism' (2011) J Trans Secur 4 54, 59.
[7]Virginia Page Fortna, Nicholas J. Lotito and Michael A. Rubin, 'Don't Bite the Hand that Feeds: Rebels Funding Sources and the Use of Terrorism in Civil Wars' (2018) *International Studies Quarterly* 62 782, 783
[8]Audrey Kurth Cronin, "Behind the curve: globalization and international terrorism", (2002-2003) *International Security* 27 3 30, 33
[9]Jonathan Clough, *Principles of Cybercrime* (Cambridge University Press 2012), 11.

definition of terrorism, cyberterrorism has evolved with different definitions that can be separated into two broad categories: when terrorists use technology to facilitate their objectives and when terrorists use computer network tools to harm or shut down national infrastructures[10]. The first definition involves encryption communication systems between the members of the organization or the use of DoS attacks against government websites or servers. In the second one will be added a threatened harm to persons, property or essential services. So the first is not linked with civilian victims, but the second one is closer to the classical concept that we are using and is, in my opinion, the right approach.

The idea of introducing this concept will be explained in greater detail later, but to start understanding terrorism in the twenty-first century we need to see that nowadays the modus operandi of terrorist groups is the use of computer networks to facilitate their activities or to target them. In the first set of tools we will focus on the virtual funding of terrorism.

In the European Union Terrorist Situations and Trends Report (TESAT)[11] of 2018 the Reporters speak of the current role of the new technologies. Internet plays an important role in the radicalization of some perpetrators. Online propaganda and networking via social media are still essential to terrorist attempts to reach out to EU audiences for recruitment, radicalization and fundraising, particular with Islamic terrorism. But, as the report highlights, not only does religious terrorism use this tool for its aims, so do right and left wing terrorists. The case of the right wing attack in Christchurch shows how the internet can be exploited to this end. The attack on two mosques in New Zealand was broadcast through livestreaming video and the gunman's manifesto went viral.

There are three important areas -proselytism, information and funding- in which internet plays an important role in terrorist acts. Encrypted social networks, such as Telegram, WhatsApp and Facebook are used to recruit new terrorists, make contact between different hubs and to deliver propaganda, making all these viral with very little effort[12]. Another possibility is to get bomb-making instructions from internet or file-sharing both from the surface web and from Darknet. The trend is to use fundraising campaigns by crowdfunding and by economic crime. Bitcoin payments gained popularity due to their key characteristics that include ease of access, anonymity, safe transactions, low cost and high speed for international transfers.

We are going to focus on this last point in this chapter. As we will see, one key factor in the fight against terrorism is how these groups get the resources to make their operations a reality. Such groups need to finance two activities: terrorist attacks (operational resources) and the infrastructure of the group (broad organizational requirements)[13]. Both are important for their activities, but the second is more expensive than the first. In the next section we will see how these activities are pursued by European Law.

**Financing terrorism**

---

[10]Ibid., 12.

[11] European Union Terrorism Situation and Trend Report 2018 (TESAT)https://www.europol.europa.eu/activities-services/main-reports/european-union-terrorism-situation-and-trend-report-2018-tesat-2018 accessed 9 November 2019

[12] European Union Internet Organized Crime Threat Assessment 2019 (IOCTA) p. 9. https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2019 accessed 9 November 2019

[13]Hamed Tofangsaz, "Rethinking terrorist financing; where does all this lead?" (2015) JMLC, 18, 1, 113-114.

The first international legal act against financing terrorism was the International Convention for Suppression of Financing of Terrorism of 1999 but it was not a success[14]. We had to wait until the terrorist attack of 9/11 to see a real attempt to regulate and fight terrorist finance. In 2001, in an Extraordinary Plenary Session, UNO created the FATS 8 Special Recommendations against Terrorist Financing. This was the start of signed resolutions that had been waited for from 1999, a process that ended with Security Council Resolution 1373, which includes eight Recommendations, one month later they were taken.

This extremely quick reaction was not only taken in UNO, but in the European Union as well. The European Council started a battery of actions in the extraordinary European Council meeting on 21 September 2001, setting out a list of terrorist organizations and a plan against terrorist funding[15]. As a result of this plan the Framework Decision 2002/475/JHA was adopted to tackle terrorism. This norm tries to give a general definition of terrorist groups based on what kind of crime it commits, as we have seen above, but it also focuses on liability of legal persons, taking into account victims of terrorism attacks and, what it is important for our work, two offences linked to funding terrorist activities: aggravated theft and extortion. These changes give an idea of the financial structure of terrorist activities, the need for money for the activities that not only come from illegal activities such as theft and extortion, but from legal resources, as we will see, and the necessity for legal persons to manage this money to pay for the needs of the group.

