Cyber Capacity Building as a Development Issue: What Role for Regional Organisations?

International conference hosted by
the EU Institute for Security Studies

Paris, 13-14 March 2014

CONTENTS

WELCOME MESSAGE

Dear Participants,

Welcome to Paris and to this high level Conference that the EUISS has organised in close cooperation with the EEAS.

In order to take global capacity-building work forward, we need to get a comprehensive overview of existing initiatives and to concentrate on better coordination of existing and future efforts. In the long run, we need to find ways to leverage the best practices of both technologically advanced countries and the private sector, with a view to creating a resilient information infrastructure that fosters open societies and economic growth worldwide. We should also look for synergies across various development policy areas on how to build trustworthy IT infrastructure, provide basic e-skills education, and ensure respect of human rights online. Those objectives will be difficult to achieve without including voices from other regional organisations and international partners, in particular those in the developing world.

The EUISS conference contributes to this goal by bringing together the development aid and cyber policy communities, the public and the private sectors, technologically advanced and less advanced countries. We strongly hope that such a unique mix of experts, officials and relevant stakeholders will also translate into a meeting of minds and thus pave the way for further exchanges and bolder achievements.

Joëlle JENNY

Director
Security Policy and Conflict Prevention Division
European External Action Service

Antonio MISSIROLI

Director
EU Institute for Security Studies

CONCEPT NOTE

The European Cyber Security Strategy establishes capacity building as a priority for the EU's international cyberspace policy. The EU has already started work on promoting the rule of law to address global cybercrime and develop training programmes.

Capacity building in this area requires a horizontal approach across different development policy fields, focusing on improving governance, protecting infrastructure, endorsing the rule of law and providing training. These requirements will be included into various EU instruments available for development assistance. In the future, a considerable increase in funding is foreseen for cyber capacity building programmes conducted by the EU.

The objectives of this conference are the following:

1. **To address the link between cyber capacities and development policies**
   The need to integrate cyber capacity building and development policies has been recognised by the cyber community. However, there is a clear need for a deeper dialogue with the development community and recipient countries in order to better understand how cyber capacities can contribute to the achievement of broader development goals.

2. **To agree on the regional and functional focus of cyber capacity building efforts**
   There is a need to set priorities and identify indicators of success and failure. To steer this process, this conference aims to bring together different communities from the fields of development assistance, cybersecurity, the private sector, and civil society.

3. **To develop international coordination in capacity building, for instance through regional organisations**
   Many stakeholders are involved in cyber issues. To achieve a better overview of initiatives and avoid duplication, it may be necessary to set up a clearing-house mechanism between donors and recipients. A better understanding of the added value of working through regional organisations and their contribution to capacity building efforts would also be highly beneficial.

Consequently, the main questions that will be addressed during the event include:

- To what extent are the objectives and missions of different communities (security, development, IT) compatible and coherent (or not) when dealing with cyberspace?
- How can they feed into each other's work and support each other's tasks?
- Where and when has cooperation between these communities yielded particularly good results?
- How can regional organisations facilitate this process?

OFFICIAL PROGRAMME

13 March 2014

13.00 – 13.30	Registration (Salon Boudoir)
13.30 – 14.00	**Welcoming remarks and keynote speech by Ms Joëlle Jenny, Director for Security Policy and Conflict Prevention, European External Action Service** (Grand Salon)
14.00 – 15.15	**Roundtable I** (Grand Salon) Bringing international players together: challenges and opportunities
15.15 – 15.30	*Coffee break* (Salon Boudoir)
15.30 – 18.00	**Parallel working sessions**
	Working session I (Salon Poincaré) The rule of law and justice in cyberspace
	Working session II (Salon Arago) Frameworks for capacity building
	Working session III (Salon Gay Lussac) Multistakeholder process as a driver of development
18.00 – 21.30	**Cocktail and opening dinner with speech by Mr Getachew Engida, Deputy Director General of UNESCO** (Salon Watteau, Salon Le Brun and Salon Manilève)

14 March 2014

10.00 – 10.30	*Registration and coffee* (Salon Boudoir)
10.30 – 11.30	**Roundtable II** (Grand Salon) Current approaches to cyber capacity building: what works, what does not?
11.30 - 11.45	*Coffee break* (Salon Boudoir)
11.45 – 13.00	**Roundtable III** (Grand Salon) Resilient and open networks: how can governments keep up?
13.00 - 14.30	*Lunch* (Salon Le Brun and Salon Manilève)
14.30 - 16.00	**Roundtable IV** (Grand Salon) Cyber capacity at the service of development: assessing common solutions to shared problems
16.00 - 16.30	**Closing remarks by Ms Emmanuelle d'Achon, Deputy Secretary General and Cyber Affairs Coordinator, Ministry of Foreign Affairs** (Grand Salon)
16.30	*Afternoon tea – End of the conference* (Salon Boudoir)

DETAILED PROGRAMME

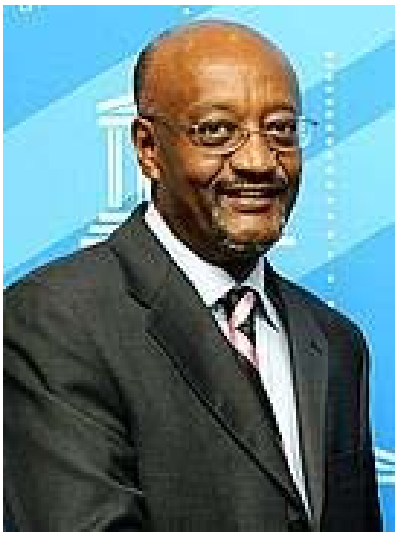
Welcoming remarks by Mr Antonio Missiroli, Director of the European Union Institute for Security Studies, Paris

Dr Antonio Missiroli has a long career in various research and government institutions. Before becoming the Director of the EUISS, he was Adviser at the Bureau of European Policy Advisers (BEPA) of the European Commission, in charge of European outreach, including relations with think tanks and research centres across the Union and beyond. Previous to this he was Director of Studies at the European Policy Centre in Brussels, Research Fellow and Senior Research Fellow at the W/EU Institute for Security Studies in Paris, and a Visiting Fellow at St Antony's College, Oxford University. As well as being a professional journalist, he has also taught at the Universities of Bath and Trento, as well as Boston University and SAIS/Johns Hopkins (Bologna). He is currently visiting lecturer at the College of Europe (Bruges) and Sciences Po (Paris). Dr Missiroli holds a PhD degree in Contemporary History from the Scuola Normale Superiore (Pisa) and a Master's degree in International Public Policy from SAIS/Johns Hopkins University.

