ACCRA CALL ACTION STORIES

BUILDING A CYBER RESILIENT FUTURE FOR ALL

The Accra Call Action Stories are a collection of 11 concise, real-world examples showcasing how organizations have brought their Accra Call pledges and/or endorsements to life since 2023.

These stories demonstrate how the Accra Call is shaping action across sectors and regions — making cyber resilience a tangible part of sustainable development.

ACCRA CALL SUPPORTER

GC3B Global Conference on Cyber Capacity Building

13-14 May 2025

Geneva | Switzerland

ACCRA CALL ACTION STORIES

AUSTRALIAN DEPARTMENT OF FOREIGN AFFAIRS AND TRADE

ENDORSEMENT

Australian Government
Department of Foreign Affairs and Trade

ACCRA CALL SUPPORTER

Why does the Accra Call matter to your organization and your community?

We endorse the Accra Call, consistent with Australia's role as a leader on cyber in the Indo-Pacific committed to supporting the strengthening of cyber resilience in the region.

The **Accra Call is a useful framework for strategic consideration** of how our cyber capacity activities can better foster development within recipient countries and regionally, improve donor coordination, make more efficient and effective the activities we take forward, and meet the needs of our recipients.

How has the Accra Call inspired you to take action?

The establishment of our **Southeast Asia and Pacific Cyber Program (SEA-PAC Cyber)** responds to the Accra Call. SEA-PAC Cyber is an agile and flexible program, utilizing a mixture of ODA and non-ODA funding. It brings together our regional cooperation initiatives funded through Australia's 2023-2030 Cyber Security Strategy under one overarching, cohesive program. It enables progress against all four pillars of the Accra Call.

We enable cyber development by **recognizing the breadth and complexity of cyber capacity needs and targeting funding** to address different core issues in different regions. For example, our program includes support for cyber incident response work in the Pacific through **Cyber RAPID**, and cyber exercising to build capability through Partnerships with Southeast Asia.

We look to advance demand-driven and sustainable work. Australia listens to and responds to partner countries in Southeast Asia and the Pacific and works to improve transparency and coordination with other donors, including through the **GFCE's Cybil Portal, and Australia's participation in Partners in the Blue Pacific**.

SEA-PAC Cyber also **leverages public-private partnerships** with industry, tertiary education institutions, civil society and other non-government entities to deliver our support.

Concrete achievements

- We expanded our cyber capacity building efforts in Southeast Asia resulting in **new education opportunities for cyber professionals** through tertiary institutions and direct professional training programs including in **Indonesia, Vietnam, and the Philippines.**
- We increased work with the GFCE and other non-governmental organizations in the region to **understand baseline capacities**.
- Through Partners in the Blue Pacific, we established a **Pacific Cyber Capacity Building and Coordination Conference (P4C)**. The first P4C was held in October 2023 and plans are in progress for the next conference in August 2025.

ACCRA CALL ACTION STORIES

CYBERPEACE INSTITUTE

PLEDGE: ACTION 6, 7, 11 AND 13

CyberPeace Institute

ACCRA CALL SUPPORTER

Why does the Accra Call matter to your organization and your community?

Civil society plays a critical role in protecting the most vulnerable and is a cornerstone of the global international development ecosystem—yet it remains disproportionately targeted by cyber threats.

The CyberPeace Institute **endorsed the Accra Call to help close this protection gap through collaboration, transparency, and action.** Our pledge reflects a deep commitment to responsible cybersecurity—ensuring that civil society organizations advancing peace, rights, and humanitarian action can operate securely online.

The **Accra Call is a vital step toward building a more inclusive, resilient, and trusted digital ecosystem,** and reinforces our shared responsibility to protect those on the frontlines of justice.

How has the Accra Call inspired you to take action?

Strengthening cybersecurity for non-profits protects not only their missions but the communities they serve. By engaging governments, the private sector, and international organizations, we are building an ecosystem of trust, resilience, and equity—nation by nation, organization by organization.

