CEPS TASK FORCE

ARTIFICIAL INTELLIGENCE AND CYBERSECURITY: TECHNOLOGY, GOVERNANCE AND POLICY CHALLENGES

PROSPECTUS

Artificial intelligence is showing enormous promise for improving our daily life. Countless applications in many sectors of the economy are already being developed and more can be expected over the long term. As this new world emerges, we need to seize the opportunity to decide how AI can help us promote a better society and a more sustainable future. Indeed, AI developments, as for any powerful general purpose, dual use technology, not only bring extensive possibilities, but also challenges to match, with people able to use AI to achieve both honourable and malevolent goals. Cybersecurity is a case in point. AI in the form of machine learning and deep learning will make an escalation of cyber-attacks easier, allowing for faster, better targeted and more destructive attacks. At the same time, AI could improve cybersecurity and defence measures allowing for greater system robustness, resilience and responsiveness. However, the application of AI in cybersecurity poses security as well as ethical concerns. For instance, while AI systems can exceed human performance in launching aggressive counter cyber operations, they could also fail in ways that a human never would. If this is the case, should 'kill switches' be incorporated in the systems? Furthermore, using AI for cybersecurity increases the need for better information sharing and collection of real time threat data. In parallel, cybersecurity for AI would need to be developed to make systems safe and secure. How can autonomous and intelligent systems be protected from malicious attacks? What are the implications of the vulnerabilities of AI-enabled systems to manipulation such as data poisoning and adversarial examples? How should the search for undiscovered exploits and well-known vulnerabilities be framed in the AI domain?

Furthermore, the Ethics Guidelines for Trustworthy Artificial Intelligence recently published by the High Level Expert Group on Artificial Intelligence set by the European Commission, mention that a crucial component of achieving Trustworthy AI is technical robustness and safety to be accomplished through resilience to attack and through security.

Following the successful completion of the Artificial Intelligence Task Force in 2018, CEPS is launching a Task Force on AI and Cybersecurity as the first of a series focused on in-depth vertical study of the implications of the use of AI in various sectors. This Task force will bring attention to the market, technical, ethical and governance challenges posed by the intersection of AI and cybersecurity, focusing in particular on EU policy, but also looking at developments in other parts of the world. It will be composed of academics, industry players from various sectors, policymakers and civil society. And it will discuss issues such as: the state and evolution of the application of AI in cybersecurity; the debate on the role that AI could play in the dynamics between cyber attackers and defenders; the increasing need for sharing information on threats and how to deal with the vulnerabilities of AI-enabled systems; options for policy experimentation; and possible EU policy measures to ease the adoption of AI in cybersecurity in Europe.

MEETINGS AND TIMELINE

The CEPS Task Force will conduct its activities across four meetings, with approximately monthly frequency, structured along these lines:

Meeting 1. What is the state of the interplay between AI & Cybersecurity? Stocktaking with experts from various backgrounds. Presentations by the private sector, and the European Commission

Meeting 2. AI for Cybersecurity:

- AI empowerments of different actors.
- Systems robustness, resilience and response: technological, ethical and governance issues

Meeting 3. Cybersecurity for AI:

- AI and better information and real time threat data sharing
- AI and safety (data poisoning, adversarial examples)
- AI misuses vs malicious uses
- AI and the search for undiscovered exploits and vulnerabilities

Meeting 4. The governance of the interplay between AI and cybersecurity: ensuring fruitful public-private cooperation and future-proof public policy

Meeting 5. Presentation of the Final Report

The CEPS Task Force on AI & Cybersecurity aims at involving a significant number of stakeholders, such as industry players (Internet companies, software companies, security companies, energy, telecoms, banking/insurance, healthcare, manufacturing, etc.); academics and experts (see below for a preliminary list); the European Commission (DG CONNECT, GROW, RTD) and other European Institutions.

The activity of the Task Force is expected to start in July 2019 and continue through to December.

