GLOBAL THREAT ASSESMENT 2026

Liu Chunlin [1], **Rohan Gunaratna**[2]

K&C Protective Technologies Pte Ltd, Nanyang Technological University

Abstract:

The *Global Threat Assessment 2026* examines the evolving global security environment shaped by superpower rivalry, geopolitical fragmentation, and the persistence of terrorism and extremism. While attacks in Western states will remain limited, the vast majority of terrorist violence will occur in Africa, the Middle East, and Asia, driven primarily by Islamic State and Al Qaeda affiliates and state-sponsored militant proxies. The assessment highlights the growing convergence of state and non-state actors, the rise of hybrid and irregular warfare, and the expanding role of digital platforms in radicalisation, recruitment, and operations. It concludes that terrorism will remain the preeminent national security threat in 2026, requiring preventive counterterrorism strategies, stronger regulation of physical and digital spaces, and sustained international cooperation across ideological divides.

Keywords: Global terrorism, extremism; hybrid warfare, State-sponsored militancy, irregular warfare; counterterrorism, radicalization, digital extremism, geopolitical rivalry, global security.

***Titulo en Español**: Evaluación Global de las Amenazas en 2026*

Resumen:

Este artículo sobre la Evaluación Global de Amenazas en 2026 analiza el entorno de seguridad internacional en un contexto de rivalidad entre grandes potencias, fragmentación geopolítica y persistencia del terrorismo y el extremismo. Aunque los atentados en Occidente seguirán siendo limitados, la mayoría de la violencia terrorista se concentrará en África, Oriente Medio y Asia, impulsada principalmente por filiales del Estado Islámico, Al Qaeda y milicias apoyadas por Estados. El informe destaca la creciente cooperación entre actores estatales y no estatales, el auge de la guerra híbrida e irregular y el papel central del entorno digital en la radicalización y las operaciones terroristas. El artículo concluye afirmando que el terrorismo seguirá siendo una amenaza muy importante para la seguridad nacional en 2026 lo que requerirá estrategias preventivas de lucha contra el terrorismo, una regulación más estricta de los espacios físicos y digitales y una cooperación internacional sostenida más allá de las divisiones ideológicas.

***Palabras Clave**: Terrorismo global, extremismo, guerra híbrida, militancia patrocinada por el Estado, guerra irregular, contraterrorismo, radicalización, extremismo digital, rivalidad geopolítica, seguridad global.*

[1] Liu Chunlin is Chief Scientist, K&C Protective Technologies Pte. Ltd, Singapore. E-mail: <liu.chun.lin@kcpt.com.sg>

[2] Rohan Gunaratna is Professor of Security Studies at Nanyang Technological University, Singapore. E-mail:<ISRKGunaratna@ntu.edu.sg>

DOI: http://dx.doi.org/10.31439/UNISCI-266

1. Synopsis

The *Global Threat Assessment 2026* warns that terrorism will remain a major security threat, driven by extremist groups, state proxies, and great-power rivalry. Most attacks will occur in Africa, the Middle East, and Asia, while the West faces fewer but high-impact incidents. The report stresses the need for preventive counterterrorism, digital regulation, and stronger international cooperation to curb rising hybrid and extremist threats.

2. Introduction

In 2026, the superpower rivalry and geopolitical competition will influence and shape the global threat environment. In parallel, non-state armed groups driven by religious, ethnic, right- and left-wing ideologies will threaten both governments and social harmony in parts of Asia, Africa, and the Middle East.

The insurgent and terrorist entities will mount attacks in Asia, Middle East, Africa, Latin America and the West in 2026. While over 95% of the attacks will occur in conflict zones of Sudan, Mali, Somalia, Libya, Nigeria, Afghanistan and Pakistan, less than 5% of the attacks will occur in North America, Europe, Australia and New Zealand. Several major western cities scaled back or canceled New Year's Eve celebrations for 2025-2026, due to heightened security concerns, general public safety worries, and recent local tragic events. Nonetheless, the primary theatres of terrorism will be in the global south notably in Asia, Middle East and Africa.

The fewer attacks staged in the West will draw global attention like the family-based attack in Bondi beach in Sydney in December 2025. As long as migrant and diaspora communities are not integrated, extremism will linger in the physical and digital spaces radicalising communities, and the west will suffer from periodic attacks in 2026. Religious spaces should be tightly regulated, hate preachers and their institutions should be investigated, charities and their donors should be monitored, and protests and campaigns instigating violence should be banned. In partnership with community leaders, government leadership is vital to promote moderation, tolerance and coexistence.

