Germany

Implementing the UN Global Counter-Terrorism Strategy

Over the last years, Germany has implemented manifold threat prevention measures, in full accordance with international law and the principles of human rights and in line with the provisions of the UN Security Council Resolutions. Accordingly, it had achieved a high implementation standard already before 2016. Based on the Federal Government's comprehensive strategic approach to fight terrorism in line with the aims of the EU's strategy, Germany's counter-terrorism policy responded to the new dimensions of threats posed by international terrorism by adopting a holistic approach, covering civic education, counselling services and security measures.

Germany cooperates constructively in all relevant international institutions, contributes to Europol and supports Interpol activities and projects aimed at enhancing the law enforcement capacities of other Member States. All measures are aimed at dismantling terrorist structures, ensuring early recognition and prevention, strengthening international cooperation, protecting citizens and reducing Germany's vulnerability.

The following measures are particularly crucial from our point of view:

Germany applies the European Union Counter-Terrorism Strategy and the associated implementing guidelines for combating radicalization and recruitment to terrorism.

Although Germany has not introduced a distinct counter-terrorism law (all criminal offences in this respect are already an integral part of our Criminal Code), Germany has taken legislative steps to amend criminal provisions on terrorism in accordance with resolution 2178 (2014) on Foreign Terrorist Fighters. Section 89a of the Criminal Code has been supplemented with a further preparatory offence covering travel and attempt to travel for terrorist purposes. The criminalisation of the financing of such travel is covered in terrorist financing provisions introduced in Section 89c of the Criminal Code on collecting, receiving and providing financial means which a third person might use to commit an offence under Section 89a.

Germany adopted further counter-terrorism measures in addition to the changes in the Criminal Code, e.g. authorising relevant authorities to refuse to issue a national identity card to supporters of ISIL or to revoke their national ID cards. Under the Identity Card Act and Passport Act, national identity cards and passports of German citizens who threaten internal or external security or other significant German interests may be revoked. Like the previous generation of passports, the new EU passports of the Federal Republic of Germany are among the most secure in the world. A number of new and advanced security features protect this new passport series from forgery and abuse. For example, Identigram®, a complex, full-surface feature applied on a polycarbonate data page with a colour photograph, securely integrated into the material of the card, prevents copying. From May 2024, other unique safety features were integrated, among others, the contour feature in the facial image. From May 2025, the application process domestically should be completely freed from scanning paper-based facial images and the

possibility of capturing facial image within the passport authorities (live enrolment) will be introduced nationwide.

As early as in December 2004, Germany established the Joint Counter-Terrorism Centre (GTAZ) in Berlin to address Islamist terrorism. Additionally, in 2012, Germany established the Joint Centre for Countering Extremism and Terrorism (GETZ) that deals inter alia with far right violent and far left violent extremist threats. The GETZ plays a vital role in intensifying the communication and coordination of nationwide measures between all relevant agencies. Through this joint cooperation and communications platform, 40 security agencies collaborate in the fight against terrorism and extremism by sharing information on a regular basis and discussing individual cases. The bodies involved in the work of the GTAZ as well as the GETZ include the police forces of the federal states, the federal and state offices for the protection of the Constitution, the Military Counter-Intelligence Service, the Federal Intelligence Service, the Customs Criminological Office, the Federal Police and the Federal Public Prosecutor.

Germany has fully implemented the API system since 2004 (EU Directive 2004/82/EC) and has implemented a PNR system (PNR Directive 2016/681 of 27 April 2016).

Furthermore, Germany facilitated the deportation of foreigners considered a danger to national security. Moreover, the Federal Criminal Police Act allows Germany to fit electronic tags to potential terrorists. In addition, German law provides for the opportunity to ban an association if its purposes or activities are contrary to the criminal laws or if it violates the constitutional order or the thought of international understanding. As a consequence, i.a., the association's assets are confiscated and seized. Amongst others, Germany banned all activities related to ISIL in Germany already in 2014. This encompasses advertising on behalf of the organisation, displaying its symbols, providing support of any kind (such as financial or material support) and recruiting fighters. Violations are punishable according to Section 20 of the Act on Associations as well as section 85 of the German Criminal Code under the conditions specified therein. Since the entry into force of the Act on Associations in 1964, numerous extremist (right-wing, left-wing, Islamist etc.) organisations have been banned on the federal as well as state ("Länder") level.

The terrorist attack on a Christmas market in Berlin in 2016 underlined the importance of these measures to prevent attacks and to protect both soft targets and critical infrastructure from terrorist attacks, and it illustrated the need for more activities:

In accordance with Security Council resolution 2341 (2017) and with the relevant EU Regulations, Germany implemented a series of measures, including training and awareness-raising activities with the private sector.