Keynote opening speech by Ms Joëlle Jenny, Director of Security Policy and Conflict Prevention Division, European External Action Service, Brussels

Joëlle Jenny is Director for Security Policy and Conflict Prevention at the European External Action Service. Prior to joining the EEAS she worked successively as a Swiss and a British diplomat, covering international security issues, non-proliferation/arms control, and conflict prevention and peace building, including at the UN. She has worked for the UK's Department for International Development, the Swiss Foreign Ministry and the International Committee of the Red Cross. She worked extensively in Iraq, Yemen and the Palestinian Territories, and held postings in New York, Angola, Bosnia-Herzegovina, Cambodia, Rwanda and the former Yugoslav Republic of Macedonia. She was also a research assistant at NATO. She holds a Master in International Security from the Fletcher School of Law and Diplomacy in Boston, USA.

Opening dinner speech by Mr Getachew Engida, Deputy Director-General of United Nations Educational, Scientific and Cultural Organisation (UNESCO), Paris



Getachew Engida is the Deputy Director-General of UNESCO. He started his career in 1981 as an Audit Supervisor at Messrs Ernst & Young, Chartered Accountants in London. In 1985, he joined Industrial Gases Company (BOC Ltd) in Surrey (UK) as Group Research Accountant. From 1987 to 1995, he was a Financial Manager for Reuters Ltd in London and Nairobi (Kenya). In 1995, he joined the International Fund for Agricultural Development (IFAD) in Rome (Italy) as Assistant Comptroller: during his tenure, he served as Secretary of the Finance and Audit Committee of the IFAD Executive Board, and as Chief Financial Officer and later as Director of Finance, Human Resources and Administration of the World Bank/FAO/CGIAR supported the International Livestock Research Institute (ILRI) (1999-2004), based in Nairobi (Kenya). Engida joined UNESCO as Deputy Assistant Director-General for Administration and Comptroller in the Sector for Administration in June 2004. As from 1 July 2010, Engida has taken on the added responsibility of managing the Communication and Information Programme of UNESCO. He holds a B.A. (Honours) degree in Economics from the University of Manchester and an MBA with Commendations in International Business and Finance from City University Business School in London.

Keynote closing remarks by Ms Emmanuelle d'Achon, Deputy Secretary General and Cyber Affairs Coordinator, Ministry of Foreign Affairs, Paris

Emmanuelle d'Achon is Deputy Secretary-General of the French Ministry of Foreign Affairs, Paris. Prior to this she served as Ambassador of France to Ireland, Ambassador of France to Tanzania and in various roles in French embassies around the world. She was also involved in the early years of the European External Action Service, in her role as Counsellor to the Secretary General of MFA, with responsibility for covering the establishment of the EEAS. She holds a BA in French Literature from the University of Caen (Normandy) and also studied at the Institute of Political Science (Sciences Po) in Paris, French School of Oriental Studies (INALCO), and the National School of Administration (ENA).

Roundtable I
Bringing international players together: challenges and opportunities

Chair **James Lewis,** Director and Senior Fellow, Strategic Technologies Programme, Center for Strategic and International Studies**,** Washington, D.C.

This opening session seeks to take stock of the ongoing cyber capacity building efforts. The general focus will be on ways to strengthen cooperation between regional organisations. How do they see their role in the process and what are their expectations towards each other? What are the 'low-hanging fruits' or elements that could be implemented in the medium term? What are the challenges to this cooperation? What are the specific expectations of others with regard to the European Union?

Speakers **Joëlle Jenny,** Director, Security Policy and Conflict Prevention, European External Action Service, Brussels
Thomas Dukes, Deputy Coordinator for Cyber Issues, U.S. Department of State, Washington, D.C.
Laurent Bernat, Cyber Security Risk Policy Analyst, Directorate for Science, Technology and Industry, OECD, Paris
Neil Klopfenstein, Executive Secretary, Organisation of American States, Inter-American Committee against Terrorism, Washington, D.C.
Matias Bertino Matondo, Advisor, Office of Chairperson, African Union Commission, Addis Ababa

Working session I
The rule of law and justice in cyberspace

Chair **Zahid Jamil**, Director, Center for Strategic and Policy Analysis, Center for Strategic and Policy Analysis, Islamabad

Associate **Maria Grazia Porcedda**, Research Assistant, Surveillance, Privacy and Security Project, European University Institute, Florence

The fight against cybercrime is a policy area in which the spectrum of capacity building initiatives is probably most visible, and the efforts most advanced and measurable. This is partly due to the adoption of the principles of the Budapest Convention, which has provided a solid basis for structured international cooperation against cybercrime. To date, 41 countries have signed the Convention and approximately 120 countries have followed its principles as a model for their national legislation. The remaining challenges are to ensure that countries have the capacities to fight rapidly increasing cybercrime offences and to start addressing cybercrime as a policy objective related to strengthening good governance, the rule of law and economic development. This session aims to indicate concrete steps that could be taken in both aspects.

The questions that this session will address include:

- What have we learned so far about cyber capacity building in the area of fighting cybercrime?

- What concrete examples can we identify in order to make a better case for the fight against cybercrime as a development issue?
- How can we combine or learn from legal approaches in different regions?
- In what ways can cooperation between the private sector, international organisations and development agencies be a driver for effectively achieving measurable results in this area?

Speakers **Alexander Seger**, Executive Secretary, Cybercrime Convention Committee, Council of Europe, Strasbourg
Joash Dache, Secretary - CEO, Kenya Law Reform Commission, Nairobi
Jayantha Fernando, Programme Director, Information and Communication Technology Agency, Colombo
Abdul Karim H. Chukkol, Deputy Chief Director, Economic and Financial Crime Commission, Lagos
Kah-kin Ho, Strategic Security Manager, CISCO, Geneva

Working session II
Frameworks for capacity building

Chair **Nick Coleman**, Global Head Cyber Intelligence, IBM Services, London

Associate **Neil Robinson**, Research Leader, RAND Europe, Brussels

Finding a suitable framework for securing vital infrastructure, while being able to fully enjoy the benefits of technological advancement ,is the holy grail of the cyber community. Despite the many efforts undertaken at national and international level, building capacities of individual countries or across regions remains a challenge. This is partly related to difficulties with defining what capabilities are required and how to develop them. The purpose of this session will be to look at the existing frameworks for capacity building, to identify capacity building blocks and concrete steps which could lead to their attainment (e.g. through public-private partnerships, etc.). The discussion will also aim to investigate the cost-benefit aspect of those frameworks in order to ensure that their sustainability is one of the guiding principles.

The questions that this session will address include:

- How different regions and/or countries have approached the subject and how can we combine or learn from various regional approaches?
- How to constantly improve capacities so that they are effective in the global context and make capacity building a part of economic growth agendas?
- What have we learned so far about fostering an IT risk management culture in developing countries?
- What concrete examples of challenges can we identify in order to make a better case for cyber resilience as a development issue?