3. The Context

The epicentre of global terrorism has shifted out of the Middle East into Africa and Asia. Nonetheless, threat groups remain active in Iraq, Syria, and Lebanon in the Levant and in Yemen in the Gulf. Iran’s Axis of Resistance - Shi’ite groups in Iraq, Syria and Lebanon and Yemen as well as a Sunni groups in Gaza - failed to deter Israel from striking Iran. Nonetheless to contain Israel, Iran seeks to restore its ring of fire by renewing support to Lebanese Hezbollah and Yemeni Ansarallah, severely weakened by Israel. With the exception of Iran, a state sponsor of both Shi’ite and Sunni threat groups, Middle Eastern governments have rejected terrorism. After the devastating war in Gaza following the Hamas-led attack on Israel on October 7, 2023, there is neither public support nor appetite for violence.

The West will witness the steadfast rise of both the extreme right wing and the extreme left wing resulting in intermittent attacks. The rise of far-right political parties will enable far-right extremism in 2026 and in the foreseeable future. Due to enhanced security and intelligence cooperation in the west, most attacks by the far left and far right and Islamist groups will be detected and disrupted in the planning and preparation phases. The FBI disrupted coordinated bomb attacks across five locations in Los Angeles on New Year's Eve. The Turtle Island Liberation Front – a far-left, pro-Palestine, anti-government, and anti-capitalist group has 939 followers, and its Instagram features images with the phrases "Death to America" and "Peaceful Protest Will Never Be Enough."

As in 2025, most attacks in the year 2026 will be in the Global South. Around 60-70% of the terrorist attacks will occur in Africa's north, south, east, west and in the center. Islamic State and Al Qaeda affiliates in Africa remain the deadliest terrorist organisations in 2026. Unless the war between Israel and Hamas and its allies resumes, around 15-20% attacks will be in the Levant and the Gulf. In 2026, attacks by Tareek-e-Taliban Pakistan (TTP) targeting Pakistan will surpass the attacks by Islamic State Khorasan Province (ISKP) and Islamic State Pakistan Province (ISPP). Al Qaeda-aligned TTP attacks mounted from Afghanistan could prompt a war between Afghanistan and Pakistan. Similarly, attacks by Pakistan and India could prompt a war between two nuclear powers. Likewise, extremism, the precursor of terrorism is on the rise in Bangladesh. With Bangladeshi Islamists and the Afghan Taliban exchanging visits throughout 2025, there will be calls for implementing Shariah and minorities in Bangladesh notably Hindus and Christians will suffer more attacks in 2026.

Most South and Central Asians are recruited by ISKP both when in their own countries and in the diaspora. With Central Asian governments regulating the religious space, the potential for radicalisation and recruitment in-country has diminished. Nonetheless, Central Asians working overseas has been enlisted by both the Islamic State and Al Qaeda to mount attacks in Russia, Europe, and elsewhere.

The threat in Southeast Asia has diminished but remnants of Islamic State and Al Qaeda continue to operate. Although two foreign terrorist fighters visited Mindanao in the Philippines for three weeks in November 2025 in the lead up to the terrorist attacks in Australia, the Manila government has done much to integrate the terrorists to mainstream politics. Similarly, Indonesia's counter terrorism force D88 dissolved Jemaah Islamiyah (JI), both an Al Qaeda and an Islamic State affiliate. A game changer in the fight against terrorism, JI supreme leader Para Wijayanto and D88 Intelligence Chief Ami Prindani worked together to remove the region's biggest threat after two decades of JI attacks. Likewise, Malaysian Special Branch dismantled an Islamic State in Bangladesh network in Johor, bordering Singapore. Similarly other threat groups based in Bangladesh and Myanmar continue to operate overseas through their labour diaspora.

4. Understanding the threat

The security posture of governments should be determined by national security agencies working in consultation with law enforcement authorities and military forces. Global terrorism will remain a persistent and pervasive threat to the stability and peace of the world. The Islamic State, Al Qaeda, and Iran-sponsored Shiite and Sunni militia have contributed to the widespread instability of the world. Their attacks have destabilised nations, regions, and even the global order. Terrorist attacks and state responses create ripple effects - they do not just shape battlefields but redefine states, fragment societies and radicalise communities with long term security implications.