The Accra Call has been a **powerful catalyst**, reinforcing our resolve to build a secure and inclusive digital future. It inspired us to expand support for civil society, accelerate skills development, and deepen cross-sector collaboration. For instance, recognizing the scale of the challenge, we launched **Beyond125.org** to reach 10,000 NGOs with essential cyber and AI skills. In collaboration with **Common Good Cyber and the GFCE,** we are activating a global coalition to protect those who protect others.

Concrete achievements

- By measuring the real-world harm of cyberattacks through the **CyberPeace Tracer**, which monitors targeted attacks on civil society, we transform threat intelligence into actionable protection strategies and capacity-building priorities rooted in lived impact.
- Through the **CyberPeace Builders**, we are empowering 400+ NGOs with cybersecurity skills and threat intelligence, supported by 50+ corporate partners and 1,300+ volunteers.
- The **CyberPeace Academy** and **AI Skills Initiative** equip non-profits to both defend themselves and harness AI responsibly.
- We have developed knowledge products available to the whole community, including the **Cybersecurity Assessment Tool** to guide nonprofits to identify and close security gaps and **Harms Methodology** for measuring and communicating the real-world impact of cyberattacks on nonprofits.

CREST

PLEDGE: ACTION 2

ACCRA CALL SUPPORTER

Why does the Accra Call matter to your organization and your community?

The **Accra Call enables CREST to add sustainable development to CREST's mission** to build global cybersecurity capability and consistency. By endorsing it, CREST has reaffirmed our commitment to strengthening cybersecurity service providers in emerging markets.

As a result of our Accra Call Commitment, **CREST now actively promotes capacity-building as a development priority,** ensuring cybersecurity is not just a technical issue but a core enabler of economic growth, digital trust, and secure online environments.

The Accra Call inspired CREST to reinforce its commitment to building sustainable cyber ecosystems by **bridging the gap between local cybersecurity providers and internationally recognised standards.**

How has the Accra Call inspired you to take action?

Since endorsing the Accra Call, CREST has brought these capabilities together into **CREST CAMP**. We have translated beneficiaries' self-assessment findings into concrete, evidence-based action plans that pinpoint specific gaps in their capacity and capability. We also paired them with existing CREST members to refine services and build business maturity. This has now been launched in 14 countries.

Within FCDO CREST CAMP we paired 32 local cybersecurity companies with CREST accredited members to accelerate their readiness for accreditation. We are also facilitating skills development by establishing 5 new CREST training partners in Kenya, Malaysia, Bahrain, Thailand and Georgia, enabling professional development aligned with international standards.

We also used the CREST CAMP process to **address gender disparity in cybersecurity by prioritising inclusive mentorship and capacity-building**, ensuring that underrepresented groups have access to career-enhancing opportunities. We are now actively collaborating with national authorities to draw on the CREST CAMP experience to embed CREST-aligned accreditation frameworks into national cyber strategies.

Concrete achievements

- We introduced a **50% discount** on all exam and membership fees for cybersecurity service providers in low- and lower-middle-income countries.
- We **published CREST standards as a free capacity building resource** for service providers globally and developed the CREST Accreditation Pathway with specific toolsets as a route through which aspiring service providers can improve their maturity.
- We created, piloted and rolled out CREST CAMP as a capacity building approach, including in low-middle income countries. We **supported 68 companies** in self-assessment against CREST's standards. We **mentored 32 companies** in identifying their development priorities. Our new partners provided **training** in penetration testing, threat intelligence or incident response **to 159 cybersecurity professionals.**

CYBER DEFENCE AFRICA

ENDORSEMENT

CYBER DEFENSE AFRICA

ACCRA CALL SUPPORTER

Why does the Accra Call matter to your organization and your community?

The Accra Call provides a collaborative framework that aligns perfectly with the mission of Cyber Defense Africa to strengthen cyber resilience in Africa and **guides our efforts in building capacity, coordinating research, and fostering inclusive digital development**. For both Cyber Defense Africa and the Togolese government, our endorsement of the Accra Call represents a commitment to regional cooperation and sustainable action in cybersecurity.

How has the Accra Call inspired you to take action?

Following the inaugural Global Conference on Cyber Capacity Building in 2023, and in direct alignment with the Accra Call and the Lomé Declaration on cybersecurity and the fight against cybercrime, we initiated the creation of the African Center for Coordination and Research in Cybersecurity in Togo.