Speakers **Jose Clastornik**, Executive Director, Agency for e-Government and Information Society (AGESIC), Montevideo
Anita Sohan, International Affairs Officer, Ministry of National Security, Port of Spain
Samia Melhem, Lead ICT Specialist, World Bank, Washington, D.C.
Mariko Miya, Security Analyst, Cyber Defence Institute, Tokyo

Working session III
Multistakeholder process as a driver of development

Chair **Paul Twomey,** Founder, CEO Argo Pacific, Sydney

Associate **Taylor Roberts**, Research Fellow, Global Cyber Security Capacity Centre, Oxford University, Oxford

The point of departure for the discussion in this session is the assumption that the multistakeholder model – where the private sector, civil society and governments participate on an equal footing – contributes to economic and societal development. But there are many models of multistakeholder processes and there is a clear need to understand them better.

The questions that this session will address include:

- How do the multistakeholder processes take into account development objectives? Are there specific examples or models worth mentioning? What are their strengths and weaknesses?
- How can we ensure their scalability and sustainability in the long run?
- How can governments benefit from numerous grassroots initiatives in a more efficient way without undermining their innovative nature?

Speakers **Panagiota-Nayia Barmpaliou,** Programme Manager, European Commission, DG Development and Cooperation – EuropeAid, Brussels
Serge Kapto, Policy Specialist, E-governance and Access to Information, Unated Nations Development Programme, New York
Preetam Maloor, Strategy and Policy Advisor, International Policy, International Telecommunication Union, Geneva
Timothy Noonan, Director, International Trade Union Confederation, Brussels
Bawani Selvaratnam, Director, Malaysian Communications and Multi-media Commission, Kuala Lumpur

Roundtable II
Current approaches to cyber capacity building: what works, what does not?

Chair **Patryk Pawlak**, Senior Analyst, EU Institute for Security Studies, Paris

The continuing emergence of cyber capacity building on the policy agendas of various international and regional institutions calls for a clear definition of objectives and expected outcomes. Even though some countries or organisations are generally recognised to be champions in capacity building – due to their past experiences – we still have limited knowledge about ongoing capacity building activities worldwide: either due to the absence of data or due to limited coordination between different actors. The understanding of capacity building efforts also varies depending on the focus of the activities. This session will focus on exchanging experiences in capacity building, including on strengthening various elements of national cyber resilience systems: strategies, cross-agency cooperation, and legal frameworks.

The questions that will be addressed in this session include:

- What are the 'speed bumps' and 'accelerators' in cyber capacity building?
- How to improve sustainability and scalability of capacity building projects?
- Are there specific business models worth promoting?
- What region-specific factors need to be taken into account?

Speakers **Zahid Jamil**, Director, Center for Strategic and Policy Analysis, Center for Strategic and Policy Analysis, Islamabad
Paul Twomey, Founder, CEO, Argo Pacific, Sydney
Nick Coleman, Global Head Cyber Intelligence, IBM Services, London
Olivier Burgersdijk, Head of Strategy, European Cybercrime Centre (EC3), The Hague
Juliana Garcia Vargas, Director, Public Security and Critical Infrastructure, Ministry of National Defence, Bogota

Roundtable III
Resilient and open networks: how can governments keep up?

Chair **Derek O'Halloran,** Head of IT Industry, World Economic Forum, New York

The use of new technologies as a means to advance social and economic development is not a new item on the policy agendas. Numerous international organisations and agencies – such as the World Bank, UNDP or OECD – have recognised the role of ICT in strengthening democratic governance (i.e. by tackling poverty, social exclusion, and inequality) or the contribution of the internet economy to close development gaps. According to the OECD, the share of developing countries in the total number of mobile phone subscriptions has increased from 35% in 2000 to 76.6% in 2013. Moreover, an increasing number of small businesses now use portable devices for work purposes. But these developments bring about not only opportunities but also new challenges to the functioning of societies and states that are not always ready to deal with them – be it through ensuring an appropriate level of cybercrime legislation or the resilience of critical information systems.

The aim of this roundtable is to focus on the needs and challenges that governments in developing countries face when implementing specific programmes.

The questions that will be addressed in this session include:

- What are the main challenges for the recipient countries and vulnerabilities in the existing cyber resilience systems?
- What are the main challenges, for instance, with regard to sustainability and retention of knowledge?
- How is it possible to improve the efforts of the donor community?

Speakers **Barbara-Chiara Ubaldi,** E-Government Project Manager, Organisation for Economic Co-operation and Development (OECD), Paris
Samia Melhem, Lead ICT Specialist, World Bank, Washington, D.C.
Raul Millan, Director CSIRT-Panama, AIG, Panama City
Chanki Park, Manager, Global Project Division, Korea Internet and Security Agency (KISA), Seoul
David Pollington, Director, International Security Relations, Microsoft, London
Ilyse Stempler, Senior Policy Advisor, United States Agency for International Development (USAID), Washington, D.C.

Roundtable IV
Cyber capacity at the service of development: assessing common solutions to shared problems

Chair **Sadie Creese**, Director, Global Cyber Security Capacity Building Centre, Oxford University, Oxford

The development community has been involved in various ICT related projects for many years now. The positive contribution that technological developments make in promoting economic, political and social development has been noted in the Busan Partnership for Effective Development Cooperation of 2011. But the challenges related to technological progress are also significant: adjusting financial instruments, designing partnerships between the private sector and governments or ensuring the sustainability of capacity building projects. In recent years, the focus has been on economic growth facilitated by new technologies in emerging markets and developing countries. At the same time, the benefits offered by increased connectivity can be jeopardised by rising threats to the resilience of ICT networks and systems – a well-established subject on the cyber community agenda. For this reason, the complementarity of development goals and cyber capacity building needs to be clearly identified and analysed.

The questions that will be addressed in this session include:

- What development and cyber communities could learn from each other in building sustainable efforts in cyber resilience? What are the challenges they face?
- What development objectives are linked to cyber resilience (e.g. reliable e-governance, online public services for the population, online education, etc.)?

- How to fully exploit the synergies between the development and cyber capacity building?

Speakers **Belisario Contreras**, Cyber Security Program Manager, Organization of American States, Washington, D.C.
Serge Kapto, Policy Specialist, E-governance and Access to Information, Unated Nations Development Programme, New York
Jens Karberg, Advisor and Programme Manager for ICT for Development, Swedish International Development Cooperation Agency (SIDA), Stockholm
Adriane LaPointe, Senior Policy Advisor,Office of the Coordinator for Cyber Issues, U.S. Department of State, Washington, D.C.
Steve Purser, Head of Core Operations Department, ENISA, Heraklion
Heli Tiirmaa-Klaar, Head, Cyber Policy Coordination, European External Action Service, Brussels

ABOUT THE SPEAKERS (alphabetical order)

Panagiota Nayia Barmpaliou is a Programme Manager for cybercrime and cybersecurity in the Unit of the Instrument contributing to Stability and Peace (IcSP) at the European Commission's DG Development and Cooperation - EuropeAid. She is managing cooperation programmes that are at the heart of the security-development nexus addressing global and trans-regional threats, namely against organised crime. She has worked extensively in the area of EU external relations from both a policy and an operational perspective, most notably on human rights and rule of law issues, while her geographic expertise covers South East Asia, Iraq and Iran. Prior to her work at the European Commission, she worked as a political advisor at the EU Delegation to the Philippines, and as a human rights fellow at the European Parliament. Prior to her work for EU institutions, she practised law as a Barrister in Greece in criminal law and anti-discrimination cases.

