GLOBAL CYBER EXPERTISE MAGAZINE

Volume 12, September 2024

Global Cyber Expertise Magazine

Volume 12, September 2024

GLOBAL

REGIONAL | AMERICAS AND CARIBBEAN

REGIONAL | PACIFIC

REGIONAL | EUROPE

REGIONAL | AFRICA

REGIONAL | SOUTH-EAST ASIA

GUEST COLUMN

Foreword

Welcome to Issue 12 of the Global Cyber Expertise Magazine! We are delighted to present this edition during the GFCE Annual Meeting 2024. We hope it gives you valuable updates and insights on cyber capacity building projects, policies and developments across the globe.

The magazine showcases the people and organizations working hard to secure the critical infrastructure and digital economy which underlie the rich array of opportunity our online world can bring. In this edition, we have articles from each of our regions, and also a new column; "Interview with a Guest Expert". Our first expert is Dr. Patryk Pawlak, who looks back to what got him involved in cyber policy in the first place, and forward to the upcoming GC3B conference to be hosted by the GFCE and Switzerland in 2025.

Our three featured articles show the range and value of the GFCE's global network. "How to Narrow the Cyber Skills Gap by Widening the Talent Pool" puts the spotlight on diversity initiatives in Africa and the Middle East that are helping to plug the cyber security skills gap. "APT Threat Landscape: Global Cybersecurity Responses & Perspective from Western Balkans", by Drinor Selmanaj, is a fascinating and deeply informative look at a security topic of profound importance. And finally, "The Impact of the CSIRTAmericas Network on the Caribbean Incident Response Ecosystem" showcases the practical benefits and human impacts of the network-building at the heart of what we do.

No one is an island in a connected world; our cybersecurity stands or falls on the capabilities and practices of others. Or to put it another way, cybersecurity is a collective endeavor, not a solo pursuit. That is why our networked approach works. It reflects both the shared vulnerabilities of a globally connected world, and the fundamental human wisdom that if we want to go far, we must go together.

We thank our guest writers for their valuable contributions and we hope you enjoy reading the Global Cyber Expertise Magazine!

On behalf of the Editorial Board.

David van Duren, Director, The Global Forum on Cyber Expertise (GFCE)

Marjo Baayen, Director, The Global Forum on Cyber Expertise (GFCE)

HOW TO NARROW THE CYBER SKILLS GAP BY WIDENING THE TALENT POOL

***Written by:** Luanda Domi, Gender Mainstreaming and Cyber Skills Development Manager, Global Forum on Cyber Expertise (GFCE).*

Diversity in cybersecurity is not just about fairness; it is a strategic necessity.

The cyber security challenge; growing and evolving threats, skills and workforce deficits, and low diversity

The ever-increasing complexity of the cybersecurity landscape means we need a broad range of skills and perspectives to effectively combat evolving threats. Growing demand for cybersecurity professionals worldwide is driven by rapid technological development and the evolving nature of cyber threats, requiring continuous upskilling and reskilling of the workforce. However, there is an alarming shortage of cybersecurity professionals; in 2023 the World Economic Forum projected a deficit of 3.4 million cybersecurity experts globally.[1] Yet on the supply side there are insufficient educational programs and often inadequate development of existing employees' skills. At the same time, the cybersecurity workforce typically lacks diversity, cutting women and other underrepresented groups off from key opportunities.

One approach has the potential to address all these problems; developing a more diverse talent pool by actively integrating women and other underrepresented groups.[2]

What Diversity, Equity, Inclusion, and Accessibility (DEIA) Can Do For Cybersecurity

Even though women make up more than half of the world's population, they are a minority of the cybersecurity workforce. This gap represents a failure, but also an opportunity. The sector has not yet tapped the full spectrum of available talent, but it still can. This requires a strategic approach.

In 2023, the United States approved

its National Cyber Workforce and Education Strategy, which aims to address structural challenges to building a diverse cyber workforce. The strategy shows how to transform cyber education and workforce development to include women and other under-represented groups, including neuro-diverse people.[3] Strategic initiatives like this are essential to meet the current skills demand, facilitate ongoing employee development, and prepare learners for the future.

The benefits are huge. Diverse teams bring different perspectives to problem-solving and enable more innovative and comprehensive approaches, including by anticipating a broader range of cyber threats.[4] Broadening diversity to include not just diverse social groups but people who have come to cyber security via non-traditional routes can bring more and non-obvious ways to deal with the growing complexity of cyber threats.

Integrating Diversity, Equity, Inclusion, and Accessibility (DEIA) in cybersecurity improves the range and effectiveness of security strategies. As Marjo Baayen, GFCE Director says; *"Diversity in cybersecurity is essential. It's not just about fairness or social justice; it is about enhancing the effectiveness of our security strategies."*

However, diversity does not happen by itself. A coordinated strategy is needed.

The Cyber Skills Gap; It's not just about workforce numbers but their lack of necessary skills

The cyber skills gap[5] is a critical issue worldwide. In Europe, there is an estimated shortage of 350,000 experts. This gap is not just about numbers; it encompasses a lack of necessary skills within the existing workforce, and an insufficient skills pipeline. Europe has high demand for skills such as incident response, threat intelligence, and penetration testing, but also for non-technical skills such as communication and leadership, which are critical to preventing and responding to incidents effectively. For governments, regulation is continually evolving to meet the demands of new technologies and threats, especially in data protection and cybersecurity standards, so there is a growing need for standardization, governance and compliance experts.

In Africa, there is growing interest in cybersecurity careers, but structural issues persist. African countries face significant cybersecurity challenges due to rapid digital growth and a lack of preparedness. Many organizations expect to hire fully trained professionals, but neglect to incubate home-grown talent. This

Women in Cyber Capacity Building Network (WiCCB)
Marjo Baayen
GLOBAL FORUM ON CYBER EXPERTISE
Women in Cyber Capac Building Network (WiC
Luanda Domi
Elisa Stamo NAECCS (Unverified)
Women in Cyber Capacity Building Network (WiCCB)
Nina Olesen (External)
Women in Cyber Capacity Building Network (WiCCB)
Confidence Staveley (External)
GLOBAL FORUM ON CYBER EXPERTISE
Women in Cyber Capa Building Network (Wi
Irene Corpuz (External)

GFCE's Women in Cyber Capacity Building (WiCCB) Network's event - "Synergy in Cybersecurity: Women Leading Across Networks for Global Impact."

creates a cyclical problem where potential talent is overlooked or underdeveloped. Additionally, women represent only 9% of the cybersecurity workforce, reflecting broader gender disparities in the IT field.

The Middle East also faces a substantial skilled workforce gap, with a shortage of 112,000 cybersecurity professionals.[6] The region is investing heavily in technology, including smart cities and digital economies, which increases the demand for advanced cybersecurity capabilities in cloud security and AI. Skills in these areas, and also machine learning, incident response and zero trust architecture, are in high demand. Yet, while women in the Middle East are more likely than in other regions to earn IT-related degrees,cultural barriers and limited support systems hinder their integration into the cybersecurity workforce.

As Marjo Baayen, Director of GFCE, says: *"Talent is universal, but opportunity is not. Women represent half of the world's population, but are still drastically underrepresented in cybersecurity today."* So, who is working to bridge that gap?

The Cyber Skills Pipeline

The GFCE is involved with several key initiatives to address the gender side of the cyber skills gap. In the Middle East, regional networks like the *Women in Cybersecurity Middle East* promote awareness and mentorship to support women entering in the field. And in Africa, the Cybersafe Foundation is working directly on the cyber security skills pipeline.

Africa's vibrant startup ecosystem and the digitization of critical infrastructures drive demand for cybersecurity skills, but opportunities to develop them are few.[7] Confidence Stavely, founder of Cybersafe Foundation, says young people need opportunities to grow their skills; *"We must mature the skills stack to fill the skills gap."* Key skills include incident response, cloud security, application security, and governance, risk, and compliance (GRC). The *CyberSafe Foundation's* Cyber Girls Fellowship[8] is running in 27 African countries. It gives training and mentorship to women from diverse educational backgrounds, helping them gain cybersecurity roles. The program works closely with industry to provide the right skills to successfully funnel women into cyber roles across different industries.

The Cybersafe Foundation opens up access to cybersecurity to women from different and often nontraditional career pathways. It works to overcome an "inside the box only" mentality that companies may have about what the "typical" cybersecurity professional looks like, i.e. gender biases, or computer science-only graduates. The foundation works specifically to acquire a range of talent and bridge the gap so that *"we're able to attract more women …and making sure that they are skilled for those roles."*[9]

Expanding the Talent Pool through Mind-Set Change and Mentoring

Expanding the talent pool requires creating pathways for women and other under-represented groups to enter and thrive in cybersecurity careers. We need to look beyond traditional pipelines and formal education pathways to attract candidates from other fields. Human resources departments and recruiters need to be more realistic in their demands, and identify nontraditional candidates who can be up-skilled or re-skilled, rather than having to tick each single box. So, in the cases of career changers, hiring teams should recognize transferable skills and relevant abilities that bring the ability to grow. This 'skills-first' approach focuses on *"whether someone has the right skills and competences for a particular role, rather than how the skills have been acquired"*.[10] This mind-set change in hiring teams can help address talent shortages, close skills gaps and boost business growth.

To support this, *Women 4 Cyber Foundation,* in collaboration with the *European Cybersecurity Organisation* (ECSO), run a platform called *Road to Cyber* that facilitates skills development and access to jobs. They promote an agile approach to skills development and career progression in cyber with a platform for skills development and access to jobs, European cyber recruitment initiatives, and dedicated support tools. *Road to Cyber* enables a "life-time of skills"[11] by providing access to

CyberGirls Cohort 3 Orientation Ceremony 2023 in Kenya. Courtesy of Cybersafe Foundation.

youth education initiatives, mentorship, and training opportunities.

In the Middle East, role models are a key force in attracting women to male-dominated sectors, and, just as importantly, helping them to stay and develop their careers. At GFCE's recent Women in Cyber Capacity Building (WiCCB) Network event, Irene Corpuz, Co-Founder and Board Member of the Women in Cyber Security Middle East said: *"If you see that there are some women in the region who are already leading in cyber, or in a leadership position, you can see that there are a lot of women, younger generation following them. So, it is very important to have a support system place, whether this is family, education, the employers."*[12]

Mentorship programs provide this support system throughout the cybersecurity journey, providing targeted guidance on CV or interview preparation, how to move into leadership positions, and so on. In Africa, through training coupled with mentorship programs, women have experienced between 200 to 450% increase in their income.[13] Programs like these don't just close the skills gap and make industries more inclusive and diverse; they change the lives of women for the better.

Connecting Programs to Build Scale: The GFCE Women in Cyber Capacity Building Network

The GFCE Women in Cyber Capacity Building Network (WiCCB) illustrates the power of collaboration, and inclusivity in building a stronger, more diverse cybersecurity workforce. It is a network of networks, connecting regional programs to a global platform. This network fosters collaboration, knowledge-sharing, and the scaling of successful initiatives across regions. By leveraging the expertise and resources of its global community, WiCCB network supports the development of cyber skills and promotes gender diversity in cybersecurity worldwide.

Conclusion

The cybersecurity skills gap requires an immediate and sustained response. Women and other under-represented groups bring unique insights and approaches that are crucial in a field as dynamic as cybersecurity. To benefit, organizations and institutions must adopt strategic approaches; investing in education, promoting inclusive hiring practices, and fostering a culture of lifelong learning. By actively and supportively expanding the talent pool, we will harness broader skills and perspectives essential to tackling cyber threats. Diversity in cybersecurity is not just a matter of fairness; it is a strategic necessity and a golden opportunity for change.

WHAT DOES AI MEAN FOR CYBER CAPACITY BUILDING?

AI is a double-edged sword for cybersecurity, and the need for cyber capacity building has never been greater.

Written by: *Chris Buckridge, Senior Strategy Advisor, GFCE.*

Artificial intelligence is ubiquitous, and yet still an enigma. As the latest iterations of this technology have made their way into widespread use - large language models (LLMs) and generative AI applications, in particular - the barrage of information, rhetoric, advice, and even policy has been remarkable, not only in sheer volume, but also divergent opinions. You'll find a commentator, vendor, or policymaker arguing for every position from "AI will save the world" to "AI will destroy the world". Society at large is grappling to understand and predict just what adoption of this new technology will mean.

What's clear is that the astonishing uptake of AI has serious implications for technology users of all kinds, from governments to companies to individuals. In today's society, we're all technology users, and AI technologies are already affecting how we communicate with our customers and clients, how we work, and how we engage with online services of all kinds. Ensuring that we are all sufficiently informed users of technology has been the challenge of this century, and that challenge is made all the more urgent by AI-enabled applications and services that, in emulating human feedback and interactions, are often designed to go unrecognized and unchallenged.

Cyber expertise - and the capacity building essential to developing that expertise - needs to develop and evolve rapidly to meet a challenge whose scope we are only beginning to understand.

AI: Changing the Cyber Threat Landscape

It's approaching ten years since a multistakeholder, geographically diverse community established the Global Forum on Cyber Expertise (GFCE), recognizing the importance of cybersecurity-related capacity building and the intrinsically cross-sectoral nature of that effort. Part of that cross-sectoral necessity stems from the fact that the cyber threat landscape is not static - it is constantly evolving across various planes. New technologies, new vulnerabilities, new threat actors, and new use cases mean that an open channel for communication and cooperation between government, industry, and the technical and research communities is essential to effective cyber capacity building.

