HEINRICH BÖLL STIFTUNG
The Green Political Foundation

Co-funded by the
Europe for Citizens Programme
of the European Union

How to face the terrorist threat and defend freedom?

Published on 10 December 2015 by Camino Mortera

It was as if they had done it on purpose. The day could not have been grimmer, when French brothers Cherif and Said Kouachi broke into the offices of satirical magazine Charlie Hebdo and killed 12 people. The celebre Parisian ‘grisaille’ (greyness), which descends over the city every winter, served as the perfect backdrop for what turned to be every security service’s deepest nightmare: with the two fugitives in the run, another attack was unravelling at a Jewish store in the South West of the city. Amedy Coulibaly, another French citizen, killed four people during the siege. The day before, he had killed a policewoman. The whole Europe held its breath. For three days, nobody knew what could happen next. European citizens took to the social media, the streets and whichever other mean they had to express their anger and, for a while, everybody was Charlie. Leaders of all around the world gathered in Paris for an unprecedented demonstration against terrorism. The European Council declared that the EU should offer a united front against terrorism and announced far-reaching measures.

And then, slowly, we all began to forget. Other million crises took over (2015 arguably being one of the most eventful years in the history of the EU) and Europeans turned their attention to refugees, Greece, the Eurozone. But terrorism, and the terrorist threat, was not going anywhere, anytime soon. Paris, again, served as the stage for a tragic reminder: that terrorists strike when we least expect them to. On Friday November 13th 2015, almost ten months after the Charlie Hebdo massacre, three suicide bombers blew themselves up outside Paris’ Stade de France, killing one passer-by. Simultaneously, gunmen attacked four restaurants and cafés in the city’s trendy 10th district, killing 39 people and injuring many others. A suicide bomber detonated a vest inside another café, injuring 15 people. Only fifteen minutes later, heavily armed terrorists opened fired inside Paris’ ‘Bataclan’ concert hall, killing 89. In total, 129 people died and 352 were injured. François Hollande, France’s president, declared that his country was ‘at war’ with the Islamic State, the terrorist organisation behind both the Charlie Hebdo and the November attacks. His government immediately declared the state of emergency, suspending some civil liberties and procedural rights. France invoked, for the first time, a ‘mutual defence’ clause contained in the Treaty of Lisbon (Article 42.7), asking all EU member-states to support the French state in its fight against Islamic terrorism. A week after the Paris attacks, Belgian authorities raised the country’s emergency level to the maximum: according to the Belgian government, there was strong evidence suggesting than a similar attack was being planned to hit Belgian soil. They were also concerned with the whereabouts of one of Paris’ shooters, Salam Abdeslam, who was thought to be hiding in Brussels. Belgium activated the protocol for imminent terrorist attacks and Brussels, the country’s capital, was placed under a general lockdown for four consecutive days. Metros and schools closed, and citizens were advised to reduce to the maximum their activities outside their homes. For some days, the only people one could see in the streets were soldiers and the police. The city fell into a state of fear, disbelief and shock, with many people wondering whether it was all that worth it.

The Charlie Hebdo slaughter was an attack on the freedom of expression. The November attacks, a blow on the Western lifestyle, on France's renowned joie de vivre. The subsequent events in Brussels only contributed to a general feeling that Europe is playing into the hands of terrorists, by cutting down the very core civil liberties that make up the continent's values. In these uncertain times, Europe needs to be strong, but cold-headed. It needs to use all the tools at its disposal to fight against terrorism, without giving into panic. And that is the most difficult thing of all: how to fight terrorism and defend freedom.