Laurent Bernat is a Cyber Security Risk Policy Analyst at the OECD in the Department of Technology and Industry. He is in charge of technology issues and policies that are associated to information security and privacy protection. Before joining the organization in 2003, he was Associate Director of Projetweb, an agency specialising in internet communications strategy particularly in the health sector. He was previously project manager for information and communication to the National Commission on Informatics and Liberties (CNIL), the French data protection authority.

Olivier Burgersdijk is Head of Strategy within the European Cybercrime Centre with responsibility for strategic analysis, prevention, outreach, communication, expertise, R&D, specialised forensic tools & techniques. Previously he was active within Europol in different functions with responsibilities for information exchange with non-EU States; product management of all operational information management products and services; management of the implementation of EU policies related to information management, including the Swedish Initiative, Prüm Helpdesk and the Principle of Availability; supervision of the Europol-led action points under the EU Council Working Party on Information Exchange and Data Protection (DAPIX). Before joining Europol, Burgersdijk worked for the serious and organised crime department of the Rotterdam-Rijnmond police force (1998-2001) and supported, as consultant, various regional police forces and prosecution services in the Netherlands (2001-2006).

Abdulkarim Chukkol is the Head of the Advance Fee Fraud Section of the Economic and Financial Crimes Commission (EFCC), Nigeria. He is a Certified Fraud Examiner with ten years of experience in investigating frauds ranging from mass marketing fraud to cybercrime. He is a proactive anti-fraud professional with a successful record of managing and prioritising complex investigation cases both locally and internationally.

Jose Clastornik is the first and current Executive Director of the Presidential Agency for e-Government and Information Society, the organisation that has the role both of articulating the country's digital policy, and of leading e-Government strategies and key projects. Clastornik is a member of various governing bodies at the domestic and international level, such as the executive boards of the regulatory units for personal data protection, for access to public information and for electronic certification, the commission on policies of Plan Ceibal (one laptop per child), the Public Procurement Agency, the steering committee of the international conference of Data Protection and Privacy commissioners and ICANN's Governmental Advisory Committee. He is also the President of the coordinating Bureau of the Digital Agenda for LATAM. Clastornik also has extensive experience working in the private sector. He was CEO of HG, the IT enterprise of the government's Telco company. He has held executive positions in multinationals such as America Negocios and IBM.

Nick Coleman is Global Head Cyber Security Intelligence Services at IBM. Prior to this time in IBM he was The UK Government Reviewer and authored the 'Coleman Report' published by the Cabinet Office. He is a Fellow of the Institution of Engineering and Technology (IET) and a Fellow of the British Computer Society (BCS). He chairs the Cyber for Business Initiative enabling current and future business leaders with cyber skills. He was the Founding CEO of the Institute of Information Security Professionals. He serves on the Advisory Board of the EU Security Agency (ENISA). He holds an MBA with Distinction.

Belisario Contreras is the Cyber Security Program Manager at the Secretariat of the Inter-American Committee against Terrorism (CICTE) of the Organization of American States (OAS). As Program Manger he provides programmatic and management support to the CICTE Secretariat in the planning, organisation and execution of cybersecurity initiatives in the Americas including the Creation and Development of Computer Emergency Response Teams (CERTs); provision of technical training; implementation of crisis management exercises; capacity building on Industrial Control Systems (ICS), and coordinating outreach and collaboration with other international and regional organizations working on cyber issues. Contreras is a Colombian citizen, and prior to joining the CICTE Secretariat worked at the Young American Business Trust (YABT). He was also a fellow of the Department of National Planning of Colombia in 2011.

Sadie Creese is Professor of Cybersecurity in the Department of Computer Science at the University of Oxford. She is Director of Oxford’s Cyber Security Centre, Director of the Global Centre for Cyber Security Capacity Building at the Oxford Martin School, and a co-Director of the Institute for the Future of Computing at the Oxford Martin School. Her research experience spans time spent in academia, industry and government. She is engaged in a broad portfolio of cybersecurity research spanning situational awareness, visual analytics, risk propagation and communication, threat modelling and detection, network defence, dependability and resilience, and formal analysis. Prior to joining Oxford in October 2011 Creese was Professor and Director of e-Security at the University of Warwick’s International Digital Laboratory. Creese joined Warwick in 2007 from QinetiQ where she most recently served as Director of Strategic Programmes for QinetiQ’s Trusted Information Management Division.

Joash Dache is Secretary/Chief Executive Officer of the Kenya Law Reform Commission. He is a CPS (K) and an advocate of the High Court of Kenya, Commissioner for Oaths and a Notary Public. He was educated at the University of Nairobi, University of London and Monash University. Dache has substantial experience in constitutional and law reform, legal and policy research, legislative drafting, programme coordination and general administration which comprise the core of his duties at the Kenya Law Reform Commission. He has participated in the constitutional review, reform and implementation process and formulation and preparation of several pieces of legislation and policy documents. These include legislation and policies which anchored the National Accord and Agenda Four [4] Commissions and those required for the operationalisation of the new constitution including those relating to judicial, electoral, institutional, policy and legal reforms, constitutional commissions and devolution.

Thomas Dukes is Deputy Coordinator for Cyber Issues at the U.S. Department of State where he focuses on cybercrime, cybersecurity, and capacity building issues, as well as overall management of personnel, budget and strategic planning. He chairs the G8 Roma-Lyon Group's High-Tech Crime Subgroup, and also serves as a cyber operations lawyer in the US Air Force reserve. Prior to joining the State Department in 2011, Dukes was a senior prosecutor in the Computer Crime and Intellectual Property Section at the US Department of Justice (2005-2011), a national security lawyer with the US Department of Homeland Security's Office of the General Counsel (2004), and an active duty Air Force JAG officer at military bases in the U.S. and UK (1994-2004).

Jayantha Fernando is an internet law and policy expert who has pioneered and given leadership to the ICT legal policy reform as well as internet governance processes in Sri Lanka for over 15 years. Presently, he is leading efforts to formulate a Data Protection framework. In drafting legislation he was instrumental in ensuring that Sri Lanka conformed to international best practices, such as the Budapest Cyber Crime Convention, UNCITRAL Model Laws and the UN Electronic Communications convention. He also did a USAID assignment drafting an e-Commerce Model Law for South African SADC Secretariat. He co-chairs the Task Force with Central Bank to establish a National Certification Authority in Sri Lanka. Fernando is Director and Legal Advisor at the ICT Agency of Sri Lanka and is part of its three-member leadership team, responsible for the '*e-Sri Lanka Development Project*', the flagship ICT4D initiative supported by the World Bank. He has served in numerous capacities within ICANN, including Vice Chair of ICANN GAC (2008-10) and Associate Chair of ICANN Nominating Committee (2005).