The emergence of AI has highlighted that fundamental truth - its application by actors on all sides is changing the landscape drastically, in ways both positive and negative. Several recent studies have sought to understand these changes and how they are perceived by cybersecurity professionals. ISC2, the member association for cybersecurity professionals, surveyed over 1,100 members and found that 82% expect AI to improve job efficiency in the cybersecurity space by helping to analyze user behavior, automate tasks, detect malware, and predict areas of weakness.[1] Tellingly, however, respondents were split almost evenly (across agree/disagree/don't know) on whether AI will benefit cybersecurity professionals more than bad actors, while 54% reported a substantial increase in cyberattacks over the last six months that they suspected were AI-enhanced:

> ***"Arguably, if an AI LLM is working well, you won't know the difference between automated and human-based attacks. The clues will be more nuanced, such as speed and repetition of attack that appear implausibly fast for a human (or a room full of humans) to conduct."[2]***

Research conducted last year by Cisco described AI adoption as "a once-in-a-generation technology shift that is impacting almost every area of business and daily life", but found that "intentions of adopting and leveraging AI are far outpacing the abilities to do so".[3] The survey of more than 8,000 companies in 30 markets found that 86% of the companies questioned were "not fully prepared to leverage AI and AI-powered technologies to the fullest potential". However, 90% of surveyed organizations are investing in AI skills-related training, and 83% identify cybersecurity as a priority area in developing their AI-related strategy. The Cisco report found an awareness of the need to act:

> ***"Given the scale of the challenge, companies realize that cybersecurity needs to be tackled at machine scale, not human scale, and the Index showed an increased adoption of AI-powered solutions among organizations for such purpose."***

These and many similar reported findings show that security professionals in the private sector recognize the double-edged nature of AI. Tools already available in the marketplace (and rapidly improving) are upping the ante for both attackers and defenders. A recent Microsoft publication highlighted the potential for increased efficiencies and improved insights, and said organizations are already using AI tools to help analyze data from past incidents, identify vulnerabilities, and develop appropriate measures.[4]

However, the same kinds of tools are also being used to develop ever more destructive and hard-to-defend attacks. And while larger companies can take the lead, and shoulder the expense, of implementing the latest tools and technology in cyber defense, the offensive capabilities enabled by AI are broadly targeted, often seeking out the most vulnerable targets. A potential "digital divide" between those who can defend against AI-enhanced threats and those who cannot is not just a concern for companies in the Global South, but a broader systemic issue with the potential to undermine cybersecurity globally.

The growing impact of AI technologies on the cybersecurity ecosystem means the need for collective and inclusive commitment to cyber capacity building has never been greater.

AI and Cyber: The Policymakers' Perspective

In the policy space, the discussion around AI, and especially AI governance, is extremely wide-ranging. It touches on issues including data governance, intellectual property rights, environmental impact concerns, and the future of work itself. The range of regulatory and public policy responses produced in 2024 reflects this:

- The Council of Europe's groundbreaking Framework Convention on Artificial Intelligence,[5] the first international legally binding treaty regarding AI, prioritizes ensuring that AI systems are "consistent with human rights, democracy and the rule of law".

- The European Union's AI Act[6] seeks to regulate AI systems in the EU internal market, both to promote their development and to protect European businesses and consumers.

- ASEAN (the Association of Southeast Asian Nations) recently published its Guide on AI Governance and Ethics,[7] which aims to build regional cooperation to address the challenges posed by AI.

Additionally, the G7, G20, OECD, African Union, and many other international bodies have all published various positions and policies on AI in just the past two years.

Amidst all this, the cybersecurity dimension could easily become lost, yet its significance cannot be underestimated. Governments and policymakers in dedicated cyber discussions are paying attention, however, as shown by the recently adopted Third Annual Progress Report of the UN General Assembly (UNGA) OEWG on security of and in the use of ICTs, in which Member States noted:

> ***"…AI can be used to enhance ICT security, increase resilience, improve response time to ICT incidents and strengthen networks. States also highlighted that AI is likely to increase the volume and heighten the impact of ICT attacks through the evolution and enhancement of existing tactics, techniques and procedures. … States underscored that there was a need to better understand the risks associated with new and emerging technologies, including AI, in terms of how they related to ICT security, and to implement and strengthen security throughout the life cycle of these technologies, so as to fully seize the opportunities presented by such technologies."[9]***

Almost concurrently, the UNGA was passing its second AI-related resolution in the space of less than six months, which encourages Member States:

> ***"…to increase capacity-building cooperation, including policy exchanges, knowledge sharing activities and the transfer of technology on mutually agreed terms, technical assistance, lifelong learning, personnel training, skilling of workforce, international research cooperation, voluntary joint international research laboratories and artificial intelligence capacity-building centres, …and to hold training courses, seminars and workshops, among others for sharing experiences and best practices".***

The UNGA resolution concludes with a request to the UN Secretary-General to report to the 2025 session of the General Assembly on the "unique challenges faced by developing countries in artificial intelligence capacity-building, with recommendations that address those challenges."

This range of policy activity reflects the importance of AI and provides a useful grounding to collectively tackle the global cyber capacity building challenge.

The Way Ahead

However, despite these constructive initiatives, the question of how states and non-state stakeholders will address these challenges remains open. Governments and regulators are watching developments closely, assessing the risks as they evolve, while watching their peers and neighbors to see which strategies are most effective. The private sector understands the double-edged sword that AI presents in a cybersecurity sense, and is working hard to ensure that defense wins out over a new generation of AI-enhanced offence. Aligning the interests and approaches of these different stakeholders will be essential to strengthen cybersecurity globally, and requires cooperation to ensure no region or sector is left behind.

Cyber capacity building is a key response to meet these challenges, and recent discussions in the GFCE Working Groups have highlighted the need for existing efforts to incorporate AI considerations. A meeting of GFCE Working Group E (Standards and Emerging Technologies),[10] which took place alongside the WSIS+20 Forum High-Level Event and the ITU's AI For Good conference in Geneva, stressed the opportunities that AI presents to develop capacity building activities that will reach more people with deeper content.

Working together to harness these AI opportunities offers our best chance to meet the challenges of an AI-enhanced threat landscape. Leveraging and improving our existing models for cooperation and coordination (such as the GFCE) will allow us to move quickly and effectively - as we must!

THE GLOBAL CONFERENCE ON CYBER CAPACITY BUILDING:

ROAD TO GENEVA 2025

***Written by:** Nayia Barmpaliou, GC3B Program Advisor and Noemi Abeniacar, Advisor, The Global Forum on Cyber Expertise (GFCE).*

The GC3B bridges network, knowledge, and cooperation gaps in the cyber and development communities to strengthen our collective cyber resilience.

In an era defined by the world's increased digital reliance and interdependence, new demands have emerged on the skills, expertise, resources, and cooperation needed to reap the transformational opportunities of digital technologies and manage the new risks and vulnerabilities they create. The expanded roll-out of digital infrastructures and online services as enablers of socioeconomic growth across the globe also means that the need for digital resilience has never been greater. Against an evolving cyber threat landscape, it is essential to ensure that the digital transition is secure, sustainable, and resilient against cyber-threats. Cyber capacity building (CCB) is a key international cooperation modality for countries and organizations to achieve that. Responding to the need for a high-level platform that elevates CCB in global governance and development agendas, the Global Conference on Cyber Capacity Building (GC3B) was launched in 2023 in Accra, Ghana. It brought together policymakers and leading experts from around the world to catalyze action for cyber resilient development. Building on the outcomes of the inaugural conference, the second iteration of the GC3B will be held in Geneva on 14-15 May 2025 to drive continued action on inclusive and effective stewardship for cyber resilience in international cooperation and development.

Looking Back: Getting to the 2023 GC3B

The rapid digitization across all sectors, organizations, businesses, and governments around the globe has brought immense benefits in terms of increased productivity, efficiency, and development. Most, if not all, countries have embarked on a digital transformation journey, prioritizing digitization and connectivity to foster economic growth, advance human and social development, enable skills development, and encourage modernization. The game-changing potential of the digital dividends has put digitalization at the heart of efforts to realize the Sustainable Development Goals.

Yet, the swift uptake of digital transformation strategies, digital development programs, and rapid deployment of digital solutions can only be sustainable, secure, and resilient if they are accompanied by adequate investments and capacities in cybersecurity to address and manage the increasing risks that digital interdependence brings. This necessity has led to a growing demand for CCB, particularly by developing countries, that has evolved in the past two decades into a community of practice amongst governments, international organizations, companies, academia, and civil society, all working together to address cyber-related capacity gaps and needs.

While such international cooperation efforts have expanded over time, many have occurred on the periphery of international development cooperation. The need for a shift in this paradigm gained traction as cyber resilience was more and more understood as a key enabler for sustainable and resilient development, instead of as an afterthought or a technical issue. At this point, the GC3B was born out of the need for a high-level platform to energize an actionable dialogue on mainstreaming cyber resilience and elevating CCB to the global governance and development agendas. The inaugural edition of the GC3B was held in Accra, Ghana in November 2023, co-organized by the Global Forum on Cyber Expertise (GFCE), Cyber Peace Institute, World Economic Forum, and World Bank, and hosted by the Ministry of Communication and Digitalisation of Ghana. It brought together leaders, decision-makers, and experts across sectors – public, private, academia, civil society – from the cybersecurity, CCB, and international development fields to work on common goals and solutions in supporting all countries develop the requisite expertise, skills, and resources for a secure and resilient digital transformation.

The outcomes of the conference were captured in the Accra Call for Cyber Resilient Development, an action framework aimed at stimulating action and voluntary commitments by all stakeholders within their respective mandates to elevate cyber resilience across international and national development agendas and to promote CCB that supports broader development goals.

The Accra Call for Cyber Resilient Development: From Pledges to Actions

The Accra Call was developed through numerous consultations with diverse stakeholders, drawing from existing shared commitments, ongoing relevant efforts in international fora and processes, and lessons learned by the CCB and development communities. It serves as both a blueprint and motivation for voluntary action for all stakeholders to strengthen the role of cyber resilience in sustainable development, advance effective CCB, foster stronger partnerships and better coordination, and unlock financial resources for cyber resilience.

Thus far, the Accra Call has been endorsed by over sixty-five stakeholders worldwide, who have affirmed their willingness to support and contribute to the realization of its objectives within their mandates and processes. In addition, organizations are encouraged to make pledges on how they concretely plan to implement certain actions of the Accra Call, which a multitude of organizations have already contributed to.

The Accra Call sets out key principles, priorities and specific steps, all voluntary and non-binding, that stakeholders can take to build cyber resilience. It emphasizes the need for a coordinated, global approach where countries support each other in developing the necessary resources, knowledge and skills. As in an interconnected digital world a chain is only as strong as its weakest link, the Accra Call underscores that no country should be left behind in its digital evolution.

The launch of the Accra Call is significant as it is a community-based, inclusive process, whereby the endorsers, pledgers, and other interested stakeholders use its structure to prioritize specific actions closer to their interests and mandates, drive improvements in their practices, share their experiences, and learn from others. Shepherded by the GFCE, this inclusive, multi-stakeholder community - that brings together diverse parts of the cybersecurity, capacity building, and development ecosystems - has the potential to incubate ideas for new CCB solutions and approaches that its members can test within their own mandates and, if successful, promote evidence-based solutions for the broader community. Each GC3B iteration is a great opportunity for periodical positive feedback loops on stakeholders' collective progress and adaptation moving forward.

Looking Ahead: The GC3B 2025 in Geneva, Switzerland

Building on the successes of the inaugural event, the second edition of the GC3B will be held in Geneva, Switzerland, on May 14-15, 2025, hosted by the Swiss Federal Department of Foreign Affairs. It aims to bring together even more stakeholders from different communities, disciplines and functions – notably government authorities, development donors and actors, multilateral and bilateral financial institutions, international and regional organizations,

Senior Presidential Advisor of Ghana H.E. Yaw Osafo-Maafo signs the Accra Call, in presence of Hon. Minister of Communications and Digitalisation Ursula Owusu-Ekuful (left) and Director-General of the Cyber Security Authority, Dr. Albert Antwi-Boasiako (right)

the private sector, the technical community, civil society, academia, philanthropic institutions, tech and social entrepreneurs – for a meaningful and structured dialogue on CCB and cyber resilience.

GC3B 2025 will serve as a global platform to:

- Increase awareness and expand knowledge of existing good practices, tools, methods, and lessons for improving CCB and cyber resilience for development.
- Generate new insights and out-of-the-box thinking for CCB in ways that complement and challenge traditional approaches.
- Bring together communities and stakeholders engaged in CCB and development cooperation to bridge siloed approaches, accelerate expertise-sharing, and foster stronger cooperation locally, regionally and globally.
- Drive collective action on existing commitments, solutions, and plans, or propose new solutions to strengthen cyber resilience.

All stakeholders and communities will be invited to reflect on existing approaches to international cooperation and partnerships for cyber resilience and capacity building. The discussions will be defined by the needs and expertise of developing countries, drawing on their experiences as well as considering the role of new and emerging technologies.

With GC3B 2025 already in the works for a Geneva iteration, this conference is positioning itself as a key driver of cyber resilient development globally. The GC3B, in all its subsequent editions, will strive to bridge network, knowledge, and cooperation gaps in the cyber and development communities, and help CCB efforts pivot to more mature, effective, and sustainable models that can strengthen our collective cyber resilience.

Members of TT-CSIRT with members of the OAS CSIRTAmericas Team.

THE IMPACT OF THE CSIRTAmericas NETWORK

ON THE CARIBBEAN INCIDENT RESPONSE ECOSYSTEM

***Written by:** Mr. Anish Bachu, ICT Security Specialist – Team Lead Operations, Trinidad and Tobago Cyber Security Incident Response Team.*

“Being a member of the CSIRTAmericas Network has improved service delivery to our constituents and helped establish us as a trusted partner in the Trinidad and Tobago cyber-security landscape.”

The digital environment in the Caribbean is evolving rapidly as it races to keep up with the rest of the world. Digital transformation initiatives and new technologies bring benefits, but also increase the attack surface for cyber threats, creating a target-rich environment for an ever-expanding repertoire of threat actors. This can seem an insurmountable challenge for any country, but particularly for the small island developing states in the Caribbean.

Cyber threats are a national security concern and require concerted action and resources

In Trinidad and Tobago we have seen a massive increase in cyber security incidents over the past five years, affecting multiple sectors. The number of reported incidents has more than doubled, increasing by 125% from 2019 to 2023. This increase is in keeping with global incident trends, and shows why cyber security is now an area of national security concern. Governments had already recognized this in 2013, when heads of government at CARICOM, the twenty-country organization of the Caribbean Community, adopted its Crime and Security Strategy, categorizing cybercrime under “Tier 1 – Immediate Significant Threats”. Since then, the threat and subsequent need to share information and increase cyber threat response capacity – both nationally and regionally - has grown.

Yet despite the growing threat to national interests and security, most Caribbean nations do not have dedicated Cyber Security Incident Response Teams (CSIRTs). Even in countries where there is a CSIRT, it has acute resource challenges. The heightened threats and scant resources mean Caribbean CSIRTs need to leverage resources available from the international community. In that light, the CSIRTAmericas Network plays a vital role in the Caribbean cybersecurity ecosystem, by providing invaluable resources that help us combat, respond to and prepare for cyber threats. These resources include cyber threat intelligence, training, and seamless access to the regional community.