Parallel to this normative develop, the money laundering regulation of 2005 introduced the scope of terrorist financing, defined as the "provision or collection of funds, by any means, directly or indirectly, with the intention that they should be used or in the knowledge that they are to be used, in full or in part, in order to carry out any of the offences" established in the Framework Decision 2002/475/JHA. Basically, this regulation enforces a system of due diligence and tracking of money transfer information, allowing the authorities to follow the transactions of money, with the help of people, financing institutions, casinos and money transfers. This Framework Decision had an update in 2015 in the Directive (EU) 2015/849 particularly, adapting the amount of money and some institutions such as gambling services like casinos. During these twelve years money involved in games of chance have moved to other platforms such as online betting web sites. Thus these new gambling systems have to be included and taken as possible targets. The concept of terrorist financing has no changes. Something new is the risk assessment (Article 7 of the Directive (UE) 2015/849) that the states should implement in their money control systems, which will be important later in this work. The final version of the European normative on financing terrorism is the last update that deals with electronic transfer of money (virtual currencies, wallet providers and electronic money updates) and promotes the criminalization of terrorist financing.

As a summary of this regulation the exchange of data is the key factor to combat terrorist financing and the collaboration between institutions. All this information provides new ways of controlling and fighting against terrorism. The efforts made by the legislative institutions of the European Union to combat terrorist financing by new methods have been really strong in the last decade, but Europol, in its Terrorism Situation and Trend Report of 2018, states that the use

[14] Nicholas Ridley and Dean C. Alexander "Combating terrorist financing in the first decade of the twenty-first decade" (2012) JMLC 15, 1, 40.

[15] Miryam Rodríguez Izquierdo Serrano, 'El terrorismo en la evolución del espacio de libertad, seguridad y justicia' (2010) 36 RDCE 531, p. 541.

of virtual currencies remains very low[16]. On the other hand, Europol in its report on Internet Organized Crime Threat Assessment of 2019, highlights the convergence of cyber and terrorism, how terrorist groups adopt the new technologies for their strategy in online propaganda and recruitment operations, but the adoptions of these new technologies could also include cryptocurrencies[17] in their plan to use the new technologies with the idea of expanding and diversifying their methods to reach their goals more easily and safely.

**Economic evidence**

The new instrument for cooperation in criminal matters, implemented by the Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters, goes a step further in the fight against terrorist financing.

The European investigation order (EIO) is a great change from the original criminal judicial cooperation system, based on the Council Framework Decision 2003/577/JHA of 22 July 2003 on the execution in the European Union of orders freezing property or evidence and the Council Framework Decision 2008/978/JHA of 18 December 2008 on the European evidence warrant for the purpose of obtaining objects, documents and data for use in proceedings in criminal matters. The new legal instrument tries to speed up the process of requesting evidence in some crimes with an order that all involved member States will facilitate the evidence requested by one partner.

Of all the types of evidence included in this norm, transfer of suspects, hearing by teleconference or by telephone, gathering of evidence in real time, covert investigation, interception of communications and provisional measures, the one that we are interested in for this work is the request for bank or financial accounts and banking and financial information. Whereas under numbers 27, 28 and 29 an EIO may be issued in order to obtain evidence concerning the accounts, of whatever nature, held in any bank or any non-banking financial institution by a person subject to it, this possibility is to be understood broadly as comprising not only suspected or accused persons but also any other person in respect of whom such information is found necessary by the competent authorities in the course of criminal proceedings, according to Article 3 of the Directive 2005/60/EC on money laundering and financing terrorism. The details requested by an EIO should be understood as the name and address of the account holder, details of any powers of attorney held over the account and any other details and documents linked to the account.

**Reality**

From the legal point of view we have legal instruments for the fight against terrorist financing, but we can see in reality that some difficulties appear. After 9/11 the investigation focused on Islamic banks and financial systems, but the answer from these institutions were weak. Either they had no information or they did not want to collaborate.[18] Although there are some irregularities and some lack of control that enables illicit money to move through Islamic bank

[16]European Union Terrorism Situation and Trend Report 2018 (TESAT)https://www.europol.europa.eu/activities-services/main-reports/european-union-terrorism-situation-and-trend-report-2018-tesat-2018 accessed 2 January 2020

[17]European Union Internet Organized Crime Threat Assessment 2019 (IOCTA) p. 48. https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2019 accessed 2 January 2020.

