Magyar Rendészet 2026/2. 205–232.
DOI: 10.32577/MR.2026.2.13

TERRORELHÁRÍTÁS

Current and Future Challenges of Terrorism

Krunoslav ANTOLIŠ,[1] Dániel RÉMAI[2]

Counterterrorism is a dynamic field focused on adapting to the evolving nature of terrorism and developing effective strategies to prevent and address these threats. As terrorism becomes more decentralised, utilising technologies like social media, cyber tools and lone-wolf attacks, it becomes increasingly difficult to track and combat. To counter this, strategies involve intelligence gathering, military operations, law enforcement coordination, and efforts to counter radicalisation, with new technologies such as surveillance and data analysis playing a significant role.

Current challenges include the rise of online extremism, difficulties in distinguishing between legitimate political actions and terrorism, and the instability in fragile or failed states. Looking ahead, the future of terrorism may see emerging threats such as cyberterrorism, the use of artificial intelligence in attacks, and the exploitation of global crises like pandemics or economic collapses by terrorist groups.

Ethical and legal concerns also complicate counterterrorism efforts, raising questions about privacy, potential discrimination, and the legality of actions like surveillance and drone strikes. Furthermore, terrorism increasingly intersects with global challenges such as climate change and migration, making it harder to address.

A successful counterterrorism approach requires a comprehensive strategy that blends military, law enforcement, diplomatic and ideological efforts, along with strong international cooperation. Ultimately, counterterrorism must remain flexible in the face of evolving threats while balancing security concerns with respect for human rights.

Aim: This paper aims to examine the evolving nature of contemporary terrorism and to assess how counterterrorism strategies must adapt to increasingly decentralised, technology-enabled threat environments. It seeks

[1] Full Professor, PhD, University of Applied Sciences in Criminal Investigation and Public Security, Police Academy "First Croatian Police Officer", Ministry of Internal Affairs, Republic of Croatia

[2] Assistant Lecturer, Ludovika University of Public Service, Law Enforcement Faculty, Counter Terrorism Department, e-mail: remai.daniel@uni-nke.hu

to identify key operational, technological, legal, and ethical challenges shaping current and future counterterrorism efforts.

Methodology: The analysis is based on a conceptual and strategic review of current counterterrorism practices and emerging threat trends. It integrates perspectives from security studies, law enforcement practice, technological development (e.g. surveillance systems, data analytics, artificial intelligence), and international governance frameworks. The approach is analytical and forward-looking, focusing on pattern identification rather than case-specific empirical analysis.

Value: The study highlights the structural transformation of terrorism – marked by decentralisation, online radicalisation, lone-actor dynamics and the growing relevance of cyber capabilities – and maps these changes onto existing counterterrorism architectures. It underscores critical tensions between security and civil liberties, particularly in relation to surveillance, data use, targeted operations and the legal classification of violent acts. By addressing emerging risks such as cyberterrorism, AI-assisted attacks, and the exploitation of systemic crises (e.g. pandemics, economic instability, fragile state environments), the paper contributes to a more integrated understanding of future threat trajectories. It also emphasises the increasing interconnection between terrorism and broader global stressors, including migration pressures and climate-related instability.

Conclusion: Effective counterterrorism requires a comprehensive and adaptive framework that integrates military capabilities, law enforcement coordination, intelligence sharing, diplomatic engagement and counter-radicalisation efforts. Long-term success depends on strong international cooperation and institutional flexibility in responding to technological and geopolitical shifts. At the same time, sustainable counterterrorism policy must carefully balance operational effectiveness with adherence to legal standards and the protection of fundamental rights.

Keywords: counterterrorism, radicalisation, technology, international cooperation, human rights

Introduction

The landscape of terrorism is continually evolving, presenting a range of new challenges and complexities for counterterrorism efforts. As terrorism adapts to global changes, counterterrorism strategies must be flexible, multifaceted and forward-looking. Here, we explore the evolving nature of terrorism, current challenges, future risks, and the comprehensive approaches needed to address these issues.

Terrorist organisations have increasingly leveraged modern technology to plan, execute and expand their activities. The internet, social media, and encrypted communication platforms have become essential tools for recruitment, propaganda and

coordination, significantly complicating counterterrorism efforts (Weimann 2015). These technologies offer both anonymity and global reach, allowing terrorist groups to operate with greater stealth and efficiency.

One of the most concerning developments is cyberterrorism, where terrorists exploit digital infrastructure to disrupt economies, attack critical infrastructure and spread fear. Cyberattacks against government and private sector systems, as well as the spreading of misinformation to manipulate public perception, are becoming more frequent (Lewis 2022). These new forms of digital warfare add another layer of complexity to traditional counterterrorism measures, demanding both technical expertise and international cooperation to combat effectively.

Moreover, terrorist organisations are no longer relying solely on large, centralised networks. The rise of lone-wolf attacks, where individuals inspired by extremist ideologies act independently or in small groups, has introduced a new dimension of unpredictability (Spaaij 2012). These attacks are difficult to detect and prevent because they often occur without prior warning or direct coordination with a formal terrorist group. Radicalisation plays a significant role in this shift. With the help of online platforms, terrorist organisations are targeting vulnerable individuals, particularly through social media and encrypted platforms, to incite violent actions (Neumann 2016).

Terrorism in the modern era has become more decentralised, tech-driven and unpredictable. The use of the internet, encrypted communication and cyberattacks, combined with the rise of lone-wolf terrorism, presents significant challenges to counterterrorism efforts (Cronin 2021). These trends require an integrated approach that combines traditional intelligence and law enforcement strategies with advanced technological tools and international collaboration.

The problem of definitions – Common background

The definition of terrorism has always been one of the most contentious aspects in both scholarly and practical terms. As noted in the works of Schmid, terrorism is not simply one-dimensional; it is inherently political, shaped by legal considerations and influenced by societal viewpoints. This multifaceted nature of the phenomenon makes it difficult to pinpoint a universally accepted definition. Various attempts at defining terrorism often reflect the political, social and historical contexts in which they are created. For instance, the political dynamics of a given state or international body frequently lead to definitions that suit specific geopolitical objectives or security concerns (Schmid 2004).

Moreover, as pointed out by scholars like Alexander Schmid and Bruce Hoffman, the fluidity and ideological baggage associated with defining terrorism are compounded by the evolving nature of its tactics and motivations. While there are some common elements – violence or the threat of violence intended to instil fear – the manifestations of terrorism can differ dramatically across time and space. The definition of terrorism remains in constant flux due to its complexity and the various interests that drive it. For instance, while some define terrorism based on the scale and intensity of violence (e.g. attacks on civilians), others may focus on the intentions behind the violence or the

status of the actors involved, such as non-state actors versus state-sponsored terrorism (Hoffman 2006).

For an in-depth analysis, references such as the works by Silke (2008) on terrorism research after 9/11, and the typologies proposed by Marie-Helen Maras in *Terrorism* (2016) provide valuable insights into the evolving frameworks of terrorist activities and their impact on policy formation.

Counterterrorism strategies and tools

Counterterrorism strategies require a multifaceted and coordinated approach that integrates intelligence gathering, international cooperation, military and police actions, legal frameworks and judicial processes. These efforts must be dynamic, adaptable and sensitive to the evolving nature of terrorist threats while ensuring the protection of civil liberties (Byman 2015).

This is how these components interact and enhance one another in the broader counterterrorism landscape.

