BRIEFING

European Parliament

US counter-terrorism since 9/11

Trends under the Trump administration

SUMMARY

The fight against terrorism has dominated the national security agenda in the United States since Al Qaeda's terrorist attacks of 11 September 2001 (9/11). To improve the country's intelligence and homeland security apparatus, the presidential administrations of George W. Bush and Barack Obama implemented a series of legislative, organisational, policy, and personnel reforms.

The new administration under Donald Trump is continuing these efforts and has put particular emphasis on restricting the entry of and tightening the vetting process for refugees and immigrants. The administration has released a series of documents that provide strategic guidance for the US approach to national security and defence.

Today, the US domestic counter-terrorism strategy focuses on radical Islamic terrorist threats, stopping the movement of foreign terrorist fighters, and countering the spread of radicalisation. In this context, cyberspace is of particular interest, since the internet provides opportunities for terrorists to inspire, radicalise and recruit followers; raise funds; communicate through encrypted apps; and supply guidance and instructions to followers for carrying out attacks.

The European Union and the United States are key partners in the fight against terrorism, including through NATO.

In this Briefing

EPRS | European Parliamentary Research Service

Authors: Michael Kaczmarek and Elena Lazarou with Miguel Guevara and Benjamin Fogel
Members' Research Service & EPRS – European Parliament Liaison Office, Washington DC

PE 621.898 – May 2018

EN

9/11 and its aftermath

The terrorist attacks on the United States on 11 September 2001 killed nearly 3 000 people. Soon after the 9/11 attacks, the US administration set up the National Commission on Terrorist Attacks Upon the United States (commonly known as the 9/11 Commission), an independent, bipartisan commission, chartered to prepare a full and complete account of the circumstances surrounding 9/11, including preparedness for and the immediate response to the terrorist attacks. In July 2004, the 9/11 Commission released its public report which included 41 concrete recommendations to guard against future attacks. The Congressional Research Service (CRS) provided an overview of the 9/11 Commission report, its recommendations and the associated US anti-terror strategy of the time.

Key legislation and intelligence reforms

In the year after the attacks, more than 130 pieces of 9/11-related legislation were introduced in the US Congress, with 48 bills and resolutions approved or signed into law.

The USA Patriot Act: Preserving Life and Liberty of 2001 is one of the most substantial legislative changes since 9/11. It facilitated information-sharing and cooperation among government agencies, and allowed law enforcement to use surveillance and other means that were already available to investigate perceived terrorism-related activities, organised crime, and drug trafficking. Expiring provisions of the Act were reauthorised by subsequent legislation in 2005, 2009 and 2011, and with the USA Freedom Act of 2015.

The Department of Homeland Security (DHS) was established in 2002 and integrated 22 separate federal departments and agencies into a single Cabinet department. The Implementing Recommendations of the 9/11 Commission Act of 2007 address a wide range of DHS missions, including cargo security, critical infrastructure protection, grant administration, intelligence and information-sharing, privacy, and transport security. DHS is now the third largest department, with over 240 000 employees and a 2018 fiscal year budget of US$44.1 billion.

The US intelligence community

The US intelligence community (IC) is composed of 17 organisations:

- two independent agencies: the Office of the Director of National Intelligence (ODNI) and the Central Intelligence Agency (CIA);
- eight Department of Defense (DoD) elements: the Defense Intelligence Agency (DIA), the National Security Agency (NSA), the National Geospatial Intelligence Agency (NGA), the National Reconnaissance Office (NRO), and intelligence elements of the four DoD services: the Army, Navy, Marine Corps and Air Force;
- and seven elements of other departments and agencies: the Department of Energy's Office of Intelligence and Counter-Intelligence; the Department of Homeland Security's Office of Intelligence and Analysis and US Coast Guard Intelligence; the Department of Justice's Federal Bureau of Investigation, and the Drug Enforcement Agency's Office of National Security Intelligence; the Department of State's Bureau of Intelligence and Research; and the Department of the Treasury's Office of Intelligence and Analysis.

Source: ODNI website.