One important element is the National Strategy for Critical Infrastructure Protection of 2009, which includes different measures and recommendations.

In addition, Germany is preparing its first cross-sectoral legislation on the physical protection of critical infrastructure. This legislation will transpose the European Directive on the resilience of critical entities (CER Directive) and will strengthen the physical resilience of critical

infrastructure in Germany and the EU by identifying critical infrastructure and its vulnerabilities, by setting minimum standards for resilience measures and by setting up a system of incident notification.

The National Plan for the Protection of Information Infrastructures, introduced in 2005, was followed by the National Cybersecurity Strategy in February 2011, which was revised in November 2016 and September 2021. One continual objective of the strategy is to protect critical information infrastructure.

Germany adopted an IT Security Act in 2015. The act improved cyber security in Germany by imposing minimum standards and an obligation to report cyber security incidents occurring at operators of critical infrastructures. It followed a cooperative approach where operators and security authorities work hand in hand, thus partly anticipating the Directive (EU) 2016/1148 (NIS Directive) which harmonized cyber security and reporting obligations and introduced a supervision and cooperation framework on an EU level. The NIS directive was implemented on a national level in 2017. A continually elevated cyber threat level and lessons learnt from the IT Security Act and new political parameters led to the adoption of the IT-Security Act 2.0 in 2021. One of its main goals was strengthening the protection of the economy by adopting further measures for critical infrastructures, including critical components (in – amongst others – 5G networks). Germany is currently in the process of transposing the Directive (EU) 2022/2555 (NIS-2 Directive) and combining it with a national initiative to further strengthen the cybersecurity of entities of the federal government. The NIS-2 Directive imposes stricter and more detailed minimum cybersecurity requirements as well as reporting obligations on companies and critical infrastructures. The scope of affected companies will be significantly expanded – for Germany there will be a rise from roughly 4,500 to 29,000 covered companies. The EU Digital Services Act (DSA) is the first EU-wide, harmonised, comprehensive set of rules for (online) intermediary services offered to users in the EU. Due to its full harmonization approach, the DSA replaces national legislation like the Network Enforcement Act in most parts. Since 25 August 2023 it applies for very large online platforms (VLOPs) and very large online search engines (VLOSEs), that were designated by the EU Commission, since 25 August 2023. For all other intermediary services, it applies directly in all Member States since 17 February 2024. The DSA provides a level playing field for all intermediary services with users in the EU (major online marketplaces and social media platforms to comparison and booking portals, employment websites, exchange platforms, cloud services, app stores etc.). The DSA promotes fairness and transparency and covers all illegal content that is not in compliance with Union law or the national law of any Member State, including the provisions of the Criminal Code. Online platforms are obliged to process any notices that they receive and take their decisions in in a timely, diligent, non- arbitrary and objective manner (notice and action). The main elements of the new rules are liability regulations as well as due diligence and transparency obligations and information requirements for providers, complaint and dispute settlement mechanisms; and notification and action mechanisms for illegal content. They protect users and provide companies with legal certainty. Germany has implemented the DSA at the national level through the Digital Services Law ("Digitale-Dienste-Gesetz" - DDG), which came into force on May 14 2024. This law empowers the German Federal Network Agency as the National Digital Services Coordinator to ensure compliance with the new DSA

rules, in coordination with other competent authorities concerning specific DSA provisions on data protection and the protection of minors.

The EU Terrorist Content Online Regulation (TCO REGULATION (EU) 2021/784 on addressing the dissemination of terrorist content online) is fully implemented in Germany. The TCO achieves a uniform, legally certain and coordinated approach between EU Member States towards companies offering hosting services in the EU and in collaboration with Europol. Member States can issue removal orders and the hosting service providers must comply within one hour (Articles 3 and 4 TCO Regulation). Hosting service providers will also be required to better protect themselves against terrorist content (Article 5 TCO Regulation). Terrorist content leading to an imminent threat to life must be reported to the responsible authorities of the Member States (Article 14(5) TCO Regulation).

In 2017, the Aviation Security Act, which aims to protect civil aviation against terrorist attacks, was comprehensively amended. Several new provisions have been incorporated, for example on flight bans in case of severe threats to aviation security and on certification procedures for security equipment. A number of other provisions have been tightened, for example the provision on background checks to fight insider threats.

German authorities have raised the frequency of consulting databases during checks at the external borders in order to detect foreign terrorist fighters at an early stage. Since the revised Schengen Borders Code came into force in April 2017, German border authorities have systematically consulted databases at Germany's external borders.