[18] Nicholas Ridley and Dean C. Alexander (n 9), 49.

institutions, this action from USA and EU legal enforcement agencies was found to be an intrusion from Western countries[19]. This interest in classical banking and financial systems was based on how Al-Qaeda was financed by Osama Bin Laden through different accounts under fake names since he lived in Sudan[20]. But this first attempt to control terrorist financing just made a change of the financing system to an informal money exchange, such as Hawala in Islamic societies, Hundi in India o Fie chi'ien in China[21]. The second way to transfer money is by physical movement of funds, but this imposes a limit on the quantity of money that can be transferred and does not work for large sums of money. The third one is by trade. Trade allows the possibility of transferring valuables and goods through trade flows, giving terrorist groups access to materials and goods that they need for their operations[22].

Islamic terrorism is not the only one that needs funding. The empirical study of Fortna, Lotito and Rubin, focused on terrorist and rebels groups from different countries, found a terrorist group is more likely to be created when they have access to natural sources and external financing than the groups based on civilian support[23]. This is important because their financial strengths depend on the geographical situation of the terrorist group activities, basically drug trafficking[24], but also on other criminal activities. To give an idea on how popular drug trafficking was to financing terrorist groups we have these examples: Kosovo Liberation Army, Basque Homeland and Liberty or ETA in Spain, and the Islamic Movement of Uzbekistan, all well-known as drug traffickers. Groups like FARC obtained weapons and communications technology by trafficking cocaine. In Australia an investigation found money laundering operations in that country linked to Hezbollah. Producer countries are often the least profitable part of the process; the lion's share of earnings is garnered by those who refine and market the drugs[25].

The second key point is the external financing that was a major factor in some cases of national terrorism, particularly in those regions with geostrategic interests such as Central America and near East. But not all national terrorism has this influx of money from external actors. The reality of new forms of terrorism such as international Islamic terrorism and far right actions show that the external actor has a considerable influence by encouraging their attacks and by financing them as we have seen before.

The fact is terrorist groups need money for operational activities, basically, for the terrorist attack, which include the cost of the attack, the salary of the terrorist, communications, training, travel and logistics. But large groups also need broad organizational requirements to create, maintain and develop the infrastructure[26]. In this second case the need for money is considerable; while a terrorist attack by a lone wolf is not very expensive, to have an

[19] Ibid.
[20]Hamed Tofangsaz, 'Rethinking terrorist financing; where does all this lead?' (2015) JMLC 18 1 112, 117.
[21] Steve Kiser, *Financing Terror. An Analysis and Simulation for Affecting Al Qaeda's Financial Infrastructure* (Rand Corporation 2005), 90.
[22]Hamed Tofangsaz (n 15), 117-118.
[23]Virginia Page Fortna, Nicholas J. Lotito and Michael A. Rubin, (n 7), 789.
[24]Colin P.Clarke, 'Drugs & Thugs: Funding Terrorism through Narcotics Trafficking.' (2016) Journal of Strategic Security 9 3 15, 9.
[25]Ibid, 3.
[26]Hamed Tofangsaz (n 15), 113-114.

infrastructure needing many people and resources is. In some cases, the members pay with their own money, particularly, when the terrorist acts as a lone wolf[27].

We have already seen how geographical factors can facilitate the terrorist group, but it is also true that the financing method can change the way that terrorist attacks are produced. Thus, there are illegal and legal sources of funding. The first are motivated by the decrease of state-sponsored terrorism, to some extent because of the development of legal controls on money transfers, as we have seen. This factor has created new ways of financing through criminal acts such as drug trafficking, extortion, economic crimes, organized crime and kidnap-for-ransom[28]. The latest development is cybercrime since organized crime is changing the modus operandi on the Internet as well[29]. The use of new ways of financing such as cryptocurrency transactions is a reality[30]. As Vittori has highlighted, globalization of international monetary systems has opened up new ways of financing on a global scale anytime and anywhere[31].

Legal forms of financing have multiple faces. There are donations and charities, non-governmental organization can help terrorist activities and investment in legitimate business[32] can be sources from legal money that ends in terrorist groups' hands.

This point is important because, depending on the financial source, the type of terrorism can change. Thus, we can classify terrorist groups into six different kinds depending on how they get their money supplies. The first one is a state-sponsored group, which receives money from a State that has the same political objectives[33]. A second possibility is a shell States, an area where the terrorist group exercises its power inside a National state. In this case funding comes from natural resources or criminal acts inside its territory. This is the case of terrorist group linked to narcotrafficking[34]. The third group is a franchise category. It is an evolution from the first one. The resources come from a state, but part also from individual sponsors. These two sources allow the terrorist group to make a survey in case one of the sources ends its funding[35]. A more sophisticated way is the bundled support, in which the number of supporters is bigger than in the franchise category, the majority being small private donors with a national or ethnicity link to the group[36]. The problem is to find a way where all these small contributions can reach the terrorist group and here is where the legislation about money transfers is strong, but technology has left a door open via cryptocurrencies.