GOVERNANCE OF THE TASK FORCE

Members of the Scientific board

Joanna Bryson is a Reader (tenured Associate Professor) at the University of Bath. She has broad academic interests in the structure and utility of intelligence, both natural and artificial. Venues for her research range from reddit to Science. She is best known for her work in systems AI and AI ethics, both of which she began during her PhD in the 1990s, but she and her colleagues publish broadly, in biology, anthropology, sociology, philosophy, cognitive science, and politics. Current projects include "The Limits of Transparency for Humanoid Robotics" funded by AXA Research, and "Public Goods and Artificial Intelligence" (with Alin Coman of Princeton University's Department of Psychology and Mark Riedl of Georgia Tech) funded by Princeton's University Center for Human Values. Other current research includes understanding the causality behind the correlation between wealth inequality and political polarization, generating transparency for AI systems, and research on machine prejudice deriving from human semantics. She holds degrees in Psychology from Chicago and Edinburgh, and in Artificial Intelligence from Edinburgh and MIT. At Bath she founded the Artificial Intelligence research group (one of four in the Department of Computer Science) and heads their Artificial Models of Natural Intelligence.

Jean-Marc Rickli is the Head of Global Risk and Resilience at the Geneva Centre for Security Policy (GCSP) in Geneva, Switzerland. He is also a research fellow at King's College London and a non-resident fellow in modern warfare and security at TRENDS Research and Advisory in Abu Dhabi. He is a senior advisor for the AI (Artificial Intelligence) Initiative at the Future Society at Harvard Kennedy School and an expert on autonomous weapons systems for the United Nations in the framework of the Governmental Group of Experts on Lethal Autonomous Weapons Systems (LAWS). He is also a member of The IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems and the co-chair of the NATO Partnership for Peace Consortium on Emerging Security Challenges Working Group. His expertise is on the security implications of AI especially its misuses such as Deepfakes and its malicious uses through its weaponization or its use in computational propaganda. Prior to these appointments, Dr. Rickli was an assistant professor at the Department of Defence Studies of King's College London and at the Joint Command and Staff College in Doha. He was also an assistant professor at the Institute for International and Civil Security at Khalifa University in Abu Dhabi. Dr. Rickli received his PhD and MPhil in International Relations from Oxford University, UK, where he was also a Berrow scholar at Lincoln College.

Marc Ph. Stoecklin is a Principal Research Scientist and Manager of the Cognitive Cybersecurity Intelligence (CCSI) group at the IBM T.J. Watson Research Center in Yorktown Heights, NY. He leads the cognitive security research activities at IBM, with a particular focus on applying artificial intelligence (AI) and machine learning to cybersecurity, including advanced threat detection, security/threat intelligence

consolidation, active cyber deception, big data cybersecurity analytics as well as malware and security analysis (ethical hacking). Marc's interest span different facets of cyber security, including how new technologies affect the threat landscape and how the same technologies can be used to build stronger security tools. He is also interested in helping security teams to be more efficient in day-to-day operations with trusted advisors, automation and consumable insights. Marc holds a PhD degree in Computer, Communication and Information sciences from École Polytechnique Fédérale de Lausanne (EPFL), Switzerland.

Mariarosaria Taddeo is Research Fellow (Assistant Professor) at the Oxford Internet Institute, University of Oxford, where she is the Deputy Director of the Digital Ethics Lab and is Faculty Fellow at the Alan Turing Institute. Her recent work focuses mainly on the ethical analysis of Artificial Intelligence, cyber security, cyber conflicts, and ethics of digital innovation. Her area of expertise is Philosophy and Ethics of Information, although she has worked on issues concerning Epistemology, Logic, and Philosophy of AI. She has been listed among the top 50 most inspiring Italian women working in AI in 2018. Dr Taddeo has been awarded The Simon Award for Outstanding Research in Computing and Philosophy. She also received the World Technology Award for Ethics acknowledging the originality and her research on the ethics of cyber conflicts, and the social impact of the work that she developed in this area. Since 2016, Taddeo serves as editor-in-chief of Minds & Machines (SpringerNature) and of Philosophical Studies Series (SpringerNature).

