12 November 2021

Cooperation against Cybercrime

Octopus Conference 2021

16 -18 November 2021 – Online

Overview

Tue, 16 November (Please note that time is in CET)		
13h00 – 19h00 CET	**Plenary session:** Special event organised in cooperation with the Hungarian Chairmanship of the Committee of Ministers on the occasion of the: **20th anniversary of the Budapest Convention on Cybercrime** **&** **2nd Additional Protocol on enhanced cooperation and disclosure of electronic evidence** ► Opening ► 20 years of Budapest Convention – benefits and impact ► The 2nd Additional Protocol to the Convention on Cybercrime ► High-level interventions	
Wed, 17 November		
7h00 – 8h50	WS 1: Regional Workshop for Asia	
9h00 – 10h50	WS 2: COVID-19 and cybercrime	WS 3: Regional Workshop for Africa
11h00 – 12h50	WS 4: Crime and crypto currencies	WS 5: The global state of cybercrime legislation
13h00 – 14h00	Break	
14h00 – 15h50	WS 6: Automated detection of child sexual abuse materials	WS 7: Ransomware
16h00 – 17h50	WS 8: Cybercrime and artificial intelligence	Lightning talks I
18h00 – 19h50	WS 9: Regional Workshop for Latin America and the Caribbean	
Thu, 18 November		
7h00 – 8h50	Workshop 10: Regional Workshop for Pacific	
9h00 – 10h50	Workshop 11: Capacity building: judicial training	Workshop 12: Cybercrime victims
11h00 – 12h50	Workshop 13: Capacity building: guides and tools	Workshop 14: Cybercrime: Offenders
13h00 – 13h45		Lightning talks II
13h45 – 14h30	Break	
14h30 – 15h15	Outlook 1: Cybercrime – threats and trends	
15h30 – 16h15	Outlook 2: Human rights and rule of law in cyberspace	
16h15 – 16h30	Break	
16h30 – 17h15	Outlook 3: Cooperation against cybercrime in 2022	
17h15 – 18h00	Conclusions – Octopus take-aways	
18h00	*End of conference*	

Detailed Programme

TUE, 16 NOVEMBER – SPECIAL EVENT	
Plenary	Languages: English / French / Spanish / Hungarian
13h00 – 19h00	**20th anniversary of the Budapest Convention on Cybercrime** **&** **2nd Additional Protocol on enhanced cooperation and disclosure of electronic evidence** Moderator: Jan Kleijssen (Director of Information Society and Action against Crime, Council of Europe) ► **Opening** – Sándor Pintér (Minister of Interior, Hungary) – Marija Pejčinović Burić (Secretary General, Council of Europe) ► **Interventions I** – Interventions by ministers/senior officials ► **Panel: 20 years of Budapest Convention – global impact** – Moderators: Cristina Schulman (Chair of the Cybercrime Convention Committee (T-CY), Ministry of Justice, Romania) / Alexander Seger (Executive Secretary, T-CY, Council of Europe) – Panellists: Betty Shave (formerly US Department of Justice, USA), Pedro Verdelho (Vice-Chair of the T-CY, Public Prosecutor, Portugal), Papa Assane Touré (Magistrate, Deputy General Secretary of the Government, Senegal), Claudio Peguero (General Inspector General of the National Police, Dominican Republic), Jayantha Fernando (Director, Sri Lanka CERT and General Counsel, ICT Agency of Sri Lanka), Gareth Sansom (Department of Justice, Canada)
14h45-15h15	*Break*
	► **Interventions II** – Interventions by ministers/senior officials ► **Panel: The 2nd Additional Protocol to the Convention on Cybercrime - expectations** – Moderators: Cristina Schulman (Chair of the Cybercrime Convention Committee, Romania) / Alexander Seger (Executive Secretary, T-CY, Council of Europe) – Panellists: Kenneth Harris (Senior Counsel for International Criminal Matters, Department of Justice, US Mission to the European Union, USA), Jacqueline Palumbo (Senior General Counsel and Head of Treaty Negotiations, International Assistance Group, Justice Canada), Nathan Whiteman (Director, Department of Home Affairs, Australia), Tjabbe Bos (Team Leader, Unit 'Security in the digital age', Directorate-General for Migration and Home Affairs, European Union Commission) ► **Interventions III** – Interventions by Ministers/senior officials ► **Conclusions**