In this increase of structural and financing dimensions of a terrorist group, the latest evolution is the transnational corporation model[37]. This is the structure that Al Qaeda used by implanting a transnational corporation business model into a terrorist group by using technology, sources, and methods. Once this model was destroyed by the international legislation the next

[27] Inmaculada Marrero Rocha, 'Nuevas dinámicas en las relaciones entre crimen organizado y grupos terroristas' (2017) REDI 69 2 145, 154
[28] Ibid, 115.
[29] IOCTA (n 12) 48.
[30] Angela S.M. Irwin and George Milad, 'The use of cryptocurrencies in funding violent jihad' (2016) JMLC 19 4 407, 410.
[31] Jodi Vittory, *Terrorist Financing and Resourcing* (Palgrade Macmillan 2011) 25
[32]Hamed Tofangsaz (n 15) 115-116.
[33] Jodi Vittory (n 25) 8.
[34]Hamed Tofangsaz (n 15) 118.
[35] Jodi Vittory (n 25) 8.
[36]HamedTofangsaz (n 15) 118.
[37]Audrey KurthCronin(n 8)

standardization has been the lone wolf[38]. This is low cost terrorism where the need for supplies of money and resources are very modest.

The international regulation on money laundry and terrorist financing can be evaluated as a good legal instrument. It was a step forward and, working with other regulations that we have seen, gives instruments to fight terrorism. It is because of this success that terrorist groups and organized crime are evolving to cybercrime ways of funding.

Technology-adapted terrorism makes administrative tasks in transnational organizations easy and with enhanced efficiency, as well as coordination of operations, recruitment of potential members, and communication with adherents, attraction of sympathizers[39] and transfer of money. The reason for that change is easily explained by cybercrime.

There are six key factors for cybercrime. The first one is Scale. That means Internet allows user to reach many people cheaply and easily. This make it possible to get more people to sponsor terrorism attacks, but at the same time to communicate with many potential supporters. The second one is Accessibility, the technology has developed so fast and so cheaply that nearly everyone has access to a device connected to Internet at any time or anywhere, not only with a computer but with a smartphone. The third one, Anonymity, is one of the most important for terrorist goals. It is an advantage for the terrorist and for sponsors to make the transfer of money nearly untraceable. This anonymity can be obtained by proxy servers, fake emails or IP addresses or anonymous emailers. The fourth, Encryption technologies are easy to get and use so that money transmissions are untraceable. The network enables money to go through different legislations so that it is easy for funding terrorism to pass through an offshore country. Digital technologies have the advantage of easy portability and transferability. One of the possibilities is to store enormous amounts of data in a small space and replicate that data with no appreciable diminution of quality. But not only that, digitalization has the ability to change tangible things into intangible things, in our case the movement of money that is not physical but electronic. The fifth key is Global reach. As we shall see later the global reach of the networks has facilitated the latest update of a terrorist group to an international terrorist organization. Finally, the sixth point, an important one, is the Absence of capable guardians t0 enable these new ways of financing to be detected and prosecuted. Electronic data need complicated forensic techniques to ensure they can be used as evidence in a trial. But surveillance is very complicated as well. The fact that the infrastructure belongs to the private sector and the communication is routered in different jurisdictions makes the need for interchange of information a big challenge[40].

**The use of artificial intelligent to combat terrorism**

As Internet is the space where many terrorist activities are committed and the need to find electronic evidence and intelligence information to combat it, the only way to fight it properly is with new technologies. Here is where artificial intelligent gives important tools to scrutinize the network to intercept communication, find evidence, detect recruitment of members, make propaganda and exchange of money for funding.

[38]Hamed Tofangsaz (n 15) 118.
[39] Audrey Kurth Cronin (n 31) 47
[40]Jonathan Clough (n 9), 5-9.

To use artificial intelligence, we must first understand that, in this case, it will be a process of acquisition and use of information about events, trends and relationships in a particular environment to support decision making and planning[41]. To use it against terrorism it is necessary to identify indicators and facilitators of present and future development of these criminal activities. There are signals that anticipate the possible development of the scenarios and these signals should be related with some statistical indicator of some events. With the statistical models the artificial intelligent "learns" where to look and what kind of evidence is relevant or not[42].