The Intelligence Reform and Terrorism Prevention Act of 2004 is considered to be the most significant legislation affecting the US intelligence community since the National Security Act of 1947. Principal among the enacted changes was the establishment of a new position of Director of National Intelligence (DNI) to serve as head of the intelligence community (IC). The director also serves as principal adviser to the President on intelligence matters related to national security, and oversees as well as directs the implementation of the National Intelligence Program. However, observers are divided over the success of the Office of the Director of National Intelligence (ODNI), as described in CRS reports of 2010, 2011 and 2016.

Within the ODNI, the National Counter-terrorism Center (NCTC) was established as a central knowledge bank for information about known and suspected terrorists, and serves to coordinate

and monitor the counter-terrorism efforts of all government agencies. The NCTC is also tasked with fusing foreign and domestic intelligence.

Assessment and challenges

In 2011, the Department of Justice published a comprehensive overview of the structural and legal reforms carried out in the US since 2001. The report highlights the centralisation of counter-terrorism and intelligence units within law enforcement agencies, noting the formation of a single Federal Bureau of Investigation (FBI) National Security Branch in 2005, and the Department of Justice's National Security Division in 2006. According to a *Washington Post* investigation, more than 260 government organisations were either created or reorganised following the attacks, to focus on terrorism-related issues and enhance information-sharing processes. This has been a priority of the intelligence and law enforcement communities since the Department of Justice highlighted the FBI's 'severe deficiencies' in intelligence analysis and information-sharing capabilities and processes in its 2003 audit report. In 2010, more than 1 200 government organisations and 1 900 private companies were involved in work related to counter-terrorism, homeland security, and intelligence. A further investigation tracks the dramatic budgetary increase within the US intelligence and law enforcement communities from 2004 to 2013, including: the Central Intelligence Agency (+56 %), the National Security Agency (+53 %), Department of Justice (+129 %), the Office for the Director of National Intelligence (+341 %), the Department of Homeland Security (+84 %), and the Department of the Treasury (+841 %).

Altogether, by 2010, analysts at these organisations were producing 50 000 intelligence reports annually. The growing number of organisations and overwhelming volume of information they produce have complicated efforts to reform information-sharing processes. Some government officials have raised concerns about duplication of efforts and an inability to process and review many of the reports. Thus, information-sharing remains a significant challenge to the intelligence, law enforcement, and national security establishment.

FISA Section 702

Shortly after the 9/11 terrorist attacks, President George W. Bush authorised a highly classified intelligence collection programme. The Terrorist Surveillance Program (TSP) authorised the National Security Agency (NSA) to intercept, without warrants, international telephone and e-mail communication into and out of the United States by 'persons linked to al Qaeda or related terrorist organisations'.

Following its media disclosure and controversial debates over this secret electronic surveillance programme, Congress enacted the Foreign Intelligence Surveillance Act (FISA) Amendments Act of 2008, which – through Section 702 – authorised the surveillance of non-US persons while they are outside the United States. It prohibits the US government from using it to target Americans or persons located in the United States.

Title VII of FISA was reauthorised by subsequent legislation, most recently in January 2018, providing a six-year extension up until the end of 2023.

Terrorist threats within the US

A report by the DOJ's National Security Division reveals that between 9/11 and 31 December 2016, more than 549 individuals were convicted of international terrorism-related charges in US federal courts. Over the same period, US Immigration and Customs Enforcement removed approximately 1 716 aliens on account of national security concerns.

Nonetheless, the US House Committee on Homeland Security's 2017 Terrorist Threat Snapshot relates that there are, or have been, 215 terrorist threats in the US homeland since 9/11 and notes that 'cases of homegrown Islamist extremism in the US are on the rise'. The Terrorism in America After 9/11 project of Washington DC-based think-tank, New America, counts over 400 cases since 9/11 of individuals who have been 'charged with or died engaging in jihadist terrorism or related activities inside the United States, and Americans accused of such activity abroad'.

The terrorist threat today

In his January 2018 statement on the FISA Amendments Reauthorization Act of 2017, President Trump declared that the United States faces 'a constant threat from foreign terrorist networks and other foreign actors who would do us harm'.

The intelligence community lists Jihadist terrorist organisations such as ISIL/Da'esh as the principal terrorist threats to the United States. Its loss of territory in Iraq and Syria and a precipitous decline in the number of foreign terrorist fighters, has resulted in the rise of self-directed attacks on soft targets (e.g. hotels, tourist resorts, concert venues, public events, cultural sites) outside the Syria/Iraq conflict zone.