Juliana García Vargas is Director of Public Security and Infrastructure of the Colombian Ministry of Defence. She has worked with various organisations, including the National Planning Department, the Andean Development Corporation and the German Agency for Development Cooperation. As the Director of Justice, Security and Government at the National Planning Department, she led the development of Policy Guidelines for Cyber Security and Cyber Defense. Since 2013, she is the head of the ColCERT, the Colombian Computer Emergency Response Team.

Kah-Kin Ho has been with Cisco for 18 years and in his current role as the Head of Strategic Security in Cisco's Corporate Technology Group, he is responsible for identifying disruptive security technology and business models that would help address key customer security challenges, thereby steering and shaping Cisco's strategic investment in the security area. In his previous role as the Head of Cyber Security Business Development he provided thought leadership to private and public sector organizations on how to respond to cyber risk and threat. He graduated from the State University of New York at Buffalo with bachelor's and master's degrees in Electrical Engineering, and he also has a master's degree in Security Policy and Crisis Management from ETH Zürich.

Zahid Jamil is a Senior Partner with the family law firm. He serves as an expert to the Council of Europe Convention on Cybercrime and has provided in-country assistance to developing country legislation on cybercrime on their behalf. In conjunction with the US Department of Justice, he has been conducting regular trainings on cybercrime and terrorism prosecution for prosecutors in Pakistan. As a consultant and expert of the Council of Europe Convention on Cybercrime, he is providing support and advice to country's IT Association and the Parliamentary Select Committee on Cybercrime (PECO) and drafting the Cybercrime Bill. He serves as a member and rapporteur of the Commonwealth's Cybercrime Experts Working Group. He assisted the Commonwealth IGF develop and obtain Commonwealth Heads of Government approval for the Commonwealth Cybercrime Initiative to the 2011 proposal and then briefly served as legal advisor to the Board of the Commonwealth's Cybercrime Initiative. He serves on the Multistakeholder Advisory Group to the UN Secretary General on Internet Governance.

Serge Kapto is Policy Specialist for E-governance and Access to Information in the Democratic Governance Group of the United Nations Development Programme (UNDP) at its headquarters in New York. A citizen of Cameroon, Serge joined UNDP in 1999 to work for the Sustainable Development Networking Programme, a pioneering initiative that played a major role in introducing the internet to many developing countries. Serge then went on to UNDESA where he remained involved in ICT for Development issues at the United Nations ICT Task Force and the Global Alliance for ICT and Development. Prior to returning to UNDP, Serge worked on ICT for Development and e-governance at the Global Centre for ICT in Parliament in Rome. Serge also covers Governance and Post-2015, as part of the UNDP team in charge of managing the United Nations global consultations on the Post-2015 Development Agenda.

Jens Karberg is an advisor and programme manager on ICT for development for the Swedish International Development Cooperation Agency (Sida). He is responsible for developing and coordinating the overall work in the area of ICT for development, but also programming of major global initiatives. Karberg has over 15 years of experience in the field of international development from the Swedish government agency Sida, Swedish embassies and international NGOs.

Neil Klopfenstein is the Executive Secretary for the Inter-American Committee against Terrorism (CICTE). A career member of the US Senior Foreign Service, Klopfenstein is currently seconded by the State Department to the international staff of the Organization of American States. In his 25 year career, Klopfenstein has served as the Deputy Chief of Mission at the US Embassy in Iceland, as well as in assignments to US missions in Oslo, Sao Paulo, Recife and Bangkok. In Washington, Klopfenstein served in the State Department Bureau of Public Affairs as Director of the Washington and New York Foreign Press Centres. He has also held positions in the State Department's Bureaus of Western Hemisphere Affairs and International Information Programs.

Adriane Lapointe is a senior policy advisor in the State Department Office of the Cyber Coordinator, where she works on issues including cybersecurity, internet governance, and cyber capacity building as a detailee from the National Security Agency. Before joining the State Department, she represented the White House on the US Delegation to the World Conference on International Telecommunications (WCIT). Her most recent NSA assignments have included 2 years as the Chief of Policy, Oversight, and Compliance in the NSA/CSS Threat Operations Center (NTOC), and 2 years as Special Assistant for Cyber to the NSA Director of Foreign Affairs. Lapointe started at NSA in 1998 as a cryptanalysis intern, and subsequent agency assignments included 3 years in NSA Policy, where she was the lead for information sharing, governance, and technology policy, and work in the SIGINT Forensics Lab, on the Chief Financial Manager's staff, and on the staff of the Director of the National Security Agency. Lapointe received her Ph.D from the University of Chicago.

James Andrew Lewis is a Senior Fellow and Director of the Strategic Technologies Program at the Center for Strategic and International Studies (CSIS). Before joining CSIS, he worked at the Departments of State and Commerce as a Foreign Service Officer and as a member of the Senior Executive Service. Lewis was the Rapporteur for the UN's Group of Government Experts on Information Security and leads a Track II dialogue on cybersecurity with China. He has authored numerous publications and is an internationally recognized expert on cybersecurity. Lewis received his Ph.D. from the University of Chicago.

Preetam Maloor is a Strategy and Policy Advisor in the Corporate Strategy Division of the ITU General Secretariat and an expert on international internet-related public policy matters. He holds several Masters degrees in Computer Science from Texas A&M University, College Station, and in Engineering and Public Policy from the University of Maryland, College Park. He has a Bachelor degree in Computer Science and Engineering from the University of Mumbai.

Matias Bertino Matondo is an Advisor with the Intelligence and Security Committee, Office of the Chairperson of the African Union Commission. He is responsible for the research and analysis of threats (social, economic, military, transnational organised crime, Cybercrime, illegal migration, terrorism etc.) to peace and security, stability and development of the African continent. A career diplomat, he has served in various roles in several Angolan embassies including in Tanzania, United States of America, South Africa and Spain. Matondo received a Masters in Political Science from the US Military University and a Bachelor of Science in Business administration from Strayer University, Virginia. He

also studied Law at the Agostinho Neto University, Luanda, Angola, and for a Diploma in Economic Planning in Cuba. He is currently completing a Ph.D degree in Public Administration and Law.

Samia Melhem is the chair of the e-Development Community of Practice, and leads the ICT unit's Transformation practice as well as its Knowledge, Learning and Partnership functions. Her current operational advisory responsibilities include technical assistance and advisory services related to using technology for transformation, growth and development in client countries. In her 20 years of experience in development at the World Bank Group, Melhem has worked on ICT4D in several sectors: telecoms policy ICT for public sector reform (taxes, customs, trade), education, innovation, knowledge economy and private sector development. Melhem held several positions as regional coordinator in different regions such as Africa, the Middle East and Europe and Central Asia and has experience in more than 40 countries, having managed a multitude of lending operations and analytical projects. She has authored working papers, case studies and policy notes focusing on ICTs for governance, public sector reform, governance, accountability and inclusion.