Artificial intelligence applied to combat crime can be formulated in five steps. The first is data acquisition. This task is done by trawling the Internet, Deepweb and Darknet looking for specific information about terrorism chats, webs and forums where information for activities can be found as well as open data sources that could be linked to the case. For that task it is necessary to process natural language in order to extract information that can be processed by a machine.

Once the data are stored, an intelligent extraction of the right information must be made and it must be enriched. Thus, if we find a terrorist chat with conversation it is possible to understand the messages now if the source is good enough. With the additional information from users, geographical connections, time where the chat users connect we can have data that with an enrichment process from open information can make connections with other online activities and give full information from the subjects, the particular object, money accounts and transfers, etc. If we have information of automatics guns sold in the dark markets, we can enrich this information with the kind of bullets they will need, how they can be developed to a more powerful machine, what other guns should be used and with registers of gun shops if they have potentials clients.

This kind of extra investigation work is crucial and takes us to the next step. Discovery of information that is on Internet but is not connected to the particular case is one of the possibilities that this kind of tool provides. Thus, the nicknames of terrorist chats' members can be tracked on the web to discover where they have other activities. This discovery phase allows legal enforcement agencies to find information that in other situations will be hidden and lets us break one of the key points, as we have seen above, of the cybercrime activity, anonymization. Of course, this is not the end of the process. In this phase the work is concentrated; particular data that are separate from the normal ones can be found with no statistical significance but that may be interesting in the investigation[43].

An assessment phase should be opened to analyze the information given by the artificial intelligence tool and should be carried out by an analyst with the intention of avoiding false information. To facilitate this work, artificial intelligence presents this knowledge in a convenient way, normally, by a customized human machine interface.

The last action is forecasting. Intelligence tools give the possibility to forecast future terrorist acts by analyzing information and previous cases. This last phase has a strong power to prevent future actions in two ways: firstly, by looking at past situation to avoid new cases and secondly,

---

[41]Chun Wei Choo,'The art of scanning the environment'(1999) *Bulletin of the American Society for Information Science and Technology*, 25 3 21, 21.

[42] Javier Valls-Prieto and Juan Gómez-Romero, 'Use of Big Data and the Prediction of Organized Crime' in Joan Balcells Padullés, et al. (eds.), Building a European Digital Space (Huygens 2016), 369.

[43]Ibid., 370-371.

by creating the need to create new ways to commit terrorist attacks that lowers the possibilities of terrorist attacks.

**Cryptocurrencies**

Cryptocurrencies allow money to be transferred over the Internet with little control. One of the problems we have observed in the different finance systems of terrorism is that small donations by private individuals and cash transfers, such as the Hawala, create problems to restrict the money to international terrorist groups and to finance terrorist cells outside the geographical control of the groups. Hawala, for example, works through trusted traders because the money does not really change hands. It is a system where the person in charge gives the money from his/her resources and has a credit with the other trader in the country where the transfer order comes from. This means you need a person whom you can trust and who will not inform authorities about the transaction. Cryptocurrencies let the terrorist organizations manage funds in the world with more opacity and fewer risks, giving terrorist groups more flexibility and operability. To operate with cryptocurrencies a person has first to open a wallet, that is, the holder of the wallet authorizes a third party to receive and store cryptocurrencies on their behalf. The identity of the holder remains anonymous. The transfer of money goes in packets, secured by blockchain technology managed by miners that can be tracked from point to point. Finally, the money ends in another wallet. All this process secures anonymity but the process can be traced and followed by the currency's address[44]. The weak point is when the subject wants to change the cryptocurrency into real money, needing to give a bank account or a credit card number to receive the money because this information about the real money is under the control of the bank and the financial system and is under the scope of the European regulation explained above. To avoid this control the terrorist can use a cryptocurrency ATM that automatically changes cryptocurrencies to cash without any record. In reverse, it also changes cash into cryptocurrencies[45]. Fortunately, these transactions work only for limited amounts and not with large sums of money or cryptocurrencies.

To avoid this there are three ways to sell crypto currencies: direct-trade with another individual with an intermediary facilitating the connection in an off-shore country; online exchange, where the trade is with the exchange rather than an individual; and in a trading marketplace where the sale of products is direct, shipping the purchase to the customer without any intermediary. This third form is the most popular as the terrorists can buy many of their supplies in the Darkmarket to commit a terrorist attack without risks.

These three situations are good examples of where the classical fight against terrorism fails because of the amount of information and the lack of links between this information. Artificial intelligence offer tools to manage all this information and the connections between them in a short time. This time could be crucial to avoid a terrorist attack. As we have said before the automatic decision making should be controlled by humans, but it is true that the help given by these machines could be crucial in terrorist fighting.