Today, the terrorist threat is more diverse than it was following 9/11, as intelligence and law enforcement experts outlined during a House committee hearing in November and a Senate committee hearing in December 2017. The spectrum of ISIL/Da'esh attack plots ranges from those 'inspired' by the group (when ISIL/Da'esh claims responsibility for an attack whose perpetrators have no direct ties to the group) to attacks 'enabled' by the group (when ISIL/Da'esh contacts individuals through secure communications to prompt an attack) and attacks 'directed' (when the group provides direct support from Iraq and Syria for attacks).

The most immediate threat to the US comes from homegrown violent extremists (HVEs) – 'a person of any citizenship who has lived and/or operated primarily in the United States or its territories who advocates, is engaged in, or is preparing to engage in ideologically motivated terrorist activities (including providing support to terrorism) in furtherance of political or social objectives promoted by a foreign terrorist organisation, but is acting independently of direction by a foreign terrorist organisation'. As 'lone wolves' or in small insular groups, HVEs use simple, opportunistic tactics that do not require advanced skills or outside training, and plan soft-target attacks. Last fiscal year alone, the FBI maintained approximately 1 000 investigations of HVEs and 1 000 ISIS-related investigations.

Jihadist terrorists use virtual networks (e.g. the internet, social media) and physical networks around the world to share propaganda, to radicalise isolated individuals, exploit vulnerable populations, and to inspire and direct plots. Terrorist actors are able to communicate with each other outside the reach of US law enforcement using encrypted communications. This presents serious challenges to law enforcement's ability to identify, investigate, and disrupt terrorist threats and other crimes.

In the 2017 fiscal year, the FBI was unable to access the content of approximately 7 800 mobile devices, even though there was legal authority to do so. This figure represents slightly over half of all the mobile devices the FBI attempted to access in that timeframe.

While terrorist groups change tactics and targets, and innovate using emerging technologies (e.g. drones, robotics) to test for security vulnerabilities, aviation targets remain a focus of ISIL/Da'esh owing to the potential economic damage, high loss of life, and media attention. The DHS reacted in 2017 by implementing enhanced security measures for all commercial flights to the US. These measures include enhanced screening of passengers and electronic devices as well as heightened security standards for aircraft and airports.

Today, most national security and criminal threats are now cyber-based or technologically facilitated. Cyber-threats are increasing in scope and scale, and the frequency and impact of cyber-attacks on private sector and government networks are expected to grow. Sophisticated cyber-threats arise not only from terrorists but also from foreign intelligence agencies, hackers for hire, and organised crime syndicates.

Current US national security, defence, and counter-terrorism strategies

The new administration under President Trump has released a series of documents that provides strategic guidance for the US approach to national security and defence. In December 2017,

President Trump published a new national security strategy (NSS); in January, the 2018 national defence strategy (NDS) followed, and in February came the 2018 nuclear posture review (NPR). Notably, the new NSS posits that Jihadist terrorist organisations which advance a totalitarian vision for a global Islamic caliphate, 'present the most dangerous terrorist threat to the nation'. This phrasing presents a discursive shift from the Obama administration's use of the term 'violent extremism' rather than 'jihadi terrorism'.

A new counter-terrorism strategy is reportedly scheduled to be published in 2018, and will replace President Barack Obama's 2011 national strategy for counter-terrorism.

US counter-terrorism priority actions

US Secretary of Homeland Security, Kirstjen M. Nielsen, laid out, in January 2018, four priority actions for the Trump administration to combat terrorism. First, thwarting terrorist plots and countering emerging threats. Second, blocking terrorists from reaching the United States, through tougher vetting and tighter screening. Third, combatting terrorist radicalisation and recruitment, and, fourth, pursuing threats to their source. All of these priority actions are consistent with the 2017 NSS and 2018 NDS. The DHS 2019 budget request further expresses its priorities, and emphasises border security (including the construction of a physical border wall with Mexico), immigration law enforcement and removal operations, cyber-security, and aviation security.