Terrorism is nothing new in Europe. From Italy's Red Brigades to Spain's ETA, European nations are used to deal with the threat of politically-motivated attacks. But terrorism—in Europe and worldwide—has changed rapidly over the last few decades, and cannot longer be restricted within the borders of the nation-state. National groups gave way to a new, more scary way of terrorism which was officially inaugurated with the 9/11 attacks. This terrorism was new because it was religiously inspired, global, and multi-targeted. It was more scary because, unlike its predecessors, the new terrorists did not fear death. They actually considered it as a reward. Someone that does not mind dying has, by definition, nothing to lose. And that is a very dangerous enemy to fight. Mostly, this new terrorism was Islamic-inspired. The most powerful amongst the many groups carrying out attacks was al Qaeda, a terrorist group founded in the late 80's by Osama bin Laden, among others, initially to fight the Soviet invasion in Afghanistan. After the spectacular take down of the World Trade Centre in New York, al Qaeda turned to Europe. In 2004, the group bombed four trains in Madrid, killing 193 people. In 2005, terrorists detonated three bombs in the London Underground and one in a London bus. There were 52 casualties.

The attacks in Madrid and London were amongst the worst in the history of the EU and triggered a battery of law and policy responses. On its part, the US engaged in its very own 'War on Terror', a war that would forever redefine the premises of 'ius belli' (the law of war): for the first time in history, a country was fighting an undefined enemy in an indefinite territory. The 'War on Terror' was, by definition, not bound by any idea of time or space. In May 2011, a team of US special forces killed Osama bin Laden in his hideout in Abbottabad, Pakistan. The death of bin Laden and the weakening of al Qaeda's leadership structures gave way to a 'new new terrorism': without its spiritual leader, the top-down approach of al-Qaeda morphed into much less organised actions, often conducted by relatively isolated individuals—such as the Kouachi brothers. Bin Laden's death also contributed to the strengthening of rebellious and scented organisations, previously affiliated to al Qaeda. The most notorious of these is the self-proclaimed Islamic State. The Islamic State (Daesh, in its Arabic acronym) displays an unprecedented command of social media and the Internet. Media-savvy IS knows that life in 2015 cannot be understood without the Internet. And neither can wars. Which explains why a terrorist group whose main aim is to re-instate a 1,500 year-old law is so enthusiastic about Facebook.

And so the West needs to confront a new threat: foreigners (Europeans, Americans or Australians) who, for one reason or another, adhere to the jihadist cause and travel to fight in

Syria, Iraq, Libya, Pakistan or Somalia. They may, or may not, later return to their homeland. There are also the ‘jihadi brides’: women (mostly young) who travel to conflict zones lured by the prospect of marrying a ‘hero’ (this is IS’ communication machine at its best—the ‘soldiers’ offered to these women have the allure of a rock star and nothing to envy to the likes of Justin Bieber or One Direction). Lone wolves, foreign fighters and returnees are enough of a risk for any country. But risks multiply in Europe: terrorists, like any other EU citizen, enjoy freedom of movement. And they are certainly using it. In May 2014, French citizen Mehdi Nemmouche killed four people at the Brussels’ Jewish museum. He later tried to flee to France, only to be arrested in Marseille, where he had arrived after having taken a bus from Amsterdam via Brussels. The Kouachi brothers had acquired their arsenal in Brussels and then brought the weapons to France. Coulibaly’s wife reportedly flew to Syria via Madrid, without being stopped. The terrorists involved in the Paris attacks of November 13th were later discovered to be French and Belgian citizens, and the massacre was allegedly organised by Belgian national Abdelhamid Abaaoud, killed two days later in a police raid in Saint-Denis, north of Paris. Abaaoud is thought to have been travelling back and forth from the Schengen area to Syria without being detected. Of the eight terrorists carrying out the attacks, seven died and one, Salah Abdeslam, fled, allegedly to Belgium and from there to Syria. And the target of Danish-born terrorist Abdel Hamid El-Hussein, who killed three people in February 2015 in Copenhagen, was a Swedish artist.

There is simply no option for Europe: the EU needs to adopt a common approach to terrorism, so that terrorists cannot travel more freely than law enforcement does. There are, of course, limits to what the European Union can do to fight terrorism. The EU is not a sovereign state and has restricted competences in the security field. But member-states are starting to realise that they need to agree on some common policies at European level, if they want to combat a globalised network of terrorists.