**How to combat terrorism and its funding**

[44]Angela S.M. Irwin and George Millad (n 24) 412.
[45] Ibid, 414.

Being aware of the difficulties to combat a phenomenon that is changing and transforming itself very quickly, the experts have provided different solutions to fight terrorism. From an American point of view Ridley and Alexander affirm that more manpower, financial resources, and attention are needed, but also greater collaboration, information-sharing and fewer turf wars. The government needs to focus on the fact that terrorist groups also need to live in the real world to fund their activities. This means that much financial information has to be exchanged between law enforcement and financial institutions as well as collaboration with the private sector[46]. In a similar approach Abeyratne asks for the adoption of practical measures to discourage the commission of terrorist acts. They are a) the improvement of the intelligence system which will inform the state concerned about the risk of a terrorist attack, b) establishment of counter-terrorism mechanisms focusing on collection of arms, ammunition and weaponry, c) the adoption of such practical measures of self-help and attack in case of a terrorist attack, d) the existence of the necessary machinery to retain the confidence and sympathy of the public at all times, and e) persuasion to convince the public that terrorism of any kind is evil and should not be condoned[47].

From an economic point of view financing terrorism can be fought by taxing some products needed for this financing, e.g. instruments needed for narcotics production and export[48]. Moreover, from an economic perspective Hausken proposes terrorism can be avoided by the increase of terrorists' costs and decrease in government costs. The cost of terrorism could be increased through law, surveillance, detection, prosecution, etc., making criminal efforts less lucrative, preventing large efficient organizations from financing it and by encouraging benefactors not to fund terrorists engaged in crime. To increase the cost of terrorism Governments can make crime costly, encourage benefactors to punish crime, decrease terrorist resources, and confiscate, freeze, and prevent the accumulation of resources, block benefactors' funding of terrorism, block funding, criminalize terrorist funding, inhibit crime production and prevent effective crime production[49].

It is true that terrorism is a multifactorial problem and there is not only one solution, but what is also true is that the classical solutions will not work anymore and we need new proposals to solve the problem. In fact, continuing with old attitudes could be dangerous[50].

One example of the use of new techniques to fight terrorism funding is the MIDAS project developed by IBM. This machine has capabilities to extract information from fines adopted by the control bodies in the USA in money laundering cases and terrorist financing[51]. This information can be reused with artificial intelligence tools to improve tracking of companies involved and provide a methodology about how to find financial information.

As we have seen before, one of the key factors of terrorist fighting is surveillance and for this to be effective the balance of cost between government actions and terrorist attacks should be lower for the government institutions than for terrorists. This means effective surveillance has

[46]Nicholas Ridley and Dean C. Alexander (n 9) 52.
[47]Ruwantissa Abeyratne (n 6), 67.
[48] Peter Berck and Jonathan Lipow, 'Trade, tariffs and terrorism' (2012) Applied Economics Letters 19 1847, 1849.
[49]Kjell-Hausken, 'Government Protection against Terrorists Funded by Benefactor and Crime: An Economical Model' (2017) 11 5 1, 24
[50]Audrey Kurth Cronin (n 31) 31
[51]Vassilis Plachouras and Jochen L. Leidner, 'Information Extraction of Regulatory Enforcement Actions: From Anti-Money Laundering Compliance to Countering Terrorism Finance' (2015) ASONAM 950, 951.

to be as cheap as possible. Here is where the use of artificial intelligence has its place. Surveillance of the Internet is admittedly complicated and human resources expensive. If we can develop strong surveillance systems the odds to win the fight against terrorism without the latest technology is really low. Particularly, because as we have seen before, Internet allows anonymity and escape from police control and the only way to fight in this space is with these kinds of tools.

**Problems related to the use of artificial intelligence fighting terrorism**

**A**rtificial intelligence is not free from doubts. There are both positive and negative impacts in its use to fight terrorist funding,. On the positive side, as we have seen, is the possibility of tracking money transfers and cryptocurrencies through financial systems, and the possibility of surveillance of terrorist information on the internet. All this will have a positive impact on people's safety. But we must think of the rights of privacy, the presumption of innocence and freedom from discrimination. As Raso et al. have demonstrated, the access of artificial intelligence in criminal justice has a negative impact on the right of privacy, of being considered innocent and the public hearing[52]. At the same time its use has a positive impact in safety rights, as we have seen before, because dealing with such a complicated mass of information and finding evidence on the Internet can be really difficult for humans. In the middle term, it could have an impact on rights such as nondiscrimination; the machine may have a bias but at the same time it can avoid human bias, thus it can be positive or negative, and this may happen with the right of freedom from arbitrary arrest, detention and exile[53].