We work collaboratively to get cyber threat information to where it’s needed, when it’s needed

TT-CSIRT has built trust among our constituents by providing accurate, actionable and timely cyber threat intelligence. Put simply, we get critical information to the people who need it to protect their organizations and our nation’s critical infrastructure. The data provided by the CSIRTAmericas Network via their feeds and dashboards is a major component of our cyber threat intelligence program. The dashboards give an instant picture of the national cybersecurity landscape to identify areas of concern and inform remediation action. The data also feeds into systems that support the sectorial Information-Sharing and Analysis Centers (ISACs).

International resources are essential, but skilled and committed people working at the national level are fundamental. The talented members of TT-CSIRT are the driving force behind our successful service delivery. We boast a young and innovative team comprised 50% of women.

How do we ensure our team and community are prepared to face the evolving threat?

We are constantly improving through targeted training and capacity-building, both for our own team and our community. The CSIRTAmericas Network is the single largest provider of training for TT-CSIRT, helping keep us prepared to defend and respond to cyber-attacks. The trainings are available for free and are delivered by members of the network as well as third-party organizations.

A CSIRT's most valuable resource is the CSIRT community, the collaborative network of organizations working together to share information and best practice. Collaboration is in our organizational DNA; it was one of the five pillars that defined our 2012 Trinidad and Tobago National Cyber Security Strategy. The national strategy emphasized international information exchange and called for a mechanism to bring a variety of perspectives, expertise, and knowledge together to reach consensus to enhance security. TT-CSIRT serves that role today, as a focus for national collaboration and to access international information and skills via the CSIRTAmericas Network.

CSIRTAmericas Network helps us do a tough job better

Our ability to draw on the knowledge and experience of other CSIRTs at a moment's notice via the CSIRTAmericas Network has directly increased the effectiveness of our incident response capability and CTI program. The CSIRTAmericas Network has developed into a "neighbourhood watch" where CSIRTs can share any information

TT-CSIRT's international women's day 2024 promotion for women in cyber.

National Cyber Security Capability Development Program (NCSCDP) - Goals

The late Angus Smith, former manager of TT-CSIRT addresses government cybersecurity professionals at a table top exercise hosted by the OAS and TT-CSIRT in Port of Spain, Trinidad and Tobago in February 28th 2023.

they find about other member countries. This supports regional security while expanding our detection capacity beyond just the members of our team. On more than one occasion we have used our connections in the CSIRTAmericas Network to help during incident response or to refine our cyber threat intelligence.

In short, the CSIRTAmericas Network has bolstered TT-CSIRT's capability, capacity and operational efficiency. Most importantly, it has helped to establish TT-CSIRT as a trusted partner in the Trinidad and Tobago cybersecurity landscape, and as a leader among Caribbean CSIRTs. By increasing both our capacity and capabilities, the CSIRTAmericas Network has helped us earn and deepen the trust of our community to protect Trinidad and Tobago's digital landscape, now and into the future.

REGIONAL

SECURING CARIBBEAN CYBERSPACE:

A DECADE OF PROGRESS AND PARTNERSHIP WITH CARICOM IMPACS

***Written by:** CARICOM Implementation Agency for Crime and Security (IMPACS).*

CARICOM IMPACS is working systematically and effectively with a range of international partners to truly deliver for the Caribbean region.

The Caribbean region has made significant strides in cybersecurity over the past decade, with key achievements and initiatives led by the CARICOM Implementation Agency for Crime and Security (IMPACS). The agency has been instrumental in enhancing the detection, investigation, and prevention of cybercrime in CARIFORUM Member States, in compliance with international standards.

Lt. Col. Michael Jones, Executive Director of CARICOM IMPACS, highlights the importance of this work:

> ***"We are ensuring that people, organizations, and countries are equipped with the competencies, tools, and continued support they need to prevent and deal with these types of incidents, if and when they occur, by creating a culture of security and strengthening our technological defenses."***

A significant milestone in this journey was the cyber component of the 11th European Development Funded (EDF) Project, which began in January 2019 and ran until January 2024. This project has enhanced the detection and investigation of cybercrime in CARIFORUM Member States. The project provided technical assistance for anti-cybercrime and cybersecurity legislative and policy establishment, improvements, and amendments. Key achievements under this project include:

- The development of a regional cybercrime policy and legislative guidance document to direct the establishment of harmonized policy and legislation within Member States, in keeping with the objectives of the CARICOM Cyber Security and Cybercrime Action Plan (CCSCAP).

- The design, development, and delivery of targeted training on cybercrime and cybersecurity for law enforcement and judiciary professionals in Member States, integrated into the curricula of regional universities and educational institutions.

- The delivery of regional awareness-raising sessions targeting senior officials, ministers, parliamentarians, policymakers, and the public, which reduced the risk of cybercrime and implemented mechanisms to enhance cybersecurity.

- Better regional and international cooperation and collaboration for enhanced incident response, cybercrime investigation, and capacity building for CARICOM IMPACS as the lead implementing agency of the CCSCAP.

In January 2024, CARICOM IMPACS formed the Cyber Fusion Unit (CFU) at the Regional Intelligence Fusion Centre (RIFC), CARICOM IMPACS Headquarters, Port of Spain, Trinidad, The CFU was formed to further operationalize the five priority areas of the CCSCAP:

- **Public awareness**
- **Building sustainable capacity**
- **Technical standards and infrastructure**
- **Legal environment**
- **Regional and international cooperation collaboration: incident response, cybercrime investigation, and capacity building**

The CFU's mission is to protect critical infrastructure, promote trust and cooperation, and enhance the region's overall cyber resilience. The CFU has been operationalizing a regional platform, the Digital Forensic Management Platform, to enhance and coordinate regional cyber response efforts.

The GFCE, with its network of regional hubs and liaison offices, has supported CARICOM IMPACS by providing guidance, expertise, and support to bolster cyber resilience in the Caribbean Community. The GFCE's hub for the Americas and the Caribbean promotes cooperation, trust, and knowledge sharing.

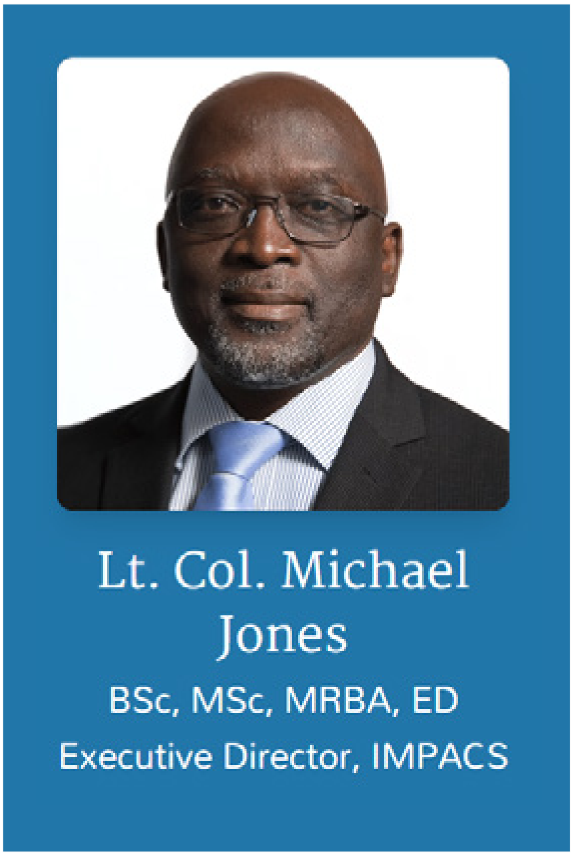
CARICOM IMPACS has also been tasked with participating in the World Bank Digital Transformation project targeted at Organization of Eastern Caribbean States (OECS) Member States. This project is providing technical oversight of the project activities under Subcomponent 1.3: Cybersecurity, Data Protection, and Privacy: Legal and Regulatory Environment.

Additionally, CARICOM IMPACS has contributed to the ongoing process of crafting the CARICOM Cyber Resilience Strategy - 2030, led by the CARICOM Secretariat. The strategy focuses on six key areas: mature governance across the CARICOM region, human capital management, increasing public awareness and cyber literacy, defending critical information and infrastructure, regional laws and regulations with cooperation and reciprocity, and regional information-sharing and incident response capabilities.

CARICOM IMPACS has also partnered with the United States State Department Bureau of International Narcotics and Law Enforcement Affairs (INL) to conduct a research-based project mapping crypto-currencies and virtual assets to criminal activity in CARICOM Member States.

In conclusion, the past decade has seen significant progress in securing Caribbean cyberspace through the efforts of CARICOM IMPACS and its partners. By focusing on public awareness, building sustainable capacity, establishing technical standards and infrastructure, improving the legal environment, and fostering regional and international cooperation, the agency has made great strides in creating a culture of security and strengthening technological defenses in the region.

Executive Director
CARICOM IMPACS.



Ms. Tupou Vainikolo (Tonga) intervening during the UN Adhoc Committee's session on Cybercrime, New-York, August 7th, 2024. Photo Credits: Mr. Domingo Kabunare (Kiribati)

MAKING SURE PACIFIC VOICES ARE HEARD AT UNITED NATIONS CYBER MEETINGS

***Written by:** Susan Garae Project Associate, GFCE – WiC, Pacific Hub.*

We must act practically and inclusively to ensure UN cybercrime frameworks reflect Pacific Island countries' experiences and interests.

The landscape of cybercrime is rapidly evolving, necessitating a unified global response. International treaties and conventions are pivotal frameworks for fostering collaboration and establishing standardized approaches to cyber threats. The ongoing negotiations at the UN Ad Hoc Committee (AHC) on Cybercrime are especially important for Pacific Island countries (PICs).

PICs are geographically isolated, with limited resources and unique vulnerabilities. They rely heavily on constrained internet infrastructure, making them susceptible to cyberattacks that can devastate essential services and disrupt communication networks. The escalating challenges of climate change, such as rising sea levels and extreme weather events, further imperil critical infrastructure - including vulnerable undersea cables – and amplify PICs' digital fragility.

In this context, the need for robust international cybersecurity agreements cannot be overstated. These agreements can fortify defenses and help PICs to access the support and resources they need to mitigate their exceptional vulnerabilities and risks. They can also facilitate the provision of cyber capacity-building (CCB) initiatives tailored to the specific needs of PICs.

However, in order to be relevant and practical, these international agreements need to reflect the distinctive context and challenges of the Pacific region. This requires ensuring that Pacific Islanders are aware of, can access and contribute effectively to UN discussions. That is why a considerable part of our work at the GFCE – WiC is focused on increasing and deepening our regional participation in UN processes, especially the ongoing negotiations at the UN's Ad Hoc Committee (AHC) on Cybercrime and its Open-Ended Working Group on security and ICTs (OEWG).[1]

The challenge: Low awareness of and participation in UN cyber diplomacy

Pacific voices at UN cyber meetings are far too few. The region is inadequately represented in processes where decisions are made that impact the governing of our national systems. For example, the ongoing UN cybercrime convention negotiations have a very small number of active participants from the Pacific, and this capable but tiny team struggles to keep abreast of all relevant issues and participate in the parallel sessions held at these meetings.

We conducted a survey to quantify and deepen our understanding of relatively low participation levels, in order to better strategize effective responses to get Pacific voices truly heard.

In early 2024, GFCE's Pacific Hub carried out a survey on the awareness and understanding of the UN Ad Hoc Committee on Cybercrime. It was completed by thirty-two relevant government officials across the Pacific Islands. Of this dedicated group, only two individuals reported that they were very familiar with this key UN Committee.

Officials were asked:

"How familiar are you with the United Nations Ad Hoc Committee on Cybercrime and its objectives?

- Very familiar
- Somewhat familiar
- Not familiar at all?"

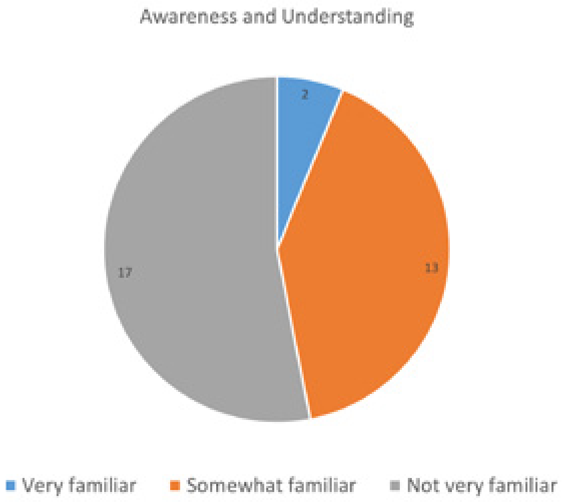


Figure 1: Participant familiarity with United Nations Ad Hoc Committee on Cybercrime

As the chart shows, more than half of the officials surveyed were not very familiar with the work of this key committee. This finding highlights the stark reality of low participation and familiarity with the UN systems. To be clear, governments want to participate effectively, but they face significant barriers.

Another survey question asked respondents which were the main challenges they encountered on joining the UN Ad Hoc Committee on Cybercrime. Almost two thirds said a lack of funding and support was the top challenge, with the next most common barriers being limited technical expertise and resources, and limited access to information.

When asked to comment further on the barriers to effective participation, respondents added:

- *"Lack of human resources, which is linked to funding, to cover parallel sessions during the UN AHC negotiations."*

- *"Not enough officers to be attending the meetings abroad.*

- *One person performing many tasks, and responsibilities."*

Although the survey focused on the UN AHC on Cybercrime, we expect that PIC participants in the UN OWEG experience the same challenges. Our survey findings strongly indicate that additional help and support are needed so that officials can effectively represent their countries in both these processes.

Convening Regional Players to Galvanize Action

Using the survey results to guide the program, we then organized a webinar in May 2024 entitled: "The Crucial Role of Country Representation in UN Cyber Meetings, Focused on Ad Hoc Committee on Cybercrime". The seminar was held by the GFCE Pacific Hub under the UN Women in Cyber & Internet Multistakeholder webinar project.

