POLICY SUMMIT
"MAKING THE INTERNET SAFER FOR DEMOCRACIES"
AGENDA PACK

Wednesday 29th November, 13:00 – 21:30 h
Google Safety Engineering Center (GSEC), Málaga (P.º de la Farola 6, 29016 Málaga)

AGENDA

REGISTRATION AND LUNCH	
13:00 14:00	Light cocktail at the ground floor of the GSEC building.
OPENING SESSION, Auditorium	
14:00 15:00	**Welcome words by** Giorgia Abeltino, Director of Public Policy and South Europe, Google Italy, José Ignacio Torreblanca, Head of Office and Senior Policy Fellow, ECFR, and María Teresa Arcos, Director General, ESYS. **Fireside chat** with Annette Kroeber-Riel, VP GAPP Europe, and two startup founders, Yosra Jarraya, Co-Founder & CEO of Astran, and Joaquín Fernández, Co-Founder & COO of Build38, chaired by Arturo Varvelli, Head of Rome Office and Senior Policy Fellow, ECFR. **Scene-setter for policy summit and workshops** by Carla Hobbs, Deputy Director, European Power Programme, ECFR.
POLICY SESSIONS	
15:00 16:30	**A.-** "Navigating Cybersecurity and Safety Challenges for States, Businesses, and Citizens", moderated by Vicente Moret, Secretary General, ESYS. **B.-** "Economic and Social Opportunities in the Era of Artificial Intelligence", moderated by José Ignacio Torreblanca, ECFR and María Teresa Arcos, ESYS. **C.-** "The Digital Front Line: Hybrid Threats amid Geopolitical Tensions", moderated by Alejandro Romero, Constella Intelligence.
COFFEE BREAK, Auditorium	
16:30 17:00	Coffee and networking break.
INSTITUTIONAL CEREMONY, GSEC Rooftop	
17:00 17:30	Institutional ceremony of GSEC Málaga with José Luis Escrivá, Spanish Minister of Digital Transformation, and Francisco de la Torre, Major of Malaga
POLICY SESSION | WRAP-UP, Auditorium	
17:30 18:00	Presentation of key ideas by rapporteurs from the break-out sessions followed by Q&A. Moderated by Raquel Jorge, Research Director, ESYS and concluded by Carlos López Blanco, Chairman, ESYS.
PLENARY CLOSING SESSION, Auditorium	

18:00 18:30	**Closing fireside chat** between Kent Walker, President of Global Affairs at Google and Alphabet and Julissa Reynoso, US Ambassador to Spain and Andorra - Moderated by Miguel Escassi, Google.
VISIT TO CENTRE POMPIDOU MALAGA	
18:30 19:50	Guided tour of the Centre Pompidou Malaga, adjacent to the GSEC.
DINNER	
20:00 21:30	Networking cocktail dinner at Málaga City Hall, Hall of Mirrors. Closing words by the organisers and Francisco de la Torre, Major of Malaga.
END OF POLICY SUMMIT	

POLICY SESSIONS

Following the policy summit's opening session at the Auditorium taking place between 14:00 and 15:00, participants will be invited to join one of **three policy sessions** that will run in parallel to one another: (1) Navigating cybersecurity and safety challenges for states, businesses, and citizens; (2) Economic and social opportunities in the era of artificial intelligence; (3) The digital front line: hybrid threats amid geopolitical tensions.

The policy sessions provide an opportunity for participants to engage in frank, no-holds-barred conversations, delving deeper into certain issues and identifying tangible, innovative and actionable **policy recommendations**. To facilitate the open exchange of ideas, discussions will be held under the **Chatham House Rule** of non-attribution. Each policy session will have a moderator who will also act as **rapporteur** for the group during the closing plenary session, reporting back to Carlos López Blanco and the rest of the summit's participants.

All the participants are invited to the policy sessions in speaking capacity. We envisage these sessions as **dynamic exchanges** with all present actively participating and sharing their insights and views. As such, we warmly invite you to **consider the guiding questions** provided on the following pages for your particular policy session in advance. Each policy session brings together purposefully engineered mixed groups comprising approximately 15-17 representatives from governments, cybersecurity agencies, private sector, academia, think tanks, and NGOs.

After the policy sessions, participants will meet back in the **plenary** at 17:00 after a break, where each rapporteur will convey the main results of the debate to the plenary and answer questions by both the participants and the main rapporteur, followed by a **wrapping up session**, to take place between 18:00 and 18:30.