Intelligence gathering and sharing

Intelligence is the cornerstone of effective counterterrorism. Comprehensive intelligence operations allow agencies to detect, monitor and preempt terrorist activities. This includes surveillance, human intelligence (HUMINT), signals intelligence (SIGINT) and cyber intelligence (CYBINT) (Hulnick 2004). The timely sharing of intelligence across borders and agencies is essential for identifying emerging threats, especially given that terrorism is often a transnational issue.

Using AI and machine learning to process massive amounts of data, helping to identify terrorist activity (Brynjolfsson–McAfee 2016).

Governments, military and intelligence agencies must ensure seamless sharing of intelligence, leveraging platforms like the EU's Secure Information Exchange or the Five Eyes alliance (U.S., U.K., Canada, Australia and New Zealand) (Aldrich 2009).

Tools like Interpol's secure global police network help synchronise real-time intelligence across borders (Interpol 2020).

International cooperation

Terrorism is no longer confined to local or national borders, making international cooperation indispensable. Transnational threats like ISIS, Al-Qaeda, and regional terror groups exploit weak state structures and cross-border connections, necessitating joint operations and information-sharing between countries (Gunaratna 2016).

- Global initiatives such as the United Nations Counter-Terrorism Implementation Task Force (CTITF) and the GCTF (Global Counterterrorism

Forum) foster collaboration between member states to create common standards and strategies for combating terrorism (United Nations 2011).
- Countries often form multinational task forces to undertake joint operations. This could involve coordinated military operations in one country to disrupt terrorist networks operating in others (Byman 2015).
- Countries enter into extradition agreements and harmonise anti-terrorism legislation to facilitate the arrest and prosecution of suspected terrorists internationally (Roach 2011).

Military and police actions

Counterterrorism operations typically involve both military force and domestic policing. Military action is often necessary when terrorist organisations control territory, while law enforcement agencies are crucial for disrupting cells, apprehending suspects, and preventing attacks at the community level (Hoffman 2006).
- Military and elite law enforcement units (e.g. U.S. Navy SEALs, British SAS, FBI's Hostage Rescue Team) conduct high-risk operations against terrorist leaders or cells. These units are specially trained in counterterrorism tactics, including hostage rescue, hostage negotiation and urban warfare.
- Used for targeting high-value individuals (e.g. drone strikes against terrorist leaders) and disrupting terrorist training camps or infrastructure, particularly in ungoverned spaces (Zenko 2015).
- Police efforts to build trust within communities to prevent radicalisation are essential. This includes intelligence gathering at the local level and counter-radicalisation programs aimed at disengaging individuals from extremist ideologies (Kundnani 2014).

Legal and judicial approaches

The legal framework surrounding counterterrorism must strike a delicate balance between ensuring national security and safeguarding individual rights. Effective counterterrorism legislation enables the prosecution of terrorists while respecting due process and civil liberties (Roach 2011). It is essential for legal systems to remain flexible and adapt to emerging tactics and threats.
- Laws must define terrorism clearly and allow for the detention, prosecution and sentencing of individuals involved in terrorist acts. These laws should be periodically updated to address emerging trends, like cyberterrorism or the use of drones in attacks (Scheinin 2016).
- Instruments like the International Convention for the Suppression of Terrorist Bombings and the UN Security Council Resolutions (e.g. Resolution 1373) lay the foundation for cooperation among states in combating terrorism (United Nations 2011).

- Countries must ensure that suspects are fairly tried in courts, using the evidence gathered while also respecting international human rights standards. Special terrorism courts can be used in certain cases to handle complex, high-profile cases (Roach 2011).

Coordination between agencies

The coordination between military, intelligence and law enforcement agencies remains crucial in tackling terrorism effectively. A fragmented approach, with insufficient sharing of data and resources, can lead to missed opportunities or even security lapses (Frey 2004).

- National counterterrorism centres (e.g. the U.S. National Counterterrorism Center) coordinate information and resources between various agencies (FBI, CIA, NSA, Homeland Security) to develop a unified operational response to threats (Byman 2015).
- Military, police and intelligence agencies should engage in regular joint exercises to practice coordinated responses to terrorist attacks, strengthening communication and operational efficiency (Hulnick 2004).
- In the modern era, the private sector, including tech companies and banks, must work closely with governments to combat financing of terrorism, prevent the use of social media for recruitment, and disrupt cyberterrorism (Biersteker–Eckert 2008).

Challenges in counterterrorism

The drive to prevent terrorism must not come at the cost of infringing on basic freedoms. Policies such as mass surveillance or indefinite detention without trial can alienate communities and foster resentment (Kundnani 2014).

- The nature of terrorism is evolving with new technologies (e.g. cyberattacks, drones), and so counterterrorism efforts must continuously adapt (Cronin 2021).
- A key element of long-term counterterrorism strategy is preventing individuals from becoming radicalised in the first place. This involves improving community relations, addressing grievances, and offering alternative pathways for those at risk (Neumann 2016).

A comprehensive counterterrorism strategy is not a static process but a dynamic system that blends military, legal and intelligence operations with international cooperation. Intelligence-sharing, legal frameworks, community engagement, and careful consideration of human rights form the backbone of these efforts (Byman 2015). The ongoing challenge lies in adapting to the constantly evolving nature of terrorism while ensuring a balanced

approach that safeguards both security and civil freedoms. Effective counterterrorism requires global cooperation, local action, and continuous adaptation to emerging threats.

Terrorism as part of hybrid threats

Terrorism is increasingly being understood as a key component of broader hybrid threats. Hybrid threats are complex and multidimensional, often combining conventional military tactics, non-state actors, cyberattacks, and other forms of subversive activity to destabilise states or societies (Laqueur 1996). These hybrid threats have blurred the lines between state and non-state actors and have increasingly involved not only direct military engagement but also information warfare, cyberattacks and financial warfare.

A significant aspect of these hybrid threats is the role of non-state actors, such as terrorist organisations, in using unconventional tactics that are combined with more traditional military strategies. For example, the rise of ISIS was not only a military insurgency but also a global ideological movement that utilised social media and cyber capabilities for recruitment and to spread its propaganda (Stern–Berger 2015). This makes terrorism a part of a wider strategy of destabilisation, in which traditional counterterrorism approaches may be insufficient.

In response, counterterrorism strategies must adapt to these hybrid threats, incorporating military, intelligence, diplomatic and cyber capacities in a coordinated effort. This hybridised approach is essential for countering the increasingly complex nature of modern terrorism.

Challenges in the current landscape

In the current counterterrorism landscape, the challenges are increasingly complex and multifaceted, shaped by globalisation, technological advances, and shifting dynamics in terrorism itself. These factors intertwine, creating an environment where combating terrorism requires a broad, nuanced approach.

Globalisation of terrorism

The rise of global terrorism networks has made it significantly harder to contain extremist groups. Organisations like ISIS and Al-Qaeda have demonstrated the ability to operate across borders, leveraging global networks to recruit, fund and execute attacks (Gunaratna 2016). Their decentralised structures, where leadership and operational cells are often dispersed across multiple regions, make it difficult for any single nation to effectively combat them. Moreover, the ideological appeal of these groups transcends geographical boundaries, creating a persistent and adaptable threat (Cronin 2021).

Effective counterterrorism requires seamless international cooperation in intelligence-sharing, military operations, and legal frameworks. Countries must work

together to disrupt these networks before they can cause significant harm, which can be complicated by political and diplomatic differences (Byman 2015).

The role of the internet

The internet has become both a weapon and a platform for terrorist groups. Terrorists can now use online spaces to spread radical ideologies, recruit followers, raise funds and plan attacks (Weimann 2015). Social media platforms, encrypted messaging services, and even the dark web provide terrorists with tools to operate with relative anonymity, making it difficult for authorities to track their activities. Governments and tech companies face immense pressure to balance freedom of speech with national security. Effective countermeasures must include technological tools to detect online radicalisation, monitor extremist content, and disable recruitment networks. However, this can raise concerns around privacy and censorship (Neumann 2016).