It included almost forty experts and stakeholders from across the Pacific and Southeast Asia. Mr. Saia Vaipuna, Director of the GFCE Pacific Hub, opened the seminar, and Ms. Briony Daley Whitworth, Director of the Cyber & Tech Multilateral Engagement Section at the Department of Foreign Affairs and Trade, Australia, gave a keynote speech.

Ms. Daley said active involvement in UN cyber negotiations is crucial to prevent nations from being side-lined, potentially compromising their national interests, and weakening global cyber governance overall. She emphasized the importance of sending skilled and committed representatives to ensure every nation's voice is heard and their interests safeguarded.

A panel discussion moderated by Mr. Bart Hogeveen, GFCE, focused on the experiences of three experienced country representatives in cyber processes; Mr. Domingo Bauro Kabunare of Kiribati's Digital Transformation Office, Ms. Nathaya Vongvorakam of Thailand's Ministry of Foreign Affairs, and Mr. Josaia Naigulevu, Public Prosecutor from Vanuatu. The panellists identified the key challenges of capacity constraints, and resource limitations. They proposed strategies to improve participation from developing countries in the Pacific and Southeast Asia. In his closing remarks, Mr. Vaipuna called for strengthened engagement from all nations to ensure balanced and effective cyber governance.

The webinar underscored the need for active and effective participation to ensure our individual and collective voices contribute to shaping the global cyber governance landscape, and that our national and regional interests should not only be represented but fiercely protected.

We're already working on it: Regional Efforts and Support

The message is clear. We need more resources, better support and also more active coordination within the region to maximize our impact at international processes. Some of this work is already being done. Existing initiatives have already produced successful results:

- **Global Action Against Cybercrime (GLACY project)**

The GLACY project and its later iterations (GLACY+ and GLACY Extended) have strengthened criminal justice capacity through training and advice, resulting in Tonga, Fiji and Kiribati becoming parties to the Budapest Convention on Cybercrime.

- **Women in International Security and Cyberspace Fellowship (WiC)**

WiC currently supports attendance at the UN OEWG, delivering negotiation skills trainings to women diplomats from all regions in United Nations cyber negotiations.

- **UN Cyber Diplomacy in the Pacific**

Implemented by Independent Diplomat, this project builds the capacity of Pacific leaders, officials and negotiators to play an active role in UN cyber discussions. It supports them to understand the issues at stake and the role of responsible state behavior in cyberspace, to develop and articulate their country's positions and responses, and to increase their engagement in cyber diplomacy in support of a free and open internet.

The project offers strategic advice on OEWG and cybercrime processes, and supports the development of confidence-building measures. In our own survey, this project was brought up as being particularly helpful. One respondent said: *"… Independent Diplomat has assisted us initially in person and in subsequent sessions online, by providing summaries during the meeting, offering advice and to draft interventions for the negotiations. This helps with the lack of human resource challenge."*

Together, these initiatives both fortify PICs' defenses against cyber threats and help them to shape global cybersecurity frameworks and agreements so that they reflect the particular needs and goals of this region. Moving forward, continued and enhanced support and collaboration are essential to sustain this momentum and further empower PICs in safeguarding their digital landscapes.

Empowering Each Other

As well as highlighting resource scarcity and a need for ongoing CCB for participating officials, our survey found that coordination within and between Pacific Island governments needs to be boosted. One respondent identified the *"lack of coordination between the Pacific bloc (nations) to ensure that there is strength in negotiating positions and needs. Most work in silo and often we try to lean towards proposals from nations we share a similar position on."*

Sometimes, low-resource methods to facilitate better coordination can work well. One of the practical tools the Pacific GFCE Hub employs is a dedicated WhatsApp group called "Pacific CCB Community". It's an informal way to exchange experiences, discuss potential initiatives and activities, facilitate feedback and foster collaboration within the community.

We hope to see more approaches like this to enhance regional cooperation and keep building robust cyber capacity among PICs. By sharing our experiences, we empower and learn from each other. And by coordinating how we develop and put forward our positions, we can ensure better coverage at the many parallel meetings and lasting impact at the UN and elsewhere.

Conclusion

We are motivated to keep going by the words of one of our survey respondents: *"Representing a nation is not that simple, it is a big shoe to fill. Having a supportive community can help."* Our role is to help that emerging and supportive community to flourish so it can shape current and future international cyber diplomacy.

Clearly, ensuring the most effective participation of PICs is of great benefit to the Pacific Islands' security and economies, and a question of fairness and inclusivity. However, we believe the future cybercrime framework and other UN processes will benefit tangibly from the active involvement of our region.

Our challenges of infrastructure fragility and relatively low levels of available public resources are shared by other countries and regions. Our insights and perspectives help to ensure that international instruments are robust and applicable for everyone, everywhere. The global cyber security chain is only as strong as its weakest link, and strengthening our involvement and contribution to global deliberative processes helps to make them better for everyone.

APT THREAT LANDSCAPE: GLOBAL CYBERSECURITY RESPONSES & PERSPECTIVE FROM WESTERN BALKANS

***Written by:** Drinor Selmanaj, CEO of Cyber Academy, specializing in adversary emulation and the operational strategies of advanced threat actors.*

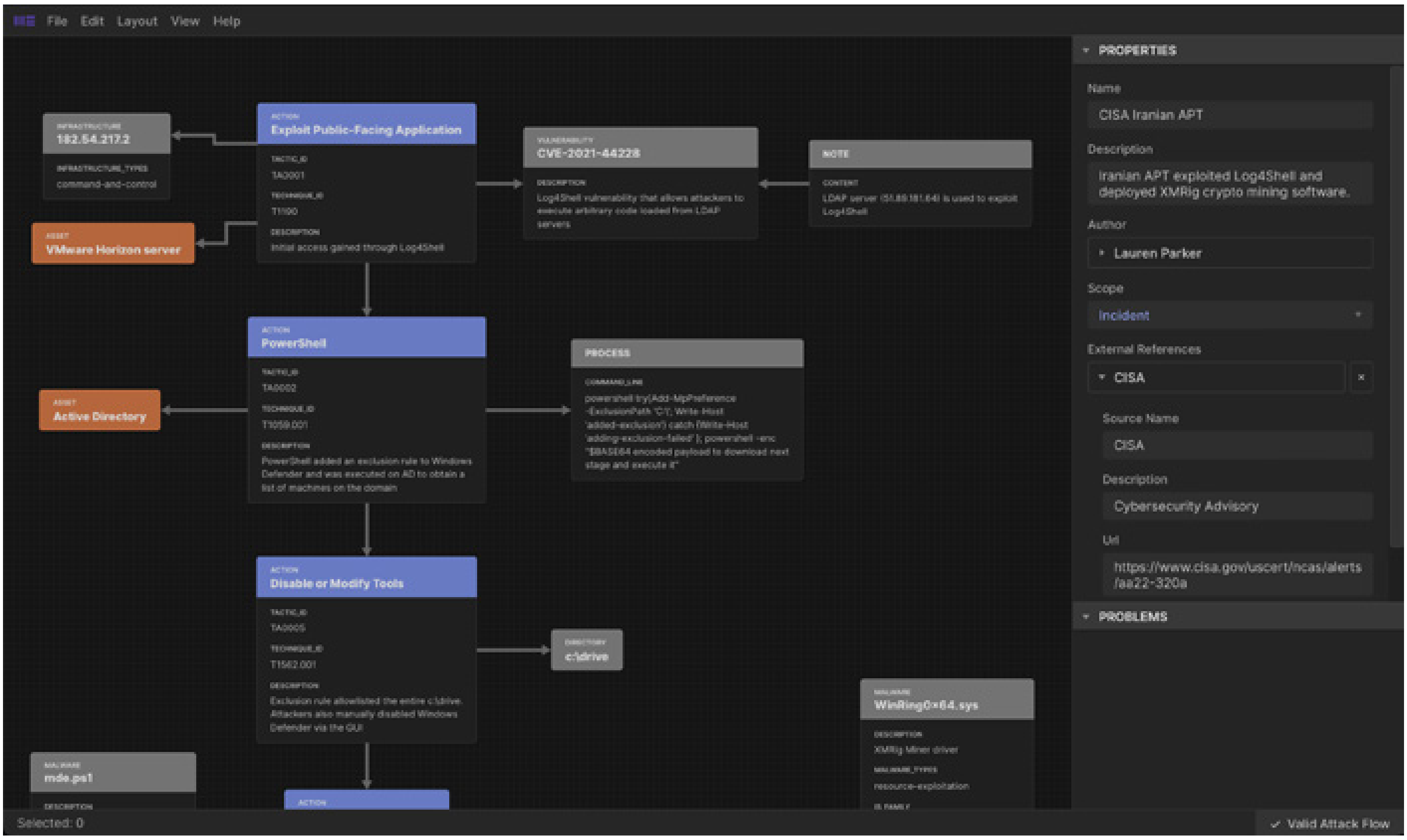
Navigating differing national policies, the complexities of international law, and geopolitical tensions is challenging, but working together is crucial for a unified approach.

Advanced Persistent Threats (APTs) are among the most sophisticated cyber threats, known for their resilience, strategic focus, and ability to remain undetected for prolonged periods. This article examines the tactics of hostile nation-states, the long-term economic and political effects of cyberattacks, and the current state of cybersecurity in the West Balkans.

The Cyber Threat Landscape

The sophistication of APTs lies in their complex tactics, techniques, and procedures (TTPs). These cyber threats are not merely about immediate data theft - they involve prolonged campaigns designed to infiltrate and compromise critical systems over time. Effective mitigation of APTs requires an integrated approach that combines advanced defense mechanisms with international cooperation. Cyber-interference's economic and political ramifications underscore the urgent need for nations to bolster their cybersecurity infrastructures.

For those interested in delving deeper into the complex profiles of APTs, the Europol APT Profiles[1] provide a comprehensive resource. This repository offers detailed analyses of various groups, outlining their operations, targeted sectors, and notable incidents.



INFRASTRUCTURE
182.54.217.2
INFRASTRUCTURE_TYPES
command-and-control

ASSET
VMware Horizon server

ACTION
Exploit Public-Facing Application
TACTIC_ID
TA0001
TECHNIQUE_ID
T1190
DESCRIPTION
Initial access gained through Log4Shell

VULNERABILITY
CVE-2021-44228
DESCRIPTION
Log4Shell vulnerability that allows attackers to execute arbitrary code loaded from LDAP servers

NOTE
CONTENT
LDAP server (51.89.181.64) is used to exploit Log4Shell

ASSET
Active Directory

ACTION
PowerShell
TACTIC_ID
TA0002
TECHNIQUE_ID
T1059.001
DESCRIPTION
PowerShell added an exclusion rule to Windows Defender and was executed on AD to obtain a list of machines on the domain

PROCESS
COMMAND_LINE
```
powershell try{Add-MpPreference
-ExclusionPath 'C:\'; Write-Host
'added-exclusion'} catch {Write-Host
'adding-exclusion-failed' }; powershell -enc
"$BASE64 encoded payload to download next
stage and execute it"
```

ACTION
Disable or Modify Tools
TACTIC_ID
TA0005
TECHNIQUE_ID
T1562.001
DESCRIPTION
Exclusion rule allowlisted the entire c:\drive. Attackers also manually disabled Windows Defender via the GUI

DIRECTORY
c:\drive

MALWARE
WinRing0x64.sys
DESCRIPTION
XMRig Miner driver
MALWARE_TYPES
resource-exploitation
IS_FAMILY

MALWARE
mde.ps1
DESCRIPTION

ACTION

Name
CISA Iranian APT
Description
Iranian APT exploited Log4Shell and deployed XMRig crypto mining software.
Author
Lauren Parker
Scope
Incident
External References
CISA
Source Name
CISA
Description
Cybersecurity Advisory
Url
https://www.cisa.gov/uscert/ncas/alerts/aa22-320a

Figure 1: Iranian APT Exploiting Log4Shell to Deploy XMRig Miner, Visualized with Attack Flow.

Pre-Positioning in Cyber Space

Adversarial nation-states employ various sophisticated strategies to achieve their objectives. One prominent approach involves pre-positioning attacks, where adversaries infiltrate critical systems to establish a foothold for potential future sabotage. Unlike immediate data theft or intelligence gathering, pre-positioning aims to compromise systems in advance, allowing attackers to launch cyber-attacks at critical moments. This poses significant risks, including the potential to disrupt essential services such as power grids and communication networks, compromise national security by accessing sensitive military and government networks, and cause economic damage through attacks on financial systems and manufacturing processes.[2]

Examples of Pre-Positioning in Cyber Space:

1. **Operation Cloud Hopper:** This campaign, attributed to the Chinese APT group APT10, targeted managed IT service providers (MSPs) to gain access to the networks of their clients, including multiple global corporations. The attackers used this access to steal sensitive business information and establish long-term footholds for future exploitation[3]

2. **Operation Aurora:** In 2009, Chinese cyber attackers infiltrated the networks of major corporations, including Google, Adobe, and others, to steal intellectual property and gain access to corporate systems. This attack highlighted the sophisticated nature of pre-positioning cyber threats[4/5/6]