As a new technology, and one that has not been tried out over a long period of time, we have to take care to avoid risks linked to its use. That is the fundamental idea of the ethics guidelines for trustworthy artificial intelligence[54]. These guidelines have seven main points for the use of artificial intelligence, in general, but as well as for it use in security matters. The first one is human agency and oversight. With that the idea is that artificial intelligence should help and empower humans but not replace them. The systems have to be technically robust and safe, that means the system needs to be resilient and secure, ensure a fall back plan in case something goes wrong. It should respect privacy and has to work with data of integrity and of good quality. The system should be built thinking of diversity and nondiscrimination. They have to be sustainable and environmentally friendly, thinking of future generations. Finally, there have to be mechanisms to ensure responsibility and accountability of the outcomes.

To deal with this configuration it is necessary to make a human rights assessment. This is important because the possibility of bias against particular groups of population is all too easy. Virginia Eubanks describes a good example in the city of Los Angeles where poor people (the majority black) were targeted as dangerous when artificial intelligence used social services data e.g. post code, general income of the neighborhood, education level or psychological illness in

[52] Filippo Raso, Hannah Hilligoss, Vivekkrishnamurthy, Cristopher Baviz and Levin Kim, 'Artificial Intelligence & Human Rights: Opportunities and Risks' (2018) Berkman Klein Center for Internet & Society Research Publication <http://nrs.harvard.edu/urn-3:HUL.InstRepos:38021439> accessed 9 January 2020.
[53] Ibid.
[54] Ethics Guidelines for Trustworthy Artificial Intelligence, (2019) <https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai> accessed 9 January 2020.

Skid Row[55]. There are not too many works in the field of security. One possibility is to start with the baseline of the surveillance assessment done by Wright et al. In an attempt to legitimize surveillance by state institutions that creates an assessment by actors: state institutions, private sector, citizens, ONGs and society. First they put a list of generic questions that all sector workers should ask themselves before using these surveillance tools. It is a total of 15 questions that are as follows:

1. What is the purpose of the system?
2. Is it really necessary? Is it lawful? Is it proportionate to the envisaged purpose?
3. What less intrusive alternatives are available?
4. Who will develop, operate and authorize it?
5. Who will have access to the data collected by it?
6. How long will the collected data be stored? When will the data be deleted? What measures will be put in place to store or transmit the data securely?
7. To what extent will stakeholders, including the public, be consulted about it and its effects?
8. What external oversight is in place, including a regular, independent, third-party, publicly available audit?
9. How will system operators be trained so that they are sensitive to any harmful consequences?
10. Does the system enable individuals to be identified? If so, is that necessary? Does it provide individuals with a means to opt out?
11. Does the system process "sensitive" personal data? If so, is that necessary?
12. Whose interests does the system serve?
13. Does the system create identifiable harms, e.g., social, environmental, economic or human rights-related harms?
14. If surveillance cannot be avoided or its effects mitigated, how can society be empowered to build capacities to deal with its consequences?
15. Have the possible negative impacts and risks of the implementation or continuation of the particular surveillance system been considered? How do these relate to the benefits?[56];

These questions have to be answered, not with a simple yes or no; the aim is to think how technological surveillance will have an impact on the society. This works for legal enforcement agencies, intelligence services but also for technology developers in the private sector.

Extra questions have to be answered by policy-makers and regulators:

1. Is the surveillance necessary, legitimate, transparent and proportionate? How are these judgments made? Are there any less intrusive alternatives?

[55]Virginia Eubanks, Automating inequality. How high-tech tools profile, police, and punish the poor (St. Martin's Press 2018), 84.

[56] David Wright, Rowena Rodrigues, Charles Raab, Richard Jones, Iván Székely, Kirstie Ball, Rocco Bellanova and Stine Bergersen, 'Questioning surveillance' (2015) Computer Law & Security Review 31 280, 283

