The International Counter Ransomware Initiative: Building Coalitions to Confront Cyber Threats
Open Forum Background Paper

History and Structure

The International Counter Ransomware Initiative began in 2021 to combat the growing threat of ransomware. It aims to build cross-border resilience and collectively disrupt and defend against malicious cyber actors through concerted international cooperation.

The CRI comprises more than 60 member states and organizations and is structured into three pillars – the International Counter Ransomware Taskforce (ICRTF), the Policy Pillar, and the Diplomacy and Capacity-Building (DCB) Pillar.

The Policy Pillar, led by the UK and Singapore, undertakes policy research and produces recommendations on ransomware-related topics with the CRI. A key outcome of the work of the Policy Pillar in 2023 was a joint statement of the CRI Summit in Washington, D.C. that endorsed national governments not paying ransomware demands to cybercriminals – marking an important step in international counter ransomware efforts.

The Diplomacy and Capacity Building Pillar is led by Germany and Nigeria. It is responsible for on-boarding new members to the CRI, diplomatic engagement and outreach, and facilitating the participation of CRI members in capacity building initiatives.

The ICRTF, co-chaired by Australia and Lithuania, focuses on delivering projects aimed at delivering practical tools to build resilience against malicious cyber actors and disrupt ransomware.

Goals: 2024 and Beyond

The CRI is working to combat the global ransomware threat through international cooperation to improve resilience, disrupt ransomware actors, counter illicit finance, enhance public-private partnership, and strengthen diplomatic and capacity building efforts. Engagement with non-government stakeholders is needed to ensure the success of this work.

The CRI provides an opportunity to create long-term cooperative approaches and common understandings of accountability in cyberspace, consistent with international law as well as state actions as embodied in the Framework for Responsible State Behavior in Cyberspace, endorsed by all United Nations member states.

Members (As of May 2024)

Albania	Estonia	Lithuania	Sierra Leone
Australia	European Union	Mexico	Singapore
Austria	Finland	Moldova, Republic of	Slovakia
Bahrain	France	By Morocco	Slovenia

Belgium	Germany	Netherlands	South Africa
Brazil	GFCE	New Zealand	South Korea
Bulgaria	Greece	Nigeria	Spain
Cameroon	India	Norway	Sweden
Canada	INTERPOL	OAS	Switzerland
Colombia	Ireland	Papua New Guinea	Ukraine
Costa Rica	Israel	Philippines	United Arab Emirates
Croatia	Italy	Poland	United Kingdom
Czech Republic	Japan	Portugal	United States of America
Dominican Republic	Jordan	Romania	Uruguay
Egypt	Kenya	Rwanda	Vanuatu
			Vietnam