This strategic project – funded by the World Bank & KPMG – aims to enhance cybersecurity resilience across the continent through collaborative research, knowledge-sharing, and sustained capacity-building efforts.

The Accra Call has **inspired us to think regionally, act inclusively, and build a permanent structure for cyber expertise coordination**. It has also encouraged stronger ties between public and private sectors and the involvement of underrepresented groups, including youth and women, in shaping the future of Africa's cybersecurity landscape.

Concrete achievements

- We launched the **African Center for Coordination and Research in Cybersecurity in Togo** to facilitate regional cooperation in cybersecurity and support the development, promotion and implementation of regional cybersecurity solutions, best practices and cyber capacity building initiatives for Africa.
- We secured strategic funding from the World Bank that allowed us to **expand our cyber capacity building efforts**, engaging along the way key stakeholders from governments, the private sector, and international organizations.
- We contributed to **knowledge exchange and the promotion of best practices** across the continent.

ACCRA CALL ACTION STORIES

GLOBAL CYBER ALLIANCE

PLEDGE: ACTION 11, 12 & 14

Why does the Accra Call matter to your organization and your community?

The aim of the Accra Call to stimulate global action to elevate cyber resilience aligns closely with the goals of the Global Cyber Alliance. GCA believes that we all deserve a secure and trustworthy Internet. We help people reduce the risks they face online while working to solve systemic issues that cause online harm.

Alongside our mission of working with communities to improve the Internet and help people and organizations be more secure online, the Accra Call serves as a **compass to elevate cyber resilience across development agendas** and to promote cyber capacity building.

How has the Accra Call inspired you to take action?

In the words of our Ambassador, **Towela Nyirenda-Jere**, the GCA **"found value in listening to the diverse experiences and expertise that the 2023 GC3B conference brought together, enabling us to connect with new partners and identify gaps and opportunities in cyber capacity building"**.

In line with the vision of meaningful and sustainable partnerships outlined in the Accra Call, GCA galvanizes our global network to implement programs and drive collective action on ecosystem-level issues that affect a large proportion of Internet users. Cyber capacity building is a critical component of our work, making our mission and work naturally aligned with the Accra Call.

GCA also leads **Common Good Cyber**, which aims to sustain the non-profits that maintain the critical cybersecurity infrastructure and deliver scalable solutions to secure high-risk actors from digital harm. This work directly seeks to elevate cyber resilience as a key element in driving development, economic growth, and progress.

Concrete achievements

Under the umbrella of the Common Good Cyber initiative, we:

- **Built private-public partnerships** with like-minded organizations and governments that understand the need for sustainable funding to those that tirelessly safeguard digital safety in the public interest, but who work on razor-thin, inconsistent budgets.

- Created a **database of free cybersecurity tools, services, and platforms** deployed to make the Internet safer in the public interest.

- **Prepared to launch a joint funding mechanism** for nonprofit organizations that aim to protect high-risk actors and the public by March 2026.

ACCRA CALL ACTION STORIES

INTERNATIONAL CHAMBER OF COMMERCE (ICC)

PLEDGE: ACTION 1 & 11

Why does the Accra Call matter to your organization and your community?

By endorsing the Accra Call, ICC demonstrates **commitment to tackling critical cybersecurity challenges and fostering trust in digital technologies**. Our endorsement of the Accra Call signifies our commitment to mobilise our global business network.

ICC aims to build capacity that strengthens national institutional capabilities to implement global commitments to decrease cyber threats, thus ensuring the protection of individuals, communities and businesses worldwide.

How has the Accra Call inspired you to take action?

The Accra Call has **inspired ICC to mobilise its global network of 45 million businesses across 170 countries** to contribute towards addressing the challenges by sharing best practices and considerations for safeguarding the cyberspace and increasing cyber resilience.

ICC continued to **contribute evidence-based recommendations** to uphold international law and norms, adopt multistakeholder approaches, and bolster cross-border cooperation to strengthen cybersecurity, inform the development of effective international provisions to help curb cybercrime and inspire coordinated international and multistakeholder action to enhance global cybersecurity for development.