2. How has the decision to use surveillance weighed up the costs, benefits and risks, including the consequences of surveillance for human rights, freedoms and democracy? Is the decision-making process publicly documented?
3. What deliberations have taken place concerning the necessity and proportionality of the intrusion into individuals' private lives by means of the surveillance measure or policy? Is the decision-making process publicly documented?
4. How have the views of different stakeholders, especially the public, been taken into account?
5. Have policy-makers identified potential harms e who is harmed by and who benefits from surveillance, what are potential knock-on effects, what are the social consequences? After trying to identify all of the consequences, have policy-makers thought about what they can reasonably do to combat the harms?
6. What systems are in place for adequate supervision, review and oversight of surveillance practices?
7. Have the targets of surveillance (which may be the general public) been informed of the existence of the surveillance system and its general purpose? How can they find out more about the scope of the system? How can they seek personal redress for harm? How can they question, or fundamentally challenge the surveillance system?
8. How can the political and policy-making process best control the proliferation of surveillance?
9. If surveillance cannot be avoided, how can society be empowered to build capacities to deal with its consequences?
10. How are the effects of surveillance to be continuously assessed or monitored?
11. How can international regulatory co-operation and standardisation best meet the challenge of the global flow of personal information?
12. How can the political and policy-making process best control the proliferation of surveillance?[57]

These authors also propose six political and regulatory measures. Although it is a general approach to other technologies than artificial intelligence, many of them can be extended or adapted to this computing system. The first one is accountability and oversight that should be introduced through political processes. Accountability requires procedures and rules reporting publicly and engaging in possible challenges to the accounts given. The oversight should be done by independent agencies with public service in mind. Consent, in this investigation process, obviously cannot be given by individuals. In this case it has to be a societal agreement between state and society. The third point is to make stronger legal protection of privacy. The Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of persons is a good way of protecting and legitimating the use of artificial intelligence in financing terrorism investigations. Unfortunately, it has not had as much success as the data protection Regulatory from the same year, but it is true that the impact assessment is included in it and, if it is done as we have said before, it could be a strong legitimating system as well as a baseline for an international standard as is the data protection regulatory. But what is certain, as we have seen in this work, is that the

[57] Ibid, 284.

combat against terrorist financing without the use of new technologies, as the terrorists are doing, is a chimera nowadays.

**Conclusion**

As we have seen in this work, the new forms of terrorism are challenging not only national states but the international community. The ways in which terrorist groups change their modus operandi is the key point of their actions, particularly because law enforcement agencies do not have this same ability.

As we have found in the solutions from the terrorist experts there are two points in which it is possible to make advances: changing citizens' perception of terrorism, and financial supporters, and controlling the money. Both are being developed in Internet because the network is cheap, offers great flexibility, global access and anonymity.

To face the new forms of terrorism and, particularly, to fight on Internet, we need to use artificial intelligence to be, at least, at the same level as terrorists. Otherwise, the possibilities of avoiding police control and increasing the risks for society will be easy for any person who wants to have a political impact in a society.

In our opinion, the use of these tools is necessary. But it is true that we could go from fear of terrorism to a fear of state control[58]. That is the reason we need a legitimate system to use these kinds of tools between civil society, the private sector and the state[59]. In this work we suggest the first step for this new social contract: the impact assessment. As we have seen, the work of Wright et al. put on the table some questions that should be on the mind of all people involved in the development and use of these machines. They can be strongly powerful in the fight against terrorism, but in the wrong hands could put democracy at risk. The first step is their ethical use. The second is the rethinking of privacy protection, in particular, and human rights, in general, from the administrative and criminal points of view[60]. Finally, from international law, an international agreement is needed to deal with online surveillance and financial tracking.

Here there are some clues about how to start regulating the use of artificial intelligence in the sector of security. The advances from the European Union to regulate the field could have a major impact in international society and in the private sector. The Ethics Guidelines for Trustworthy Artificial Intelligent prepared by the High-Level Expert Group on Artificial Intelligence focuses on a human development in this field, based on respect for human rights. This is a challenge for lawyers. Knowing how to translate the principles from the ethic analysis into new rights for the citizens probably requires a rethinking of the whole legal system. The impact of this technology in life is huge, for good and for bad. If normal life is to be ruled by it in many spheres, its use in security, intelligence and crime will have a strong impact on citizens' rights.

We need to open a debate about this. We must react soon about the impact that all this could have because there are two important risks: on one hand, not to use these tools would mean that terrorism and organized crime will have a space of impunity and, in the other hand, it use

[58] Bruce Sheneier, *Data and Goliath* (W. W. Norton and Company 2015)
[59] Ibid. 259.
[60] Javier Valls Prieto, *Problemas jurídico penales asociados a las nuevas técnicas de prevención y persecución del crimen mediante inteligencia artificial* (Dikynson, 2018)

without any limit will destroy citizens' trust in state institutions. And this, in democracy, is exactly on what our system is based.

Working together, citizens, private sector and state, can produce a new social contract in which respect for human rights will be at the top of the priorities, which will produce new forms of security in our societies, and will base trust on the institutions for an "intelligent democracy". It is in our hands to fight the terrorist with the rule of law, but human rights should be our first and guiding priority.