FORMAT

- **Welcome words:** Moderator welcomes all, briefly explains dynamic of policy session, and pitches guiding questions to the group *(5 mins)*
- **Open discussion:** Reactions from the group amid a dynamic exchange of views steered by the moderator *(50 minutes)*
- **Wrap-up:** Group agrees upon the key points and recommendations that they wish the moderator to report on in the plenary session *(5 minutes)*

POLICY SESSION 1

"Navigating Cybersecurity and Safety Challenges for States, Businesses, and Citizens"

Cybersecurity is the greatest challenge for the digital transformation of our societies. While digital disruption is facilitating extraordinary economic, social and environmental development, this paradigm shift must be accompanied by the necessary guarantees for citizens' fundamental rights and public freedoms in the framework of secure societies. We are witnessing a constant increase in cyber-attacks carried out by malicious actors, be they states or criminal organisations, and the cybersecurity threat landscape is becoming increasingly complex to manage for governments, companies and citizens. In this context, governments are implementing policies and measures to protect their citizens and businesses. The difficulty of using the traditional mechanisms of state action (laws and actions of law enforcement agencies as well as other reaction mechanisms to protect national security) should encourage us to seek new courses of action to meet this major challenge.

Efforts are already underway in the EU with the approval of the DORA regulation and the NIS 1 and 2 Directives, and the upcoming adoption of the Cyber Resilience Act and Cyber Solidarity Act. Yet further action is sorely needed. Secondly, there is a need for increased international cooperation in the prosecution of cybercrime, with the Budapest Convention being a key example of how much can be achieved. Additionally, it is necessary to deepen the scope of public-private cooperation given that private companies hold many of the capacities and responsibilities in the field of cybersecurity, especially with regards to critical infrastructures. The ultimate goal is for all stakeholders to reach a proper level of cybersecurity that protects our societies.

Moderator and Rapporteur

Vicente Moret - Secretary General, Fundación ESYS. Of counsel Deloitte Legal.

Guiding questions

We're aiming to identify issues which current policies are missing or not addressing properly, challenges ahead, next policy steps, and how to improve the public-private dimension of international cooperation:

- Which actions should be undertaken by governments and parliaments to improve the security of citizens - and companies - in the digital sphere?

- How should public-private cooperation mechanisms be strengthened to boost cybersecurity in EU member states?

- Bearing in mind that a large part of the cyber incidents faced by companies originate from the IT services supply chain, which measures should be put in place to tackle this issue?

Suggested reading materials

- ENISA Threat Landscape 2023
- Cybersecurity Forecast 2024. Insights for future planning. Google.
- M-Trends 2023: Cybersecurity Insights From the Frontlines. Mandiant
- 2023 Global Future of Cyber Survey. Deloitte
- Internet Organised Crime Assessment (IOCTA)2023. EUROPOL
- Ciberamenazas y tendencias 2023. CCN-CERT

Participants

1. Roberto Baldoni – Professor; Former Director General, Italian National Cybersecurity Agency
2. Federico Casani – Director, EMEA Cybersphere Center, Deloitte
3. Cristina Durante – Cybersecurity Associate, Deloitte Legal
4. Joaquín Fernández – Co-Founder & COO, Build38
5. José Esteban García Ruiz – Head of Analysis Unit, Global Directorate of Intelligence, Research and Technical Support, Telefónica S. A.
6. Alicia Izquierdo – Deputy Major Delegate for Innovation, Digitalization, Promotion and Attraction, Málaga City Hall
7. Yosra Jarraya – Co-Founder& CEO, Astran
8. Rosa Kariger – Global Security Governance, Intelligence and Control, Iberia
9. Rosario Martínez Tornay – Chief Inspector, International Cooperation Division, Spanish National Police
10. María Mora Castilla – Manager of the IT Centre, Málaga City Hall
11. Vicente Moret – Secretary General, Fundación ESYS
12. Eduvigis Ortiz – Founder and President, Women4Cyber Spain
13. Nicolás Pascual de la Parte – Ambassador at Large for Cybersecurity and Hybrid Threats Ministry of Foreign Affairs, European Union, and Cooperation of Spain
14. Alberto Redondo – Head of Cybercrime Intelligence Area, Judicial Police
15. Carla Redondo – Secretary General, INCIBE
16. Margarita Robles Carillo – Professor of International Public and EU Law, University of Granada
17. Matthias Sachs – Cybersecurity Policy Lead Europe, Google
18. Víctor Solla – Director of Urban Transformation and Digitalization, Malaga City Hall

POLICY SESSION 2

"Economic and Social Opportunities in the Era of Artificial Intelligence"

The purpose of this policy session is to explore the opportunities and challenges posed by recent innovations in the realm of Artificial Intelligence (AI). Discussants will address how regulation can support sustainable innovation, particularly in the European, but also at the global context, exploring how countries can harness the benefits of this emerging disruptive technology whilst mitigating against its more harmful effects. This will include examining the potentials of AI to boost the EU's economic competitiveness, contribute to the effective government provision of public services, the re-industrialisation of global economies, and the environment sustainability agenda while mitigating risks such as data bias, algorithmic discrimination, and potential dual-use applications, among others. The important role of ethics, safety, privacy protection, education, and public investment will also be explored. Finally, multilateral cooperation in this increasingly geopoliticised domain will be highlighted and policy efforts spearheaded by the G-7, UNESCO, the OECD and through the UN Global Digital Compact unpacked.

