THE SOCIETY FOR THE POLICING OF CYBERSPACE (POLCYB)
Presents:
ANNUAL POLCYB INTERNATIONAL SUMMIT 2025 BANGKOK
17th - 20th March, 2025 (Monday – Thursday)
Organized In Partnership With:
The Council Of Europe (COE), France, & Cyber Security Malaysia, Malaysia

Location: Bangkok Marriott Sukhumvit, Thailand

Theme: "Navigating Public Safety in the Era of Technological Innovation: Thought Leadership in Effective Cybercrime Management and Global Collaboration." (TBC)

SUMMIT OVERVIEW (Working Draft)

The **Annual POLCYB International Summit 2025** will bring together **regional and international subject matter experts and practitioners from criminal justice sectors, international organizations, governmental agencies, industry sectors and academia to share collaborative strategies, policies, and perspectives in cybercrime prevention, detection, and response.**

Duration: 4 Days	**Dates : 17th -20th March, 2025**	**No. of Participants (TBD): 100 - 150**

SUMMIT FORMAT:

CLOSED, PLENARY PANEL SESSIONS – 3 full days (Days 1-3):

Our international subject matter experts will share thought-provoking, strategic perspectives on cybercrime management, case examples, and lessons learnt.

Panel discussions will include, but not limited to: implications of evolving technologies upon executive decision-making; prevalent trends and threats in cybercrime, serious and organized crime; strategic approaches to cybercrime prevention; risk management; addressing challenges in operationalization of cybercrime strategies; international cooperation and private-public partnerships in cybercrime investigation, intelligence-sharing, and prosecution; privacy and data protection; capacity-building; policy development, enforcement, and compliance.

1. **Evolving Technologies** to be discussed will include, but not limited to: ***IoT; Cognitive Systems; Artificial Intelligence, including analytic tools and Generative AI; Metaverse; Quantum Computing & Cryptography; 5G technology; Intellectual Property Protection; Blockchain; Biometrics & Neuro-measurements; Telehealth; Nano Technology and Nano-medical Hacking; Digital, IOT, Cloud Management and Forensics; Cryptocurrencies, Dark Web; FINTECH, Forensic Accounting, e- Payment Apps; Mobile Apps & Social Media technologies.***

2. **POLCYB INTERNATIONAL LAW ENFORCEMENT AWARD (I.L.E.C.A.) 2025 – Presentation of Awards – Day 1/ following Opening Ceremony.**

3. **"TECHNOLOGY SHOWCASE" – 3 days (Days 1-3)**
   Stay abreast of state-of-the-art technologies, including tomorrow's IoT's, Robotics, Cognitive Systems, Neuro-measurement technologies, and other emerging technologies which could impact and/or support your efforts in Cybercrime Management.

4. **POLCYB CERTIFIED INTERNATIONAL CYBERCRIME PROFESSIONAL - EXECUTIVE LEVEL (C.I.C.P.-EX): CERTIFICATE PRESENTATION**

5. **FACILITATED "SUBJECT-MATTER EXPERT THINK-TANK" SESSIONS – Day 4 Morning**
   On the final day, all Participants are invited to participate in one of their preferred facilitated, Special Interest Think-Tank Sessions to transform Summit discussions into tangible, post-Summit strategic plans and solutions. Share your expertise at your preferred "**Think-Tank**" to explore recommendations for **tangible, Post-Summit Action Items with anticipated outcomes, and measurable milestones.** All participants will return to the Closing Plenary Session to share summaries from Group Facilitators. Join other "**Think-tank Champions"** to further develop the action items and / or strategic plans after the Summit.

6. **HANDS-ON DIGITAL INVESTIGATION TRAINING - 1 to 2 days (TBD)**

TENTATIVE SUMMIT TOPICS

Tentative Panel Discussions will include, but not limited to, the following intertwined issues:

1. Contribution of Evolving Technologies to Public Safety and Impact on Cybercrime:
   - Evolving Technologies to be discussed include, but are not limited to: Smart Cities; Connected Vehicles; Critical Infrastructure Protection; Cognitive Systems; AI Data Analytics & Generative AI; Cloud Security, etc.
   - Global Landscape of Cybercrime Trends and Threats and Threat Intelligence
   - Metaverse technologies; Nano technologies; 5G; Intellectual Property Protection; Blockchain; Biometrics & Neuro-measurements; Telehealth; Cryptocurrencies, FINTECH and e-Payment Apps; Regional use of Mobile & Social Media technologies; Cryptography; Online Child Protection.
   - Impact of Quantum Cryptography upon Public Safety.