Societies organise themselves on the basis of a set of rules—the law—that departs from the simple premise of trading some individual rights in favour of a common good. Because we live in society, we cannot simply do whatever we want. Criminal laws seek to punish individual behaviour threatening other individuals (like murder) or the society as a whole (like drug dealing). In this social pact, the state plays a privileged role by which it can exercise ‘force’ to prevent, or punish, actions that societies considered as criminal. So, the practical implementation of criminal law will, almost invariably, result in some degree of restriction to civil liberties. Counter-terrorism is, arguably, the most liberty-restricting part of criminal law. Terrorism is a form of political violence, directed not at an individual (personal casualties are the means through which terrorists seek to attain their end-goal), but at the state. Terrorism is also a very spectacular form of crime, which objective is, precisely, to terrorise and coerce citizens. The state, as the target of terrorists, feels entitled to take repressive measures against the terrorists, and scared citizens agree to that, for the sake of public security. Counter-terrorist laws and policies are often a mine-field where the state risks to go beyond its powers to prevent attacks and pursue terrorists.

There is a clear trade-off between security and civil liberties, and every other sovereign state needs to pick a side. Often, this choice depends heavily on the country’s history and experience. Terrorist-stricken countries such as the UK or Spain have rather restrictive laws in place and their citizens tend to be more lenient towards the securitisation of the state. Others, like Germany, still hold bitter memories of a past when the state was everywhere and knew everything; as such, they attach great importance to individual liberties, as a way to content the state.

Our world is now more connected than ever. Some refer to the Internet as ‘the sixth continent’, because physical space is no longer an absolute measure. We can now meet people, buy things and work, all without leaving our house. Nearly everybody has a smartphone, an email address and a Facebook account. Personal data has become the new currency of trade. Almost without realising, our whole life is out there for everybody—from Google to the NSA—to see. So it is no wonder that, amongst the extensive catalogue of civil liberties protected by the law, 21st century citizens attach a particular importance to the right to privacy. The booming of the Internet also means that whatever we say now has the potential of reaching thousands, millions of people. The online world provides the ultimate platform for freedom of expression and has made possible things were unthinkable only some years ago. The Arab Spring owes very much to online activists. Whistle-blowers, dissidents and people living under oppressing regimes can use the ‘darknet’ (a lesser-known part of the web deploying technologies that conceal the users’ identity) to circumvent censorship. But the Internet is a two-sided coin: the bad guys can use it, too. Indeed, the ‘darknet’ is home to some of the world’s worst criminals (including paedophiles and drug dealers); terrorist groups use social media and other channels to disseminate propaganda and recruit ‘fighters’; like anybody else, criminals use phones, emails, social media to go about their business. So, in its quest for security, the state is confronted with the dilemma of deciding when (and how) is it proportional to intrude into people’s lives, and to limit their freedom of expression. In 2015, security must be balanced, first and foremost, against privacy and free speech.

The balance between security and civil liberties is a delicate one. Sovereign states often struggle to find the equilibrium point. Things become more difficult when it is a club of countries that needs to take this decision. Which is precisely what is happening in the European Union right now. The EU cannot tip-toe around the question of security versus civil liberties any longer: the Lisbon Treaty made security issues a matter of EU law (before, it was up to member-states to decide; now, both the European Commission and the Parliament have a say); and new forms of organised crime and terrorism require a co-ordinated response at EU level. The EU is now fully part of the security/civil liberties game and, like any other player, it needs to pick a side.