Border security and the vetting of immigrants and refugees

National security became a priority in the debate over US immigration policy in the years after 9/11. The Enhanced Border Security and Visa Entry Reform Act of 2002, introduced in response to the 9/11 attacks, aimed to improve the ability to screen aliens seeking to enter the US, to facilitate the sharing of border-related information among US agencies, and to improve efforts to keep track of visa holders. Upon being elected, President Trump characterised the existing US immigration system as a threat to national security, focusing his criticism primarily on chain migration and the Diversity Immigrant Visa Programme. Other immigration priorities of the Trump administration include building a wall on the border with Mexico and removing unlawful entrants.

The federal government utilises several tools to prevent individuals from travelling to, from, or within the United States to commit acts of terrorism. In addition to the federal immigration laws, these measures include, inter alia, terrorist databases and the 'no fly' list, stricter guidelines on passenger and luggage screening, criminal sanctions, and passport restrictions on travel to specific countries.

Tougher vetting and the 'travel ban'

President Trump issued a series of executive actions commonly referred to as the 'travel ban', which restrict the entry of specified categories of non-US nationals from Yemen, Libya, Chad, Syria, Somalia and Iran, as well as North Korea, and some government officials from Venezuela, into the US. On 27 January 2017, within a week of his inauguration, Trump issued Executive Order (EO) 13769 ('Protecting the nation from foreign terrorist entry into the United States'). Since the implementation of this EO has been delayed by litigation and critical provisions of have been halted by courts, Trump replaced the EO, in March 2017, with EO 13780. According to DHS's initial report, the actions directed by EO 13780 have raised the baseline for vetting and screening of foreign nationals and improved the government's ability to prevent the entry of malicious actors.

According to the report, in fiscal year 2017, DHS had 2 554 encounters with individuals on the FBI's Terrorist Screening Database traveling to the US. Of those encounters, most (2 170) were attempting to enter by air. Between FY 2010 and FY 2016, a total of 73 261 foreign travellers destined for the US have been prevented from boarding their flights on account of a perceived immigration or security risk.

The Trump administration also introduced additional enhanced security procedures for refugees from 11 high-risk countries (Egypt, Iran, Iraq, Libya, Mali, North Korea, Somalia, South Sudan, Sudan, Syria and Yemen) seeking resettlement in the US. Additionally, the number of admissions to the US Refugee Admissions Program (USRAP) was capped at 45 000 for fiscal year 2018, a significant decrease from the 110 000 cap of fiscal year 2017.

In February 2018, President Trump signed a National Security Presidential Memorandum tasking the DHS and other government agencies with establishing, within the next six months, a National Vetting Center (NVC) to be led by the DHS. The NVC seeks to improve the vetting process for individuals coming into the US, to improve the identification of individuals who present a threat to national security or public safety.

Internationally, the DHS engages with foreign allies to share analytical and targeting methodology, to mutually enhance the ability to identify individuals and travel routes, and prevent foreign fighters travelling to and from foreign conflict zones. In this context, the US obliges all foreign countries to cooperate on information-sharing for immigration vetting. However, DHS remains concerned, according to Secretary Nielsen, that some countries do not meet baseline requirements on border security, international traveller screening and speed of intelligence-sharing.

Preventing terrorism and countering radicalisation

Radicalisation takes place on the internet, in prisons and in neighbourhoods, both at home and abroad. Several programmes have been established to combat the threats of radicalisation and home-grown terrorism. In 2011, the Obama administration adopted a counter-radicalisation strategy and a corresponding strategic implementation plan. The latter was updated in October 2016. The strategy addresses the radicalisation of all types of potential terrorists in the United States but focuses on those inspired by Al Qaeda.

Today, the intelligence community and law enforcement agencies worry about 'virtual safe-havens' provided by the internet, social media, and the use of encrypted apps. These virtual tools allow terrorist groups to spread propaganda and identify vulnerable people. Accordingly, these tools are used to plan attacks, and to inspire, radicalise, and recruit vulnerable individuals. The Trump administration responded in November 2017 by reorganising the Office for Community Partnerships (OCP) into the Office of Terrorism Prevention Partnerships (OTPP). The Terrorism Prevention Partnerships prioritise education and community awareness to help people recognise the signs of radicalisation and suspicious behaviour. This includes the public dissemination of the Terrorism and Extremist Violence in the US (TEVUS) portal and the profiles of individual radicalisation (PIRUS) datasets through the National Consortium for the Study of Terrorism and Responses to Terrorism (START).