2. International Conventions on Cybercrime (Council of Europe / UNODC):
   - The Budapest Convention on Cybercrime and the forthcoming United Nations treaty: differences, added value, and synergies.
   - Criminalization, Investigation, and Cooperation in Online Child Sexual Exploitation and Abuse, Grooming and the Non-consensual Dissemination of Intimate Images under these Treaties.

3. Metaverse technologies and Metaverse Crime.
   - Follow the Money: Search and Seizure of Virtual Assets in Online Fraud.
   - Investigation, Prosecution, Privacy considerations in the Metaverse, e.g. Investments in Virtual Properties and Money Laundering; “new” crimes, e.g. sexual assault, stalking, bullying in the Metaverse.

4. Preparing Today’s Leadership to Manage Tomorrow’s Cybercrime and Technologies:
   - International Perspectives on Capacity- building for Executives in Criminal Justice and Industry sectors.

5. Holistic Perspectives on development of a Scalable Cybercrime Management Framework.

6. Considerations for International Collaboration and Private-Public Partnerships in Investigation and Prosecution:
   - Disrupting Transnational Organized Crime, Financial Crime, and Online Fraud, including “pig-butchering”.
   - Terrorism Financing; Money Laundering (including Gaming and Sports Betting); Child Exploitation; Human Trafficking; Data Theft, Ransomware, Phishing, Hacking of IoT & Mobile Apps; Illegitimate use of AI; Nano-medical Hacking.
   - Considerations for Privacy, Regional Cybersecurity Laws and Regulations.
   - Digital Evidence and Asset Recovery: Privacy, Legal, and Capacity-building Considerations.
   - Case Studies and Lessons Learnt.

7. Impact of the Global and Regional Disasters on Fraud and Organized Crime.
   - Regional and Cultural Perspectives on Privacy considerations for Proactive Policies, Risk Assessment and Mitigation; Private-Public Partnerships and International Collaboration in Cybercrime Prevention and Mitigation; Shadow IT Threats and Remote Working.

8. Updates on Cyber Security & Cybercrime Laws and Initiatives around the Globe: Considerations for International Cooperation, e.g. COE, UNODC, Interpol, ASEAN, Europol, ITU, ENISA, OECD.

9. Addressing Public Safety Challenges posed by Digital Economy:
   - Understanding Impact of Regional Cyber Security Laws upon Governance and Compliance of Digital Economy; Asset Recovery; Digital Evidence Management; Risk Management; International Collaboration.

10. Removing barriers to Community Engagement in Cybercrime Prevention, and Innovative Responses to Digital Threats: Implications for Public Education, Cybercrime Reporting, Community Policing, and Collaboration.

11. Building Trusted Communities for Information-sharing: Reaching beyond Criminal Justice agencies for Collaboration.

WHO SHOULD ATTEND?

Regional and International Executive/Senior Management, and Practitioners who work in Public Safety and Industry sectors, including, but not limited to,:

- C-Suite Leaders.
- Executive & Senior Management in Public Safety and Governmental agencies.
- Judges; Public Prosecutors; Corporate Legal Counsels.
- Policymakers; Policy Enforcement.
- Leaders in Science, Technology, & Innovation.
- Investigative Supervisors/Managers.
- Human Resources; Recruitment; Training.
- Law Enforcement Training Academies.
- Corporate Fraud & Risk Management; Business Continuity; Loss Prevention.
- Academia.

BENEFITS FOR GLOBAL SUMMIT DELEGATES

- Prominent, international practitioners from private and public sectors will come together at ***the POLCYB International Summit 2025***. Our regional and international panelists will provide interactive and thought-provoking discussions for organizational leaders to develop collaborative and tangible action items.

- Delegates will share perspectives of how Advanced Technologies impact upon Cybercrime Management amongst Executive and Senior Management Leadership; Regional and Global Cybercrime Trends and Threats, and most of all, Innovative and Practical Approaches in enhancing Partnerships in managing cybercrime. They also will gain new knowledge on lessons learnt, initiatives that worked, and some that did not.

- **POLCYB Summit 2025 Think-tank Champions will collaborate with Post-Summit Working Group Members to further develop and advance action items and strategies.**

For Further Information, please contact:
Bessie Pang, Executive Director| bessie-pang@polcyb.org | www.polcyb.org