At a high-level, governments worldwide should work together to criminalise the Muslim Brotherhood, the foundational ideology of the Islamic State, Al Qaeda, Hamas and many other likeminded groups. Although the balance of power in the Middle East has started to shift, the patronage of such ideologies and their leaders remain intact. In 2026, the dissent and protests against the Ayatollah regime over the plunging currency and a decline in living conditions will grow. Arab countries will work closely with the U.S. to weaken Iranian regime and its partner Yemen's Ansarullah. Like the two attempts to assassinate President Trump by Tehran's intelligence service, the Iranian Revolutionary Guard Corps (IRGC), Tehran will retaliate attempting to assassinate public officials and conduct attacks directly and through proxies. Unless there is regime change in Iran, Tehran will continue to support threat groups worldwide. With Tehran determined to restore its military nuclear and missile programs, Israel will degrade

Iran's conventional and unconventional capabilities in 2026. With the support of the US, Israel is likely to re-establish deterrence but the region will remain unstable. The US strategy is to manage threats rather than engage in an all-out war. Due to the geopolitical complexity, global shipping and commerce will be affected in 2026 and a full secure return to Red Sea shipping will be unlikely in the immediate or the short term.

With the Hamas and its allies releasing all the living and dead hostages except one, the Trump Peace Plan will move from Phase One to Phase Two in 2026. In addition to the disarmament and demobilisation of Hamas, Palestinian Islamic Jihad, Palestinian Mujahidin Brigade and seven other threat entities in Gaza, a Palestinian body to govern Gaza supported by the International Stabilisation Force will be established. Qatar, Turkey and Egypt mediators will work with the US to ensure the implementation of Phase Two. With Trump's close ties to the mediators and King Abdullah II of Jordan, Crown Prince Mohamed bin Salman of Saudi Arabia and other Muslim countries, the number of countries joining the Abraham Accords will increase in 2026. Although the fighting in Syria has ended, restoring stability in the country will take a decade. For 13 years, starting in March 2011, the conflict in Syria ravaged a country of 22 million killing over half a million people. With help from Russia, Iran, Iraq and Lebanese

Off on a new trajectory, Syrian leader Ahmed Al Sharaa was engaged by Turkey, Saudi Arabia, and the West preempting its descent to chaos.

After the formation of the Ministry of Defence by HTS, its core strength of 40,000 fighters was joined by 50,000 from allied groups. In regions, where HTS- implemented its model of Salafi-Jihadism, Christians, Alawites, Druze, Ismailis, Kurds and moderate Muslims have suffered.

Today, Syria's Al Hol and Roj camps under the control of the US-supported SDF hold 17,000 Syrians, 20,500 Iraqis and 9000 third-country nationals from over 60 countries. Of 46,500 IDPs in these camps, there are 9500 non-Iraq and non-Syrians. SDF controls 9000 IS fighters including 1600 from Iraq and 1800 outside Iraq and Syria. Although 5,500 FTFs and families were repatriated from Syria to 21 countries within 2024, the global threat of terrorism will spike if they are freed. Some foreign governments have risen to the impending threat. In 2025, Indonesia has started repatriating 529 of its citizens. As there was no effective deradicalisation program in the facilities in Syria, foreign governments should focus on bringing their national's home. To implement a multi stakeholder reintegration program, capabilities should be built in religious and spiritual, educational, vocational, social and family, financial, creative and performance art and psychological rehabilitation

After its territorial defeat in Syria, Islamic State shifted to Somalia its al-Karrar office, the hub responsible for coordinating training and funding affiliates. Al-Karrar support Islamic State affiliates in Democratic Republic of Congo, Mozambique and South Africa and even as far Europe and Asia. After the Abby Gate bombing in Afghanistan by ISKP funded by Al-Karrar, US Navy SEAL Team 6 killed in Somalia the Islamic State finance chief Bilal al-Sudani who had previously served Al Qaeda. Nonetheless al-Karrar still functions in Africa including engaging in cryptocurrency.

With the threat cascading from Maghreb to its south, the Sahel recorded the highest levels of violence in Africa. In addition to Islamic State in the Greater Sahara (ISGS), Jama'at Nusrat al Islam wal Muslimin (JNIM) has intensified their attacks expanding their territorial control in Mali, Burkina Faso, and Niger. Russia's Africa Corps were invited by Central African Republic, Mali, and Burkina Faso to displace the French military presence and Niger to replace the US military presence. Al Qaeda and Islamic State affiliates has deepened in Africa's west, east and south in 2025. In Southeast Asia, the threat diminished with relentless operations against the Islami State affiliates in Singapore, Malaysia, Indonesia and the Philippines. By coordinating, cooperating and collaborating across governments transnational threats can be mitigated. The dissolution of an Al Qaeda affiliate Jemaah Islamiyah in Indonesia is a game changer in the fight against terrorism. Nonetheless, the formers need to be engaged, and remnants continuously monitored. The key lesson is that any threat entity can be neutralised by governments committed to ending violence especially terrorism.