These efforts are aimed at enabling local partners – including law enforcement, social services providers, schools and communities – to identify and create alternative pathways for individuals that otherwise might be receptive to violent ideologies, both foreign and domestic.

Countering terrorist financing

Since 9/11, the tracking and freezing of terrorist assets has been an important pillar of US counter-terrorism efforts. The Patriot Act expanded the ability of the Treasury to detect, track, and prosecute individuals suspected of money laundering and terrorist financing.

As part of these efforts, the US plays a leading role in the 1989-established international Financial Action Task Force on Money Laundering (FATF) – originally organised to develop and promote policies to combat money laundering. After the 9/11 attacks, the body expanded its role to include identifying sources and methods of terrorist financing, and adopted nine special recommendations on terrorist financing to track terrorists' funds.

Until recently, ISIL/Da'esh was described as one of the best-funded terrorist organisations. Therefore, countering ISIL/Da'esh's financial resources has been a significant national security priority for US policymakers and allies. The Counter-ISIL Finance Group (CIFG) was established in 2015, as part of the Global Coalition to defeat ISIS, and the United Nations Security Council has authorised several international actions against ISIS financing.

In the current 115th Congress, further legislative proposals have been introduced to counter terrorism and illicit finance.

Counter-terrorism partnerships and cooperation

Two of the most important field-based organisations for information-sharing and counter-terrorism are the FBI-led joint terrorism task forces (JTTFs) and fusion centres. JTTFs bring together specialists from federal, state, and local law enforcement and intelligence agencies in more than 100 cities, and are charged with investigating terrorism and terrorist-related activity to offer 'investigative support to ongoing FBI counterterrorism activities'. Fusion centres, by contrast, 'operate as state and major urban area focal points for the receipt, analysis, gathering, and sharing of threat-related information between federal; state, local, tribal, territorial (SLTT); and private-sector partners'. The DHS shares intelligence and threat information with SLTT partners through its Office of Intelligence and Analysis, and produces tailored assessments on the motivations of home-grown violent extremists, suspicious behavioural patterns, likely tactics and techniques and preferred targets.

Department of State, Bureau of Counterterrorism

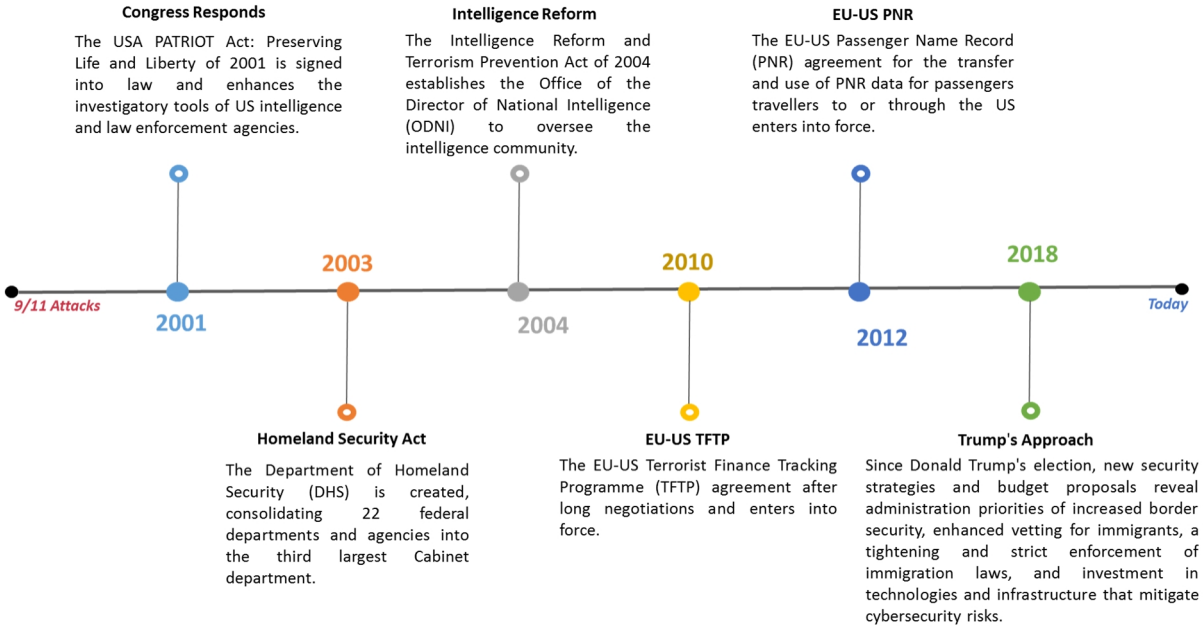
The Bureau of Counterterrorism within the Department of State operates several counter-terrorism programmes and initiatives that aim to strengthen partnerships, civilian capacity, and information-sharing around the world. The priority rests on three key programmes: the Counter-terrorism Partnership Fund (CTPF), the Antiterrorism Assistance (ATA) programme, and the Terrorist Interdiction Program (TIP). The focus areas for these programmes include crisis response, aviation and border security, counter-terrorism legal frameworks (i.e. prosecutions and investigations), counter-terrorism financing, and action to address terrorist radicalisation, recruitment, and rehabilitation.