Concrete achievements

- The global business community has made significant and continuing investments in securing technologies and developing defensive cyber tools, skills, and procedures. Despite these major contributions, the number of cyber threats keeps rising. We **called for urgent and concrete actions by governments** on various fronts.
- We offered concrete recommendations to encourage the international community to take action to **ensure the cyberspace is safe and secure** for all by fostering urgent, large-scale and effective implementation of the widely agreed existing norms and rules for state behaviour in cyberspace as well as reaching common understanding on international rules on cybercrime and facilitating cooperation.
- We stressed the importance of common goals, supported by a concrete framework for national implementation, to **effectively put existing agreed norms and international law into operation**. We called for shared goals for cyber action; an actionable, collaboratively drafted and agreed agenda to increase the security of the digital economy to drive inclusive development.
- We delved into the complexities of **safeguarding critical infrastructure and essential services** and offered actionable insights and a holistic approach to addressing evolving cyber threats. We made proposals focused on striking the right balance between regulation and sustainable controls supported by both the voluntary actions of the private sector and decisive action from governments.

ACCRA CALL ACTION STORIES

INSTITUTE FOR SECURITY AND TECHNOLOGY (IST)

PLEDGE: ACTION 11

IST Institute for SECURITY + TECHNOLOGY

ACCRA CALL SUPPORTER

Why does the Accra Call matter to your organization and your community?

The Institute for Security and Technology (IST)'s mission is to "**unite technology and policy leaders to create actionable solutions to emerging security challenges.**" The Accra Call's focus on cross-sector engagement affirms this goal and aligns with our belief that meaningful progress in cybersecurity depends on diverse perspectives and shared action.

In joining this global initiative, we are reaffirming our **commitment to building effective and inclusive approaches to cyber issues**—reflected in efforts like the Brazil Ransomware Task Force—and contributing to a more resilient and secure digital environment.

The Accra Call has shaped our approach to cyber capacity building by emphasizing the importance of inclusive, multi-stakeholder collaboration and public-private partnerships. Specifically, the Accra Call's focus on fostering stronger partnerships and better coordination, strengthened our commitment to building frameworks that are both locally grounded and globally informed.

How has the Accra Call inspired you to take action?

A key example is the development of the Brazil Ransomware Task Force (RTF), a multi-stakeholder effort led by Brazil's Ministry of Foreign Affairs and the Organization of American States (OAS), and supported by IST's expertise and efforts. Grounded in four pillars—Deter, Disrupt, Prepare, and Respond—the Brazil RTF convenes approximately 60 representatives from across government, industry, academia, and civil society to co-develop practical, context-specific strategies for ransomware resilience.

In line with the Accra Call's emphasis on equitable participation, the Brazil RTF process was designed to be **community-informed**, including a public consultation conducted in Portuguese to ensure broader access and input. The final Brazil RTF report, to be released in mid-2025, will present recommendations tailored to Brazil's national context while contributing to regional and global ransomware resilience.

Concrete achievements

- In partnership with the Brazilian Ministry of Foreign Affairs and the OAS, we convened a two-day, in-person **Brazil Ransomware Task Force conference** in Brasília. During the conference, we facilitated working group sessions and cross-pillar discussions to develop and refine national ransomware response recommendations.

- Collaborated on a **public consultation** (in Portuguese) to gather input from Brazil's broader **multi-stakeholder community**, including government, industry, academia, and civil society.

- Final Brazil Ransomware Task Force **report, with actionable recommendations**, to be published by the end of Q2 2025.

ACCRA CALL ACTION STORIES

ITALIAN MINISTRY OF FOREIGN AFFAIRS

PLEDGE: ACTION 11

Ministry of Foreign Affairs
and International Cooperation

ACCRA CALL SUPPORTER

Why does the Accra Call matter to your organization and your community?

The Accra Call is highly relevant to Italy's cyber and development communities, as it highlights cyber resilience as a key enabler of sustainable development. This **aligns with Italy's strategic vision**, which integrates cybersecurity into broader development policies. The Accra Call promotes a balanced approach to digital progress, safeguarding rights, trust, and critical infrastructure.