WED, 17 NOVEMBER – WORKSHOP SESSIONS	
Wed, 17 Nov 7h00 – 8h50	**Workshop 1 – Regional workshop for Asia: Strengthening international cooperation on cybercrime and electronic evidence in the region: Challenges and solutions** Language: EN Purpose: In Asia, substantive legislation for combatting cybercrimes is either largely or partially in place, while approximately 60% of the countries have procedural powers in this respect. The workshop aims to provide a platform for dialogue between decision-makers and practitioners in the region, to identify the particular challenges and good practices for international cooperation on cybercrime and electronic evidence in Asia. The workshop is structured as a roundtable discussion between decision-makers and practitioners from the region, with emphasis on participant engagement. The workshop is co-organised with the United Nations Office on Drugs and Crime (UNODC) Moderator/s: Vu Trung Hoang (Cybercrime Operations Officer, INTERPOL) Rapporteur: Betty Shave (Consultant, USA) Secretariat: Martha Stickings / Cosmina Menghes (GLACY +, C-PROC, Council of Europe) ► **Introduction and objective of the workshop** – Vu Trung Hoang (Cybercrime Operations Officer, INTERPOL) ► **Key challenges to international cooperation on cybercrime and electronic evidence. What are the specific problems of international cooperation on cybercrime and e-evidence in Asia? How do criminal justice authorities in Asia obtain evidence from other states?** – Alexandru Caciuloiu (Cybercrime and Cryptocurrency Advisor and Programme Coordinator for Southeast Asia and Pacific, UNODC) – Yeongsu Jeong (Senior Prosecutor, Director of Cybercrime Investigation Division, Forensic Science Investigation Department, Supreme Prosecutors' Office, Republic of Korea) ► **Best practices in international cooperation in Asia** – Jayantha Fernando (Director, Sri Lanka CERT and General Counsel, ICT Agency of Sri Lanka) – Norikazu Otaki (Deputy Chief for International Affairs, Japan Prosecutors unit on Emerging Crimes (JPEC), Supreme Public Prosecutors Office, Japan) – Vu Trung Hoang (Cybercrime Operations Officer, INTERPOL) ► **Recommendations on improving international cooperation in the region and beyond** – All panellists (Session moderated by Vu Trung Hoang (Cybercrime Operations Officer, INTERPOL) ► **Conclusions**
Wed, 17 Nov 9h00 – 10h50	**Workshop 2 – COVID-19 and Cybercrime**

	Languages: EN/FR/ES Purpose: The COVID-19 pandemic is accompanied by an unprecedented increase in cybercrime, further weakening the ability of public authorities to respond to cyberattacks. This weakening of defences is likely to be further exploited for criminal purposes and possibly for terrorist use of information and communication technologies, such as denial of service attacks against hospitals or interference with systems and data of health research facilities, ransomware etc. In this context, the importance of an effective response to cybercrime and other crime involving electronic evidence is undeniable. Criminal justice authorities need to undertake domestic investigations and engage in international and other forms of cooperation to detect, investigate, attribute and prosecute the above offences. The objective of the workshop is to identify challenges encountered by the criminal justice authorities and to seek solutions for possible future crises drawing lessons from the current pandemic. Moderator/s: Albert Rees (Cybercrime expert, USA) Rapporteur: Angela Marie de Gracia-Cruz (State Counsel, Department of Justice, Republic of the Philippines) Secretariat: Cristiana Mitea / Irina Drexler (Octopus Project, C-PROC, Council of Europe) ► **Introduction and objectives of the workshop** – Albert Rees (Cybercrime expert, USA) ► **Threat landscape and key challenges to investigation, prosecution and adjudication of COVID-19 related cybercrime, including the collection of e-evidence** – Focus on COVID-19, the perfect storm for cybercrime (Doug Witschi, Assistant Director Cybercrime Threat Response, INTERPOL) – Links between COVID-19 and organized crime (Simone Haysom, Senior Analyst, Global Initiative Against Transnational Organized Crime #CovidCrimeWatch initiative) ► **The criminal justice response, reshaped by COVID-19** – Covid 19 and Cybercrime - the Romanian experience (Daniel Marius Cuciurianu, Head of Bucharest Cybercrime Department, Romanian Police) – Khaled Youssef, Head of IT security Division, Manager for International Support, ISF, Lebanon – Bogdan Botezatu, Director of Threat Research and Reporting, Bitdefender – Discussions with participants and Q&A ► **How prepared are we for the next crises: recommendations** – Presentation of the interim results of the COVID-19 related cybercrime study for Asia (Geronimo L Sy, Founder, Office of Cybercrime, Department of Justice, Republic of the Philippines) – Open discussions on challenges and possible solutions ► **Conclusions**

Wed, 17 Nov 9h00 – 10h50	**Workshop 3 – Regional workshop for Africa: Strengthening cooperation on cybercrime and electronic evidence in the region – Challenges and solutions** Languages: EN/FR/PT/AR Purpose: Internet penetration and related services such as mobile-based financial services, are rapidly growing in Africa. This is accompanied by increasing cybercrime. Many countries in Africa have made it a priority to develop legal frameworks to efficiently criminalize offences against and by means of computers, permit domestic investigations and allow for effective international cooperation between criminal justice authorities, in line with international standards, in particular those of the Budapest and Malabo Convention. The benefits of cooperative approaches were confirmed on the occasion of the First Africa Forum on cybercrime in 2018 and again in the Second Africa Forum in June 2021. This workshop is to follow up on the agreement reached in these forums to further strengthen domestic and international cooperation on cybercrime in Africa as well as on the commitment by regional and international organisations to support such efforts. The specific aim is to identify concrete initiatives to be undertaken in the near future. This workshop is co-organized with the African Union Commission (AUC) and with the support of Global Forum for Cyber Expertise (GFCE) and the ECOWAS Commission. Moderator/s: Jean-Robert Hountomey (African Union Cyber Security Expert Group) Rapporteur: Hein Dries (OCWAR-C Project) Secretariat: Martha Stickings (GLACY+ Project, C-PROC, Council of Europe) ► **Introduction and objective of the workshop** – Jean-Robert Hountomey (African Union Cyber Security Expert Group) ► **Setting the scene** – Abdul Hakeem Ajijola (Chair of the African Union Cyber Security Expert Group) ► **Domestic coordination and international cooperation on cybercrime in Africa: needs and challenges** – Albert Antwi-Boasiako (Acting Director-General, Cyber Security Authority, Ghana) – Speaker TBC ► **What initiatives to enhance domestic and international cooperation?** – Dean Watkinson (Cybercrime Specialized Officer, INTERPOL) – Papa Assane Touré (Magistrate, Deputy General Secretary of the Government, Senegal) – Adel Jomni (Research professor, Business Law Centre, University of Montpellier) ► **Recommendations on improving international cooperation in the region and beyond** – Open discussions panel moderated by Moctar Yedaly, Global Forum on Cyber Expertise (GFCE)