Moderator and Rapporteur

- José Ignacio Torreblanca - Head of the Madrid Office and Senior Policy Fellow, ECFR
- María Teresa Arcos - Director General, Fundación ESYS

Guiding questions

With the help of the three guiding questions below we seek to identify the issues that current AI policies and developments are missing or not addressing properly. The conclusions should examine the challenges ahead and propose next policy steps, always with a view on how to improve public-private and international cooperation:

- The EU AI Act is in its final negotiation stage. What do you make of its capacity to promote innovation while at the same time ensuring the maximum level of safety and rights? What are we missing in this process? What will be the implementation challenges across EU member states?

- In parallel to the EU AI Act, President Biden has enacted an Executive Order on AI. The OECD, UNESCO, the G-7, Latin American countries, the UN, and other governments, have also issued AI principles and guidelines. How compatible are these exercises? Do they signal a convergence process ending in, if not a single regulatory framework, at least compatible ones? Instead, do they spell a fragmented patchwork of regulations generating confusion and legal uncertainty?

- How are companies and start-ups that develop AI Systems responding to this collection of regulations and internationally agreed guiding principles and codes of conduct (such as sharing testing and safety-related critical information with governments, developing standards and tools to protect users and consumers)? What kind of difficulties are they experiencing and what are the lessons learned?
- Digital inequalities are growing, both between and within countries. Yet, digitalisation is a key element of the 2030 Agenda and therefore an essential

instrument for economies in transition. It is also key to make sure that AI is developed in a sustainable way. How can these AI governance processes help close rather than widen the digital divide and make sure that the benefits of AI reach everybody?

Suggested reading materials

- EU AI Act EP Briefing on the AI ACT
- OECD Recommendation if the Council on Artificial Intelligence
- President Biden Executive order on AI
- Hiroshima G7 Leaders statement & International Guiding Principles for Organizations Developing Advanced AI system
- UK AI Safety Summit Conclusions (Bletchey Declaration)
- Final Report on AI by the US National Security Commission
- UNESCO declaration on AI
- Google A shared agenda for responsible AI progress
- Google A policy agenda for responsible AI progress: Opportunity, Responsibility, Security
- Google Our commitment to advancing bold and responsible AI, together
- Microsoft's Governing AI: A Blueprint for the Future
- Google AI principles 20022 Update?
- A shared agenda for responsible AI progress
- A policy agenda for responsible AI progress: Opportunity, Responsibility, Security
- Our commitment to advancing bold and responsible AI, together

Participants

1. Giorgia Abeltino – Director, Public Policy and South Europe, Google Italy
2. María Teresa Arcos – Director General, Fundación ESYS
3. Almudena de la Mata – CEO, Blockchain Intelligence
4. Fernando Domínguez-Pinuaga – Vice President, Sandbox AQ
5. Rosario Duaso Calés – Professor of Law, CEU San Pablo University
6. Maria da Graça Canto – Professor, Nova University
7. Carla Hobbs – Deputy Programme Director, European Power, ECFR
8. Stefano Mele – President, ICT Authority, Republic of San Marino
9. Ángel Melguizo – Partner, ARGIA Green, Tech & Economics
10. Pedro Mier – President, Ametic
11. Andrés Ortega Klein – Writer and Analyst
12. José Luis Piñar – Professor of Administrative Law, CEU San Pablo University
13. Christian Schroeder de Witt – Postdoctoral Research Assistant, University of Oxford
14. César Tello – Director General, Adigital
15. José Juan Timermans – Madrid Office Assistant, ECFR
16. José Ignacio Torreblanca – Head of the Madrid Office and Senior Policy Fellow, ECFR
17. Georgios Yannopoulos – Associate Professor, Legal Informatics, University of Athens' Law School
18. Vincenzo Zeno-Zencovich – Comparative Law Professor, University of Rome Tre

POLICY SESSION 3

"The Digital Front Line: Hybrid Threats amid Geopolitical Tensions"

As is widely known, in the era of strategic competition, the weaponization of any domain represents some of the most pressing challenges to liberal democracies. In essence, hybrid methods of warfare and competition are not new, what has changed is the technological framework, the information environment, and the digitalization of societies and with that the speed, scale, complexity, and intensity of hybrid attacks. The spread of Foreign Information, Manipulation and Interference (FIMI), cyberattacks or hacktivism in combination with hybrid threats in more traditional domains such as space, legal, culture, societal, diplomacy or economy are formidable weapons against our shared values and our democratic institutions.