The Economic and Political Impact of Cyber-Interference

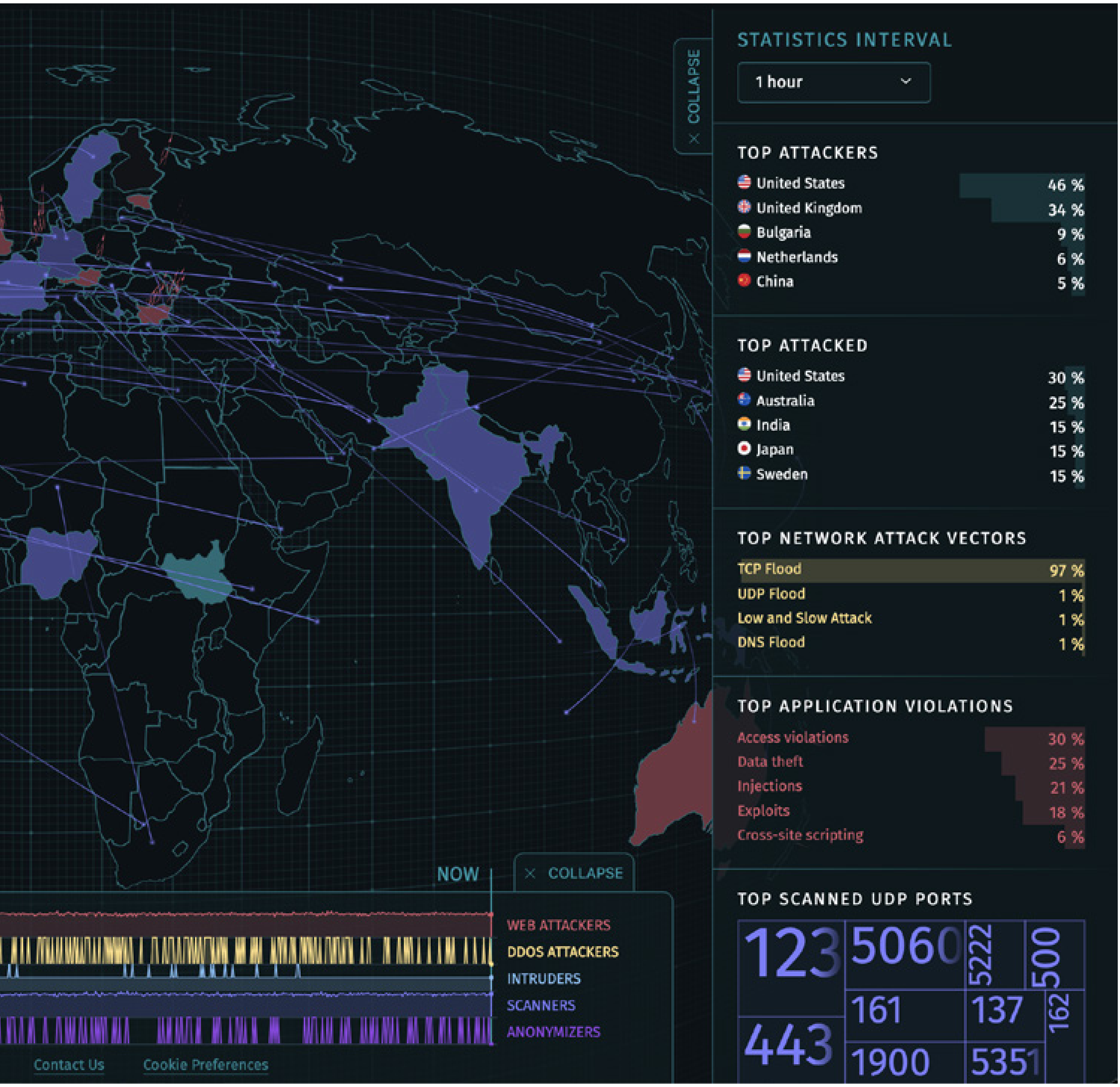
The financial toll of cybercrime has been staggering. Recent surveys estimate that cyber-attacks cost the German economy 206 billion euros in 2023 alone.[7] This figure reflects the increasing sophistication of cyber-attacks, the widespread digitalization of businesses, and the adoption of remote work practices.[8] The direct financial losses from activities such as ransomware attacks, data breaches, and phishing scams are compounded by indirect costs, including operational disruptions, legal and regulatory expenses, reputational damage, and substantial investments in cybersecurity measures.

The political consequences of cyber-interference are equally concerning, as evidenced by incidents targeting the UK. State-sponsored cyber-espionage campaigns have increasingly focused on democratic institutions and governance processes.[9] The objectives often include stealing login credentials, deploying malware, and gathering intelligence to influence political processes.[10] These campaigns aim to undermine democratic processes, erode public trust in government institutions, and gain strategic advantages on the global stage.[11]

Strategic Cybersecurity Approaches

A denial-based approach to cybersecurity aims to prevent cyber-attacks by making it exceedingly difficult for adversaries to achieve their objectives.[12] This strategy includes strengthening the robustness of critical infrastructure, which enhances the resilience and security of essential systems and services to withstand cyber-attacks.[13] It also involves developing advanced defense mechanisms and implementing sophisticated technologies and practices to detect, prevent and respond to cyber threats.[14] Fostering collaboration with international allies to share intelligence, resources, and best practices is crucial for creating a unified defense front against cyber threats.[15] Despite its effectiveness, the denial-based approach faces several challenges, such as ensuring consistent cybersecurity standards across regions with varying levels of technological advancement and resource allocation, addressing legislative and regulatory obstacles that can impede swift action and adaptation to emerging cyber threats, and managing the high costs associated with implementing and maintaining robust cybersecurity defenses, which can be particularly burdensome for entities with limited resources.[16]

ATTACK TYPES
✓ Web Attackers
✓ DDoS Attackers
✓ Intruders
✓ Scanners
✓ Anonymizers
21:10
21:30
© Copyright 2024 Radware Ltd. – All Rights Reserved
ⓘ What is the Radware Live Threat Map?



STATISTICS INTERVAL

1 hour

TOP ATTACKERS

United States	46 %
United Kingdom	34 %
Bulgaria	9 %
Netherlands	6 %
China	5 %

TOP ATTACKED

United States	30 %
Australia	25 %
India	15 %
Japan	15 %
Sweden	15 %

TOP NETWORK ATTACK VECTORS

TCP Flood	97 %
UDP Flood	1 %
Low and Slow Attack	1 %
DNS Flood	1 %

TOP APPLICATION VIOLATIONS

Access violations	30 %
Data theft	25 %
Injections	21 %
Exploits	18 %
Cross-site scripting	6 %

TOP SCANNED UDP PORTS

123 5060 5222 500 161 137 162 443 1900 5351

Figure 2: This visualization highlights the various cyber-attack types targeting different regions worldwide.

Alternatively, a proactive "Defend Forward" strategy involves preemptively disrupting malicious cyber activities before they can cause harm.[17] This approach emphasizes taking the initiative in cybersecurity by identifying and neutralizing cyber threats before they reach their targets, often through offensive cyber operations.[18] Proponents of this strategy underscore the importance of proactive measures, highlighting the need for early intervention and continuous monitoring to prevent cyber-attacks from succeeding.[19] This strategy contrasts with the more conservative stance of European nations, which prefer deterrence by denial due to legal and public sentiment concerns.

The Western Balkans Perspective

The Western Balkans face significant cybersecurity challenges, exacerbated by geopolitical complexities and varying levels of technological advancement among their nations. State-sponsored adversaries often target this region as a proxy battleground for greater geopolitical struggles. Countries in the Western Balkans are increasingly becoming targets for cyber espionage, primarily aimed at destabilizing political environments and gathering intelligence on political, military, and economic activities. The financial constraints of many nations in the region mean that resources for robust cybersecurity measures are often limited, making them vulnerable to sophisticated cyber-attacks. Politically, the Western Balkans have seen attempts to influence elections and political processes through cyber means. These cyber operations aim to undermine trust in democratic institutions, spread misinformation, and create political instability. The influence of external state actors through cyber means has been a growing concern, with implications for regional stability and security.

According to the PwC Cybersecurity Ecosystem Report (2022), North Macedonia's MKD-CIRT reported 1443 incidents in 2020, up from 1060 in 2019, with phishing being the most common type of attack. In Serbia, SRB-CERT reported 276 incidents in 2020, up from 152 in 2019, with phishing and DDoS attacks becoming increasingly prevalent. A major cyber event not covered in the PwC report occurred in 2022 when Iranian APT actors launched significant cyberattacks against Albania, claimed by a group called "Homeland Justice." Albania's primary cybersecurity threats include spam, malware, phishing, and email spoofing. These statistics highlight the region's increasing frequency, underscoring the need for improved cybersecurity measures and regional cooperation.[20]

During her speech at the High-Level Cybersecurity Conference in Tirana on July 9, 2024, Majlinda Bregu, Secretary of the Regional Cooperation Council (RCC), underscored several critical trends concerning APTs. The region experienced a 40% surge in cyber incidents over the past year, with data breaches compromising over 1.2 million personal records. Although ransomware represents a distinct threat, the rise in such attacks underscores the region's overall vulnerability, which APTs can exploit. Additionally, 75% of businesses in the Western Balkans reported phishing attacks last year, often used by APTs as an initial vector to infiltrate systems. APTs frequently exploit critical vulnerabilities in cloud environments to establish prolonged access and conduct extensive data exfiltration. The RCC's Balkan Barometer revealed significant public concern regarding potential cyberattacks and disinformation, critical elements of APT campaigns to destabilize regions.

The EU's Growth Plan for the Western Balkans, presented on December 6, 2023, outlines several strategic initiatives to mitigate APT threats. Enhancing digital skills across the region will bolster the capacity to recognize and respond to APTs, addressing the acute shortage of cyber skills and talent. Integrating the ID-Wallet into the EU Single Market will facilitate more robust authentication measures, complicating efforts by APTs to compromise identities and access sensitive systems. Aligning with the EU acquis, particularly the NIS 2 Directive, will strengthen the region's legal and regulatory framework to counter APT threats more effectively. The Common Regional Market (CRM) 2025-2028 prioritizes cybersecurity as a crucial area for digital transformation, encompassing policy reforms and cyber capacity building (CCB). These initiatives and strategic efforts highlight the continuous and necessary measures to enhance cybersecurity resilience in the Western Balkans, particularly against advanced threat actors.

Future Directions in Cybersecurity

Investing in cutting-edge technologies like artificial intelligence (AI) and machine learning (ML) is not just a step, but a leap towards supercharging our defense against cyber threats. These technologies, by analyzing massive amounts of data, can swiftly identify patterns and anomalies that could indicate potential threats, enabling faster and more accurate responses.[21] While there are challenges to overcome, such as ensuring data privacy and managing the resources required, the potential for these technologies in cybersecurity is enormous and truly exciting! Quantum computing, a game-changer on the horizon, holds the promise of revolutionizing encryption methods. This advancement could significantly raise the bar for adversaries attempting to breach secure systems.[22] While we're still in the early stages, with much research and development ahead, initiatives like those by the United States National Institute of Standards and Technology (NIST) to create quantum-resistant encryption algorithms are paving the way for a more secure future.

When government entities and the private sector collaborate, sharing threat intelligence, best practices, and resources, we get a more comprehensive and effective defense against cyber threats.[23] The Cybersecurity and Infrastructure Security Agency (CISA) teaming up with industry leaders is a perfect example of what we can achieve together. Aligning diverse interests and protecting sensitive data while sharing information can be tricky, but the benefits far outweigh the challenges. Given the global nature of cyber threats, international cooperation is not just beneficial, but a necessity. Nations must unite to set common cybersecurity standards and coordinate responses to incidents through international frameworks and agreements.[24] The Budapest Convention on Cybercrime and the European Union Agency for Cybersecurity (ENISA) are prime examples of international collaboration. While navigating differing national policies, the complexities of international law, and geopolitical tensions can be challenging, working together is crucial for a unified approach. Developing and enforcing comprehensive cybersecurity regulations and policies is vital for a resilient cyber environment. These regulations provide clear guidelines for organizations and ensure adaptability to emerging threats.[25] The NIS 2 Directive, implemented across EU member states, is a significant step in the right direction. Consistent enforcement across jurisdictions and keeping regulations up-to-date with rapidly evolving threats can be challenging, but it's essential for maintaining robust security.

Lastly, building a skilled cybersecurity workforce is critical. Continuous education and training programs help professionals stay updated with the latest adversarial TTPs. Encouraging cybersecurity education at all levels ensures a steady pipeline of skilled professionals.[26] Initiatives like the Global Forum on Cyber Expertise (GFCE) aim to enhance cybersecurity skills worldwide. While the high demand for cybersecurity professionals outstrips supply, and educational resources vary globally, the focus on continuous learning helps us keep pace with evolving threats.

REGIONAL

CONNECTING CYBER DIPLOMACY AND DEVELOPMENT COOPERATION FOR A MORE HUMAN-CENTRIC DIGITAL WORLD

***Written by:** Jonathan Voigt, D4D Expert at the D4D Hub Secretariat.*

Multilateral and multi-stakeholder coordination on cyber diplomacy and CCB are delivering an attractive “Team Europe” approach globally.

Combining cyber diplomacy efforts and cooperation on cyber capacity building is the key to fostering a human-centric digital transformation worldwide and keeping malicious actors at bay. The D4D (Digital for Development) Hub is a platform for bringing together the European Union (EU), its Member States and partners. It has a track record of supporting cyber security and capacity building (CCB) in Latin America and the Caribbean.

Rapid developments in disruptive technologies, such as AI and the growing pressure of keeping digital infrastructure secure, show the importance of cyber and digital on the diplomatic stage. Geopolitical challenges, such as the Russian war of aggression, further prove that a concerted EU effort is needed to promote universal human rights and democratic principles in the digital space, as outlined in the 2023 European Council Conclusions on the Team Europe approach.[1]

The Team Europe approach should also include development cooperation. As digital technologies directly benefit 70% of the sustainable development goal targets,[2] there has been an increase in digital development cooperation projects. These projects help build capacity to bridge the digital divide, and support a sustainable and resilient digital transformation in partner countries. CCB and investment in cyber infrastructure resilience help governments and societies to understand and build resilience against growing global threats and attacks.

By supporting a coherent and all-encompassing approach to digital transformation, through CCB and cyber diplomacy - but also secure and resilient connectivity and the responsible use of AI - the EU presents an appealing offer of cooperation that can help build more inclusive digital economies and societies in which all citizens have equal opportunities to participate in the digital world.

Better coordination for a better offer

For a more unified approach, the EU and its Member States launched the D4D Hub in December 2020.[3] It is a platform for multi-stakeholder partnerships and to boost joint investments to advance a human-centric digital transformation worldwide. Sixteen EU Member States have now joined, working alongside the European Commission, the European External Action Service (EEAS) and the European Investment Bank (EIB). The D4D Hub is building bridges between digital and cyber diplomacy and development cooperation. It is a key instrument to deliver the digital and security objectives of the EU's Global Gateway strategy.[4]

The cornerstone of the D4D Hub is its multi-stakeholder approach. The D4D Hub structure has regional branches, thematic working groups co-led by EU Member States, their implementing agencies and specialist organizations, as well as two advisory groups that include the private sector, academia, and civil society.

The D4D Hub Secretariat implements the strategy, and connects bilateral activities and thematic focal points to upscale efforts to cross-regional partnerships. This engages organizations beyond the development policy community to include national space or cyber agencies. As a trusted coordinator, the D4D Hub helps to organize high-level policy dialogues internationally, enhancing the visibility of Team Europe as a leading actor in the digital for development domain.