	► **Conclusions**

Wed, 17 Nov 11h00 – 12h50	**Workshop 4 – Crime and cryptocurrencies** Languages: EN/FR/ES Purpose: Considering the difficulty to follow a money trail in the blockchain and the somewhat anonymity that surrounds transactions using cryptocurrencies, this virtual asset is preferred by cybercriminals when conducting their illicit activities and laundering the proceeds resulted from them. Ransomware, hacking and other types of cybercrime are without doubt highly inter-connected with cryptocurrency and the response of judicial authorities is sometimes hampered by the complexity of this mix of crimes. The lack of legislation on virtual assets and even more importantly, on seizing them also contributes to this void that cybercriminals exploit. The COVID-19 Pandemic only increased the use in virtual assets both for legitimate and illegitimate purposes. The aim of this workshop is to provide participants with information on how criminals abuse cryptocurrencies in hiding the illicit gains resulted from criminal endeavours and emphasise on the importance of defining legislation on domestic level in relation to handling and seizing this type of currency. Moderators: Jan Kerkhofs (Federal magistrate, Cyber Unit of the Belgian Federal Prosecutor's Office) / Paul Darcy (Senior Investigator, Ireland's Department of Justice) Rapporteur: Hania Elhelweh (Judge, President of the first instance court in the north of Lebanon) Secretariat: Alexandru Cristea / Liliana Trofim (iPROCEEDS-2 Project, C-PROC, Council of Europe) ► **Introduction and objective of the workshop** – Jan Kerkhofs and Paul Darcy ► **Crime and cryptocurrencies: case studies and typologies** – Knock-knock: who's there in the Blockchain? (Bart De Vlaminck, Detective ICT Crime, Federal Computer Crime Unit of Belgium) – How to co-ordinate mitigating virtual assets facilitated crimes (Jung Kee You, Criminal Intelligence Officer, INTERPOL's Financial Crimes Unit) – The 69,370 BTC Seizure from Silk Road (Claudia Quiroz, Assistant Attorney, Department of Justice, United States of America) ► **Investigating the criminal use of cryptocurrencies: tools, regulations and good practices** – Red flags related to the use of cryptocurrencies (Janet Ho, Policy Analyst, Financial Action Task Force (FATF)) – Regulating Virtual Asset Service Providers (VASP's), discussion (Irina Talianu, Head of Unit, Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism (MONEYVAL), Council of Europe) – Regulating cryptocurrencies, El Salvador's example (Ana Virginia Samayoa Baron, Director, Financial Intelligence Unit, El Salvador) – Following the money, cryptocurrency tracing introduction (Brian Carter, Senior Cybercrimes Specialist, Chainalysis ► **Conclusions**

Wed, 17 Nov 11h00 – 12h50	**Workshop 5 – The global state of cybercrime legislation: progress, challenges and lessons learnt** Languages: EN/FR/ES Purpose: Specific legislation is the basis for criminal justice action on cybercrime and electronic evidence. Many governments around the world have undertaken legal reforms, often using the Budapest Convention on Cybercrime as a guideline. However, cybercrime legislation also needs to meet human rights and rule of law requirements to prevent misuse. The aim of this workshop is to review progress made worldwide in terms of cybercrime legislation and to identify possible risks and challenges. Moderators: Zahid Jamil (Barrister-at-law, Jamil & Jamil, Pakistan) Rapporteur: Pedro Verdelho (Public Prosecutor, General Prosecutor's Office of Lisbon, Procuradoria General da Republica, Portugal) Secretariat: Giorgi Jokhadze / Natalia Mardari (CyberEast project, C-PROC, Council of Europe) ► **Introduction and objective of the workshop** ► **From 2013 to 2021: overview of progress made in the adoption of legislation on cybercrime and electronic evidence** – Results of a survey by the Cybercrime Programme Office of the Council of Europe (Giorgi Jokhadze, C-PROC) – Discussion ► **Examples of recent reforms** – Examples of good practices and recent reforms: - James Lutui (Director of Public Prosecution, Tonga) - Jacqueline Fick (Advocate, Chief Executive Officer, VizStrat Solutions, South Africa) - David Simmons (Chairman, Law Reform Commission, Barbados) ► **Challenges and risks** – Challenges of implementing procedural law from the perspective of safeguards and guarantees (Alexandros Ioannis Kargopoulos, Programme Officer, Research & Data Unit, EU Fundamental Rights Agency) – Discussion: meeting human rights and rule of law requirements - do's and don'ts (open discussion and examples) ► **Conclusions**
Wed, 17 Nov 14h00 – 15h50	**Workshop 6 – Automated detection of child sexual abuse materials** Languages: EN/FR Purpose: Online child sexual exploitation and abuse has been a major violation of children's rights for many years; it has been further increasing since the onset of the COVID-19 pandemic. Over the past decade multi-national service providers deployed technology for the automated detection of child sexual abuse materials (CSAM) that there uploaded or disseminated via their