The changing face of terrorism

While groups like ISIS have lost much of their territorial control, their ideological influence continues to inspire a range of extremist movements, including those with domestic or localised focuses (Hoffman 2006). The decentralised nature of modern terrorism means that even if one group is weakened, others may emerge or be inspired by the same radical ideology, continuing the cycle of violence. The persistence of extremist ideologies poses a long-term threat that is not easily defeated by military or policing efforts alone. In many cases, individuals radicalise to violence independently or through small, loosely affiliated cells that are harder to track than traditional terrorist organisations (Spaaij 2012).

Hybrid threats

Terrorism is increasingly intertwined with other forms of criminal activity, such as organised crime, human trafficking and drug smuggling (Makarenko 2004). While the term "hybrid threats" effectively captures the complexity of this phenomenon, it is important to clarify its usage in this context. In security and defence literature, the concept is primarily associated with military and state-centric strategies. Here, however, it refers specifically to the crime–terror nexus: the structural and operational convergence between terrorist organisations and transnational criminal networks, through which illicit activities serve as sources of financing, logistical support and strategic expansion.

By blending terrorist operations with transnational crime, these groups become harder to dismantle, as they operate within entrenched criminal ecosystems and, in many contexts, benefit from permissive conditions such as weak governance and systemic corruption. While corruption is not universally present in every case, it frequently

functions as a structural enabler that facilitates the resilience and adaptability of crime–terror networks.

Combating terrorism requires addressing not just the terrorist organisations themselves but also the broader criminal enterprises that support them. Coordinated action involving multiple sectors – law enforcement, military and border security – is needed to tackle these hybrid threats effectively (Biersteker–Eckert 2008).

Radicalisation and recruitment

Radicalisation has become a major challenge, particularly as online platforms provide an open avenue for extremist ideologies to reach vulnerable individuals worldwide (Neumann 2016). Young people in unstable political environments or marginalised communities are often targeted by extremist groups promising purpose and belonging. Once radicalised, individuals may be recruited to join terrorist organisations or carry out attacks on their own. Effective counter-radicalisation programs are essential to prevent individuals from falling prey to extremist ideologies. This involves not only monitoring online activity but also addressing the root causes of radicalisation, such as social alienation, economic hardship and political instability (Kundnani 2014). Successful de-radicalisation requires engaging communities, promoting alternative narratives, and providing support to individuals before they make the leap into violent extremism.

The landscape of terrorism is increasingly global, digital, and intertwined with other criminal activities. As terrorist organisations evolve and adapt, so too must counterterrorism strategies. Governments need to employ multi-dimensional approaches that integrate military, intelligence, law enforcement and community-based efforts (Byman 2015). Tackling the root causes of radicalisation, enhancing international cooperation, improving cybersecurity, and dismantling criminal networks are all critical components in mitigating the evolving threat of terrorism in today's interconnected world.

Radicalisation – Vulnerable groups

Radicalisation remains one of the most challenging aspects of modern terrorism. Vulnerable groups, such as youth in conflict zones, marginalised communities, and those affected by social exclusion, are particularly at risk of becoming radicalised. As Laqueur (1996) emphasise, extremist groups exploit these vulnerabilities by offering a sense of purpose, identity, and belonging to those who feel alienated from mainstream society.

In many cases, radicalisation occurs through a combination of personal grievances and exposure to extremist ideologies, which can happen both offline and online. The internet has become an increasingly important tool for recruiters, who use social media platforms to reach individuals across the globe. Once individuals are exposed to these ideologies, the process of radicalisation can quickly escalate, with the promise of community, identity, and a sense of belonging being used as a powerful motivator.

Efforts to prevent radicalisation must address both the individual and the structural factors that contribute to it. This requires a multifaceted approach that includes education, community engagement, and the provision of alternative narratives to counter extremist ideologies.

Social awareness systems

Social awareness systems are essential tools for preemptively combating terrorism, particularly by addressing the root causes of radicalisation. These systems involve monitoring, education, and community engagement to prevent individuals from falling into extremist ideologies. According to Rémai (2020), such systems should not only identify at-risk individuals but also integrate interventions that promote social cohesion and resilience within communities.

One of the core functions of these systems is the use of data analytics and social media monitoring to identify early warning signs of radicalisation. Recent studies have highlighted the growing role of online platforms, where extremist groups use algorithms to target vulnerable individuals and radicalise them (Schmid 2004). Moreover, social awareness programs, such as community outreach and educational initiatives, help mitigate the appeal of extremist ideologies by offering alternatives and fostering critical thinking.

To be effective, social awareness systems must involve not only government bodies but also local organisations, religious leaders, and educators in creating a unified approach that prevents extremism. Furthermore, addressing underlying social issues such as economic disparity and political marginalisation is crucial to reducing the appeal of terrorist ideologies.

Future challenges in counterterrorism

The future of counterterrorism will be shaped by an evolving landscape of technological advancements, geopolitical instability, environmental challenges and deepening social divides. As terrorist groups continue to adapt and leverage new tools, counterterrorism efforts will need to innovate and address a broad spectrum of emerging threats. In the following, an integrated view of these future challenges is presented.

Technological advancements and dual-use technologies

Artificial Intelligence (AI), Automation and Drones are rapidly becoming both a tool for terrorists and a countermeasure for agencies involved in counterterrorism (Lewis 2022). While these technologies offer new opportunities for intelligence gathering and operational efficiency, they also present new risks as terrorist groups increasingly exploit them for malicious purposes.

- Terrorist groups may use AI-driven algorithms to enhance their recruitment strategies. By analysing data from social media and online behaviours, AI can identify vulnerable individuals and tailor radicalising content to manipulate them more effectively (Brynjolfsson–McAfee 2016).
- Terrorists could use drones for reconnaissance, surveillance and even carrying out attacks, especially in urban environments where targeting is more precise (Zenko 2015). At the same time, counterterrorism agencies are adopting drones for surveillance, intelligence gathering and airstrikes against high-value targets.
- The potential of AI in cyber warfare is growing, and terrorist groups may begin to employ automated cyber tools to conduct large-scale attacks on critical infrastructure, financial systems, or government networks (Lewis 2022). As such, cybersecurity becomes a primary concern, with both terrorists and counterterrorism agencies engaging in an arms race of technology.

Challenge: Adapting counterterrorism strategies to emerging tech

Counterterrorism agencies must stay ahead of these technological advances by integrating AI and automation into their own operations, while also enhancing cyber defence capabilities. This will require new laws, regulations and partnerships between governments, tech companies, and international bodies to manage the dual-use nature of these technologies (Brynjolfsson–McAfee 2016).

Biological and chemical weapons threat

The potential for terrorist groups to develop or deploy biological, chemical, or radiological weapons represents one of the most terrifying and complex threats in the future counterterrorism landscape (Ackerman 2018). These weapons could cause mass casualties, widespread panic and long-term environmental damage, making them a priority for counterterrorism efforts.

- The increasing sophistication of biotechnology, including CRISPR (Clustered Regularly Interspaced Short Palindromic Repeats) and synthetic biology, may give terrorist groups the ability to engineer biological agents for use in attacks. The risks associated with these technologies are exacerbated by the growing difficulty of tracing their origins (Tucker 2018).
- While less advanced groups may lack the capability for biological attacks, chemical weapons (e.g. sarin gas) and radiological devices (so-called "dirty bombs") remain within the reach of some extremist organisations (Ackerman 2018).