To sustain global peace, the U.S. should work with Russia and Europe to end the war in Ukraine. As long as NATO deployed along the Russian border, Moscow will be at conflict with the West. To mitigate the rising tide of terrorism, US-China and US- Russia should partner. Their geopolitical rivalry is being exploited. For instance, when the Islamists in Mali sieged its capital Bamako, the military regime rejected western support and enlisted Russia's African Corps, previously the Wagner group. Instead of confrontation, governments across the East-West divide should cooperate to fight common threats and build partnerships to create more educational and employment opportunities for the vulnerable youth. Otherwise, China, Russia and North Korea will continue to assist governments challenged by the West. For instance, they assist Iran and Yemen to restore their military capabilities by providing precursors and dual user technologies. Against the West, China and Russia will engage in Irregular Warfare from sabotage to espionage and cyber and influence operations in 2026.

5. Global Pandemic, Cybersecurity, and Happiness Security by Design

The COVID-19 pandemic fundamentally reshaped the global security landscape, accelerating the transition from predominantly physical environments to online and hybrid domains. Remote work, cloud collaboration, digital platforms, and virtual interactions rapidly became the new normal, driving governments, organizations, and individuals to adapt at unprecedented speed. While these changes improved flexibility, productivity, and resilience, they also introduced significant cybersecurity, privacy, and human-centric challenges that traditional security models were not designed to address.

The pandemic catalysed a deep convergence between physical security and cybersecurity. As organizations shifted operations online, sensitive data moved beyond protected corporate perimeters into homes, personal devices, and cloud infrastructures. This expansion dramatically increased attack surfaces, contributing to a surge in cyber threats such as phishing, credential theft, business email compromise, data breaches, and web-application attacks. At the same time, physical security systems—such as CCTV, access control, biometric systems, and building management systems—became digitally connected, further blurring the boundary between cyber and physical risks.

Hybrid work models, now widely accepted as a long-term arrangement, amplified both opportunity and risk. Studies consistently show improved productivity and morale in remote and hybrid environments; however, many organizations implemented these models without adequate cyber-safe remote working environments. Employees working from home often lack the protection present in traditional offices, making human behaviour the weakest yet most critical link in security. Good cyber hygiene, secure remote access, controlled use of personal devices, and behavioural awareness are now essential components of modern security strategies.

This evolving threat of landscape demands integrated security strategies. Effective protection now requires multiple layers of integration: electronic security systems working together; physical security elements aligned with architecture, procedures, and personnel; coordination across security disciplines such as IT, information security, and alignment with enterprise risk management. Security can no longer function in silos. Instead, it must support organizational objectives while managing both tangible and intangible assets.

Owners, developers, and city leaders play a decisive role in shaping this integrated security future. As cities and buildings become smarter and more digitally connected, security challenges increasingly originate from the cyber domain rather than purely physical threats. Decision-makers must therefore take responsibility for both worlds, adopting holistic risk assessments, secure technologies, staff training, and expert collaboration. Proactive, prevention-focused approaches are essential, as organizations that wait for incidents before investing in security often face greater harm and cost.

Within this context the paradigm of Happiness and Security emerges by Design. Traditional security measures, while effective, can unintentionally create anxiety, distrust, and psychological discomfort when overly intrusive or visibly hostile. Happiness Security by Design reframes security as an enabler of well-being, acceptance, and sustainability. By integrating psychological, social, and emotional considerations into security planning—alongside physical and cyber requirements—security systems can protect assets while enhancing user confidence and quality of life.

This approach recognizes that modern security systems are cyber–physical–human systems. Human acceptance, trust, and behaviour directly influence security effectiveness. Design solutions such as landscaped vehicle barriers, planter-based bollards, green walls, aesthetic blast-resistant structures, and user-friendly surveillance environments demonstrate how protective measures can simultaneously enhance safety and emotional comfort. Similarly, cybersecurity controls must balance protection with usability to avoid disengagement, or risky workarounds.

Looking ahead, hybrid working and living will define the future. Homes will double as workplaces, digital platforms will remain central to communication, and cybersecurity threats will continue to scale. Leadership responses must therefore move beyond surveillance and coercion toward trust, outcome-based performance, and human-centred engagement. Governments and industries must strengthen cybersecurity capabilities, improve education and training, and foster collaboration across borders and disciplines.