services. Tens of millions of CSAM have been identified and reported in this way, and in many cases have helped rescue victims and identify and prosecute offenders worldwide. At the same time, the use of such techniques have raised rule of law and human rights concerns, for example, that they interfere with the privacy of communications or involve the transborder transfer of personal data or violate due process requirements. These concerns came to the forefront with the entry into force of the European Union's European Electronic Communication Code which brought these providers under the strict rules of the E-privacy Directive of the EU. In June 2021, the Council of Europe published an independent experts' report on this matter. The aim of the workshop is to continue the search for solutions that permit governments to meet their positive obligation to protect children against online sexual violence and enable service providers to use automated technologies to identify and report CSAM with the necessary privacy, data protection and rule of law safeguards.

Moderator/s: Jean-Christophe Le Toquin (President Point de Contact (French hotline), and managing partner SOCOGI)

Rapporteur: Katarzyna Staciwa (Independent Expert, National Research Institute/Dyzurnet.pl, Poland)

Secretariat: Gioia Scappucci (Executive Secretary, Lanzarote Committee, Council of Europe) / Cristiana Mitea & Irina Drexler (Octopus Project, Council of Europe)

► **Introduction and objective of the workshop**

- Jean-Christophe Le Toquin

► **Automated detection of child sexual abuse materials: How does it work?**

- John Shehan (Vice President, Exploited Children Division, National Centre for Missing and Exploited Children (NCMEC), USA)
- Arda Gerkens (CEO, Expertisebureau Online Kindermisbruik (EOKM), Netherlands)
- Discussion with intervention from Uri Sadeh (Coordinator, Crimes against Children Unit, VCO/Organized and Emerging Crime Directorate, INTERPOL)

► **The problem: the right to privacy v. positive obligations to protect against crime**

- Liora Lazarus (Professor of law, Peter A. Allard School of Law, University of British Columbia, Canada and Supernumerary Fellow, St. Anne's College, Oxford, United Kingdom)
- Ella Jakubowska (Policy Advisor, European Digital Rights – EDRi)
- Discussion

► **Solutions**

- Interim regulation and long-term solutions by the European Union (Cathrin Baur-Bulst, Head of Unit Security in the Digital Age, DG Home, EU Commission)
- Proposals having regard to the Lanzarote Convention (Maria José Castello-Branco, Vice-Chairperson Member of the Lanzarote Committee, Portugal)
- The Dutch Public-Private Partnership program & view of Internet industry (Michiel Steltman, Managing Director, Dutch Digital Infrastructure Association, Netherlands)
- Discussion with interventions from General Eric Freyssinet (Deputy Commander of the Gendarmerie nationale's Cyberspace Command, France) and Fred Langford (Director of Online Technology, OFCOM, UK)

	► **Conclusions**
Wed, 17 Nov 14h00 – 15h50	**Workshop 7 – Ransomware** Languages: EN/FR/ES Purpose: During the COVID-19 pandemic and due to restrictions imposed, more and more businesses switched their activities to the online environment, with their employees working from their homes. While in most business environments, methods of protection are in place to counter cyber threats, personal computers might not have the same level of compliance with Internet security rules, thus leaving their users defenceless against ransomware attacks. Ransomware attacks have been in the last two years hitting hard, targeting both personal workstations but also on critical infrastructure, exposing hospitals and medical facilities to the concentrated attacks of cybercriminals. The response of both judicial authorities and the private sector needs to be adequate to meet the challenges posed by this growing form of criminal activity. The workshop aims to provide recommendations on how to protect oneself against this form of cybercrime and provide the required tools to mitigate this threat. Another purpose is to determine how co-operation on ransomware can be further supported on Council of Europe level. Moderators: Hein Dries (CEO Vigilo Consult and Key Expert on Cybercrime in the OCWAR-C project) / James Shank (Chief Architect of Community Services, Team CYMRU and member of the Ransomware Task Force (RTF)) Rapporteur: Matteo Lucchetti (Director of CYBER 4.0, Italian Cybersecurity Competence Center) Secretariat: Alexandru Cristea / Liliana Trofim (iPROCEEDS-2 Project, C-PROC, Council of Europe) ► **Introduction and objective of the workshop** – Hein Dries and James Shank ► **Ransomware: threats and modi operandi** – A private sector perspective on ransomware, its threats and evolution over time (Alexandru Catalin Cosoi, Chief Security Strategist, Bitdefender) – Combating ransomware as a service, public-private partnership (Dominik Helble, former BKA cybercrime investigator and Head of Cyber Security of Festo, Germany) ► **Ransomware: tools, regulations, good practices** – Mitigating large ransomware attacks, the Colonial Pipeline case (Nikhil Bhagat, Federal Prosecutor within the USA Department of Justice) – No More Ransom, an EU perspective into preventing and countering ransomware (Emmanuel Kessler, Head of Team Prevention and Outreach, EUROPOL) ► **Conclusions**