The annual Country Reports on Terrorism that the Bureau of Counterterrorism submits to Congress, give a comprehensive overview of the international and country-specific terrorist threat landscape. The reports, the 2016 edition being the most recent, include the US assessment of the countries' counter-terrorism efforts and the scope of regional and international cooperation.

Partnerships with social media and technology companies

The US government also works with social media and technology companies, to report, reduce and react to terror-related activity on their platforms. The US Senate has conducted several hearings on the use of social media in terrorist radicalisation, most recently in January 2018. In April 2016, the inter-agency Global Engagement Center (GEC) replaced the State Department's Center for Strategic Counter-Terrorism Communications (CSCC) and was charged with the mission to 'lead, synchronise, and coordinate efforts of the Federal Government to recognise, understand, expose, and counter foreign state and non-state propaganda and disinformation efforts aimed at undermining United States national security interests'. The GEC was codified into law by Congress in the fiscal year 2017 National Defense Authorization Act (NDAA). The Global Internet Forum to Counter Terrorism (GIFTC), set up in June 2017 and led by Facebook, Google, Twitter, and Microsoft, aims to structure counter-terrorism efforts on the internet between companies, and to foster cooperation with governments, the EU, and the United Nations. The Digital Forum on Terrorism Prevention, led by the US inter-agency Countering Violent Extremism Task Force, brings together experts from governments, the technology industry and community organisations. The first Digital Forum was held in September 2017, followed by the 2018 Digital Forum in February.

Figure 1 – Milestones: selected acts and agreements since 9/11



Source: EPLO/EPRS.

US-EU cooperation

The US is the European Union's key partner in the area of justice and home affairs (JHA), including in the fight against terrorism. In the aftermath of 9/11, the US and the EU police agency Europol signed an operational agreement to enhance cooperation between the two parties on several areas of crime including terrorist activities. The agreement defines 'strategic information' including the sharing of information such as threat assessments and 'technical information' such as the sharing of training methods and procedures. Europol headquarters also hosts liaison officers from 11 US law enforcement agencies, including US Customs and Border Protection, the FBI, ICE, the New York Police Department, and the Transportation Security Administration (TSA). JHA ministerial meetings and senior officials' JHA meetings are held twice a year as a regular framework dialogue on all JHA topics, including counter-terrorism.

In January 2016, Europol established the European Counter Terrorism Centre (ECTC) to provide operational support upon a request from an EU Member State for investigations. It also focuses on international cooperation among counter-terrorism authorities.

However, some issues remain to be further streamlined. They include differences between EU and US designated terrorist lists, data protection, and the use of extraordinary rendition and secret detention facilities. Many in the EU, including the European Parliament, have raised serious concerns with regard to the protection of personal data in the US and possible violations of EU citizens' basic rights.

Major agreements in this area are the EU-US Terrorist Finance Tracking Programme (TFTP) agreement and the EU-US Passenger Name Record (PNR) agreement which are both subject to regular review. The TFTP entered into force on 1 August 2010 and concerns the transfer and processing of data for purposes of identifying, tracking and pursuing terrorists and their networks. Under the agreement, Europol assesses whether the data requested in any given case are necessary for the fight against terrorism and against its financing. The PNR entered into force on 1 July 2012 and concerns the transfer of air passengers' data for flights to, from, or through the US.