There are few places in the world where the trade-off between security and civil liberties materialises as clearly as in Brussels: ever since the Lisbon Treaty entered into force, the European Parliament and the Council have been quarrelling about security. A casual observer may be led to think that the Council represents the security side of things, while the Parliament is fiercely fighting for citizens’ liberties. The reality is much more complex, especially if we throw the Court of Justice of the EU (CJEU) into the mix. For the past five years, security has become one of the most conflictual policy areas in the EU, not least because of civil liberties concerns (mostly related to privacy). In 2010, the European Parliament rejected a EU/US agreement to transfer financial data to track terrorist activities (the TFTP agreement—which was eventually adopted a year later). It took five years for the Parliament and the Council to agree on a system for EU countries to share data on passengers flying into, or out, the EU (the Passenger Name

Records-PNR- directive). The CJEU annulled, in 2014, a directive (sponsored by the UK) requiring telecommunication providers to retain customer data for a period of six months to two years (the data retention directive). More recently, the Parliament has struck down a EU/US agreement for the transfer of commercial data (the Safe Harbour agreement). The latest ruling is a direct consequence of the controversial revelations of Edward Snowden, a former contractor for the US' National Security Agency (NSA). Snowden leaked to the press documents showing that the NSA had engaged in surveillance programmes that extended to Europe. Needless to say, the European Parliament was not happy about that, and asked the European Commission to revise the Safe Harbour agreement, a self-certification system that allows American companies to transfer data of European citizens to the US. While the Commission was working its diplomatic channels to address the Parliament's concerns, Max Schrems, a Austrian law student, went first to the Irish courts and then to the CJEU to try and stop Facebook transferring his data to servers located the US—on the basis that, after Snowden, America could no longer be considered as a country that offered an adequate level of protection to personal data, as EU law requires.

On the other side of the spectrum, European governments (which make up the Council) are more concerned than ever about security, and want to be able to read people's letters and listen to people's calls, to put it in the words of British Prime Minister David Cameron. In the 21st century, that means being able to break encryption codes, or even banning encryption all together. Governments across the EU (France and the Netherlands, for example) are adopting laws that grant law enforcement authorities ample powers to fight against terrorism, including the use of surveillance techniques. Some in national governments and in the Council believe that, in view of the extraordinary terrorist menace, there are few options left to the state than to become a sort of omniscient big brother, aware at all moment of what its citizens do and think. France's current state of emergency is the latest example of this tendency towards a 'super-securitisation' of the state.

Neither what the Parliament not what the EU governments are doing is necessarily right. Neither the EU nor its member-states should engage in a futile 'War on Terror' à la George W. Bush; but neither should they disregard the growing threat of terrorism and the utility of security measures. It is the role of the state-and, by extension, of the EU- to keep its citizens safe; but in doing so, it cannot ignore civil rights. Governments cannot adopt security measures without thinking on the impact they will have on people's daily lives. That is why the control of democratically elected institutions, such as the European Parliament, is so important. Unfortunately the current arrangements are not necessarily the best to ensure that there is, indeed, a proper democratic oversight of counter-terrorism laws and policies. The gridlock in security measures compromises the safety of 500 million Europeans. And the actual concerns of EU citizens get diluted in endless fights while the EU decides whether or not it wants to be a serious security actor. So, nobody wins.

The problem of the EU is that it still has not decided which threats to take seriously and how to deal with them. It is also still unsure of how to manage international partners in the fight against terrorism, such as the US. There is a good case for the EU to become stronger in the security field: as terrorism becomes more supranational, so should the measures to combat it. A single PNR system, for example, will be more efficient than 28 different ones. Having an harmonised approach to terrorist offences across the EU will help the work of law enforcement and judicial bodies alike. The EU should not offer ‘safe havens’ to criminals, and it should not be easier for a terrorist to attack Prague than Berlin. But the EU should not sacrifice civil liberties in the name of security. All the institutions involved in the decision-making process should strive to protect the fundamental rights and values the EU is so proud of. This is more than a moral requirement: the EU bases its foreign policy strategy on its ‘soft power’ as a global exporter of democracy and human rights.