Wed, 17 Nov 16h00 – 17h50	**Workshop 8 – Cybercrime, e-evidence and artificial intelligence** Languages: EN/FR/ES Purpose: Rapid progress in AI raises: ▪ additional risks of cybercrime (offenders weaponizing AI, AI detecting vulnerabilities to commit cybercrime or automate attacks. AI as target manipulated by offenders) ▪ questions of criminal liability (who is liable for decisions made and crime committed through AI technology?) ▪ complex challenges related to electronic evidence (how can e-evidence related to crime involving AI be secured and used in criminal proceedings?) On the other hand, AI may bring benefits to the criminal justice response to cybercrime (improving cybersecurity; detecting attacks; helping identify, investigate and prosecute offenders; or automating domestic and international cooperation). However, this in turn raises additional questions (how can rule of law and due process safeguards be ensured; what implications on territoriality and jurisdiction when AI-led investigations cross borders?). Organisations worldwide are currently working on questions related to artificial intelligence, including the Council of Europe. Within this context, the aim of the workshop is to identify key issues that should be taken into account when designing the future criminal justice response to cybercrime and e-evidence in relation to AI. Moderator/s: Jan Kleijssen (Director of Information Society and Action against Crime, Council of Europe) Rapporteur: Tania Schröter (Deputy Head of Unit, Procedural Criminal Law, Directorate-General for Justice and Consumers, European Union Commission) Secretariat: Martha Stickings / Gratiela Dumitrescu (GLACY+, C-PROC, Council of Europe) ► **Introduction and objective of the workshop** – Jan Kleijssen (Council of Europe) ► **Cybercrime and artificial intelligence: what are the threats and challenges, what are the opportunities?** – Malicious uses and abuses of artificial intelligence (Aglika Klayn, Cybercrime Specialist/J-CAT Coordinator, EC3, EUROPOL / Maria Eira, Information and Technology Officer, Centre for Artificial Intelligence and Robotics, United Nations Interregional Crime and Justice Research Institute / David Sancho, TrendMicro) – Provenance tech (Origin and C2PA) techniques and lessons learned from disinformation countermeasures (Ashish Jaiman, Director of Product Management, Bing Multimedia, Microsoft) – Discussion ► **AI, cybercrime and the law: fundamentals** – AI, cybercrime and criminal law: what is new and what is not new? (Dennis Baker, Professor, De Montfort University Law School, Leicester, UK) – AI, e-evidence and criminal liability (Sabine Gless, CDPC rapporteur on AI and Criminal Law, Professor of criminal law and criminal procedure law, University of Basel, Switzerland) – Discussion

	► **Conclusions**
Wed, 17 Nov 16h00 – 17h50	**Lightning talks I – Short interventions to present ideas or projects** Languages: EN/FR/ES/PT/AR Moderator/s: Elvio Salomon (GLACY+ Project, C-PROC, Council of Europe) / [TBC] Global Forum on Cyber Expertise (GFCE)
Wed, 17 Nov 18h00 – 19h50	**Workshop 9 – Regional workshop for Latin America and Caribbean: Cooperation with providers** Languages: EN/ES/PT Purpose: Obtaining subscriber information to identify the user of an Internet Protocol (IP) address used in a criminal offence or the owner of an email or social media account used for criminal purposes is crucial for any criminal justice authority investigating crime online. The same is true for domain name registration information regarding the owner of an Internet domain used for fraudulent purposes. In emergency situation where lives are at risk, expedited access to the content of an account may also be required. Often such information is held by service providers in other jurisdictions. The aim of this workshop is to identify current good practices to obtain data needed in a criminal investigation from multi-national service providers by authorities in Latin America and the Caribbean and to explain new solutions that may soon become available under the new Protocol to the Budapest Convention. Moderator/s: Anthony Teelucksingh (Chair of the OAS/REMJA Working Group on Cybercrime, US Department of Justice) Rapporteur: CARICOM IMPACS [speaker TBD] Secretariat: Catalina Stroe / Oana Tarus (GLACY+, C-PROC, Council of Europe) ► **Introduction and objective of the workshop** – Anthony Teelucksingh (Chair of the OAS/REMJA Working Group on Cybercrime, US Department of Justice) ► **Cooperation with multinational service providers** – The Chilean perspective (Mauricio Fernandez Montalban, Director, Specialized Unit on Money Laundering and Organized Crime of the National prosecution Service, Chile) – The Brazilian experience (Fernanda Teixeira Souza Domingos, Federal Prosecutor, Coordinator of the Advisory Group on Cybercrime at the Criminal Chamber of the Federal Prosecution Service, Brazil) ► **The 2nd Additional Protocol: towards enhanced cooperation with service providers across borders** – Erica O'Neil (Computer Crime and Intellectual Property Section, United States Department of Justice) – Claudio Peguero (General Inspector of the National Police, Dominican Republic) ► **How to improve cooperation between LEAs and service providers in criminal investigations in the region?**