Raul Millan is an IT professional with more than 12 years of experience in the field of Information Security. His knowledge areas include penetration testing, vulnerability analysis, remediation, and risk management. He currently serves as Head of Panama's National Incident Response Team (CSIRT PANAMA) and coordinator for the Government Cloud Computing initiative. In the past he also served as Manager for Information Security Cable & Wireless Panama, implementing major projects and establishing the first Security Operations Centre within an ISP in the country. He also holds the following certifications that accredit him as an expert in the field of information security: CISSP (Certified Information Systems Security Professional), CISM (Certified Information Security Manager), CISA (Certified Information Systems Auditor) and CEH (Certified Ethical Hacker).

Mariko Miya is the Chief Security Analyst of Cyber Defense Institute, Inc. and has expertise in and knowledge of foreign and domestic cyber policies and handling cyber threats regarding national security, ranging from security concerns in the private sector to defence and critical infrastructures. She focuses on the strategic/political side of cyber rather than the technical/operational side, giving practical support to sectors of the government in charge of foreign affairs and overseas information gathering and analysis.

Timothy Noonan is Director of Campaigns and Communications at the International Trade Union Confederation, the global organisation representing 176 million workers from 325 affiliated organisations in 161 countries. He is responsible for the ITUC's media and social media work, and the integration of this with global trade union campaign work. He also leads the ITUC's work on internet and broadband issues. In 26 years working for the ITUC and its predecessor the ICFTU, he has worked on a wide range of issues across all the continents, and led the international trade union movement's campaign against child labour during the 1990s and the early part of this century. He was closely involved in the development of International Labour Organisation Conventions 169 (Indigenous Peoples) and 182 (Worst Forms of Child Labour).

Derek O'Halloran is responsible for content development with the World Economic Forum's IT Industry Partnerships community. In this role, he leads the Forum's projects which aim to advance our understanding of the transformative impact of technology on multiple socio-economic domains as well as the emergent systemic risks in our increasingly networked and connected world. Prior to working with the Forum, Derek worked within the industry in a number of roles across the Far East, the United States and Europe, serving both private- and public-sector clients. Derek holds an MPA in International Finance and Economic Policy from Columbia University. He is currently a Global Leadership Fellow at the Forum.

Chanki Park has worked for the Korea Internet and Security Agency (KISA) in various roles for the past 15 years. He is currently involved in the Global Project Division where he works on overseas projects providing training and education in internet security. Previous to this he managed policies and systems on domain names and IP addresses. He designed a registration system for domain names and IP addresses and was the IETF RFC author on ENUM-based Softswitch Requirement. He also led the personal information protection team where he managed systems for finding Korean residence ID on the internet and also on personal information-related policy.

Patryk Pawlak is a Senior Analyst at the European Union Institute for Security Studies (EUISS) in Paris. At the EUISS, he deals with internal security policies of the EU, with a focus on border protection, counterterrorism and cybersecurity issues. He currently leads the EUISS Cyber Task Force focusing on capacity building and cybersecurity. During his career, Patryk has undertaken extensive research on data protection, the use of personal information for security purposes and smart borders. Before joining the EUISS, he worked with numerous research institutions, including the Center for Transatlantic Relations at Johns Hopkins University, the Center for Peace and Security Studies at Georgetown University and the Centre for European Policy Studies in Brussels. Since September 2006, he has also been a fellow in the European Foreign Policy Studies Programme, founded jointly by Compagnia di San Paolo, Volkswagen Stiftung and Riksbankens Jubileumsfond. Pawlak holds a PhD in Political Science from the European University Institute in Florence.

David Pollington is Microsoft's Director of International Security Relations. He is responsible for major national and international security relationships on behalf of Microsoft's Trustworthy Computing Security group. Pollington is a co-founder of Microsoft's Global Security Strategy and Diplomacy team who engage on matters of Cyber Security around the world. After 20 years in IT with experience in areas as diverse as oil exploration, cartography, flight testing, building a consultancy practice and outsourcing; Pollington joined Microsoft in 2002 with a focus on Microsoft's evolving commitment to IT security in UK Government relationships. In the course of his work, Pollington has participated in cybersecurity policy engagements in major Commonwealth countries and many pan-national institutions including: CTO, EU, ENISA, IGF, ITU, OECD and WEF. He is concerned with Critical Infrastructure Protection, representing Microsoft in several contexts and for 2 years, he was Chair of the Vendor Security Information Exchange, part of the UK's Centre for the Protection of the National Infrastructure. He is a member of the CTO Cyber Security Advisory Group and an affiliate of the cybersecurity faculty of the Oxford Martin School.

Maria Grazia Porcedda is Research Assistant at the European University Institute (EUI), where she works for the FP7 project SurPRISE, on Surveillance, Privacy and Security. She previously worked at the Centre de Recherche Informatique et Droit (CRID) on privacy and cloud computing in law enforcement matters, and as a trainee on privacy issues at both the Organization for Economic Cooperation and Development (OECD) and the European Data Protection Supervisor (EDPS). She received an LL.M. in Comparative European and International Law from the EUI.

Steve Purser is the Head of Core Operations Department at ENISA. From 1993 to 2008, he occupied the role of Information Security Manager for a number of companies in the financial sector. He joined ENISA in December 2008 as Head of the Technical Department and is currently responsible for all operational activities of ENISA. Steve is co-founder of the 'Club de Securité des Systèmes Informatiques au Luxembourg' (CLUSSIL) and is currently the ENISA representative on the ISO SC 27 working group. He frequently publishes articles in the specialised press and is the author of 'A Practical Guide to Managing Information Security' (Artech House, 2004). He obtained his Ph.D in Chemical Physics from the University of East Anglia.

Taylor Roberts has an academic and professional background in international politics and cybersecurity policy, particularly regarding China and cybersecurity. Presently, he is focusing on researching and developing maturity metrics for measuring cyber policy and cyber defence at the Global Cyber Security Capacity Centre at the University of Oxford.

Neil Robinson is a Research Leader at RAND Europe based in the Brussels office. He has been responsible for a variety of projects in the cyber defence and cybersecurity domain for European clients. He is currently leading a two-year framework project for the European Defence Agency (EDA) which includes developing an Enterprise Architecture for Cyber Defence for EU-led CSDP operations and a Training Needs Analysis for Cyber Defence in the military. In 2012 Robinson worked on a first study for the EDA into cyber defence which analysed the maturity of military cyber defence capabilities in the EU. In the area of law enforcement and criminal justice cooperation in Europe, Robinson led the 2011 Feasibility Study for a European Cybercrime Centre for DG Home which helped inform the decision to establish the EC3 at Europol. Robinson has also worked on a variety of studies for the European Union Agency for Network and Information Security (including those concerning co-operation between Computer Emergency Response Teams) and has also led a study for DG Information Society into the Privacy, Security and Trust aspects of Cloud Computing in 2010.

