The Commonwealth

Call for papers

Commonwealth Cyber Journal
Volume 4, Issue 1

'Contemporary threats in cybercrime and cybersecurity'

The Commonwealth Secretariat invites submissions for the fourth volume of the *Commonwealth Cyber Journal* (*CCJ*), a peer-reviewed publication featuring scholarly articles and expert commentary on cyberspace issues affecting Commonwealth member countries and the global community.

This issue responds to the rapidly evolving threat landscape, characterised by the rise of AI-enabled cyberattacks, the expansion of cyberwarfare capabilities, the proliferation of ransomware-as-a-service (RaaS), the increasing exploitation of supply chain vulnerabilities, and escalating threats to critical infrastructure. Collectively, these trends are driving unprecedented financial losses and large-scale data breaches worldwide.

The *CCJ* invites contributions from academics, policymakers, practitioners and technical experts that critically examine these developments and the legal, policy, institutional and multilateral responses required to address them. Submissions should aim to strengthen democratic resilience and align with the priorities outlined in the *Commonwealth Strategic Plan 2025–2030*.

Articles on the following topics and related issues are invited. This list is illustrative and not exhaustive.

AI and emerging technology threats

- AI-powered cyberattacks and autonomous threat actors
- generative AI and synthetic media in cybercrime
- AI as a tool for cyber defence and threat detection
- exploitation of legitimate AI platforms by malicious actors

Ransomware, extortion and cybercrime ecosystems

- RaaS and extortion-only models
- cybercrime-as-a-service and underground criminal marketplaces
- cybercrime and the digital economy, including digital currencies
- phishing, social engineering and credential theft at scale

Infrastructure, state threats and geopolitics

- cyberwarfare, state-sponsored attacks and hybrid threats
- threats to critical national infrastructure
- supply chain vulnerabilities and third-party risk
- internet-of-things security and connected device vulnerabilities

- cybersecurity in elections and democratic processes
- zero-day exploits and vulnerability management

Legal, policy and rights frameworks

- privacy, data protection and WHOIS access for investigations
- electronic evidence, open-source evidence and admissibility
- international legal frameworks and cross-border co-operation
- cybersecurity workforce gaps and capacity building

Crimes against persons online

- technology-facilitated violence against women
- online child exploitation and abuse
- online fraud, scams and consumer harm
- information disorder

Submission timeline

- Abstract submissions due (maximum 500 words): 20 June 2026
- Abstract acceptance notifications issued: 1 July 2026
- Full draft papers due (5,000–7,000 words): 10–25 October 2026
- Editorial decisions communicated to authors: 1 November 2026
- Review and revision process: 15–18 November 2026
- Publication: 23 December 2026

Guidelines for authors

Following the review of abstracts, selected authors will be invited to submit a full paper.

Abstracts, along with author biographies/CVs and contact details, should be submitted to Dr Nkechi Amobi at n.amobi@commonwealth.int and cyberjournal@commonwealth.int.

Full papers must include a short abstract summarising the main content and argument of the paper, and a brief biography of the author(s) (one to two sentences per author), including current position, institutional affiliation and email address.

Articles must be submitted in Microsoft Word format, using 12-point Trebuchet MS font, with justified alignment and 1.5-line spacing. All submissions must use the Harvard author–date referencing style consistently throughout.

For editorial enquiries, please contact the *CCJ* editorial team via the submission email addresses above.

See previous issues of the *CCJ*: Volume 1 | Volume 2 | Volume 3