



Task Force on
Artificial Intelligence and Cybersecurity
Technology, Governance and Policy Challenges

Agenda

3rd meeting of the CEPS Task Force - Thursday, 05 December: 12:15 – 17:15

12:15 – 13:00	Registration & Lunch
13:00 – 13:05	Opening & Welcome Lorenzo Pupillo , <i>Coordinator of the CEPS Task Force</i>
13:05 – 13:15	Roundtable presentation of Task Force Participants
	PART I: Cybersecurity for Artificial Intelligence: academic perspective
13:15 – 15:00	Artificial Intelligence Misuses vs malicious uses. Deep Fakes Jean-Marc Rickli , <i>Head of the Global Risk and Resilience GSCP, Geneva</i>
	Attacking AI: AI's Security Vulnerability and what Policymakers can do about it Marcus Comiter , <i>Harvard Kennedy School, Belfer Center</i>
	Artificial Intelligence and data sharing for network security David Clark , <i>Senior Research Scientist MIT Computer Science & Artificial Intelligence Laboratory</i>
15:00 – 15:15	<i>Coffee Break</i>
	PART II: Cybersecurity for Artificial Intelligence: industry perspective
15:15 – 17:15	Cybersecurity for AI Martin Dion , <i>CSO and VP EMEA Services, Kudelski</i>
	Cybersecurity for AI Rob Spiger , <i>Principal Security Strategist, VP, Microsoft</i>
	Blockchain and AI Data Integrity Andres Ojamaa , <i>Lead Researcher / Architect, Guardtime</i>
17:15- 17:30	Closing