Alexander Seger has been with the Council of Europe (Strasbourg, France) since 1999. He is currently the Secretary of the Cybercrime Convention Committee and Head of the Data Protection and Cybercrime Division. Prior to that he headed for many years the Economic Crime Division where he was responsible for the Council of Europe's cooperation programmes against cybercrime, corruption and money laundering. From 1989 to 1998 he was with what is now the United Nations Office on Drugs and Crime 6 in Vienna (Austria), Laos and Pakistan and a consultant for German Technical Cooperation (GTZ) in drug control matters. Seger holds a Ph.D in political science, law and social anthropology after studies in Heidelberg, Bordeaux and Bonn.

Bawani Selvaratnam is Head of Policy Department Division at the Malaysian Communications and Multimedia Commission. She is a lawyer by training and was in legal practice for nine years prior to joining the Malaysian Communications and Multimedia Commission. She has been with MCMC for 12 years. She is currently the head of the Policy Development Division, which plays a leading role in the planning, formulation and review of regulatory policies to ensure that the Commission executes its functions effectively and to promote the continued growth and evolution of the communications and multimedia industry.

Anita Sohan is an International Affairs Officer at the Ministry of National Security with responsibility for issues relating to public security. Her portfolio also includes the coordination of the Ministry's relationships with regional and international organisations. Sohan was a member of the Cabinet-appointed Inter-Ministerial Committee that developed the National Cyber-Security Strategy, which was approved by the Trinidad and Tobago Government in December 2012. She has also been directly engaged in the coordination of several cybersecurity activities that involved the implementation of the Strategy, including capacity building and cooperation with international organisations like the Organization of American States, the International Telecommunication Union and the Commonwealth Secretariat.

Ilyse Stempler is a consultant for USAID's Office of Policy in the Bureau for Policy, Planning & Learning where she works on USAID's cyber/ICT portfolio, ending extreme poverty agenda, and preparation for the post-2015 sustainable development goals. Prior to joining USAID, Stempler worked as a legal consultant for the World Food Programme and helped implement cash and voucher programs using mobile technologies. For five years, Stempler was an associate lawyer at King & Spalding LLP in Washington, DC on the Special Matters and Government Investigations team.

Heli Tiirmaa-Klaar advises the European External Action Service in Cyber Security Policy and coordinates EU external cyber relations. Prior to this position, she was seconded as a Cyber Security Policy Advisor to NATO where she helped to develop the new NATO Cyber Defence Policy and its Action Plan. She has been working on cybersecurity issues since 2007 when she led an interdepartmental working group to develop the national Cyber Security Strategy after Estonian cyberattacks. In 2008-2010 she coordinated the implementation of Estonia's Cyber Security Strategy and managed the National Cyber Security Council. She oversaw the development of Estonia's Critical Information Infrastructure Protection system and facilitated public-private partnerships at national level. She also worked closely with European Union institutions for the launch of the EU Critical Information Infrastructure Protection policy, as well as with other international organisations. She has served at various managerial positions at the Estonian Ministry of Defence between 1995 and 2005, including the Head of Security Policy Analysis Division, Head of NATO and International Organisations Department.

Paul Twomey is the CEO of Argo Pacific, an international internet and cybersecurity advisory and incubator firm. Much of Twomey's work focuses on cybersecurity for Fortune 1000 companies and public sector agencies. After four years as Chair of its Governmental Advisory Committee, Twomey served from 2003 to 2009 as President and CEO of ICANN, the international non-profit organisation that coordinates many of the key functions of the global internet. He served as Senior President until January 2010. Prior to ICANN, Twomey was founding Chief Executive Officer of the Australian National Office for the Information Economy (NOIE), and the Australian federal government's Special Adviser for the Information Economy and Technology. Twomey was formerly a senior consultant with McKinsey & Company. Twomey is a Commissioner of the recently established Global Commission on Internet Governance. He is a Board member of the Atlantic Council of the United States, and the Board lead of its Cyber-statecraft initiative.

Barbara-Chiara Ubaldi leads the OECD E-Government Project within the Division for Public Sector Reform at the Public Governance and Territorial Development Directorate since February 2009. In this capacity, she managed a number of thematic reviews on e-government and participated in several Public Governance Reviews, which include Denmark, Greece, Mexico, Italy, Estonia, Egypt, Spain and France. Ubaldi has been co-ordinating for the past five years the OECD work on e-government indicators and the analysis on the use of new technologies – e.g. cloud computing, mobile technology – to enhance the public sector's agility and mobility, as well as open government data and social media use in governments. Prior to joining the OECD she worked for more than seven years as Programme Officer at the United Nations' Department of Economic and Social Affairs in New York where she was responsible for the full scale management of technical cooperation programmes targeting e-government and ICT use in the public sector, and for developing the content of online self-assessment and capacity building tools in the area of e-government and knowledge management.

List of Participants

AMOROSO DAS NEVES, Ana Cristina, Department of Information Society, Foundation for Science and Technology (FCT) , Lisbon

ANANICZ, Katarzyna, Digital Affairs Analyst, Ministry of Foreign Affairs of Poland, Warsaw

BADA, Maria, Research Fellow, Global Cyber Security Capacity Centre, Oxford University, Oxford

BARMPALIOU, Panagiota-Nayia, Programme Manager, European Commission, DG Development and Cooperation – EuropeAid, Brussels

BENEDITTINI, Michel, Research Fellow in cyber defence, Foundation for Strategic Research (FRS), Paris

BERGER, Cathleen, Desk Officer, International Cyber Policy Coordination Staff, German Federal Foreign Office, Berlin

BERNAT, Laurent, Cyber Security Risk Policy Analyst, Directorate for Science, Technology and Industry, Organisation for Economic Co-operation and Development (OECD), Paris

BURGERSDIJK, Olivier, Head of Strategy, European Cybercrime Center (EC3), The Hague

CARTHY, Joe, Director, Centre for Cybersecurity & Cybercrime Investigation, College Principal and Dean of Science, University College Dublin (UCD), Dublin

CHAUHAN, Neil, Head of Cyber Capacity Building Programmes, Foreign and Commonwealth Office, London

CHUKKOL, Abdul Karim H., Deputy Chief Director, Economic and Financial Crime Commission, Lagos

CLASTORNIK, Jose, Executive Director, Agency for e-Government and Information Society (AGESIC), Montevideo

COLEMAN, Nick, Global Head Cyber Intelligence, IBM Services, London

CONTRERAS, Belisario, Cyber Security Program Manager, Organization of American States, Washington, D.C.

CREESE, Sadie, Director, Global Cyber Security Capacity Building Centre, Oxford University, Oxford

DACHE, Joash, Secretary - CEO, Kenya Law Reform Commission, Nairobi

D'ACHON, Emmanuelle, Deputy Secretary General and Cyber Affairs Coordinator, Ministry of Foreign Affairs of France, Paris

DE MERCEY, Laurent, Special adviser for digital economy, Assistance Technique France (ADETEF), Paris

DOTZAUER, Erwin, Senior Research Fellow, Global Cyber Security Capacity Centre, Oxford University, Oxford

DUCASS, Alain, Director of Digital Economy Department, Assistance Technique France (ADETEF), Paris

DUKES, Thomas, Deputy Coordinator for Cyber Issues, U.S. Department of State, Washington, D.C.