	– Open discussions panel moderated by CARICOM IMPACS [moderator TBD] ► **Conclusions**
THU, 18 NOVEMBER, AM: WORKSHOP SESSIONS	
Thu, 18 Nov 7h00 – 8h50	**Workshop 10 – Regional workshop for Pacific** Language: EN Purpose: Online sexual exploitation and abuse of children (OCSEA) has been a major violation of the rights of children for many years. The COVID-19 pandemic, and increasing screen time by each and every one, has exacerbated the prevalence and risks of OCSEA, including in the Pacific region. While comprehensive approaches are needed to prevent OCSEA, and identify, protect and assist victims, effective criminal justice is an important part of the response to protect children against OCSEA and bring offenders to justice. The aim of this workshop is to share information on the threat of OCSEA as well as good practices in terms of policies, legislation, institutional capacities and domestic and international cooperation on OCSEA. Moderator/s: James Lutui (Director of Public Prosecutions, Tonga) and Patricia Femia (Assistant State Counsel State Solicitor's Office Western Australia) Rapporteur: Ana Guerreiro (Programme Advisor, Children's Rights Division/Lanzarote Committee, Council of Europe) Secretariat: Catalina Stroe (GLACY+, C-PROC, Council of Europe) ► **Introduction and objective of the workshop** – James Lutui (Director of Public Prosecutions, Tonga) ► **State of play: OCSEA threats and trends during the COVID-19 pandemic** – Uri Sadeh (Coordinator, Crimes against Children Unit, INTERPOL) – Alexandru Caciuloiu (Cybercrime and Cryptocurrency Advisor and Regional Coordinator for South East Asia and the Pacific, UNODC) ► **Policy responses in the Pacific area to protect children from OCSEA** – Haya Snobar (Assistant Director, Child Protection International Partnerships, Department of Home affairs, Australia) – Sophie Harding (Assistant Director, Child Protection International Partnerships, Department of Home affairs, Australia) – Tupou Kafa Vainikolo (Crown Prosecutor, Attorney General's Office, Tonga) ► **How to ensure effective criminal justice responses to OCSEA** – Open discussions moderated by Alexandru Caciuloiu (Cybercrime and Cryptocurrency Advisor and Regional Coordinator for South East Asia and the Pacific, UNODC) ► **Conclusions**

Thu, 18 Nov 9h00 – 10h50	**Workshop 11 – Capacity building: sustainable judicial training on cybercrime and e-evidence** Languages: EN/FR/ES/PT/AR Purpose: Given that not only cybercrime but any type of crime may involve evidence on a computer system (electronic evidence) any judge or prosecutor need to have the necessary skills to prosecute or adjudicate cases involving such evidence. In 2009, the Council of Europe developed a concept for cybercrime training for judges and prosecutors. Implementation of this concept has since been supported in numerous countries, typically in cooperation with domestic judicial training institutions. More recently, networking of judges and prosecutors trained under different programmes was promoted. In order to ensure that over time, any judge or prosecutor has access to and can participate in relevant training, sustainability of such programmes and strategic approaches to training are essential. A further challenge is that due to the COVID pandemic, much training is now only available online. For this reason, C-PROC is currently developing a platform for online training that will be put at the disposal to project countries. The aim of this workshop is to review how the sustainability of judicial training on cybercrime and e-evidence can be ensured through strategic approaches to training, networking of trainers and tools such as the online platform for judicial training. Moderator/s: Marcos Salt (Criminal Law Professor, Director of the Postgraduate Studies on Cybercrime and Electronic Evidence, University of Buenos Aires, Argentina) Rapporteur: Angela Marques Rodrigues (Judge, Superior Council of Magistracy, Cabo Verde) Secretariat: Catalina Stroe / Elena Floroiu (GLACY+ Project, C-PROC, Council of Europe) ► **Introduction and objective of the workshop** – Marcos Salt (Criminal Law Professor, Director of the Postgraduate Studies on Cybercrime and Electronic Evidence, University of Buenos Aires, Argentina) ► **Cybercrime training strategies: a survey** – Hania Helweh (President of the First Instance Court of Northern Lebanon) – Open discussions on the results of the survey ► **Shaping the future** – Progress Report of the International Network of Judicial Trainers on Cybercrime and Electronic Evidence (Sharon Segura Rodriguez, Prosecutor, Unit for Capacity Building and Supervision, Costa Rican focal point for the International Network of Judicial Trainers) – Progress report on the cybercrime e-learning training platform of the Council of Europe (Victor Voelzow, Council of Europe consultant) ► **How to develop and deliver sustainable judicial training** – Open discussions moderated by Marcos Salt and Catalina Stroe ► **Conclusions**