Challenge: Preparedness and response to bio-chemical threats

To address these threats, counterterrorism efforts will require specialised biosecurity and chemical security initiatives, international cooperation in tracking dual-use technologies, and improvements in emergency response and detection systems (Tucker 2018). Cross-sector collaboration between public health, environmental and law enforcement agencies will be key in mitigating these risks.

Political instability and extremism

Political and social divisions, especially in regions with weak governance or entrenched corruption, remain a fertile ground for the growth of terrorist groups (Hoffman 2006). Terrorist organisations often exploit political instability to recruit followers and build support, especially in failed states or areas with deep social grievances.

- As governments struggle to maintain authority in fragmented or collapsing states, terrorist groups can easily fill the void, gaining control of territory and resources. Areas of fragile states like Afghanistan, Syria and parts of Africa, where governance is weak or absent, continue to be breeding grounds for extremism (Gunaratna 2016).
- Socio-political polarisation, identity conflicts and ethnic/religious tensions can fuel radicalisation and increase the appeal of extremist ideologies (Kundnani 2014).

Challenge: Addressing root causes of terrorism

Long-term counterterrorism strategies must address the underlying political, economic and social factors that enable terrorism to thrive. This requires conflict resolution, humanitarian aid, strengthening institutions and promoting inclusive governance (Byman 2015). Without addressing the root causes of instability, counterterrorism will remain a reactive rather than a proactive strategy.

Preventing radicalisation

Radicalisation remains one of the most challenging aspects of modern counterterrorism. While terrorist organisations may be weakened militarily, the ideological appeal of their messages continues to spread, often through the internet (Neumann 2016). Young, disenfranchised individuals in unstable regions or marginalised communities are especially vulnerable to recruitment by extremist groups.

- The use of social media to spread propaganda and foster ideological polarisation makes it increasingly difficult to counter radicalisation. Algorithms designed to

maximise engagement often push individuals toward extreme content, amplifying radical views (Weimann 2015).
- Communities experiencing economic hardship, political oppression, or social alienation are often prime targets for radicalisation (Kundnani 2014).

Challenge: Long-term community engagement and de-radicalisation

Counter-radicalisation strategies must focus on community-based initiatives, education, economic development and mental health support to address the factors that drive people to extremism (Neumann 2016). Effective de-radicalisation programs will require both domestic and international cooperation, as well as the active involvement of local communities, educators and religious leaders.

Climate change and terrorism

The climate crisis is an emerging and complex driver of conflict, which could exacerbate terrorism in regions already prone to instability (Mach et al. 2019). Climate-induced resource scarcity, displacement and migration may increase competition over resources and contribute to existing grievances, making regions more susceptible to extremist ideologies.
- Droughts, floods and other climate events can devastate agricultural economies, leading to poverty, displacement and competition for limited resources. This, in turn, may create fertile ground for terrorist recruitment, particularly in already unstable regions (Mach et al. 2019).
- Climate change-induced migration may contribute to social tensions and create opportunities for extremist groups to exploit vulnerable displaced populations (Mach et al. 2019).

Challenge: Integrating climate and security strategies

Future counterterrorism strategies must integrate environmental considerations, including adaptation to climate impacts, into security frameworks. Governments will need to address climate-induced migration, promote sustainable development, and prevent the exploitation of climate crises by extremist groups (Mach et al. 2019).

The future of counterterrorism is one of complex, interconnected challenges that span technological, environmental, political and social domains. While advancements in AI, drones and cyber capabilities offer new opportunities for tracking and preventing terrorist activities, they also open new vulnerabilities that terrorists may exploit (Lewis 2022). At the same time, geopolitical instability, the threat of biological and chemical weapons, and the deepening social and political divisions in certain regions will demand holistic, proactive approaches that go beyond traditional military and law enforcement tactics

(Byman 2015). To address these challenges, counterterrorism strategies must evolve to be more comprehensive, adaptive and cooperative. This will require global collaboration, innovation in technology, integrated environmental and security policies, and long-term efforts to address the root causes of extremism and instability (Cronin 2021). Balancing security with human rights, addressing climate impacts, and using technology responsibly will be critical in shaping an effective and sustainable counterterrorism future.

Foreign terrorist fighters and their relatives (women and children)

The issue of Foreign Terrorist Fighters (FTFs) and their families, particularly women and children, is increasingly significant in the context of modern terrorism. FTFs are individuals who travel abroad to engage in conflicts and participate in terrorist activities. While much attention has been given to the fighters themselves, less attention has been focused on the women and children who accompany them or are left behind when these fighters are captured or killed.

Women's roles within terrorist organisations have evolved in recent years. While traditionally women were seen as passive supporters, many have taken on more active roles, including as recruiters, logisticians, or even combatants. As noted by Silke (2008), the recruitment of women and children is increasingly a part of the broader strategy of terrorist organisations to build support networks and spread extremist ideologies.

The challenge of reintegrating FTFs and their families, particularly women and children, into society is complex. It requires an approach that balances justice with rehabilitation and reintegration. This is further complicated by the legal and social implications of returning these individuals to their home countries, where they may be viewed as a security threat. Programs aimed at reintegration must therefore address not only the security risks but also the social and psychological issues involved.

Ethical, legal concerns, and human rights issues

The intersection of counterterrorism efforts with ethical, legal and human rights concerns is one of the most challenging aspects of modern security policy. As counterterrorism measures become more sophisticated and widespread, they frequently raise significant questions about civil liberties, human rights, international law and the use of force. Finding the balance between securing national safety and upholding individual freedoms remains a critical dilemma for governments and international bodies alike. This is how these issues are interwoven and present challenges for counterterrorism strategies.

Human rights and civil liberties

Counterterrorism measures, such as mass surveillance, detention without trial and targeted killings, often raise concerns about the erosion of fundamental human rights

(Scheinin 2016). Governments face difficult choices between protecting citizens from terrorist threats and ensuring that their measures do not undermine the very freedoms they aim to protect.

- To detect and prevent terrorist plots, many countries have implemented expansive surveillance systems that monitor communications, internet usage and public spaces. While these systems can enhance security, they also risk infringing on privacy rights (Lyon 2015). The question arises: where should the line be drawn between security and personal freedom?
- In some cases, individuals suspected of terrorist activities may be detained without due process, often for extended periods. This can lead to arbitrary detention or violations of the right to a fair trial and presumption of innocence (Amnesty International 2021). Guantanamo Bay has been a highly controversial example of such practices.
- Counterterrorism measures can sometimes lead to the profiling of individuals based on race, religion, or ethnicity, which raises concerns about discrimination and stigmatisation. For instance, certain Muslim communities may disproportionately face suspicion due to their religion or cultural background, fuelling further alienation and resentment (Kundnani 2014).

Challenge: Balancing security and human rights

Counterterrorism efforts need to carefully consider human rights protections, ensuring that measures like surveillance or detention do not violate international human rights standards. Governments must develop transparent and accountable systems that protect citizens' rights while allowing for effective security measures (Roach 2011).

Civil liberties vs. security

The age-old debate between civil liberties and national security intensifies in the realm of counterterrorism. After significant terrorist attacks (e.g. 9/11, the Paris attacks), there is often public pressure to enhance security measures, even at the expense of individual freedoms (Bigo 2008). However, excessively stringent security measures can erode trust between the government and its citizens.

- Laws like the Patriot Act in the U.S. expanded government surveillance capabilities, allowing agencies like the NSA to track phone calls, emails and internet activity of individuals, often without a warrant. This, in turn, raised concerns about privacy rights and the potential for mass data collection on innocent people (ACLU 2020).
- National security laws sometimes grant authorities the power to conduct searches and seizures without probable cause or warrants, an approach that undermines the constitutional protections of citizens, especially in democratic societies (Roach 2011).