The EU-US Umbrella Agreement on Data Exchanges for Law Enforcement was signed in June 2016 and provides framework of rules governing transatlantic data exchange in the context of law

enforcement investigations. It set high standards of personal data protection for future agreements in this field. The umbrella agreement seeks to provide safeguards and guarantees of lawfulness for data transfers, thereby strengthening fundamental rights, facilitating EU-US law enforcement cooperation, and maintaining public trust. However, the agreement itself will not constitute the legal basis for any transfer of personal data to the US, but will supplement, where necessary, data protection safeguards in existing and future data-transfer agreements or national provisions authorising such transfers.

The NATO dimension of EU-US cooperation on counter-terrorism was reinforced in December 2017 with the adoption of 34 new actions as part of the ongoing implementation of the 2016 Joint Declaration.

In February 2018, the European Parliament's Subcommittee on Security and Defence (SEDE) chair Anna Fotyga (ECR, Poland) and Tunne Kelam (EPP, Estonia) noted the close cooperation between the EU and the United States on matters of security following a mission by SEDE to visit the NATO Cooperative Cyber Centre for Excellence, as well as the European Centre of Excellence for Countering Hybrid Threats in Helsinki. The US is a signatory to the Memorandum of Understanding that established the centre. On 1 March 2018, noting the continuing relevance of combating terrorist financing, the European Parliament adopted a recommendation to the Council, the Commission and the Vice-President of the Commission / High Representative of the Union for Foreign Affairs and Security Policy on cutting the sources of income for jihadists – targeting the financing of terrorism – recognising the 'successful cooperation with the US and other partners ... in the context of the EU-US agreement to share information from the US Terrorism Financing Tracking Program'.

With overlapping objectives in the domains of counter-terrorism, cyber threats, and hybrid threats, the EU and US maintain a high degree of cooperation at operational and political levels. At the legislative level, the European Parliament and US Congress continue to maintain high-level exchanges through the Transatlantic Legislators' Dialogue (TLD), acknowledging each other as 'indispensable partners in global stability, security, and economic development.' During the 80th TLD meeting, held in June 2017, both parties acknowledged that 'closer cooperation between US authorities and European agencies, such as Europol and Eurojust, would be a force-multiplier for our robust counter-terrorism relationship'.

Speaking to the European Parliament's Delegation for relations with the US in February 2018, European Commissioner, Sir Julian King, outlined the extensive counter-terrorism cooperation between the EU and the US both bilaterally, and within other organisations, such as the United Nations, the G7, the Anti-ISIL Coalition, the Financial Action Task Force (FATF), and the Global Counter-terrorism Forum. According to the Commissioner, progress is being made in the areas of aviation security and in the sharing of information taken from battlefields such as Iraq. He mentioned that other areas of mutual concern that should be addressed include the spreading of terrorist content online. This follows the European Commission's release of a set of operational measures for tackling illegal content online, to determine whether legislation on the matter will be required.

These efforts bring operational focuses in line with the EU's common legal framework on combating terrorism, including harmonised definitions of terrorist offences such as terrorist conduct committed through the internet and social media, and the necessity of cooperating with relevant third countries to secure electronic evidence. The European Union's refocus on the cybernetic operational front of terrorism, as well as electronic facilitation of terrorism, coincides with the EU's active cooperation with the United States, primarily through EU-NATO cooperation in which context the EU and US share 42 common projects.

MAIN REFERENCES

Congressional Research Service (CRS), US Anti-Terror Strategy and the 9/11 Commission Report, February 2005.

US House Committee on Homeland Security, Hearing World Wide Threats: Keeping America Secure in the New Age of Terror, November 2017.

US Senate Committee on Homeland Security & Government Affairs, Hearing Adapting to Defend the Homeland Against the Evolving International Terrorist Threat, December 2017.

The White House, National Security Strategy of the United States of America, December 2017.

US Department of Defense, 2018 National Defense Strategy, January 2018.

FURTHER READING

Immenkamp B., with Pawlak P. and Barzoukas G., EU efforts on counter-terrorism – Capacity building in third countries, EPRS, European Parliament, 2017.

DISCLAIMER AND COPYRIGHT

eprs@ep.europa.eu (contact)

www.eprs.ep.parl.union.eu (intranet)

www.europarl.europa.eu/thinktank (internet)

http://epthinktank.eu (blog)