Thu, 18 Nov 9h00-10h50	**Workshop 12 – Cybercrime: Victims** Languages: EN/FR/ES Purpose: Cybercrime is an increasingly technologically advanced and fast-growing type of crime. It is extremely costly, allegedly impacts very large number of victims, and is psychologically impactful, which makes the effects of victimization in cyberspace hard to quantify. There is limited understanding of who the victims (individuals and organisations) are and how cybercrime affects different categories of victims. Compared to traditional crime, cyber victimization entails elements of *accessibility (*perpetrators can reach significant number of victims), *anonymity*, and thus *limited detectability* (sometimes victims are not even aware they have been victimized), and is also *hard to constrain*, due to the astonishing speed with which data is shared and how volatile possible evidence is. This workshop will explore who are the cybercrime victims (individuals and organisations) and look into the criminal justice response but also alternative remedies (such as restorative justice) available to them. Moderator: Jeffrey DeMarco (Assistant Director Knowledge and Insight, Victim Support, UK) Rapporteur: Miriam Bahamonde Blanco (Senior Prosecutor, Ministry of Justice of Spain) Secretariat: Cecilia Popa (CyberEast, C-PROC, Council of Europe) ► **Introduction and objective of the workshop** – Jeffrey DeMarco ► **Who are the victims of cybercrime?** – An analysis of victim survey data (Jan Van Dijk, Fellow of the Netherlands Institute for the Study of Crime and Law Enforcement) – Victims of cybercrime: who are they and what are the issues (Marianne Junger, University of Twente) – Discussion ► **Towards a typology of victims of cybercrime?** – Support manuals for cybercrime victims (Ricardo Salgueiro Dos Santos Fernandes Estrela, Portuguese Association for Victim Support) – Companies as victims of cybercrime: ENISA Report on Cybersecurity for SMEs - Challenges and Recommendations (Anna Sarri, Cybersecurity Officer, ENISA) – Discussion ► **Obtaining justice for victims of cybercrime** – Criminal justice for victims of cybercrime - Example of cyberviolence (Gareth Sansom, Department of Justice, Canada) – Can restorative justice address victims of cybercrime? (Emanuela Biffi, Project & Events officer, European Forum for Restorative Justice) – Discussion ► **Conclusions**

Thu, 18 Nov
11h00 – 12h50

Workshop 13 – Capacity building: Guides and tools

Languages: EN/FR/ES

Purpose: Capacity building on cybercrime and electronic evidence is a complex and time and resource-intensive process, involving large numbers of organisations and practitioners. Given the growth of cybercrime and the fact that any crime may involve electronic evidence, any investigator, prosecutor or judge will be confronted to with such cases and needs to be equipped with the necessary skills to handle them. A number of guides and other tools have been developed by the Council of Europe and other organisations in recent years, to help criminal justice practitioners acquire such skills. These guides and tools may complement training programmes or serve self-learning. The aim of this workshop is to increase knowledge of participants of such guides and tools and promote their adaptation to meet domestic needs.

Moderator/s: Michele Socco (Policy Officer, European Commission, Directorate General for Migration and Home Affairs, Unit 'Security in the Digital Age')

Rapporteur: Nayia Barmpaliou (Director, Cyber Lab International, European Union Institute for Security Studies (EUISS))

Secretariat: Virgil Spiridon (Head of Operations, C-PROC, Council of Europe)

► Introduction and objective of the workshop

– Michele Socco (Policy Officer, European Commission, Directorate General for Migration and Home Affairs, Unit 'Security in the Digital Age')

► Key elements of cybercrime capacity building

– Craig Jones (Director of Cybercrime, INTERPOL)
– Renata Delgado-Schenk (Cybercrime Programme Officer, UNODC)

► Guides and tools: development, implementation and benefits

– SIRIUS Project
  - Robert Laid (Project Manager, EUROJUST)
  - Juan De Dios Toledo Martinez (Project Manager, EUROPOL)

– Wouter Veenstra (Manager Global Outreach and Partnerships, Global Forum on Cyber Expertise)

– Council of Europe: C-PROC guides
  - Victor Voelzow (CoE consultant)
  - Safia El Moutaouakil (Head of Regional Digital Laboratory, Morocco)

– Terry Wilson (Global Partnership Director, Global Cyber Alliance)

► Conclusions

Thu, 18 Nov 11h00 – 12h50	**Workshop 14 – Cybercrime: Offenders** Languages: EN/FR/ES Purpose: Cybercrime perpetrators are as diverse and complex as the cybercrime that they commit. For example, they come from different backgrounds and have different (egotistical, technical, monetary, ideological, political, professional, vengeful, sexual or other) motivations. They may or may not be professional criminals, and individuals or part of organised groups or networks (example of Advanced Persistent Threats). Some may commit crime on their own account or make their services available to others, and some may be supported by or be state actors. A better understanding of the types of perpetrators and their motivations and techniques can be instrumental for the prevention of cybercrime and for a more effective criminal justice response. The aim of this workshop is to contribute to such a better understanding and to initiate steps towards a typology of offenders. Moderator/s: Dong Uk Kim (Specialized Officer, INTERPOL Cybercrime, GLACY+ Project) Rapporteur: Silvia Portesi (Cybersecurity Expert, European Union Agency for Cybersecurity, ENISA) Secretariat: Ana Vlad / Giorgi Jokhadze (CyberEast Project, C-PROC, Council of Europe) ► **Introduction and objective of the workshop** ► **Who are the perpetrators? Towards a typology** – Financially motivated cybercriminal networks (Recording: Rutger Leukfeldt, Senior Researcher, Netherlands Institute for the Study of Crime and Law Enforcement (NSCR), and Director, Centre of Expertise Cybersecurity, The Hague University of Applied Sciences) – Typologies of cybercrime offenders in case studies (Youngjin Song, Professor, International Cybercrime Research Centre, Korean National Police University) – Findings by EUROPOL (Emmanuel Kessler, Head of Team Prevention and Outreach, EC3, the Cybercrime Centre of Europol) – Offenders: Key threats for Europe in 2021 (Georgios Chatzichristos, Officer in Cybersecurity, Operational Cooperation Unit, ENISA) – The view of the private sector (Aisling Kelly, Senior Counsel, Law Enforcement & National Security, Microsoft) – Q&A and discussion ► **Criminal justice response to state (-supported) perpetrators?** – State supported cybercrime and the US criminal justice response (Sean Newell, Deputy Chief (Cyber), Counterintelligence and Export Control Section, National Security Division, United States Department of Justice) – Private sector view (Aisling Kelly, Senior Counsel, Law Enforcement & National Security, Microsoft) – Discussion ► **An alternative look: prevention** – Prevention of cybercrime and work with offenders (Floor Jansen, National High Tech Crime Unit, Dutch Police) – Discussion