The post-pandemic world requires a fundamental shift in security thinking. The seamless integration of physical security, cybersecurity, human factors, and well-being—embodied in Happiness Security by Design—will define the next generation of resilient, trusted, and sustainable security architectures across cities, organizations, and societies.

6. The future

Superpower rivalry and geopolitical competition have polarised and fragmented the community of nations and, in some cases, compromised international security. More than ever before, political will and statesmanship is vital to fight threats and restore local, national, regional and global security. Far reaching leaders should reach out to leaders across the ideological divide to end unresolved conflicts and crisis. After the formation of the Ministry of Defence by HTS, its core strength of 40,000 fighters was joined by 50,000 from allied groups. The very same way the Afghan Taliban turned its guns on Pakistan, after creating a navy, air force and ground forces of 300,000, will the new Syrian government threaten its neighbours? To pre-empt the chemical weapon and other stockpiles of the Syrian regime from falling into the hand of HTS, Israel mounted a series of operations deep in Syria to destroy the strategic weapons. Nonetheless, HTS will inherit the capabilities to develop strategic weapons and a portion of the weapons developed by Assad's Syria.

Without triggering full-scale war, state and non-state actors pursue strategic objectives by relying on hybrid tools—armed proxies, disinformation, covert influence, militias, cyberattacks, economic coercion, and grey-zone operations. In an era marked by geopolitics, geoeconomics and geostrategy, the diffusion of low-cost technology, and the erosion of traditional deterrence frameworks, irregular warfare has become both a mode of statecraft and a persistent condition of global order.

The year 2026 will witness enhanced State sponsorship and threat groups with different ideologies working together. The Islamic Emirate of Afghanistan has provided Al Qaeda training facilities for TTP to attack Pakistan. In addition to Afghanistan Taliban hosting terrorists and terrorist camps, Iran is a haven for terrorist groups. After Aymen Al Zawahiri was killed in Afghanistan, Al Qaeda supreme leader Saif al Adil lives in Iran. Al Adil has built a working relationship between the Shi'ite and Sunni groups. Under his leadership, Al Qaeda and Hamas aligned and its propaganda mourned the death of the Hamas spokesman and praised the Islamic State attack in Sydney.

7. Conclusion

In a rapidly evolving global and political landscape, all nations require an unblinking eye to prevent and pre-empt threats from seeding, taking root, and manifesting harming the state and hurting its citizens. Public spaces in urban settings especially open facilities will be vulnerable to mass fatality and mass casualty attacks. The threat will be by state and non-state actors including lone wolf attackers. In addition to disinformation and misinformation operations, states will engage in information infrastructure attacks. The threat of cyber-attacks by both state and non-state actors will rise, compelling nations to secure the online domain. With threat groups setting up dedicated digital entities including an Al Qaeda digital command, governments will need to partner with community organisations and stringently regulate the digital space including fining tech companies. With a fourth to a fifth of the attacks being perpetrated by youth and children, governments will need to address online radicalisation in 2026.

Terrorism will remain the preeminent national security threat to most countries throughout 2026. Driven by extremist ideologies, terrorism will damage social cohesion between ethnic and religious communities. The government focus should shift from downstream to upstream counter terrorism to prevent and preempt attacks. Terror is not only a tool exploited by non-state actors, but state actors mostly through their partners and proxies. As they need plausible deniability, hostile governments will employ criminal organisations to conduct terrorist attacks. In August 2025, Australia expelled the Iranian ambassador after Tehran recruited a criminal group engaged in illicit tobacco trading attacked Jewish targets including a synagogue. The crime-terror infrastructure and politico-religious ecosystems of threat groups, networks, cells and personalities should be dismantled.

Unless Western and Eastern governments collaborate to mitigate common security threats, risks, and challenges, threat actors will continue to exploit the gaps, loopholes and weaknesses in the global security systems.

The global pandemic has fundamentally reshaped the security landscape by accelerating the shift to online and hybrid domains, significantly expanding cybersecurity risks alongside physical threats. As societies become more digitally connected, cyberattacks, disinformation, and online radicalisation now pose national security risks comparable to kinetic attacks, requiring the online domain to be secured with the same rigour as physical spaces. In responding to these hybrid threats, security approaches must move beyond enforcement alone to embrace Happiness Security by Design—integrating cybersecurity, physical protection, and human-centred design to safeguard safety while preserving trust, well-being, and social cohesion. In the post-pandemic era, security that is resilient, trusted, and psychologically accepted will be as critical as security that is strong.