Challenge: Finding the right balance

Counterterrorism policies must be designed in such a way that they enhance security without overstepping the bounds of individual freedom. Oversight and accountability mechanisms, such as independent review boards, judicial oversight and public transparency, are essential to ensure that civil liberties are not sacrificed for the sake of security (Scheinin 2016).

International law and cooperation

International law plays a critical role in defining the scope of terrorism, establishing frameworks for cooperation between countries, and setting standards for the use of force (Bassiouni 2001). However, the global nature of terrorism complicates legal frameworks because countries have different legal systems, definitions of terrorism and approaches to justice.

- Countries with divergent legal traditions (e.g. common law vs. civil law systems) may have different approaches to counterterrorism, which can lead to inconsistencies in how suspects are treated and prosecuted. The extradition of terrorism suspects can become contentious when a country's legal framework does not align with the demands of the requesting state (Roach 2011).
- International law lacks a single, universally accepted definition of terrorism, which complicates efforts to develop a cohesive global strategy. For example, some groups considered freedom fighters in certain countries may be labelled as terrorists by others, leading to political friction (Bassiouni 2001).
- Terrorism often crosses borders, and international cooperation – through organisations like Interpol, the United Nations and bilateral agreements – remains essential. However, this is hindered by issues of sovereignty, conflicting national interests and varying levels of political will (Byman 2015).

Challenge: Creating a cohesive global framework

To effectively address terrorism on a global scale, international law must evolve. This includes harmonising definitions of terrorism, creating more effective extradition and mutual legal assistance treaties, and developing international conventions to govern counterterrorism operations and prevent abuses of power (Bassiouni 2001).

The use of force in counterterrorism operations

Military force is often used in counterterrorism efforts, particularly in conflict zones or areas where terrorist groups hold territorial control (e.g. Syria, Afghanistan). While force

may be necessary to eliminate terrorist threats, it raises significant ethical and legal issues, especially when civilians are caught in the crossfire (Zenko 2015).

- In the pursuit of terrorist leaders or groups, counterterrorism operations often lead to collateral damage, including civilian deaths and injuries. Drone strikes, air raids and ground operations can inadvertently kill innocent people, which can fuel resentment and radicalisation among affected populations (Cronin 2021).
- The targeted killing of terrorist leaders is a controversial practice. While proponents argue that it eliminates imminent threats, critics assert that it circumvents due process and international law, particularly the right to a fair trial (Alston 2010).
- In conflict zones, counterterrorism actions can disrupt vital infrastructure, including healthcare, education and humanitarian assistance, exacerbating the suffering of civilians caught in the conflict (Human Rights Watch 2020).

Challenge: Minimising harm while achieving security

The ethical and legal challenge is to use military force in a way that minimises harm to civilians and adheres to international humanitarian law (IHL). This requires improved intelligence, more precise targeting, and post-strike assessments to ensure that operations comply with the principle of distinction (separating combatants from civilians) and proportionality (avoiding excessive use of force) (Alston 2010).

Ethical dilemmas in counterterrorism

As counterterrorism strategies evolve, they often raise ethical dilemmas about the extent to which the government can curtail individual freedoms for the sake of security. These dilemmas involve balancing the moral imperative to protect citizens from terrorism with the ethical obligation to respect human rights (Ignatieff 2004).

- The use of enhanced interrogation techniques (torture) to extract information from detainees is widely condemned under international law but has been used by some governments in the name of national security. The ticking bomb scenario – where torture is justified as a means to prevent an imminent attack – remains highly controversial and raises moral questions about the limits of state power (Sussman 2005).
- Governments must remain transparent in their counterterrorism operations and be held accountable for abuses of power. Lack of oversight can lead to human rights violations, such as unlawful detentions, disappearances and extrajudicial killings (Amnesty International 2021).

Challenge: Ethical frameworks for counterterrorism

Counterterrorism agencies need to adhere to international human rights standards and ethical frameworks that prioritise non-violent, legal methods of countering terrorism. This requires promoting accountability, ensuring due process, and fostering public trust in the security sector (Ignatieff 2004).

The challenge of balancing effective counterterrorism measures with human rights protections is one of the most pressing issues in contemporary security policy. While the threats posed by terrorism are real and urgent, counterterrorism strategies must be implemented in a way that does not undermine the very freedoms they aim to protect (Scheinin 2016). This requires a constant and nuanced balance between national security and civil liberties, guided by international law and ethical principles.

Governments must navigate these challenges carefully, engaging in transparent and accountable policies, upholding human rights and minimising harm. Collaborative, multilateral frameworks for international cooperation and the use of force are essential for ensuring that counterterrorism efforts do not inadvertently fuel further extremism or undermine global stability (Byman 2015).

Counterterrorism in the context of multiple crises

The challenge of counterterrorism becomes even more complex when considered within the broader context of multiple, interconnected global crises. Issues such as refugee crises, economic instability, and the war on drugs create environments that can foster the rise of terrorism, while also compounding the difficulty of effectively addressing it (Gunaratna 2016). Additionally, terrorism increasingly intersects with other global security threats, including organised crime, drug trafficking and human trafficking. This convergence necessitates a holistic approach to security that addresses the root causes of instability and integrates responses to multiple challenges simultaneously. In the following, an integrated view of how these crises and threats intersect with counterterrorism efforts is presented.

Impact of other global crises on terrorism

Various ongoing crises exacerbate the conditions that enable terrorism to flourish, particularly in regions already vulnerable due to weak governance, political instability, or economic hardship (Cronin 2021).

- The displacement of millions due to conflict, climate change and persecution often creates uncontrolled environments where terrorism can thrive. Refugee camps and urban areas with high populations of displaced people can become breeding grounds for radicalisation (Haider 2014). Terrorist organisations exploit the vulnerabilities of refugees, offering ideological support, recruitment, or logistical assistance to individuals who feel marginalised or abandoned by their host countries.

- Economic hardship, rising unemployment and wealth inequality provide fertile ground for extremism. In countries where economic opportunities are scarce, disillusioned youth may turn to terrorism as a means of empowerment or as an alternative to poverty (Piazza 2011). The global economic downturns and austerity measures often exacerbate these vulnerabilities, leading to frustration and anger, which radical groups can exploit.
- In many regions, the drug trade intersects with terrorism. For example, groups like the Colombian FARC or Mexico's drug cartels have been involved in terrorist activities, financing their operations through illicit drug trafficking (Makarenko 2004). Areas where law enforcement is weak or corrupt become zones of criminal impunity, where both terrorist and criminal organisations operate freely.

Challenge: Creating stability in fragile contexts

Counterterrorism efforts must be adapted to address these multiple crises in tandem. This requires strategies that integrate humanitarian relief, economic development and good governance with security measures to ensure that terrorist organisations do not exploit vulnerabilities created by other global challenges (Gunaratna 2016).

Intersection of terrorism with other global threats

Terrorism today no longer exists in isolation; it often intersects with other major threats, including organised crime, drug trafficking and human trafficking (Makarenko 2004). These threats operate in parallel, and addressing them in a fragmented way is ineffective. A more comprehensive and multi-dimensional approach is necessary.