	► **Conclusions**
Thu, 18 Nov 13h00 – 13h45	**Lightning talks II – Short interventions to present ideas or projects** Languages: EN/FR/ES/PT/AR Moderator/s: Elvio Salomon (GLACY+ Project, C-PROC, Council of Europe) / Elliot Global Forum on Cyber Expertise (GFCE)
13h45 – 14h30	*Break*
THURSDAY, 18 NOVEMBER PM: PLENARY SESSIONS	
Thu, 18 Nov 14h30 – 15h30	**Outlook 1: Cybercrime – threats and trends** Languages: EN/FR/ES Purpose: Reports on published by public and private sector organisations show a rapidly evolving – and at times contradictory – picture regarding cybercrime and cyberattacks. The aim of this session is to come to predictions regarding cyber threats and trends in 2022/2023 and challenges that criminal justice authorities need to be prepared for. Moderator/s: Martha Stickings (GLACY+, C-PROC, Council of Europe) Secretariat: Gratiela Dumitrescu / Floriane Spielman (GLACY+/Octopus Project, C-PROC, Council of Europe) ► **Introduction** – Martha Stickings (GLACY+, C-PROC, Council of Europe) ► **Panel on current threats, predictions for 2022/2023 and the role of the criminal justice response** – IOCTA (Emmanuel Kessler, Head of Team Prevention and Outreach, EC3, EUROPOL) – Cybercrime in Japan (Ko Ikai, Director of Cybercrime Investigation Office, National Police Agency of Japan) – Anti-Phishing Working Group (Peter Cassidy, Secretary General, APWG) – Microsoft Digital Defense Report: the state of cybercrime (Uwe Rasmussen, Lead attorney for Microsoft on malware, EMEA) – BITKOM (Sebastian Artz, Head of Cyber & Information Security, BITKOM) ► **Conclusions**
Thu, 18 Nov 15h30-16h15	**Outlook 2: Human rights and rule of law in cyberspace** Languages: EN/FR/ES Purpose: As cybercrime is a threat to human rights, governments not only have the "negative" obligation to refrain from interfering with these rights (unless certain conditions are met) but it is increasingly considered that governments have a "positive" obligation to protect individuals against interference with their rights by others. This includes, for example, the obligation to put effective means in place to protect individuals against cybercrime through criminal law. However, such means are also subject to conditions. This session

	will discuss what is takes to provide for criminal justice response that is effective and that meets human rights and rule of law requirements at the same time. Moderator: Isabelle Servoz-Gallucci (Secretary of the Committee of Convention 108 (T-PD), Head of the Data Protection Unit, Council of Europe) Secretariat: Martha Stickings (GLACY+, C-PROC, Council of Europe) ► **Introduction** – Isabelle Servoz-Gallucci ► **Panel** – Keynote: Robert Spano (President of the European Court of Human Rights) – Nnenna Ifeanyi-Ajufo (Vice-Chair African Union Cyber Security Experts Group / Senior Lecturer Law and Technology, School of Law, Swansea University, United Kingdom) – Liora Lazarus (Professor in Law, Peter A. Allard School of Law, The University of British Columbia, Canada and Supernumerary Fellow, St. Anne's College, Oxford, United Kingdom) ► **Conclusions**
16h15-16h30	*Health break*
Thu, 18 Nov 16h30-17h30	**Outlook 3: Cooperation against cybercrime in 2022** Languages: EN/FR/ES Purpose: Having discussed treats and challenges but also shared experiences and good practices throughout this conference, the aim of this session is to have organisations involved in policies, standard setting and capacity building on cybercrime present their intentions on how to enhance international cooperation on cybercrime and e-evidence in 2022. Moderator/s: Alexander Seger (Head of Cybercrime Division, Council of Europe) Secretariat: Celine Dewaele (Cybercrime Division, Council of Europe) ► **Introduction** ► **Panel** – UNODC (Neil Walsh, Chief of the Cybercrime and Anti-Money Laundering Section, UN Office on Drugs and Crime) – African Union Commission (Abdul-Hakeem Ajijola, Chair of African Union Cyber Security Expert Group) – [TBC: Russian Federation (Ernest Chernukhin, Head of Section, Department of International Information Security, Ministry of Foreign Affairs the Russian Federation)] – Organisation of American States (Anthony Teelucksingh, Chair of the OAS/REMJA Working Group on Cybercrime, US Department of Justice) – European Union (Cathrin Baur-Bulst, Head of Unit Security in the Digital Age, DG Home, European Commission) ► **Conclusions**

Thu, 18 Nov 17h30-18h00	**Conference conclusions**