ISSUE #5

COMMONWEALTH SECURITY & RESILIENCE GROUP

QUARTERLY NEWSLETTER

October 2025

Quarterly Round-Up

Of significance for all Commonwealth organisations, this quarter saw the launch of the Commonwealth Secretariat's Strategic Plan 2025-2030. For which, CWSRG joined engagements towards its development. The Plan places resilience at the centre of the Commonwealth's Democratic, Economic, and Environmental pillars and underscores the importance of formal Commonwealth organisations in advancing work across these areas. The plan also reiterates the leading role of the Commonwealth organisations in driving forward broader initiatives to support Commonwealth member states and communities. In this spirit, CWSRG is excited to continue to developing programmes that address pressing security challenges relevant to all Commonwealth countries, including those that fall outside the Plan's immediate priorities.

A central engagement in Q3 was the second CWSRG–RSIS visit, during which the CWSRG–RSIS Working Group on Extremism met at Gibraltar House. The session consisted of open discussions between researchers and organisational leaders to map pressing priorities, identify emerging research areas, and explore avenues for further collaboration on the spread of extremist ideologies and terrorism across the Commonwealth.

Looking ahead, Q3 was also marked by preparatory work for a series of upcoming programmes. Planning has begun for the Cyberpeace Summit in Delhi in 2026 and preparations finalised for the launch of the upcoming Commonwealth Security Review 2025/26, which will include dedicated chapters on maritime security, supply chain resilience in East Africa, and AI risk and digital resilience. In parallel, CWSRG has initiated preparations for the AI Risk Summit scheduled for London in September 2026 and the Second Maritime Domain Awareness Summit in Vancouver June 2026.

Upcoming

Commonwealth Security Review 2025/26, including:

Maritime Security Special Feature

and the East African Supply Chain Security Special Feature

Cyberpeace Summit 2026, New Delhi, India - Feb 2026

Commonwealth 2nd Maritime Domain Awareness Summit, Vancouver - Jun 26

AI Risk Summit, London - Sep 2026

Peace Support, Conflict and Extremism Dialogues, Africa - Through 2026

Around the Commonwealth

Stability, Crime and Disorder

Operations Island Chief and Ika Moana, both coordinated by Samoa, involve the regional joint efforts of 13 Pacific nations to fight against transnational crime, targeting illegal fishing networks across the Pacific region.

In Trinidad and Tobago a state of emergency has been declared after authorities found a criminal network across prisons to be plotting the assassination of government officials.

A South African high court sentenced seven Chinese nationals to 20 year terms for the human trafficking and forced labor of 91 Malawians at a Johannesburg factory.

Cyber and Tech

The Pacific region's digital infrastructure faces growing vulnerabilities as Australian airline, Qantas, suffers a cyberattack compromising the data of up to 6 million customers and Papua New Guinea experiences multiple cyber incidents, including a tax office breach.

Disasters and the Environment

Pakistan devastated by monsoon flooding. Heavy monsoons triggered catastrophic flooding across Pakistan, with the death toll exceeding 400 by August. Flash flooding in Gilgit-Baltistan killed three and left 15 missing in July, while August floods claimed 21 lives including eleven in Gilgit-Baltistan and ten in Karachi.

An 8.8-magnitude earthquake triggers tsunami alerts across Papua New Guinea, Vanuatu, and the Solomon Islands.

Conflict, Violent Extremism, & Global Security

Nigeria sees multiple security challenges. Boko Haram kills 63 people in Borno State, while bandit attacks claim dozens including 27 at a Katsina mosque. Additionally, an ambush in Benue State kills 11 police officers.

A Ghana Air Force helicopter crash near Obuasi, results in the death of 8, including Defence Minister Edward Omane Boamah.

Australia now advances Pacific security through agreements with Vanuatu, Nauru, and Papua New Guinea, while announcing a $1.1 billion Ghost Shark underwater drone fleet.

The 54th Pacific Islands Forum Leaders Meeting, comprising of 11 Commonwealth member states, convenes in Honiara, Solomon Islands, where leaders sign the Ocean of Peace Declaration establishing a regional security framework.

Spotlight on the Issues

The Digital Pacific

This quarter's prominent cyberattacks across Commonwealth member states in the Pacific region present an inflection moment for regional cooperation and collective action.

The digital security landscape is rapidly transforming across the Commonwealth's Pacific nations, creating heightened vulnerabilities, but also opportunities for collaboration between technologically advanced members and those still building cyber capacity. Where larger Commonwealth partners have developed sophisticated multilayered defenses through years of investment and experience, newer entrants to the digital economy face particular challenges making them highly vulnerable to cyber intrusion by criminal networks and state linked actors. Factors like resource constraints, legislative gaps, and a shortage of trained cybersecurity personnel allows for easily exploitable entry points for malicious actors, leaving them increasingly exposed to cyberattacks.