- The relationship between terrorist groups and organised crime is becoming more pronounced. Terrorist organisations often engage in illicit activities to fund their operations, including smuggling, extortion and human trafficking (Biersteker–Eckert 2008). In some cases, groups that started as criminal organisations have transformed into fully-fledged terror groups (e.g. ISIS's involvement in smuggling oil and weapons). In return, criminal networks gain from the protection and resources that terrorism offers, creating a feedback loop of violence and instability.
- The global drug trade provides a significant source of funding for terrorist groups. For instance, in Afghanistan, the Taliban profits from opium production, using the proceeds to fund its insurgency before 2021 (UNODC 2021). Similarly, groups operating in Latin America often work in tandem with drug cartels, using drug trafficking routes to smuggle fighters, weapons and resources.
- Human trafficking, particularly sex trafficking and the exploitation of migrants, intersects with terrorism in a variety of ways. Terrorist groups may engage in

human trafficking to raise funds or recruit fighters (Shelley 2014). For instance, some groups use trafficking networks to smuggle women and children for exploitation, creating additional security and humanitarian challenges.

Challenge: Coordinated, multi-sectoral approaches

Tackling the intersection of terrorism with other global threats requires a multi-agency, cross-border approach. This means coordinating counterterrorism measures with law enforcement, border control, humanitarian and development aid, as well as public health initiatives (Biersteker–Eckert 2008). The focus must not just be on countering terrorism but also on tackling the root causes of organised crime, drug trafficking and human trafficking, which often provide terrorists with the means to operate.

Governance gaps and weak states as enablers of terrorism

Weak governance or failed states are often the backdrop against which terrorism flourishes (Hoffman 2006). These states are particularly vulnerable to the convergence of multiple crises, as they lack the capacity to maintain law and order or to respond to humanitarian, economic, or security challenges.

- In countries with weak institutions or corrupt leadership, terrorist groups often fill the power vacuum by providing basic services, controlling territory and enforcing their own laws (Gunaratna 2016). Somalia, Syria and Afghanistan are examples of how state fragility can provide an environment in which terrorist groups operate with impunity, consolidating control and attracting new recruits.
- Ongoing conflicts create environments where terrorist groups can gain influence. The Syrian civil war, for example, provided fertile ground for groups like ISIS to grow by exploiting chaos and territorial disputes (Cronin 2021). In these environments, terrorist groups can recruit from displaced populations and create alliances with local criminal or militia groups.

Challenge: Building resilient states

Counterterrorism strategies must include statebuilding and institutional strengthening in fragile states. This involves promoting governance reforms, building security sector capacity, and ensuring rule of law to prevent terrorist groups from exploiting weak states (Hoffman 2006). Furthermore, peacebuilding and conflict resolution strategies must be integrated into counterterrorism approaches to address the underlying causes of instability.

Holistic security strategies

Given the convergence of terrorism with other global threats, the future of counterterrorism must focus on holistic security strategies that address not just the terrorist threat but the broader environment in which terrorism thrives (Byman 2015).

- Providing support to displaced populations through refugee aid, food security and healthcare can reduce the vulnerabilities that terrorists exploit (Haider 2014). Refugee camps, for instance, are often the primary targets for recruitment, and addressing basic needs can mitigate radicalisation risks.
- Tackling economic instability through job creation, education and entrepreneurship can reduce the appeal of terrorism (Piazza 2011). Effective economic governance in post-conflict or fragile states can provide an alternative to terrorist ideologies by improving the quality of life for marginalised communities.
- Combating the overlap between terrorism and organised crime requires stronger border security, more effective intelligence sharing and cross-border cooperation (Makarenko 2004). Smuggling and trafficking often rely on porous borders, so improving security cooperation between states is essential to disrupt the flow of weapons, drugs and people.

Challenge: Comprehensive and coordinated global responses

Global counterterrorism efforts must be holistic, integrating security with humanitarian, economic and governance interventions (Byman 2015). This requires improved cooperation between countries, international organisations, non-governmental organisations and local communities. Effective multilateral approaches and conflict-sensitive strategies are necessary to address the complex interplay of terrorism, organised crime and global crises.

In the context of multiple global crises, counterterrorism must move beyond a purely security-focused approach. Terrorism is not an isolated threat; it is deeply intertwined with economic instability, refugee crises, organised crime and human trafficking (Gunaratna 2016). To effectively combat terrorism, we must address the broader environment in which it thrives, integrating humanitarian aid, economic development, governance reforms and peacebuilding into counterterrorism strategies. A holistic approach is essential: one that does not just fight terrorism but also tackles the root causes of instability, addresses the needs of vulnerable populations, and promotes sustainable development (Cronin 2021). Only by linking counterterrorism with broader global efforts can we hope to prevent terrorism from thriving amidst the multiple crises facing the world today.

Comprehensive approaches to counterterrorism

A comprehensive approach to counterterrorism integrates multiple strategies across various sectors, emphasising not only direct security measures but also addressing the underlying causes of terrorism, improving international cooperation, and utilising the latest technological innovations. These elements must work together to create an adaptive, multi-dimensional framework that addresses both the symptoms and the root causes of terrorism (Byman 2015). This is how these approaches can be integrated effectively.

Preventive measures: Addressing root causes of terrorism

A proactive, preventive approach is essential to combat terrorism at its core. Rather than solely focusing on the aftermath of attacks, this strategy targets the underlying factors that fuel extremism, such as poverty, inequality and political disenfranchisement (Cronin 2021).

- Poverty, lack of opportunity and social exclusion are powerful drivers of radicalisation. Creating economic opportunities, improving access to education and promoting social inclusion can mitigate the conditions in which extremist ideologies take root (Piazza 2011). In areas with high levels of unemployment or economic instability, individuals may turn to terrorism as a way to gain influence or provide for their families.
- In many cases, individuals join extremist groups because they feel politically marginalised or oppressed. Political reform, good governance and the promotion of democratic values are essential to reduce this disenfranchisement (Gunaratna 2016). Ensuring that all communities have a voice in political processes can help prevent radicalisation driven by a sense of injustice or lack of representation.
- De-radicalisation programs, alongside education, community engagement and mentorship, can provide alternatives to extremist ideologies (Neumann 2016). Schools, youth programs and community centres can serve as environments where vulnerable individuals are exposed to counter-narratives that challenge extremist propaganda.

Challenge: Long-term commitment to societal transformation

These preventive measures require sustained investments in long-term development and inclusive policies. However, their effectiveness may take time to materialise, necessitating patience and consistent political will (Cronin 2021).

Intelligence sharing and international cooperation

Terrorism is a global phenomenon, with terrorist networks often operating across national borders. To combat this transnational threat effectively, international cooperation and intelligence sharing are indispensable (Byman 2015).

- Terrorism often involves cross-border activities, such as funding, training and movement of operatives. Countries must work together to share critical intelligence, conduct joint operations and coordinate responses to prevent attacks (Aldrich 2009). Multilateral organisations like the United Nations, Interpol and Europol play an essential role in facilitating international collaboration.
- Modern terrorism operates quickly and across multiple platforms, so real-time intelligence sharing is vital. The integration of data analytics, AI and cyber capabilities allows countries to share and process large volumes of information rapidly to detect threats before they materialise (Brynjolfsson–McAfee 2016).
- Countries must collaborate on counterterrorism operations, including military action, police operations and cybersecurity initiatives. Joint task forces can pool resources, intelligence and expertise to dismantle terrorist organisations effectively (Gunaratna 2016).

Challenge: Overcoming legal and political barriers

While intelligence sharing and cooperation are essential, countries must overcome significant legal, political and cultural differences to collaborate effectively. Issues related to sovereignty, jurisdiction and data privacy can hinder international cooperation and must be addressed through treaties and mutual agreements (Roach 2011).

Community-based approaches: Building local resilience

A critical component of counterterrorism is community-based engagement. Terrorism thrives in environments where communities are fragmented, isolated, or distrustful of authorities. Engaging local communities can help to prevent radicalisation and create a more resilient society (Kundnani 2014).