After the Charlie Hebdo attacks, some European governments panicked and called for re-introducing systematic passport checks within the Schengen area. This was worrying back then, but it is even more almost a year after, in light of the latest attacks and the current refugee crisis. The EU’s inability to deal with massive inflows of refugees has translated in what could very well become a serious Schengen crisis. Member-states are building fences, halting international traffic and temporary reinstalling border controls. The idea of a border-less Europe, one of the main pillars of the European project, is now put into question—something that would have been unthinkable only some years ago. But building walls in Europe is not the answer; neither for the refugee crisis nor for the threat of international terrorism. In a globalised, interconnected world, no walls, physical or otherwise, will stop people (migrants, refugees and criminals alike) from moving to one place to another. The EU should not think that by heightening the walls of ‘Fortress Europe’, it will achieve much. Instead, it needs to focus on using some of the tools already at hand, and exploring other ways to address both the phenomenon of migration and that of organised crime.

For example, national governments could make a better use of the Schengen Information System (SIS II), the EU’s database to facilitate border control and law enforcement. The Schengen Borders Code (the law that governs Schengen) allows national authorities to perform checks on ‘random’ samples of passengers, or passengers that they consider a threat, within Schengen’s internal borders. These checks mainly consist on interrogating national and European databases (the SIS II, most importantly) to verify the identity of the person and whether or not they have committed a crime, or may be considered as suspicious. The problem is, as the European Commission has rightly warned, that not all member-states are making full use of the SIS II database. National authorities can input information (‘alerts’) on people, to signal, for example, that a person is wanted for a criminal offence, that a document has been stolen, or that law enforcement considers a person as suspicious. But member-states are not consistently inputting this information, notably with regards to alerts or suspicious or potentially dangerous people. This is very much linked to the reticence of national authorities to share intelligence information with all other EU countries. When it comes to intelligence, EU countries still prefer to operate on bilateral basis, rather than pooling information at the European level, mainly because of a lack of trust. But, with this approach, countries are missing the potential of EU-level databases to fight trans-national organised crime, and turning to more radical solutions, like the imposition of border controls, instead. It should not be possible for anybody to smuggle firearms between two European countries (as the Kouachi brothers did); to travel, un-noticed, from one member-state to another, after having committed or being linked to a crime (as Salah Abdeslam or the wife of Amedy Coulibaly did); or to get in and out Schengen at will, even after having been branded as the brain behind several disrupted terrorist plots in Europe (as Abaaoud claimed to be constantly doing) . And one does not even need to think about terrorists to see the benefits of a more co-ordinated approach: in August 2014, Alice Gross, a 14-year-old English schoolgirl, was killed in London, allegedly by Arnis Zalkalns, a Latvian citizen. Zalkalns, who had been convicted in Latvia for the murder of his wife in 1997, travelled to the UK, without British authorities even knowing that he had been charged with a very serious crime back in his homeland. Cases like this could be prevented if European databases were used more efficiently.

The Islamic State has a very simple strategy: it wants us all to think it is fighting for religion, so that it can legitimise its cause and reduce to the world to a perverse confrontation of 'them against us', Christians versus Muslims. In reality, IS fights for power, money, and other geopolitical interests. It ultimately wants revenge. All this has little to do with religion, and the sooner Europe gets this, the better it will be in responding to the threat. A confrontational rhetoric has the danger of deepening already serious divisions in Europe's society. Nothing will please IS more than to fuel their cause by accusing the West to be 'anti-Muslim'. So populists are playing the terrorist's game, by implying that all Muslims are terrorists, and that the EU has an 'Islamisation problem'. In reality, many of Europe's 'foreign fighters' know very little about religion. They should be deprived of their Islamic halo and be painted as what they really are: petty criminals that evolved into major criminals. To avoid the risk of spreading hate and racism across the EU, we need to distinguish in between Muslims and the bad guys, who claim to be defending Muslims. And to do that there is nothing more efficient than knowing who the bad guys are and what are they up to. Because most of them have criminal records, European authorities could be on alert when they travel, notably to conflict zones like Syria, or when they try to go to another member-state. But, for that, governments need to start inputting information of the people they know are, or are in the process to be, the bad guys into the SIS II. In technical jargon, that is called 'Article 36 alerts'.