In 2024 the D4D Hub started to support the European Commission, EEAS, and five EU delegations to develop Informal Digital Hubs, implementing the 2022 Council Conclusions on EU Digital Diplomacy.[5] These coordination efforts will be applied nationally to deliver benefits in the piloting partner countries.

The D4D Hub continuously expands multi-stakeholder connections for its members, linking them to development financing institutions, academia and the private sector, to support a unified European offer.

Driving Positive Change in Latin America and Caribbean (LAC)

The Latin American and Caribbean region (LAC) is a good example of the D4D Hub's multi-stakeholder approach to cybersecurity.

The EU and LAC partner countries work together under the framework of the EU-LAC Digital Alliance,[6] which fosters a digital transformation based on shared digital values ahead of the EU-CELAC Summit in 2025. Cybersecurity is a key area of cooperation between both regions, as exemplified by existing initiatives such as the Latin America and Caribbean Cyber Competence Centre EULAC4.[7] Moreover, a dedicated policy dialogue took place in February 2024 in Santo Domingo, Dominican Republic.[8] The goal was to identify new opportunities to strengthen bi-regional cooperation in cybersecurity and to support cybersecurity frameworks promoting a human-centered digital transformation. New cooperation initiatives will serve three main goals: to reinforce cyber diplomacy capacities and foster bi-regional cooperation, to strengthen national, regional and bi-regional cyber ecosystems and promote triangular cooperation, and to boost the resilience of critical infrastructure. These ideas will be discussed in a planned multi-stakeholder forum in Madrid later in 2024.

Although the work in the LAC region has only just begun, it shows how capacity building flows not just in one direction. The number of participating Member States is growing and newcomers are always welcome. Sharing CCB experiences and partner projects is the key to building knowledge and driving sustainable project development for a more human-centric digital transformation for all.

European Union, 2024. EU-LAC Digital Alliance Cybersecurity Policy Dialogue in Dominican Republic.

IMPLEMENTATION OF THE AFRICA AGENDA FOR CYBER CAPACITY BUILDING (AA-CCB)

TO ENHANCE CYBER RESILIENCE

***Written by:** GFCE Africa Hub.*

Africa recognizes the importance of CCB to improve digital resilience, and is implementing a continent-spanning program to achieve it.

In today's interconnected world, enhancing cyber resilience is a top priority for governments, businesses, and individuals alike. It involves the ability to anticipate, withstand, recover from, and adapt to cyber threats effectively. Several African countries have enhanced their cyber resilience against malicious actors and emerging threats.

As cyber threats continue to evolve and become more sophisticated, the importance of enhancing cyber capacity across the world has never been more crucial. In November 2023, the GFCE, in partnership with Africa Union Development Agency (AUDA)-NEPAD, launched the Africa Agenda on Cyber Capacity Building (AA-CCB).

The aims of AA-CCB are to advance actions and priorities that aim to enhance coordination and identification of successful policies, practices, and ideas for CCB programs and initiatives in Africa. As cyber capacity, security and resilience play a significant role in supporting economic and social prosperity for the continent, there are several actors with CCB programs and initiatives on the continent.

The African Union adopted the *African Union Convention on Cyber Security and Personal Data Protection*, or *Malabo Convention*,[1] which entered into force in June 2023. The convention is a pivotal instrument for building resilient digital economies aligned to the *Digital Transformation Strategy for Africa (2020 – 2030)*[2] which supports e-commerce, e-services and free movement of people, goods and services, as envisioned in the *African Continental Free Trade Area (AfCFTA)*[3] agreement.

In light of these initiatives, the GFCE Africa Hub, which was launched in November 2023 in partnership with AUDA-NEPAD, is engaging members of the Africa CCB Coordination Committee to discuss the implementation of AA-CCB. The discussions focus on the implementation plan and activities of AA-CCB. This follows

AFRICA AGENDA FOR CYBER CAPACITY BUILDING (AA - CCB)

FROM AWARENESS TO CAPABILITY

GFCE GLOBAL FORUM ON CYBER EXPERTISE

1. Assessments and Development of National Cybersecurity Strategies
2. Legislation, Policies, Regulations and Standards
3. CIIP/CIP, CERTS/CSIRTS & Incident Management
4. Capacity Building, Awareness and Outreach
5. Technical Capabilities, Skills, Research & Development
6. National, Regional, and International Collaboration, Cooperation and Partnerships

The Africa Agenda for Cyber Capacity Building (AA-CCB) was launched at the Global Conference on Cyber Capacity Building (GC3B), held in Accra, Ghana, 28-30 November 2023.

Mr Chris Painter, President of the GFCE Foundation Board (Center), Mr Moctar Yedaly, Director of the GFCE Africa Hub (Right), and Dr Martin Koyabe, Senior Manager, GFCE Africa (Left).

the request by the *African Union Specialised Technical Committee on Communication*[4] and *ICT (CCICT-5) for AUDA-NEPAD*[5] to work with member states to mobilize resources from development partners to implement the AA-CCB.

The implementation plan will prioritize actions for AA-CCB to enhance coordination and identify successful policies, practices, and ideas for CCB programs and initiatives in Africa. The implementation will focus more on aligning AA-CCB actions and activities with both ongoing and planned CCB related activities by donor/funding agencies and implementation partners. The implementation plan will also solicit advice and support from Regional Economic Communities (RECs) in identifying and collaborating further in CCB activities within RECs based on agreed AA-CCB implementation plan activities.

Promoting Cyber Capacity and Cyber Resilience in Africa

Through initiatives such as the AU-GFCE collaboration project, the GFCE has engaged several partner organisations in Africa and signed various Memoranda of Understanding (MoU) aimed at enhancing CCB and related activities in Africa.

These partner organisations include: *AUDA-NEPAD, United Nations Economic Commission for Africa (UNECA), The African Capacity Building Foundation (ACBF), Africa Development Bank (AfDB) and Smart Africa (SA)* (see summary table on page 43).

African Union
AUDA-NEPAD
AFRICAN UNION DEVELOPMENT AGENCY
GFCE
UNECA
smart africa
CONNECT . INNOVATE . TRANSFORM
ECOWAS
SADC
COMESA
IGAD
CEEAC-ECCAS
ARTAC
EACO
CRASA
WATRA
PAPU
UPAP
AFRIPOL
African Capacity Building Foundation (ACBF)
AfricaCERT
United in promoting cyber security in Africa
AFRINIC
The Internet Numbers Registry for Africa
WACREN

The Africa CCB Coordination Committee consists of over 25 CCB oversight and coordination organization in Africa.

AUDA-NEPAD AFRICAN UNION DEVELOPMENT AGENCY	Developed joint action plan for implementing AA-CCB and Accra Call
United Nations Economic Commission for Africa	Engaging on AA-CCB and Accra Call on Africa CCB related frameworks
THE AFRICAN CAPACITY BUILDING FOUNDATION | FONDATION POUR LE RENFORCEMENT DES CAPACITES EN AFRIQUE	Engaging with ACBF to enhance AU programmes on CCB related areas
BANQUE AFRICAINE DE DEVELOPPEMENT AFRICAN DEVELOPMENT BANK AFRICAN DEVELOPMENT FUND FONDS AFRICAIN DE DEVELOPPEMENT	Engaging with AfDB in supporting and enabling secure Digital Infrastructure for SMEs and AU member states
smart africa CONNECT . INNOVATE . TRANSFORM	Promoting CCB efforts in AU member states and use of Smart Africa Digital Academy platform

List of organizations in Africa which have signed MoUs with the GFCE.

WHY WE NEED HUMAN-CENTRIC APPROACHES TO CYBER RESILIENCE IN SOUTHEAST ASIA

***Written by:** Keith Detros, Programme Manager, Tech for Good Institute.*

Cyber attacks don't just happen to systems; they happen to people. To develop resilience, cyber threat preparedness and response should consider a human-centric approach.

Like the rest of the world, Southeast Asia is undergoing rapid digital transformation. The region's digital economy has maintained an impressive compound annual growth rate of 27% since 2021.[1] Projections indicate that digitalization could contribute up to US$1 trillion to the regional economy by 2030. This growth is driven by factors such as accelerated digital adoption catalyzed by the pandemic, an increasingly mobile-first economy, the rise of digital platforms, and a thriving startup ecosystem.[2]

However, amidst these advances, technology and society are in a complex relationship. Digital solutions bring benefits, but also challenges and risks. In Southeast Asia, digital adoption has not always been accompanied by adequate digital literacy and cyber awareness measures. As more people come online, particularly for the first time, cyber criminals have more opportunities to exploit their vulnerabilities. This has led to an increase in cyber threats across the region.

Southeast Asia's Cyber Threat Landscape: The Rise of Scams and Fraud

In the World Economic Forum's Global Risk Report 2024, cyber insecurity is highlighted as a critical global concern, both in the short and long term.[3] Countries in Southeast Asia have been affected, with the cost of a data breach hitting a record high of US$3.05 million in 2023, marking a 6% increase on the previous year.[4] In the same period, cyber extortion - including ransomware and distributed denial of service (DDoS) attacks with ransom demands - surged by 42%.[5] Southeast Asian businesses also continue to grapple with challenges like business email compromise and phishing attacks.

Alarmingly, apart from threats faced by organizations, there is a rising trend of scams and fraud targeting individuals.[6] In Singapore, for example, victims lost approximately US$ 481.4 million in 2023.[7] Meanwhile, losses from scams and fraud account for an astonishing 3.6% of Vietnam's 2023 gross domestic product.[8] Scammers and fraudsters manipulate users into sharing credentials, personal data, and even financial information. This is doubly concerning, as compromised individual information can also enable unauthorized access to their organization's or personal networks.

With remote work and bring-your-own-device arrangements becoming more common, the lines between individual and organizational cybersecurity continue to blur. Personal devices can also be a vulnerability for organizational cybersecurity. Individuals both increase the available attack surface and can suffer significantly when attacks occur. Recognizing this is critical to reducing cyber risk.

Complementing Existing Initiatives: The Case for Human-Centric Cyber Resilience

Governments in Southeast Asia increasingly recognize the importance of cybersecurity and building cyber capabilities across governments, the private sector, and society.[9] At the national level, governments have begun implementing national cybersecurity strategies and enacting data protection laws, albeit with varying degrees of coverage and implementation. Regionally, the Association of Southeast Asian Nations (ASEAN) adopted the Cybersecurity Cooperation Strategy (2021-2025), a roadmap for cross-border cybersecurity cooperation. And recently, ASEAN endorsed a financial model for the regional Computer Emergency Response Team (CERT), which will help to operationalize and enhance CERT capacity across member states.[10]

However, while techno-centric approaches for regional cooperation - such as safeguarding infrastructure, systems, networks, and data - are important, the evolving nature of cyber threats, and the increase in scams and fraud targeting consumers every day, show the importance of focusing on users as well. There is a clear opportunity to complement techno-centric efforts with human-centric approaches to cybersecurity.

As the saying goes, in the cybersecurity triad of people, process, and technology, people are often considered the weakest link. Focusing effort and resources on the people part of the triad can bring big improvements. Integrating the motivations, experiences and feelings of individuals is now essential to ensure that society prevents, responds, recovers and adapts to cyber risks.[11]

How it Works: Incorporating a Holistic, Human-centered Approach to Cyber Resilience

Human-centric cybersecurity approaches are intended to complement, not replace, current cybersecurity development efforts. Southeast Asia can use existing initiatives to further improve regional cyber resilience by:

- **Building a cyber resilience culture through awareness-raising and education**

  Human-centric cybersecurity approaches start by raising awareness to reduce the risk of individuals falling victim to cyber threats. This is critical for children and youth, who have become more exposed to digital technologies due to the rise of remote and hybrid learning in education. While spending time online can bring educational benefits, it also exposes them to phishing, fraud, and scams. Integrating cyber hygiene education into formal curricula both raises awareness and promotes early interest in cybersecurity careers. ASEAN countries can collaborate to share best practices in developing cyber hygiene curricula.

Awareness raising must go beyond formal education systems by encouraging community engagement, where community champions adopt and share best practices. These champions can come from various demographics, including women and the elderly. Building resilience is a shared responsibility, and a whole-of-society approach is essential to advance comprehensive and effective cybersecurity.

- **Designing country-specific and inclusive capability development programs**

Given the diversity of the region, no one-size-fits-all framework will meet the needs of each country. As highlighted by the Cyber ASEAN project, most countries have adapted a localized and context-specific approach to implementing globally recognized frameworks.[12]

Moreover, it is crucial to involve and consult diverse stakeholders - such as nonprofit organizations, academics, and community leaders – in cyber policy formulation and the design of capability development programs. Being inclusive means establishing and, critically, institutionalizing ongoing mechanisms that go beyond cyber professionals. This ensures that capability development and awareness campaigns align with people's experiences on the ground. Putting people at the heart of cyber resilience initiatives makes those efforts more relevant and effective.

- **Developing capability in human-centric cybersecurity incident response**

The technical aspects of incident response—patching systems, isolating threats, and recovering data—are crucial, but a human-centric approach to cyber resilience also addresses the needs of victims. Beyond the technical impacts of an attack or breach, people suffer significant non-technical harms, including financial losses, reputational damage, loss of trust, and negative mental health effects. Scams and fraud are often associated with shame, which leads to underreporting and less available information about the type and scale of attacks and scams.

A human-centric approach to incident response considers the psychosocial and behavioral impacts on victims. Cyber professionals, particularly those involved in responding to cyber threats, should receive training in gender and cultural sensitivity. This ensures respect for social norms and provides appropriate and effective assistance for all, including marginalized and vulnerable individuals.

To conclude, a human-centric approach recognizes the significant attack surface of individuals in society and the growing sophistication of attackers. As the lines between individual, organizational and national cybersecurity continue to blur, an approach that recognizes the vulnerabilities and harnesses the specific perspectives and abilities of individuals is now a crucial part of overall cyber resilience.

NAVIGATING AI GOVERNANCE: INSIGHTS FROM SOUTHEAST ASIA'S EMERGING POLICIES

***Written by:** Ms. Angela C. Chaves, Development Management Officer and Research Policy Focal Person on Cybersecurity and AI, CPED, NCPAG, University of the Philippines—Diliman.*

SE Asia's collaborative and comprehensive approach to AI is a model for other regions.