DUMITRU, Marius, Key expert, Enhancing cybersecurity project, Assistance Technique France (ADETEF), Bucharest

ENGIDA, Getachew, Deputy Director-General, United Nations Educational, Scientific and Cultural Organisation (UNESCO), Paris

ESPINOSA, Rowland, Deputy Minister of Telecommunication, Ministry of Science, Technology and Telecommunications of Costa Rica, San Jose

FERNANDO, Jayantha, Programme Director, Information and Communication Technology Agency, Colombo

FRENCH, Eleanor, Strategic Communications and Programme Manager, Foreign and Commonwealth Office, London

GACUKO, Leonard, Director, National Legislation Services, Ministry of Justice of Burundi, Bujumbura

GARCIA, Juliana, Director for Public Security and Critical Infrastructure, Ministry of National Defence of Colombia, Bogota

GASPERS, Jan, Associate Analyst, RAND Europe, Cambridge

GRANGER, Jackie, Brussels Liaison Officer, EU Institute for Security Studies, Brussels

GUANES, Claudia, General Cabinet Director, National ICT Secretariat Paraguay (SENATICs), Asuncion

HEWITT, **Adrian,** Senior Research Associate, Overseas Development Institute, London

HO, Kah-kin, Strategic Security Manager, CISCO, Geneva

JAMIL, Zahid, Director, Center for Strategic and Policy Analysis, Center for Strategic and Policy Analysis, Islamabad

JENNY, Joëlle, Director, Security Policy and Conflict Prevention, European External Action Service, Brussels

KABUA, Irene, Legislative Expert, Kenya Law Reform Commission, Nairobi

KAHN, Jüri, Coordinator for the International Cooperation on e-Governance, Ministry of Foreign Affairs of Estonia, Tallin

KAPTO, Serge, Policy Specialist, E-governance and Access to Information, United Nations Development Programme, New York

KARBERG, Jens, Advisor and Programme Manager ICT for Development, Swedish International Development Cooperation Agency (SIDA), Stockholm

KLOPFENSTEIN, Neil, Executive Secretary, Organisation of American States, Washington, D.C.

KUKAJ, Agim, Head of ICT Department, Ministry of Economic Development of Kosovo, Pristina

KVOCHKO, **Elena**, Manager, IT and Telecommunications Industries, World Economic Forum, New York

LAPOINTE, Adriane, Senior Policy Advisor, Office of the Coordinator for Cyber Issues, US Department of State, Washington, D.C.

LE CLEÏ, Alicia, International Affairs, French Network and Information Security Agency (ANSSI), Paris

LE ROUX, Yvon, Vice President of Cyber Security, CISCO, Paris

LEWIS, James, Director and Senior Fellow, Strategic Technologies Programme, Center for Strategic and International Studies, Washington, D.C.

LIMAJ, Besnik, Team Leader, EU Cyber Security Transregional Project, Assistance Technique France (ADETEF), Paris

LOURENCO, **Mirta,** Chief, Media Development and Society Section, Freedom of Expression and Media Development Sector, Scientific and Cultural Organisation (UNESCO), Paris

MALOOR, Preetam, Strategy and Policy Advisor, International Policy, International Telecommunication Union, Geneva

MATONDO, **Bertino Matias,** Advisor, Office of Chairperson, African Union Commission, Addis Ababa

MELHEM, Samia, Lead ICT Specialist, World Bank, Washington, D.C.

MILLÁN, Raúl, Director, Computer Security Incident Response Team (CSIRT-Panama), National Authority for Government Innovation, Panama City

MISSIROLI, Antonio, Director, EU Institute for Security Studies, Paris

MIYA, Mariko, Security Analyst, Cyber Defense Institute, Tokyo

MKIZUNGO, Josephat, Senior State Attorney, National Prosecutions Service, Dar es Salaam

NAEL, Olivier, Head of Technical Support Unit, Computer Forensics Lab and Cybercrime Training, National Cybercrime Unit (OCLCTIC), French Ministry of Interior, Paris

NEUTZE, Jan, Director of Cybersecurity Policy, Europe/Middle East/Africa (EMEA), Microsoft, Brussels

NOONAN, Timothy, Director, International Trade Union Confederation, Brussels

O'HALLORAN, Derek, Head of IT Industry, World Economic Forum, New York

OMAR, Mohammed, Principal State Attorney, Ministry of Justice and Constitutional Affairs of Uganda, Kampala

PALIN, **Alexander**, First Secretary, Embassy of Australia to France, Paris

PALLASZ, Urszula, Senior Policy Advisor, Strategic Planning Division, European External Action Service, Brussels

PALMER, Michael, Policy Officer, European Commission, DG Home Affairs, Brussels

PARK, Chanki, Manager, Global Project Division, Korea Internet and Security Agency (KISA), Seoul

PAWLAK, Patryk, Senior Analyst, EU Institute for Security Studies, Paris

PHELAN, Caroline, Deputy Director for International Security Policy, Department of Foreign Affairs and Trade, Dublin

POLLINGTON, David, Director, International Security Relations, Microsoft, London

PORCEDDA, Maria Grazia, Researcher, Surveillance, Privacy and Security Project, European University Institute, Florence

PURSER, Steve, Head of Core Operations Department, ENISA, Heraklion

REGIEN, Ingrid, Chief Information Officer, Scientific and Cultural Organisation (UNESCO), Paris

ROBERTS, Taylor, Research Fellow, Global Cyber Security Capacity Centre, Oxford University, Oxford

ROBINSON, Neil, Research Leader, RAND Europe, Brussels

ROLLAND, Léonard, Desk officer for cybersecurity international policy, Ministry of Foreign Affairs of France, Paris

SEGER, Alexander, Executive Secretary, Cybercrime Convention Committee, Council of Europe, Strasbourg

SELVARATNAM, Bawani, Director, Malaysian Communications and Multi-media Commission, Kuala Lumpur

SOHAN, Anita, International Affairs Officer, Ministry of National Security, Port of Spain

STOLIKOVSKI, Marjan, Head of Cyber Crime Unit, Ministry of Interior, Skopje

STEMPLER, **Ilyse**, Senior Policy Advisor, Bureau for Policy, Planning, and Learning, United States Agency for International Development (USAID), Washington, D.C.

TIIRMAA-KLAAR, Heli, Head, Cyber Policy Coordination, European External Action Service, Brussels

TWOMEY, Paul, Founder, CEO, Argo Pacific, Sydney

UBALDI, Barbara, E-Government Project Manager, Organisation for Economic Co-operation and Development (OECD), Paris

VISHIK, Claire, Trust and Security Technology and Policy Manager, Intel Corporation, London