All these examples show that the use of data (and databases) is of outmost importance to fight terrorism and other forms of crime. This is almost a given in our highly-interconnected world. But the utility of data should not serve to justify just anything. The EU, and its member-states should learn to distinguish which measures are useful and can be accepted by the citizens as part of the trade-off between security and civil liberties, and which ones are just too much. Among the former category, schemes such as the EU PNR, or the Schengen Information System are very valuable tools that have proved to help in disrupting criminal activity. Within the latter category, on the other hand, national governments should not aim at a total ban of privacy-friendly technologies such as encryption.

Encryption is a technology that allows companies to encode users' data so that only wished-for recipients can access it. User's privacy can also be protected through the use of technologies facilitating anonymity, used to mask identities and digital tracks. Encryption and anonymity are not only useful for protecting privacy: they play a very important role in empowering individuals or communities to circumvent censorship in totalitarian states— the 'darknet' helps the politically prosecuted to reach out to the world and to organise themselves, although it is also used by criminals such as paedophiles or drug dealers. Encryption and anonymity are to the digital world what the right to private communications was to the analogic one: if to open a letter addressed to me, or to listen to a conversation I may be having in my living room, the state needs a judicial warrant, why should things be different in the online world? Should the state be able, by default, to open my emails and listen to my Skype calls? It should not. There are very good reasons why law enforcement authorities should be able to use data to track and trace criminals. But they should always do so through channels that allow the citizen to understand, and contest, if necessary, the use of their data. In the same manner that the police cannot enter my house or open my correspondence without a judge allowing them to, state authorities should also require the approval of a judge to snoop into my electronic communications (with the potential exception of emergency situations such as the one experienced by France after the November attacks).

In the great trade-off between security and privacy, activists have found an interesting, if slightly unexpected, ally in US giant Internet companies. It is only logical: after the Snowden revelations, many citizens, in Europe and elsewhere, began to mistrust the use that American online services providers made of their data, and this endangered the business model of these companies, which core revenue comes from exploiting people's data. So Sillicon Valley started pushing for an absolute right to encrypt their users' communications, in a bid to gain people's trust back. Some of them (such as Apple) have gone as far as to implement encryption codes that they cannot breach themselves—data on the latest version of the company's best-selling iPhone is encrypted in a way that cannot be breached by anybody (not even by Apple itself, not even if requested to by law enforcement authorities). A blanket ban on encryption is a mistake, but so is codifying data in a way that governments cannot access it, not even when a judge believes it is necessary to stop, or prosecute, a criminal. The former option amounts to telling the citizens that they will never be able to enjoy privacy in so far as they use electronic devices—which, in 2015, is pretty much all the time; the latter option would put the government in a disadvantageous position vis-à-vis terrorists and other criminals, who could enjoy the benefits of the Internet (not least, a global reach) without ever having to worry about getting caught.

We are living extremely tumultuous times. Never in the past decades has the old adagio 'the EU is now at the crossroads' been so true. Nothing seems certain any longer, everything can happen: a suspension of Schengen, the fall of the Euro, a major war conducted by a EU country, a terrorist lockdown at the heart of Europe. We are all understandably confused. We are all reasonably scared. But that is no reason to take the high road and legislate for the short term. The EU is a world-champion of human rights, and a place where many people want to live. It should continue being so. And it has very good structures in place that can be used to fight the new wave of terrorism without eroding the values that underpin the Union. To the question how to defeat terrorism and defend freedom there is only one answer: by being calm, strategic and looking at the long term. This used to be the responsibility of the member-states alone. It is now the EU's responsibility too. And it should live up to it.