Southeast Asia, a region known for its economic dynamism and digital adoption, is actively engaging in the development and governance of AI technologies. It is a diverse region, comprising ten countries with varying levels of technological advances. The Association of Southeast Asian Nations (ASEAN) recognizes AI's transformative potential and its role in fostering economic growth and improving public services. As of 2023, AI adoption in Southeast Asia is rapidly increasing, driven by government initiatives, private sector investments, and a burgeoning startup ecosystem.

Several Southeast Asian countries are emerging as key players in the AI landscape. Singapore is a global leader in AI readiness, ranking high in various internal indices. Malaysia and Thailand are also making significant strides, focusing on integrating AI into their national development plans. Indonesia and Vietnam are leveraging their large populations and digital economies to drive AI innovation.

The Philippines – AI Innovation, Governance and Practical Applications

In the Philippines, a leading AI research institution is the Center for Artificial Intelligence Research (CAIR). Launched on July 3, 2024, CAIR advances AI technologies and their application across sectors. Collaborating with both local and international partners, CAIR's mission is to transform the Philippines into a premier destination for AI-driven innovation and investments. It is developing AI solutions for regional concerns such as sustainable agriculture, urban planning, and disaster resilience.

Additionally, AI Research and Innovation Centers, often established in collaboration with universities and industry partners, play a pivotal role throughout the country, often focusing on areas such as healthcare, agriculture, and smart cities. Through multidisciplinary and cross-disciplinary research, these centers develop full-time research scientists, engineers, and R&D personnel.

The Artificial Intelligence Research Center for Community Development (AIRCoDe) is funded by the Department of Science and Technology – Philippine Council for Industry, Energy, and Emerging Technology Research and Development (DOST-PCIEERD). AIRCoDe's mission is to explore AI applications to enhance community resilience, provide avenues for discoveries, and strengthen research capabilities in AI. Its research areas include the role of AI in disaster risk management, agricultural management, community development, environmental issues, capacity building, and data-driven policy development.

The Philippines is proactive in developing policies that promote the ethical and responsible use of AI. These policies aim to create a regulatory environment that supports innovation while addressing potential risks. The Philippines' National AI Strategy outlines the government's vision for AI development and its integration into various sectors. The strategy includes initiatives to enhance AI research, develop a skilled workforce, and promote the ethical use of AI. The Department of Trade and Industry, with support from the Asian Development Bank, launched the National Artificial Intelligence Strategy Roadmap 2.0 (NAISR 2.0). Building on the first AI roadmap in 2021, NAISR 2.0 incorporates recent technological advancements, including generative AI, and recalibrates strategic actions to address emerging themes such as ethics and governance.

Several proposed AI legislation House Bills are currently being deliberated in the Philippines' House of Representatives. These bills aim to establish a regulatory framework for AI, promote AI research and development, and ensure that AI technologies are used ethically and responsibly.

Southeast Asia provides valuable insights for other regions aiming to foster an environment where technological progress is supported by informed, sound, and forward-thinking policies. By sharing knowledge and best practices, Southeast Asia contributes to the global discourse on AI governance, promoting innovation while ensuring ethical and responsible AI deployment.

Comparative Insights and Global Lessons

Southeast Asia's AI policy developments emphasize the importance of public-private partnerships, strong regulatory frameworks, and international collaborations in crafting a comprehensive approach to AI governance.

Effective AI governance in Southeast Asia hinges on the collaboration between governments, private sector entities, and academic institutions, to ensure that policy development incorporates diverse perspectives and expertise. This is evident in the region's focus on establishing clear and comprehensive regulatory frameworks, such as Singapore's Model AI Governance Framework and Malaysia's AI Ethics and Governance Framework, which are critical for the ethical and responsible deployment of AI technologies. A risk-based approach to AI regulation, as seen in the EU's AI Act, ensures that high-risk applications are effectively controlled while still fostering innovation in lower-risk areas. This method balances safety with progress, providing a model for other regions to emulate.

International collaborations are another cornerstone of Southeast Asia's strategy. Partnerships with global tech giants and other nations not only enhance innovation but also promote regulatory coherence. Singapore's extensive international collaborations serve as a prime example of this approach.

Investment in AI education and training is crucial to build a skilled workforce capable of driving AI innovation. Countries like Thailand and Vietnam exemplify this with substantial investments in AI training programs and educational initiatives.

Knowledge Exchange in ASEAN AI Policy Development

The "Securing the Future: Forum on Cybersecurity and Artificial Intelligence" was held on April 17, 2024, at the University of the Philippines National College of Public and Administration and Governance. It was a collaborative platform for experts to share knowledge, discuss regional trends, and provide insights into the legislative and policy-making processes. Organized in partnership with the UP NCPAG - Center for Policy and Executive Development (CPED) and GCFE, the forum covered the critical role of collaborative efforts in addressing the challenges posed by cybersecurity threats and AI governance.

Key insights at the forum highlighted the importance of strategic partnerships and policy innovation. In his welcome remarks, UP-NCPAG Dean, Dr. Kristoffer B. Berse, highlighted the collaboration between UP NCPAG and GFCE, and announced an upcoming Memorandum of Understanding (MOU) with the House of Representatives, UP College of Engineering, and UP College of Law, to facilitate policy research and knowledge exchange on cybersecurity and AI. UP Diliman Chancellor Atty. Keynote speaker Edgardo Carlo L. Vistan II emphasized the need to support technological solutions and incentivize innovation rather than relying solely on regulation and criminalization.

Mr. Anwer Yusoff, Head of Industry Engagement and Collaboration at Cybersecurity Malaysia, described the country's proactive stance on cybersecurity, including aligning policies and standards with international benchmarks. He said Malaysia's implementation of ISO 27001 for government offices is a model for other countries. Engr. Ava T. Taniajura from the British Standards Institution (BSI) Philippines also stressed the adoption of international cybersecurity standards to build a trustworthy digital environment.

Ms. Angela Chaves of CPED gave a comparative analysis of current proposed House Bills on AI in the Philippines, and offered insights into legislative efforts to regulate and promote AI development. Engr. Allan Cabanlong, Southeast Asia Regional Director for the GFCE, discussed the United Nations' Norms on AI and the European Union's AI Act, and emphasized a risk-based approach to AI regulation. Prof. Prospero Naval, of the University of the Philippines Department of Computer Science and Head of the department's Artificial Intelligence Program, advocated for a balanced perspective on AI, highlighting both its benefits and challenges.

Ms. Michelle Alarcon, President of the Analytics and Artificial Intelligence Association of the Philippines, emphasized the need for an industry-led interim AI task force to collaborate with government agencies in formulating and promoting AI policies.

Lastly, CPED Director, Dr. Enrico L. Basilio, concluded the forum by underscoring CPED's commitment to supporting research, policy, and extension initiatives aimed at fostering strong legislation and best practices in cybersecurity and artificial intelligence. He also emphasized that the event highlighted the critical importance of a collaborative approach in developing effective policies and regulatory frameworks, essential for securing the digital future of the Philippines and the broader ASEAN region.

By convening experts from diverse sectors, the forum facilitated a comprehensive exchange. This collaborative spirit is essential to advance policy initiatives and ensure the digital transformation of the Philippines and ASEAN region remains secure, innovative, and inclusive. The forum also highlighted the need for strategic partnerships among national and international institutions, government agencies, academic institutions, and the private sector.

The forum's insights and recommendations will guide future legislative efforts, enhance knowledge exchange, and boost the region's ability to respond effectively to technological innovations. By facilitating a comprehensive exchange of knowledge and perspectives, the forum helped to ensure that AI policy development in the Philippines and ASEAN can make the region's digital transformation both innovative and secure.

Global Forum on Cyber Expertise partners with the Center for Policy and Executive Development, National College of Public Administration and Governance, University of the Philippines- Diliman to conduct Cybersecurity and AI Forum.

INTERVIEW WITH GUEST EXPERT– DR. PATRYK PAWLAK

Our new guest expert column taps the knowledge and experience the GFCE's wide global network of professional expertise. The first person in the hot seat, answering our questions, is Dr. Patryk Pawlak.

Biography

Dr. Patryk Pawlak is a part-time Professor at the Robert Schuman Centre for Advanced Studies at the European University Institute (Italy), and a Visiting Scholar at Carnegie Europe (Belgium). He is also the Project Director of the Global Initiative on the Future of the Internet. For over a decade, Dr. Pawlak has been actively involved in developing and strengthening various international cyber capacity-building (CCB) initiatives. His research on cyber capacity building has influenced both academic debates and policy, particularly regarding the principles-based approach, the use of CCB as a foreign policy tool, and operational guidance on how to conduct CCB. Dr. Pawlak has performed different roles with the GFCE, including serving as Chair of the GFCE Advisory Board and Chair of the 2023 GC3B (Global Conference on CCB) Programme Advisory Team.

Q: Where did your interest in cyber and digital policies originate?

Everyone has their own story about how cyber entered their life. My journey with cyber began during the 2003 EU-US negotiations on the Passenger Name Record agreement, where the use of personal information for law enforcement became a key issue. At that time, I worked on topics like encryption, data integrity, and data breaches from the angle of data protection rather than cybersecurity. Ten years later, I started working on cyber issues in a more structured way. My first projects for the European Union focused on cyber capacity building, and the journey continues to this day.

Q: What has been the most interesting learning experience?

All of it. I am truly drawn to the dynamism and growing diversity of this field. At the same time, I am surprised by how predictable and stable the field has remained. Yes, the threat landscape and challenges have evolved and become more complex, but the solutions to those challenges are often the same as those we discussed back in 2013 at conferences in Paris, Brussels, and The Hague.

Q: Since you have looked at different aspects of cyber policies over the past 20 years, where do you think are the biggest gaps our community needs to address?

I think we need a collective change of mindset, with more focus on actions and results. This also requires honest conversations about the state of the discipline, which has been underdelivering for the past decade. We rarely discuss our failures because everyone wants to tell and hear success stories. We cannot advance as a community if we do not accept that failures are part of the business we are in. To achieve this, we need to collectively invest in mechanisms that focus on new incentive structures, results monitoring and accountability.

Q: You recently wrote a report on the fragmentation of the CCB landscape. Since you joined the field of cyber and digital policies, what changes have occurred in the CCB landscape that now define the current landscape?

Indeed, together with Nayia Barmpaliou, I recently published a paper on the future of cyber capacity building in a fragmented world. It is one of the very first papers to focus on the geopolitical dimension of CCB and how our field is affected by competition among major powers. One key aspect we highlight in the paper—and a significant change compared to ten years ago—is the growing ideological and operational fragmentation of the CCB ecosystem. Despite the interconnectedness of cyber-related issues, many debates today still have not adequately captured the entire CCB ecosystem.

Q: What does this imply for the field and the effectiveness of initiatives?

The result of such siloed discussions about CCB has been a waste of know-how and resources, ultimately leading to inefficiencies. In the report, we highlight three main effects on the field of CCB.

First, the number of projects, stakeholders across the world, and invested funds in CCB has drastically grown, including new funders with different visions for the digital domain. This increases the diversity in CCB approaches, leading to additional complexities in coordination.

Second, the areas of CCB interventions have also expanded compared to ten years ago, complicating coordination and prioritization of resources. In addition to interventions focused on cybercrime, national cybersecurity strategies, or CERTs/CSIRTs development, the community is increasingly interested in initiatives focused on cyber exercises, critical infrastructure protection, cyber diplomacy, and cyber workforce development.

Finally, we point out that increasing CCB demands require further adaptation to systematically incorporate development cooperation methodologies and different financing tools and options by government donors, such as the use of budget support.

Q: How can we address and mitigate the fragmentation of the CCB landscape?

In the paper, we examine the interplay between ideological and operational fragmentation, leading us to identify four different scenarios for the CCB community, which we call "zones." Our analysis concludes that the most desirable outcome for the CCB community, considering political and operational constraints, is the zone of prosperity. To achieve this, we propose a "professionalization strategy," where the ecosystem and CCB activities become more efficient and effective despite the persisting ideological fragmentation. This strategy involves increasing the use of technocratic processes and procedures to promote closer coordination, even among actors who do not necessarily share the same ideology. We also offer several concrete recommendations, but you'll need to read the paper to learn more.

Q: What CCB project or initiative that you are currently working on are you most excited about?

There are a couple of projects that I am very excited about but cannot discuss. But the one I can talk about and that is definitely in the top three is the upcoming GC3B conference that will be hosted by the GFCE and Switzerland. The program is still in development but we aim to make this edition even more exciting and inclusive than the first conference in Ghana. We have structured the program in three pillars driven by the need for the international community to rethink, evolve and anticipate adaptation across the existing approaches in international cooperation and partnerships for cyber resilience and capacity building. As always, the ultimate success of the conference will depend on the broad community engagement. We are counting on everyone to play their part.

Q: What advice would you give to young professionals starting in the field of cyber and digital policies?

That's easy: Don't reinvent the wheel. Those starting in this field should not only look at the latest developments but also review some of the solutions and discussions we've had over the past decade. Additionally, it's important to find your own niche. The field is too broad to do everything. Finally, be honest about what you do and do not know.

Thank you, Dr. Pawlak!

You can find out more about GC3B 2025 at https://gc3b.org/

p4. How to Narrow the Cyber Skills Gap

1. World Economic Forum, https://www.weforum.org/agenda/2023/05/the-cybersecurity-skills-gap-is-a-real-threat-heres-how-to-address-it/, 2 May 2023

2. GFCE's Women in Cyber Capacity Building (WiCCB) Network event on: Empowering Through Initiatives: Developing Diverse Cyber Workforce and Career Pathways, 25th April 2024

3. US Office of the National Cyber Director, Executive Office of the President, *"National Cyber Workforce and Education Strategy. Unleashing America's Cyber Talent"*, 31 July 2023.

4. Julia Slupska, Oxford Internet Institute, St Antony's International Review Vol. 15, No. 1 (May 2019), pp. 83-100 (18 pages) Published By: St. Antony's International Review, Safe at Home: *Towards a Feminist Critique of Cybersecurity* https://www.jstor.org/stable/27027755

5. A critical distinction must be made between workforce and skills gap in cybersecurity. The workforce gap refers to the quantifiable need for experts, the number of unfilled positions, whereas the skills gap is more of issue of capability building gap and having the right mechanism in place to ensure that the talent pipeline is equipped with the needed skills and abilities to match industry needs and perform specific jobs.