Its principles reflect those of **Italy's National Cybersecurity Strategy 2022–2026**, which supports inclusive, evidence-based, and development-focused initiatives with partner countries. More broadly, it **affirms that cybersecurity and sustainable development are mutually reinforcing global priorities.**

How has the Accra Call inspired you to take action?

The Accra Call has provided **valuable impetus for Italy** to further strengthen and expand its engagement in cyber initiatives at both the national and international levels.

In line with **Action Point 11 of the Call** - highlighting the importance of public-private partnerships and inclusive market incentives - Italy continues to promote a multi-stakeholder approach, encouraging dialogue and collaboration among public institutions, academia, and the private sector.

In this context, a notable step forward was the **convening of Italy's first National Conference on Cyber Capacity Building**, held on 2 July 2024, hosted by the Italian MFA, which served as a platform to enhance coordination among national actors. Reflecting the spirit of the Accra Call, Italy remains committed to aligning its initiatives with the specific needs and priorities of partner countries, with due attention to inclusivity and gender responsiveness.

Concrete achievements

- Italy has made progress in the implementation of critical elements of Italy's National Cybersecurity Strategy aimed at **building a national cyber capacity building ecosystem** (measures #78 and #79).
- Italy has **financially contributed** to the **World Bank's Cybersecurity Multi-Donor Trust Fund** and **UNIDIR's Security and Technology Programme**.
- Italy signed bilateral Memoranda of Understanding on cybersecurity with **Tunisia, Romania, Spain, Albania, and Vatican City.**
- Italy agreed to **host the Ukraine Recovery Conference (URC2025)** in Rome on 10–11 July 2025, as part of its ongoing support to Ukraine, including initiatives to strengthen civilian cyber resilience and digital development.

NETHOPE

PLEDGE: ACTION 2, 4, 7, 8, 10, 11, 12, 13, 15, AND 16

Why does the Accra Call matter to your organization and your community?

The Accra Call aligns with NetHope's mission to strengthen cybersecurity resilience across the nonprofit sector. It **emphasizes collective action**, which is key to our initiatives like the Global Humanitarian ISAC, cybersecurity sub-grants, and vCISO services. By advocating for stronger cybersecurity and data protection, it reinforces our efforts to safeguard humanitarian organizations from cyber threats. Additionally, the Accra Call supports cybersecurity training, a core component of our capacity-building programs.

By embracing its principles, NetHope and our community can **enhance digital resilience, protect vulnerable populations**, and ensure the **continuity of critical humanitarian and development operations** worldwide.

How has the Accra Call inspired you to take action?

The Accra Call has reinforced NetHope's commitment to strengthening cybersecurity resilience within the nonprofit sector. It has **inspired us to expand initiatives** like the Global Humanitarian ISAC, fostering intelligence sharing and collaboration to protect humanitarian organizations from cyber threats. Additionally, it has motivated us to increase cybersecurity sub-grants, enabling nonprofits to enhance their security posture.

Recognizing the importance of capacity-building, we are **scaling up cybersecurity training programs to empower organizations** with essential skills. The Accra Call also validates our vCISO services, ensuring nonprofits can access expert guidance for risk management and data protection.

By embracing its principles, we are **more determined than ever to equip humanitarian organizations with the tools, resources, and support needed** to navigate evolving cyber risks effectively.

Concrete achievements

- Through the **Global Humanitarian ISAC**, we've fostered real-time cyber threat intelligence sharing.
- Our **cybersecurity sub-grants** have enabled organizations to enhance their security infrastructure.
- We've delivered cybersecurity **training to hundreds of non-profit professionals**, equipping them with critical skills.
- Our **vCISO services have provided expert guidance** to organizations lacking in-house security leadership.
- Our initiatives have **collectively improved data protection, risk management, and overall cyber resilience for humanitarian organizations**, ensuring they can continue their vital missions securely and effectively.

ACCRA CALL ACTION STORIES

NEUROMETRICS CYBERSPACE

PLEDGE: ACTION 7

NEUROMETRICS

ACCRA CALL SUPPORTER

Why does the Accra Call matter to your organization and your community?