The purpose of this policy session has three areas of focus: (1) examine the current scenarios in which hybrid threats are proliferating with a strong focus on digital-related domains, assessing their impact on Europe's defence and security; (2) discuss how the wars in Ukraine and Gaza-Israel are providing clear evidence of the novel use of technology and the pivotal role being played, among others, by tech companies and non-state entities; and (3) explore the increasingly blurred line between civilian and military use of technology and the role of regulations such as the EU Digital Services Act and multilateral cooperation in addressing this.

Moderator and Rapporteur

- Alejandro Romero – COO and Co-founder, Constella Intelligence
- Jonathan Nelson - Director of Risk Intelligence, Constella Intelligence

Guiding questions

We're aiming at identifying issues which current policies are missing or not addressing properly, challenges ahead, next policy steps, how to improve public-private dimensions of international cooperation:

- Are public officials, governments, and societies at the right level of understanding of the existential challenge that hybrid threats represent? How can policies be better designed to reflect the nuanced landscape of hybrid threats? How to overcome fragmented funding and diverse definitions of the problem to devise cross-institutional responses? What role could private entities play (e.g. media and tech companies)?

- What are the examples of best practice in combating hybrid threats around the world? How can multilateral institutions such as NATO cooperate with national institutions such as the Global Engagement Center in the USA and regional institutions in the EU to address them?

- Almost all new technologies have a dual use and can be weaponized. How can we design policies to mitigate the risks stemming from these emerging disruptive technologies whilst enabling innovation in areas such as AI or quantum? How to address their misuse such as the targeted deployment of deep fakes?

Suggested reading materials

- Ulrike Franke & Jenny Soderstrom, "Star tech enterprise: Emerging technologies in Russia's war on Ukraine", ECFR, 5 September 2023
- Cyber Dimensions of the Armed Conflict in Ukraine, Quarterly Analysis Report Q2 2023 CyberPeace Institute
- Playing with lives: Cyberattacks on Healthcare are Attacks on People, CyberPeace Institute
- Constella Intelligence, "Unveiling the digital landscape on African Migration", 2023
- Constella Intelligence, "Navigate Uncertainty During the War on Ukraine", Ongoing
- José Ignacio Torreblanca & Ringhof, Julian, "The virtual front line: How EU tech power can help Ukraine", ECFR, 23 February 2022
- Isabella Garcia-Camargo and Samantha Bradshaw (2021), "Disinformation 2.0: Trends for 2021 and beyond", Working Paper July 2021, Hybrid CoE, July 2021
- Google White Paper, Kent Walker "Supporting the EU and securing its digital space" & Enhancing Cybersecurity and Digital Resilience in Europe.
- Victor Muñoz, "Si crees que ahora hay desinformación sobre las elecciones, aún no has visto nada: prepárate para la IA", El Confidencial, 4 June 2023

Participants

1. Valérie Abrell Duong – Chief Digital & Operation Officer, International Committee of the Red Cross (ICRC)
2. Kamilia Amdouni – Public Policy Advisor, Cyber-Peace Institute
3. Miguel Castro – Deputy Director, Program Communications, Bill & Melinda Gates Foundation
4. Nicolás de Pedro – Strategy Director, Earendel Associates
5. Sorin Ducaru – Director, EU Satellite Centre
6. Stéphane Grumbach – Senior Scientist, INRIA
7. Raquel Jorge – Research Director, Fundación ESYS
8. Bernardino León – Senior Adviser, Brunswick
9. Francisco Marín – Chief of Intelligence, Joint Cyber Space Command, Ministry of Defence of Spain
10. Syra Marshall – Co-Founder & CTO, Elemendar
11. Jonathan Nelson – Director of Risk Intelligence, Constella Intelligence
12. Herman Quarles van Ufford – Senior Policy Fellow, ECFR
13. Nick Reiners – Senior Analyst, Geotechnology, Eurasia Group
14. Isabel Rioja-Scott – Economic Counsellor, US Embassy to Spain and Andorra
15. Alejandro Romero – COO and co-founder, Constella Intelligence
16. Yolanda Rueda – Founder and President, Fundación Cibervoluntarios
17. Giorgio Rutelli – Editor-in-Chief, Formiche.net
18. Irene Sánchez - Madrid Programme Coordinator, ECFR
19. Jacob Tamm – Deputy Director, EEAS Stratcom
20. Arturo Varvelli – Head of Rome Office and Senior Policy Fellow, ECFR