6. Irene Corpuz, Co-Founder and Board Member of the Women in Cyber Security Middle East (WICSME), *GFCE's Women in Cyber Capacity Building (WiCCB) Network event on: Synergy in Cybersecurity: Women Leading Across Networks for Global Impact*, 27 June 2024

7. Confidence Stavely, Founder and Executive Director of Cybersafe Foundation, *GFCE's Women in Cyber Capacity Building (WiCCB) Network event on: Synergy in Cybersecurity: Women Leading Across Networks for Global Impact*, 27 June 2024

8. https://cybersafefoundation.org/cybergirls/

9. Confidence Stavely, Founder and Executive Director of Cybersafe Foundation, *GFCE's Women in Cyber Capacity Building (WiCCB) Network event on: Synergy in Cybersecurity: Women Leading Across Networks for Global Impact*, 27 June 2024

10. World Economic Forum, *Putting Skills First: Opportunities for Building Efficient and Equitable Labour Markets*, https://www.weforum.org/publications/putting-skills-first-opportunities-for-building-efficient-and-equitable-labour-markets/, January 2024

11. Nina Olesen, Chief Operating Officer of Women 4 Cyber Foundation, and Head of Skills and Human Factors Sector at the European Cyber Security Organisation (ECSO), *GFCE's Women in Cyber Capacity Building (WiCCB) Network event on: Synergy in Cybersecurity: Women Leading Across Networks for Global Impact*, 27 June 2024

12. Irene Corpuz, Co-Founder and Board Member of the Women in Cyber Security Middle East (WICSME), *GFCE's Women in Cyber Capacity Building (WiCCB) Network event on: Synergy in Cybersecurity: Women Leading Across Networks for Global Impact*, 27 June 2024

13. Confidence Stavely, Founder and Executive Director of Cybersafe Foundation, *GFCE's Women in Cyber Capacity Building (WiCCB) Network event on: Synergy in Cybersecurity: Women Leading Across Networks for Global Impact*, 27 June 2024

p8. What Does AI Mean For Cyber Capacity Building?

1. ISC2, (2024) "AI in Cyber 2024: Is the Cybersecurity Profession Ready?", https://www.isc2.org/Insights/2024/02/The-Real-World-Impact-of-AI-on-Cybersecurity-Professionals

2. ISC2, (2024) "The Real-World Impact of AI on Cybersecurity Professionals", https://www.isc2.org/Insights/2024/02/The-Real-World-Impact-of-AI-on-Cybersecurity-Professionals

3. Cisco, (2023) "Cisco AI Readiness Index: Intentions Outpacing Abilities", https://www.cisco.com/c/dam/m/en_us/solutions/ai/readiness-index/documents/cisco-global-ai-readiness-index.pdf

4. Microsoft, (2024) "Generative AI: The defenders' advantage", https://info.microsoft.com/rs/157-GQE-382/images/EN-CNTNT-Whitepaper-SRGCM11624-1.pdf

5. Council of Europe, (2024) "The Framework Convention on Artificial Intelligence", https://www.coe.int/en/web/artificial-intelligence/the-framework-convention-on-artificial-intelligence

6. European Union, (2023) "Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence",

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ%3AL_202401689

7. ASEAN, (2024) “ASEAN Guide on AI Governance and Ethics”, https://asean.org/book/asean-guide-on-ai-governance-and-ethics/

8. OEWG, (2024) “Open-ended working group on security of and in the use of information and communications technologies 2021-2025”, https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/Letter_from_OEWG_Chair_11_July_2024.pdf

9. UNGA, (2024) “Enhancing international cooperation on capacity-building of artificial intelligence”, https://documents.un.org/doc/undoc/gen/n24/197/26/pdf/n2419726.pdf

10. GFCE, Working Group E on cyber capacity building on new and emerging technologies, https://thegfce.org/theme-gfce/emerging-technologies/

p26. Making Sure Pacific Voices Are Heard at United Nations Cyber Meetings

1. United Nations Office for Disarmament Affairs, (2021) Open-ended Working Group on Security of and in the Use of Information and Communications Technologies, (OEWG), https://meetings.unoda.org/open-ended-working-group-on-information-and-communication-technologies-2021

p30. APT Threat Landscape

1. European Repository of Cyber Incidents, https://eurepoc.eu/publication_type/apt-profiles/

2. Mandiant, (2019) “APT10 (MenuPass Group): New Tools, Global Campaign Latest Manifestation of Longstanding Threat,” https://jp.stage.mandiant.com/resources/blog/apt10-menupass-group

3. CrowdStrike, (2020) “Operation Cloud Hopper: Insights into APT10’s Tactics, Techniques, and Procedures,” https://www.crowdstrike.com/blog/operation-cloud-hopper/

4. S. Pirandola et al., “Advances in Quantum Cryptography,” in Advances in Optics and Photonics, vol. 12, no. 4, pp. 1012-1236, 2020, https://www.osapublishing.org/aop/abstract.cfm?uri=aop-12-4-1012

5. Cybersecurity Ventures, (2020) “Cybercrime Damage Costs to Reach $10.5 Trillion Annually by 2025.” https://cybersecurityventures.com/cybercrime-damage-costs-10-trillion-by-2025/

6. Google, (2010) “A New Approach to China,” https://googleblog.blogspot.com/2010/01/new-approach-to-china.html

7. Bitkom, (2023) “Market for IT security growing to more than 9 billion euros,” https://www.bitkom.org/EN/List-and-detailpages/Press/Market-IT-security-growing-more-9-billion-euros

8. ibid.

9. National Cyber Security Centre (NCSC), (2024) “China state-affiliated actors target UK democratic institutions and parliamentarians,” https://www.ncsc.gov.uk/news/china-state-affiliated-actors-target-uk-democratic-institutions-parliamentarians

10. Center for Strategic and International Studies (CSIS). “Cybersecurity,” https://www.csis.org/

11. Atlantic Council, “Cyber Statecraft Initiative,” https://www.atlanticcouncil.org/programs/scowcroft-center-for-strategy-and-security/cyber-statecraft-initiative/

12. NCSC, (2024)

13. Cybersecurity & Infrastructure Security Agency (CISA), “Advanced Persistent Threats (APTs),” https://www.cisa.gov/topics/cyber-threats-and-advisories/nation-state-cyber-actors

14. MITRE ATT&CK, “ATT&CK Framework,” https://attack.mitre.org/

15. National Cyber Security Centre (NCSC), (2024)

16. Europol, “Internet Organised Crime Threat Assessment (IOCTA),” https://www.europol.europa.eu/

17. CSIS, ibid.

18. ibid.

19. Atlantic Council, ibid.

20. PwC, (2024) “Cybersecurity Ecosystem Report: Western Balkans,” https://www.pwc.rs/en/publications/cybersecurity-ecosystem-report.html#:~:text=Currently%2C%20cyber%2Dcrime%20is%20seen,of%20their%20national%20cybersecurity%20ecosystems

21. MITRE ATT&CK, “ATT&CK Framework,” https://attack.mitre.org/

p30. APT Threat Landscape

22. Pirandola et al., (2020)

23. Bitkom, (2023)

24. Europol, ibid.

25. Cybersecurity Ventures, (2020)

26. CSIS, ibid.

p36. Connecting Cyber Diplomacy and Development Cooperation

1. European Council, (2023), Team Europe approach - Council conclusions, https://www.consilium.europa.eu/en/press/press-releases/2023/11/21/the-council-approves-conclusions-on-the-team-europe-approach/

2. United Nations Development Programme, (2023) "Digital technologies directly benefit 70 percent of SDG targets, say ITU, UNDP and partners", https://www.undp.org/press-releases/digital-technologies-directly-benefit-70-percent-sdg-targets-say-itu-undp-and-partners

3. https://d4dhub.eu/

4. European Commission, (2019) Global Gateway Strategy, https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/stronger-europe-world/global-gateway_en

5. European Council, (2022) "EU digital diplomacy: Council agrees a more concerted European approach to the challenges posed by new digital technologies", https://www.consilium.europa.eu/en/press/press-releases/2022/07/18/eu-digital-diplomacy-council-agrees-a-more-concerted-european-approach-to-the-challenges-posed-by-new-digital-technologies/

6. European Commission (2023), " EU-Latin America and Caribbean: Joint Declaration on a Digital Alliance", https://ec.europa.eu/commission/presscorner/detail/pl/statement_23_3892

7. Latin American and Caribbean Cyber Competence Centre, https://www.lac4.eu/

8. D4D Hub, (2024), "EU-LAC Digital Alliance Dialogue on Cybersecurity", https://d4dhub.eu/events/eu-lac-digital-alliance-dialogue-on-cybersecurity

p40. Implementation of the Africa Agenda for Cyber Capacity Building

1. African Union (2014) African Union Convention on Cyber Security and Personal Data Protection, https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf

2. African Union, (2020) Digital Transformation Strategy for Africa 2020 – 2030, https://au.int/sites/default/files/documents/38507-doc-dts-english.pdf

3. African Union, (2018) Agreement Establishing the African Continental Free Trade Area, https://au.int/en/treaties/agreement-establishing-african-continental-free-trade-area

4. African Union, Specialised Technical Committee on Communication and Information Communications Technology (STC-CICT), https://au.int/en/stcs/stc-communication-and-information-communications-technology

5. African Union, (2023) FIFTH ORDINARY SESSION OF THE AFRICAN UNION SPECIALIZED TECHNICALCOMMITTEE ON COMMUNICATION AND ICT (CCITC-5), https://portal.africa-union.org/DVD/Documents/DOC-AU-WD/EX%20CL%201473%20(XLIV)%20_E.pdf

p44. Why We Need Human-Centric Approaches

1. Google, Temasek, and Bain. (2023). e-Conomy SEA 2023. Retrieved from https://economysea.withgoogle.com/report/

2. Tech for Good Institute. (2023). From Tech for Growth to Tech for Good. Retrieved from https://techforgoodinstitute.org/research/tfgi-reports/from-tech-for-growth-to-tech-for-good/

3. World Economic Forum. (2023). Global Risks Report 2024. Retrieved from https://www.weforum.org/publications/global-risks-report-2024/

4. IBM. (2023). Cost of a Data Breach. Retrieved from https://www.ibm.com/reports/data-breach

5. Orange Cyberdefense. (2023). The rising menace of cyber extortion attacks. Retrieved from https://www.orangecyberdefense.com/global/blog/research/the-rising-menace-of-cyber-extortion-attacks

6. Global Anti-Scam Alliance and Gogolook. (2023). Asia Scam Report. Retrieved from https://www.gasa.org/_files/ugd/b63e7d_aaaa062b799344a6897a5819fa96340f.pdf

7. Scam victims in Singapore lost S$651.8 million in 2023, with record high cases.
Business Times, 18 February 2024. Retrieved from https://www.businesstimes.com.sg/singapore/scam-victims-singapore-lost-s6518-million-2023-record-high-cases

8. Vietnamese loss 16.23 billion USD to online scams. Vietnam Plus, 8 January 2024. Retrieved from https://en.vietnamplus.vn/vietnamese-loss-1623-billion-usd-to-online-scams-post276711.vnp

9. Detros, K. (2023). Towards A Resilient Cyberspace in Southeast Asia. Retrieved from https://techforgoodinstitute.org/research/tfgi-reports/towards-a-resilient-cyberspace-in-southeast-asia/

10. Cyber Security Agency. (2024). Singapore Moves Ahead to Establish the ASEAN Regional CERT to Strengthen Regional Cybersecurity. Retrieved from https://www.csa.gov.sg/News-Events/Press-Releases/2024/singapore-moves-ahead-to-establish-the-asean-regional-cert-to-strengthen-regional-cybersecurity

11. Stuart, J. (2024). Cybersecurity Threats, Vulnerabilities and Resilience Among Women Human Rights Defenders and Civil Society in South-East Asia. Retrieved from https://unu.edu/macau/blog-post/cybersecurity-threats-vulnerabilities-and-resilience-among-women-human-rights

12. Manantan, B. (2024). Cyber ASEAN Report. Retrieved from https://cyberasean.pacforum.org/

Save the Date

GC3B

Global Conference on Cyber Capacity Building

14-15 MAY 2025

Geneva | Switzerland

Cybil knowledge portal

www.cybilportal.org

Cybil is the one-stop online knowledge hub for the international cyber capacity building (CCB) community, hosting a large repository of CCB project information and a library of resources for projects to use. It is a place where governments, funders and implementing agencies can find and share best practices and practical information to support the design and delivery of capacity building projects and activities.

Cybil offers the following information:

Lessons learnt, outcomes and research about international cyber capacity building.

175+
Publications

950+
Projects

A repository of past and present international cyber capacity building projects.

Resources to help design and deliver international cyber capacity building projects.

120+
Tools

1000+
Actors

Governments, companies and organizations involved in international cyber capacity building.

Overview of regional and global events on cyber capacity building.

Events

All new content added to Cybil goes through a curation process to improve accuracy and relevance. To sumbit content on Cybil, please send an email to contact@cybilportal.org. Scan the QR code to check the Cybil Knowledge Portal:

African Union

GFCE

ORGANIZATION OF AMERICAN STATES

OAS More rights for more people

Global Cyber Expertise Magazine Volume 12, September 2024

Colophon

Editorial Board:

Sesili Bajelidze (GFCE)
Eline Badoux (GFCE)
Laura Moralez Nuez (GFCE)
Nhu Nguyen (GFCE)

Chief editor:

Maria Farrell

Guest Editors:

Nayia Barmpaliou
Allan Salim Cabanlong
Luanda Domi
David van Duren
Pua Hunter
Caterina Morandini
Valentina Namé

Artwork & Design:

Roguer Restrepo Estrada (Nieuw Licht Grafisch Ontwerp)

Publishers

African Union, www.au.int,
contact@africa-union.org, @_AfricanUnion

European Union, www.europa.eu, SECPOL-3@eeas.europa,
eu, @EU_Commission

Global Forum on Cyber Expertise, www.thegfce.org,
contact@thegfce.org, @theGFCE

Organization of American States,
www.oas.org/cyber, cybersecurity@oas.org, @OEA_Cyber

Disclaimer

The opinions expressed in this publication are solely those of the authors and do not necessarily reflect the views of the AU, EU, GFCE or OAS, or the countries they comprise of.

Global Cyber Expertise Magazine

AU • EU • GFCE • OAS
contact@thegfce.org

Submit an article or an idea by December 20th, 2024