Germany has developed a comprehensive system for countering the financing of terrorism. In recent years, it has introduced significant legislative and institutional frameworks, including the revised 2017 Anti-Money Laundering Act incorporating the 5th EU Directive. In October 2019, the first national risk analysis to combat money laundering and terrorist financing was published. In addition, the Sectoral risk assessment on terrorist financing through (the abuse of) non-profit organizations in Germany was published in 2020. In 2025, a separate volume on terrorist financing will be published as part of the second national risk analysis in order to focus all authorities and obliged entities even more strongly on the risks. To combat money laundering and terrorist financing, the financial intelligence structures have been further developed. The Zentralstelle für Finanztransaktionsuntersuchungen is the German Financial Intelligence Unit (FIU) for collecting and analysing financial intelligence related to money laundering or terrorist financing and passing this information on to the competent domestic public authorities for the purpose of the investigation, prevention or prosecution of such offences. Especially regarding terrorism financing, the FIU has set up specific key risk areas. All Suspicious Transaction Reports (STRs) relating to terrorist financing are treated with high priority and are forwarded directly to the relevant authorities. If there are indications that the forwarding of STRs is necessary for the fulfilment of the tasks of the Federal Office for the Protection for the Constitution (Bundesamt für Verfassungsschutz, BfV), the FIU immediately transmits it there. If the FIU finds in the operational analysis that property is related to terrorist financing, it transmits the result of its analysis and all relevant information to the competent

law enforcement agencies without delay. The information is also to be transmitted to the Federal Intelligence Service (Bundesnachrichtendienst) insofar as there are factual indications that this transmission is necessary for the Federal Intelligence Service to perform its functions. Banks are required by law to prevent abuse of the financial system, for money laundering and terrorist financing purposes. The Federal Financial Supervisory Authority (BaFin), in turn, supervises the banks, also in terms of the prevention of money laundering. In addition to the police of the Länder, the Federal Criminal Police Office (BKA) is responsible for investigations in money laundering and for terrorist financing prosecutions. To ensure an institutionalised and strategic exchange of information between the private sector (i.a. banks, real estate agents, trade dealers) and public authorities, the Anti Financial Crime Alliance (AFCA), under the leadership of the FIU, was constituted on 24 September 2019. The FIU set up AFCA together with BaFin, BKA and private sector entities as a public-private partnership to strengthen and coordinate the fight against money laundering and terrorist financing. Topic-related and sector-specific working groups are established under AFCA which serves as a platform for the strategic exchange of information between regulators and the private sector on an ongoing basis. Following the Hamas terrorist attack on 7 October 2023, the FIU Germany co-initiated a number of joint efforts at both national and international level to combine and strengthen the efforts to disrupt the international money flows related to Hamas. Furthermore, Germany is engaging in the Financial Action Task Force (FATF) efforts to counter the financing of terrorism and is active on international forums concerning counter terrorism financing, such as the Counter ISIS Finance Group of the Global Coalition to Defeat ISIS and the Global Counterterrorism Forum (GCTF). In August 2022, the FATF has published its Mutual Evaluation Report on Germany and notes significant improvements to Germany's AML/CFT framework over the past years.

Also, Germany hosted the fourth 'No-Money for Terror' Conference in Munich on 13th February 2025. The conference brought together almost 400 participants from over 60 delegations, including ministers, high-level representatives from international organizations, senior policymakers, and experts from around the world. The outcomes of the 4th No Money for Terror Ministerial Conference reflected a unified commitment to addressing the multifaceted challenges of terrorism financing in a rapidly changing global landscape. Participants agreed on the necessity of implementing AML/CFT Standards and reinforcing global AML/CFT frameworks to adapt to emerging threats and evolving financial technologies. Targeted capacity building in low- and middle-capacity countries was particularly emphasized to strengthen their active participation in global efforts to combat terrorism financing. The German Biosecurity Programme, launched by the Federal Foreign Office in 2013, is part of joint efforts of the G7 Global Partnership against the Spread of Weapons and Materials of Mass Destruction. Since 2013, more than 107 million Euros have been spent. In its fourth phase (2023–25), projects are being implemented in 16 countries in the Sahel region, the Maghreb, the Western Balkans, Eastern Europe and Central Asia. In addition, a one-year Fellowship Programme and an e-Learning Platform for biological security are offered. Activities of the German Biosecurity Programme are guided by the Global Partnership's "Biological Security Deliverables" and focus on six areas: awareness raising for international instruments of non-proliferation, biosafety and biosecurity, capacity development, detection and diagnostics of high-consequence pathogens, disease surveillance and networking. The programme is part of

the Federal Government's preventive security policy. It aims at preventing the misuse of biological agents for hostile purposes, such as warfare or terrorism.