- Working with local leaders, civil society organisations and youth groups can help build trust between communities and security agencies. Local leaders, whether religious, tribal, or civic, can be instrumental in influencing behaviour and deterring radicalisation by promoting messages of peace, tolerance and coexistence (Neumann 2016).
- Communities are often the first to notice signs of radicalisation. Training local educators, social workers and community leaders to identify warning signs – such as social withdrawal, adoption of extremist views, or involvement in

violent activities – can lead to early intervention before individuals become fully radicalised (Kundnani 2014).
- Offering alternative pathways – such as employment, education and social engagement programs – can give individuals a sense of purpose and belonging, reducing the appeal of extremist groups (Piazza 2011). Successful counterterrorism strategies rely on empowering communities to take an active role in preventing radicalisation.

Challenge: Building trust in vulnerable communities

In areas where government presence is weak or distrust between communities and authorities is high, building effective community-based counterterrorism initiatives can be difficult. Counterterrorism strategies must be culturally sensitive and inclusive to avoid alienating the very communities they aim to protect (Neumann 2016).

Technology and innovation: Leveraging cutting-edge tools

As technology continues to evolve, it presents both new opportunities and challenges in the fight against terrorism. Counterterrorism agencies must leverage the latest innovations to enhance their operations and stay ahead of increasingly sophisticated terrorist tactics (Lewis 2022).
- Artificial intelligence (AI) and data analytics can revolutionise counterterrorism by enabling agencies to analyse vast amounts of data for patterns indicative of terrorist activity (Brynjolfsson–McAfee 2016). Machine learning algorithms can be used to predict potential attacks, track the financing of terrorism and monitor communication networks for extremist content. AI tools can also help in facial recognition and biometric identification to identify suspects across borders.
- As terrorism increasingly shifts to the digital realm, counterterrorism agencies must invest in advanced cybersecurity measures to disrupt terrorist operations. This includes monitoring online platforms for propaganda, recruitment and fundraising, and working to prevent terrorists from using encrypted communication or dark web resources for planning attacks (Weimann 2015).
- Drones are becoming an increasingly important tool in the counterterrorism toolkit, enabling agencies to gather intelligence, monitor terrorist camps and track the movements of suspects in real time (Zenko 2015). Similarly, satellite surveillance and internet monitoring are vital in preventing terrorist groups from moving undetected across borders or territories.

Challenge: Ethical and privacy concerns

The use of advanced technologies, particularly in surveillance and data collection, raises privacy and ethical concerns. Governments must balance the need for security with the protection of civil liberties, ensuring that the technology is used responsibly and that there is oversight to prevent abuse (Lyon 2015).

Integrating these approaches: A unified strategy

To develop a comprehensive counterterrorism strategy, it is crucial to integrate these elements into a unified approach that maximises the strengths of each (Byman 2015):

1. *Preventive measures* must address the root causes of terrorism, such as poverty and inequality, while community-based approaches foster local resilience and trust-building.
2. *International cooperation and intelligence sharing* should be paired with cutting-edge technology to ensure real-time, effective counterterrorism actions.
3. *All strategies* must emphasise collaboration and coordination – not just between national agencies but across borders, between civil society, local communities, international bodies and the private sector.

Challenge: Sustaining efforts in the long-term

Achieving long-term success in counterterrorism requires patience, resources and sustained commitment. Preventive measures take time to show results, and cooperation across sectors and nations requires the continuous effort to build trust, overcome political challenges and adapt to evolving threats (Cronin 2021).

By integrating these strategies, governments and agencies can create a dynamic, multi-layered response that not only disrupts terrorist activities but also addresses the underlying vulnerabilities that terrorists seek to exploit.

Conclusion

Counterterrorism remains an ever-evolving and multifaceted challenge that requires an adaptable, coordinated approach across a wide array of sectors, including governmental, military, law enforcement and civil society (Byman 2015). As the nature of global terrorism continues to shift – fuelled by technological advancements, political changes and the intersections with other global crises – counterterrorism efforts must evolve in tandem to remain effective. The future of counterterrorism will rely heavily on innovation, strategic foresight, and an ongoing commitment to understanding and responding to emerging threats, while simultaneously balancing national security concerns with the protection of civil liberties and democratic values (Scheinin 2016).

The ever-changing nature of terrorism, including its adaptation to new technologies and geopolitical shifts, presents both new opportunities and new risks for counterterrorism agencies. From cyberterrorism and AI-driven recruitment to biological threats and hybrid warfare, the strategies and tools employed by terrorist groups are constantly evolving (Lewis 2022). To effectively counter these threats, counterterrorism policies must remain flexible, proactive and able to adapt to new forms of radicalisation and violence, especially as terrorists use increasingly sophisticated methods.

As counterterrorism strategies evolve, they must strike a delicate balance between securing the nation and preserving the freedoms that form the cornerstone of democratic societies. Human rights and civil liberties must not be sacrificed in the pursuit of security (Roach 2011). The challenge, therefore, is to develop counterterrorism measures that uphold democratic values while remaining effective in neutralising the threats posed by terrorism.

Given the dynamic nature of the global security landscape, counterterrorism policies must be comprehensive, adaptive and cooperative (Byman 2015). These efforts require a combination of preventive measures, such as addressing the root causes of terrorism (e.g. poverty, inequality, disenfranchisement), along with security measures like intelligence sharing, joint operations and military action. Effective counterterrorism will also rely heavily on international partnerships, as terrorism is increasingly a global problem that transcends national borders.

Moreover, long-term strategies focused on community engagement, education, de-radicalisation and humanitarian support will be crucial in addressing the underlying drivers of extremism (Neumann 2016). It is essential to engage with local communities and global networks to build resilience, foster cooperation and ensure that terrorism does not thrive in environments of political instability, social alienation, or economic despair.

This broad, integrated view of counterterrorism challenges must be tailored to specific contexts depending on region, type of terrorism and available resources. Whether dealing with domestic extremism, foreign insurgencies, or transnational networks, a flexible approach that can be adapted to local realities is key to success (Gunaratna 2016). A nuanced understanding of these dynamics, along with a framework that is responsive to changing threats, is essential for future counterterrorism efforts.

Future discussions on counterterrorism should focus on analysing current trends, assessing successful strategies and considering future scenarios. These discussions should be informed by ongoing developments in technology, global politics and security threats, and they should prioritise cooperation among all stakeholders – governments, international bodies, the private sector and civil society (Cronin 2021).

Ultimately, counterterrorism will require not just military and intelligence actions but a holistic approach that integrates prevention, community engagement and international collaboration. By adopting such an integrated strategy, the global community can more effectively address the multifaceted nature of terrorism, reduce its appeal, and work toward a safer, more stable world (Byman 2015).