The impact of these vulnerabilities extends beyond the Pacific Island nations. Australia and New Zealand experience cascading effects as breaches compromise shared networks and communications infrastructure. More broadly, across the globe, where cyber systems are underdeveloped, these jurisdictions serve as transit points for money laundering and cryptocurrency-based financial crimes, undermining the wider financial system.

Cyber threats do not operate in isolation. The convergence of digital threats with other security challenges such as drug trafficking, illegal fishing, and human trafficking, increases the need for coordinated action. The same digital weaknesses that enable foreign intelligence services to access government systems provide pathways for organised criminal networks to conduct sophisticated operations with reduced risk of detection.

As these threats converge, cyberattacks open new pathways that amplify traditional crimes: compromised government databases provides criminal organisations with identity documents for trafficking; breached financial systems enable money laundering through cryptocurrency exchanges; hacked communications networks enable coordination of illegal fishing operations; and corrupted customs systems allow contraband to cross borders with false papers. Each cyber intrusion becomes a force multiplier for traditional criminal activities.

This blurring of lines between cyber threats, organised crime, and foreign interference creates complex security realities that resource-limited nations struggle to navigate on their own. State linked actors may collaborate with criminal networks in exchange for intelligence access. Criminal organisations develop sophisticated cyber capabilities that rival state actors, purchasing exploits on dark web markets and recruiting skilled hackers to conduct operations. Foreign powers exploit the same infrastructure vulnerabilities to conduct espionage that criminal enterprises use for profit, creating overlapping attack vectors.

The financial dimensions complicate this landscape. Financial cybercrime generates revenue that funds criminal groups and extremist activities, while undermining confidence in digital financial systems that developing economies increasingly rely on. When government systems are compromised, this allows criminal networks to operate freely, avoiding prosecution, influencing policy decisions, and working their way into economic structures.

Efforts are being taken to address these challenges at the regional level. Operations Island Chief and Ika Moana showcased effective coordination on shared security challenges, while the 54th Pacific Islands Forum, which saw the signing of the Ocean of Peace Declaration, advanced efforts to integrate cyber threats into the regional security framework. However, the relative maturity of maritime security cooperation contrasts sharply with the still-developing state of cyber coordination. Cyberattacks that unfold in minutes demand real-time information sharing and rapid response capabilities, mechanisms that have not yet taken shape across the region.

For the Commonwealth, this presents a critical opportunity to turn shared vulnerabilities into collective strength. The Commonwealth is well equipped to lead large-scale knowledge transfers and strengthen regional capacity in cybersecurity. The Commonwealth could facilitate threat intelligence sharing, deploy cybersecurity advisors, develop aligned cyber legislation, and strengthen response capacity across the region. Moreover, expanding existing Commonwealth law enforcement cooperation frameworks to address cyber enabled crime would further enhance collective resilience, simultaneously allowing member nations to strengthen their defensive capabilities and safeguard their digital sovereignty. As the world migrates from an era characterised by digitization to one of AI adjacency, digital and AI risk mitigation becomes wholly imperative. Earlier concepts of national resilience developing in silos is discredited - there are few causes more immediately relevant and opportune for Commonwealth cooperation.

Recent Activity

Commonwealth Strategic Plan 2025-2030

The CWSRG is tightly aligned with the Commonwealth Secretariat's 2025–2030 Strategic Plan, which is organised around strengthening democratic, economic, and environmental resilience, with a particular focus on helping member states anticipate, withstand, and adapt to evolving risks. CWSRG's mandate to build cooperation on AI risk, cybersecurity, transnational crime, counter-extremism, maritime domain awareness, and wider strategic resilience directly underpins this resilience agenda by addressing cross-border threats that undermine democratic stability, economic security, and the sustainable use of the maritime and blue economy domains.

CWSRG joined the other Commonwealth Accredited Organisations in consultation with the Commonwealth Secretary General

CWSRG-RSIS Working Group on CVE and CT

Countries across the Commonwealth continue to be impacted by threats from extremist ideology and terrorism. In spite of this, global efforts have been redirected to the growing strategic competition of great states and geopolitics. This is a mistake - terrorism blights the lives of too many across the globe; where terrorism strikes so too does economic decline, worsening domestic stability, and impacts on business and democratic freedoms. Extremist ideology and terrorism is a bed fellow of authoritarianism - often seen as the only legitimate way to protect citizens from bloodthirsty, nihilistic terror activity.

The Commonwealth has the potential to share unique insights, capabilities, and CVE/CT best practice. CWSRG welcomed friends and partners from the S. Rajaratnam School of International Studies (RSIS) in Singapore to discuss new research focuses, and initiatives to address the enduring threat of extremist ideology and terrorism.

CWSRG engaged with RSIS leadership and researchers at Gibraltar House

Contact

info@cwsrg.org

Commonwealth Security & Resilience Group
7 Adam Street
Westminster
London
UK
WC2N6AA