As part of the Group of Friends of the UN Secretary-General's Mechanism for Investigation of Alleged Use of Chemical and Biological Weapons (UNSGM), Germany supports the UN Office for Disarmament Affairs (UNODA) with nominations of expert consultants, experts and laboratories for the mechanism, the conduct of exercises and training courses for experts and laboratories in order to increase the operational readiness of the UNSGM. Security authorities in Germany are currently monitoring several persons with an extremist background who are potentially willing to commit serious violent offences in Germany. Therefore, Germany introduced – within the framework of a holistic approach – a standardised tool to reliably classify target group members belonging to Islamist and right-wing extremist spectra by their risk potential so that police measures can be prioritised. Based on a set of criteria, these persons are rated on a risk scale, and the threats they pose are assessed. The tool assists in coming to a justified decision on the police measures to be taken and the appropriate use of the resources needed in each individual case and also considers protective factors and the tertiary prevention perspective.

Prevention and deradicalisation measures are an integral part of Germany's comprehensive approach to fight terrorism and radicalization. The Federal Government's core concern is to resolutely counter all anti-constitutional efforts and to further strengthen our democracy. This includes combating extremism as well as politically motivated crime. In accordance with the coalition agreement, the Federal Government has developed a new strategy with a comprehensive approach to reflect both repressive approaches by law enforcement agencies, police and intelligence authorities as well as preventive approaches to civic education, the promotion of democracy and the prevention of extremism. This strategy was published in May 2024. In 2025, the federal and state governments will continue to promote measures to prevent extremism of all kinds, including model projects and research. Depending on their target group and aim, measures in prevention and deradicalisation can have a broader national or regional approach (e.g. through civic education), or focus on local initiatives, or address specific fields of action (e.g. prison). The efforts are usually funded by federal and/or state authorities, build cooperation among all stakeholders and integrate state bodies' and civil society's expertise. Since the process of radicalisation differs in each individual case, there is no "one size fits all" solution: Holistic approaches in prevention and deradicalisation always account for regional and local specificities, as well as individual characteristics of the target groups / target persons. Throughout the country, counselling services for disengagement and exit-work with radicalised persons and counselling for persons seeking advice on how to deal with the situation (e.g. parents, teachers) as well as counselling for victims of extremist offences are being offered. In case of necessity, measures by the security agencies are integrated in the approach. In accordance with the Federal Government's holistic approach to prevention, a large number of measures aim at the prevention of group-related hate phenomena directed e.g. against Jews or Muslims, which are an integral part of extremist ideologies

This holistic approach also applies to the fight against Far Right Extremism, where counter measures do not necessarily presuppose the use of violence by extremist actors. This approach

is reflected in the Cabinet Committee's "Catalogue of Measures to Combat Far Right Extremism and Racism" of November 2020 and in the "Action Plan Against Far Right Extremism" of March 2022; a revised and extended follow-up strategy to the Action Plan was made public in February 2024. This plan includes repressive measures such as improving disarmament of extremists as well as preventive measures as for example extended civic education online and offline. The Federal Government's strategy for a strong and resilient democracy and an open and diverse society of May 2024 has also taken this into account.The German National Security Strategy and the Defence Policy Guidelines 2023 are addressing the terrorist threat. While the majority of the national defence against terrorism resides with civilian law enforcement, the defence against terrorism and hybrid threats is also listed as a core task of the German Bundeswehr. Operationalization of the Bundeswehr's core tasks within Germany will be addressed within the framework of the Operations Plan Germany (OPLAN DEU) as Germany's military National Defence Plan.

In 2017, Germany introduced a requirement for a basic security clearance under the Security Clearance Act for all soldiers scheduled to participate in weapons training for the first time. In 2022, this requirement was extended to reservists who are to be called up for military service. The goal is to exclude individuals with knowledge of terrorism and extremism from service in the armed forces and, in particular, to deny them access to war weapons and ammunition.

Since 2015, Germany has been involved - within the Counter-DAESH/Capacity Building Iraq (CD/CB-I) mandate – in the fight against the so-called Islamic State (Operation Inherent Resolve [OIR]) as well as advising and supporting the development of the Iraqi armed and security forces – within NATO Mission Iraq (NMI) - since 2020. The aim is to provide military support and long-term stabilisation through this complementary engagement. The intention is to continue the OIR contributions agreed with our partners and Iraq and to maintain the DEU contribution to NMI. In the long term, the DEU's involvement in Iraq will be readjusted when OIR ends, probably at the end of 2026.

In addition, a broad range of measures are undertaken in order to promote democratic attitudes and critical thinking among youth and young adults in terms of primary prevention as well as to strengthen social cohesion.

One of the Federal Government's core concerns is also to further strengthen our democracy and maintain our firm opposition to anti-constitutional activities. This includes combating extremism and other forms of hostility towards democracy and vulnerable communities of people. When implementing these strategies and measures, it is essential to keep the attention focused on both aspects: On the one hand, strengthening democracy from within by means of democratic involvement, civic, political and democratic education and prevention; and on the other hand, effectively combating threats to democracy.