References

Ackerman, Gary A. (2018): Chemical, Biological, Radiological and Nuclear (CBRN) Terrorism. In Silke, Andrew (ed.): *Routledge Handbook of Terrorism and Counterterrorism.* London: Routledge, 240–252. Online: https://doi.org/10.4324/9781315744636-21

ACLU (2020): *Surveillance under the Patriot Act.* American Civil Liberties Union. Online: www.aclu.org/surveillance-under-the-patriot-act

Aldrich, Richard J. (2009): Global Intelligence Co-operation versus Accountability: New Facets to an Old Problem. *Intelligence and National Security,* 24(1), 26–56. Online: https://doi.org/10.1080/02684520902756812

Alston, Philip (2010): *Report of the Special Rapporteur on Extrajudicial, Summary, or Arbitrary Executions.* United Nations Human Rights Council. Online: https://digitallibrary.un.org/record/683892/files/A_HRC_14_24_Add.2-EN.pdf?ln=en

Amnesty International (2021): *Guantanamo Bay: A Human Rights Scandal.* Online: www.amnesty.org/en/wp-content/uploads/2021/08/amr511592006en.pdf

Bassiouni, Cherif M. (2001): *International Terrorism. Multilateral Conventions (1937–2001).* Ardsley: Transnational Publishers. Online: https://doi.org/10.1163/9789004478428

Biersteker, Thomas J. – Eckert, Sue E. (2008): *Countering the Financing of Terrorism.* London: Routledge. Online: https://doi.org/10.4324/9780203944639

Bigo, Didier (2008): Globalized (In)Security: The Field and the Ban-Opticon. In Bigo, Didier –Tsoukala, Anastassia (eds.): *Terror, Insecurity and Liberty. Illiberal Practices of Liberal Regimes after 9/11.* London: Routledge, 10–48. Online: https://doi.org/10.4324/9780203926765

Brynjolfsson, Erik – McAfee, Andrew (2016): *The Second Machine Age. Work, Progress, and Prosperity in a Time of Brilliant Technologies.* New York: W.W. Norton & Company.

Byman, Daniel (2015): *Al Qaeda, the Islamic State, and the Global Jihadist Movement. What Everyone Needs to Know.* Oxford: Oxford University Press. Online: https://doi.org/10.1093/wentk/9780190217259.001.0001

Cronin, Audrey K. (2021): *Power to the People. How Open Technological Innovation is Arming Tomorrow's Terrorists*. Oxford: Oxford University Press.

Frey, John (2004): The 9/11 Commission Report: Final Report of the National Commission on Terrorist attacks upon the United States. *British Journal of General Practice,* 54(509), 966–967.

Gunaratna, Rohan (2016): *The Global Terrorist Threat. A Comprehensive Guide*. Singapore: World Scientific.

Haider, Huma (2014): *Refugee, IDP and Host Community Radicalisation.* GSDRC Helpdesk Report. Online: https://gsdrc.org/publications/refugee-idp-and-host-community-radicalisation/

Hoffman, Bruce (2006): *Inside Terrorism*. New York: Columbia University Press.

Hulnick, Arthur S. (2004): *Keeping Us Safe. Secret Intelligence and Homeland Security.* Westport: Praeger. Online: https://doi.org/10.5040/9798400675577

Human Rights Watch (2020): *World Report 2020.* HRW Reports. Online: www.hrw.org/world-report/2020

Ignatieff, Michael (2004): *The Lesser Evil. Political Ethics in an Age of Terror.* Princeton: Princeton University Press. Online: https://doi.org/10.1515/9781400850686

Interpol (2020): *Annual Report 2020. Connecting Police for a Safer World*. Online: www.interpol.int/content/download/16499/file/Annual%20report%202020_EN_i.pdf

Kundnani, Arun (2014): *The Muslims are Coming! Islamophobia, Extremism, and the Domestic War on Terror.* London – New York: Verso Books.

Laqueur, Walter (1996): Postmodern Terrorism. *Foreign Affairs,* 75(5), 24–36. Online: https://doi.org/10.2307/20047741

Lewis, James A. (2022): *Cyber War and Ukraine.* Center for Strategic and International Studies. Online: www.csis.org/analysis/cyber-war-and-ukraine

Lyon, David (2015): *Surveillance after Snowden*. Cambridge: Polity Press.

Mach, Katharine J. et al. (2019): Climate as a Risk Factor for Armed Conflict. *Nature,* 571(7764), 193–197. Online: https://doi.org/10.1038/s41586-019-1300-6

Makarenko, Tamara (2004): The Crime-Terror Continuum: Tracing the Interplay between Transnational Crime and Terrorism. *Global Crime,* 6(1), 129–145. Online: https://doi.org/10.1080/1744057042000297025

Maras, Marie-Helen (2016): *A terrorizmus elmélete és gyakorlata*. Budapest: Antall József Tudásközpont.

Neumann, Peter R. (2016): *Radicalized. New Jihadists and the Threat to the West*. London: I. B. Tauris. Online: https://doi.org/10.5040/9781350987692

Piazza, James A. (2011): Poverty, Minority Economic Discrimination, and Domestic Terrorism. *Journal of Peace Research,* 48(3), 339–353. Online: https://doi.org/10.1177/0022343310397404

Rémai, Dániel (2020): Egy majdnem tökéletes társadalmi jelzőrendszer? [An Almost Perfect Social Signalling System?] *Arc és Álarc: A Hamvas Intézet Folyóirata,* 4(2), 189–220. Online: https://real.mtak.hu/120953/7/101_HAMVAS_2020_2.pdf

Roach, Ken (2011): *The 9/11 Effect. Comparative Counter-Terrorism*. Cambridge: Cambridge University Press. Online: https://doi.org/10.1017/CBO9781139003537

Scheinin, Martin (2016): *Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism*. United Nations General Assembly – Human Rights Council. Online: https://digitallibrary.un.org/record/595030?ln=en&v=pdf

Schmid, Alex (2004): Terrorism – The Definitional Problem. *Case Western Reserve Journal of International Law,* 36(2), 375–419. Online: https://scholarlycommons.law.case.edu/jil/vol36/iss2/8

Shelley, Louise I. (2014): *Dirty Entanglements. Corruption, Crime, and Terrorism*. Cambridge: Cambridge University Press. Online: https://doi.org/10.1017/CBO9781139059039

Silke, Andrew (2008): Research on Terrorism. A Review of the Impact of 9/11 and the Global War on Terrorism. In Chen, Hsinchun – Reid, Edna – Sinai, Joshua – Silke, Andrew – Ganor, Boaz (eds.): *Terrorism Informatics. Knowledge Management and Data Mining for Homeland Security*. New York: Springer, 27–50. Online: https://doi.org/10.1007/978-0-387-71613-8_2

Spaaij, Ramon (2012): *Understanding Lone Wolf Terrorism. Global Patterns, Motivations, and Prevention*. Dordrecht: Springer. Online: https://doi.org/10.1007/978-94-007-2981-0

Sussman, David (2005): What's Wrong with Torture? *Philosophy & Public Affairs,* 33(1), 1–33. Online: https://doi.org/10.1111/j.1088-4963.2005.00023.x

Stern, Jessica – Berger, John M. (2015): *ISIS. The State of Terror*. New York: Ecco.

Tucker, Jonathan B. ed. (2018): *Innovation, Dual Use, and Security. Managing the Risks of Emerging Biological and Chemical Technologies*. Cambridge, Mass.: MIT Press.

United Nations (2001): *Security Council Resolution 1373*. Online: https://docs.un.org/en/S/RES/1373(2001)

United Nations (2011): *Interagency Coordination in the Event of a Terrorist Attack Using Chemical or Biological Weapons or Materials*. United Nations Counter-Terrorism Implementation Task Force (CTITF). Online: www.opcw.org/sites/default/files/documents/PDF/CTITF_2011_Report.pdf

UNODC (2021): *Afghanistan Opium Survey 2021*. Vienna: United Nations Office on Drugs and Crime. Online: www.unodc.org/documents/crop-monitoring/Afghanistan/Afghanistan_Opium_Survey_2021.pdf

Weimann, Gabriel (2015): *Terrorism in Cyberspace. The Next Generation*. New York: Woodrow Wilson Center Press – Columbia University Press.

Zenko, Micah (2015): *Red Team. How to Succeed by Thinking Like the Enemy*. New York: Basic Books.