Cybersecurity and cyberdefense are two fundamental pillars for navigating this new digital landscape. Both dimensions are key to ensuring security and trust in the digital world. **Our actions in cybersecurity and cyber defense align with the objectives of the Accra Call**, particularly in strengthening cyber resilience as an enabler of sustainable development and advancing effective and sustainable cyber capacity building.

How has the Accra Call inspired you to take action?

Research in these areas is essential to **develop strategies tailored to specific needs, especially for "low-tech" countries**, such as those in Latin America, which are particularly vulnerable due to a lack of resources, knowledge, and trained personnel.

At Neurometrics, we recognize that delving into these new security dimensions is crucial to understanding technology's current and future role in the world. That is why the **Neurometrics team conducts research and projects** to contribute to developing related literature.

Specifically, our initiatives support **promoting cyber resilience knowledge and skills among international development workforce through training** programs and conferences aimed at high-ranking officers and officials in Peru. We also contribute to addressing the cybersecurity skills gap through education and professionalization efforts. These efforts demonstrate our commitment to fostering cyber resilience and capacity building in line with the priorities outlined in the Accra Call.

Concrete achievements

- We have supported strengthening skills of the government officials and services in the field of cybersecurity through trainings, education courses and conferences, such as a **Course cybersecurity for SMEs, the Conference on Cyber Defense and Artificial Intelligence, or the Conference on Artificial Intelligence** and its applications for security and defense.
- We support further **professionalization of the cyber capacity building workforce in Peru** by delivering knowledge products to support evidence-based policymaking. This includes articles and reports on evaluating the use of **digital public services**, **artificial intelligence and cyber defence**, and **digital citizenship**.

ACCRA CALL ACTION STORIES

NRD CYBER SECURITY

PLEDGE: ACTION

NRD Cyber Security

ACCRA CALL SUPPORTER

Why does the Accra Call matter to your organization and your community?

NRD Cyber Security **supports the vision of the Accra Call that resilience must be integrated into sustainable development** as a core priority. This includes mainstreaming it across international development programs, enhancing workforce skills, and uniting cyber capacity building with development efforts. To achieve this vision, NRD Cyber Security has supported many Global South countries in **securing digital ecosystems, developing strategies, protecting infrastructure, and establishing threat monitoring.**

How has the Accra Call inspired you to take action?

When implementing cyber capacity building projects around the world, we have **placed a strong emphasis on sustainability of the projects we implement**, in line with the Accra Call action to promote demand-driven, effective and sustainable cyber capacity building.

While implementing the projects, we have encouraged our clients to consider the long-term impact of the projects, i.e. not only to establish a national CSIRT, but also to identify stakeholders and funding structures for future operations.

Concrete achievements

- **Helping countries set an example for others**: We have established close collaboration with Bhutan on cyber capacity building and have seen first-hand their determination. In 2024, during the FIRST annual conference, we encouraged representatives from Bhutan to share their story on stage and inspire other small states to focus on improving cyber resilience despite a lack of resources. This **has resulted in Bhutan's advance to a Tier 3 Establishing country** (score range 55-85) in the ITU Global Cybersecurity Index 2024, improving its position from 2020.

- **Enabling knowledge sharing**: We have been working with Mongolia on strengthening its cyber resilience since 2020. Mongolia has embarked on a comprehensive digital transformation journey to modernize its economy, enhance public services, and diversify beyond its traditional mining sector. During a recent visit to Lithuania, Mongolia's met with national cybersecurity teams in Lithuania, Latvia and Estonia. The Mongolian team also met sectoral CSIRTs. We believe that **by getting an overview of how other cybersecurity teams work and engage in an open and trusted dialogue, cybersecurity teams will be able to consider different styles and opportunities** that arise when trying to build effective cyber threat monitoring systems.

ACCRA CALL ACTION STORIES

Join these organizations and demonstrate your commitment to cyber resilient development by supporting the Accra Call!

For any questions, please reach out to contact@gc3b.org

ACCRA CALL SUPPORTER

GC3B
Global
Conference
on Cyber
Capacity
Building

13-14 May 2025

Geneva | Switzerland