Task Force Leader

Lorenzo Pupillo is an Associate Senior Research Fellow at the Centre for European Policy Studies and Head of the Cybersecurity@CEPS Initiative. He is also Affiliated researcher at Columbia Institute for Tele-Information at Columbia Business School in New York and an adjunct professor of Digital Economy and Policy at LUISS University in Rome and at University of Urbino. Before joining CEPS, he served as an Executive Director in the Public & Regulatory Affairs Unit of Telecom Italia developing the company's global public policies for Internet, Cyber-Security, Next Generation Networks. He has served as an advisor to the Global Information and Communication Technologies Department of the World Bank. Before joining Telecom Italia, he was member of the technical staff at AT&T Bell Laboratories in Murray Hill - New Jersey - and served as senior economist for governmental institutions. He has worked in many areas of telecommunications demand and regulatory analysis, and published five books on Internet Policy and Economics and many papers in applied econometrics and industrial organization. Dr. Pupillo also serves on numerous scientific and advisory boards around the globe. He is also a member of the Editorial Board of the international peer-reviewed journals "Telecommunication Policy" (Elsevier) and member of the Scientific Board of European Communications Policy Research (EuroCPR). He obtained a Ph.D. and an M.A. from University of

Pennsylvania, an MBA from Istituto Adriano Olivetti in Ancona Italy and an MS in Mathematics from University of Rome, La Sapienza.

Rapporteurs

Stefano Fantin is a Legal and Policy Researcher at the Center for IT and IP Law (CITIP) of the University of Leuven (KU Leuven). He graduated from University of Trieste Law School (Italy) and TILT - Tilburg Institute for Law, Technology and Society (Netherlands), focusing on security and data protection in law enforcement, intelligence and e-Government. He gained first-hands work experience as a trainee at Europol (The Hague) and at the European Data Protection Supervisor (Brussels). He then served the British Government at the Cabinet Office (London) with the functions of Data Protection Analyst. As a civil servant, he was appointed at GDS, task force in charge of the digitization of all governmental departments and services. In Whitehall, he worked on implementation policies of GDPR, national cyber security strategy and the UK withdrawal from the European Union. Stefano joined CiTiP in October 2017 and is working on projects addressing counter-terrorism technologies, as well as on cybersecurity, internet governance and national security. Inter alia, he has also specialized in EU-Japan cybersecurity policies. Currently, he is also an Affiliated Researcher at CEPS for its Cybersecurity Initiative.

Afonso Ferreira is Directeur de Recherche with the French CNRS at the Toulouse Institute for Computer Sciences (IRIT), France, where he is Program Manager for European Affairs. He is currently leading his lab's participation in one of the four projects funded to pilot the upcoming European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres. In a career spanning more than 25 years, Afonso Ferreira has held European leadership roles in institutional policy and research. As an expert in the areas of Cybersecurity, Data Protection, Digital Transformation, and Policy Making, he recently spent six years seconded to the European Commission working as a policy and program officer. Thanks to his large knowledge of the Digital Revolution and its widespread impacts, Afonso is advising private and public actors on business development at the nexus of technology, futures, and policy, including Asian and South-American companies, the European Parliament, and the European Commission. Afonso is also member of the Scientific Leadership Committee at EAI – the European Alliance for Innovation. In addition to his Institutional past, he worked in research and innovation in the areas of Communication Networks, High Performance Computing, and Algorithms, having published more than 100 papers in the forefront of scientific research. He has been member of more than 70 Technical Committees for international organisations and events and he is an editorial board member for international scientific journals. He holds a PhD in Computer Science.

TASK FORCE TIMELINE

The timeline for the AI Task Force is the following:

1st meeting: 10 September 2019

2nd meeting: 29 October 2019

3rd meeting: 5 December 2019

4th meeting: 22 January 2020

Last meeting : Report Presentation 18 February 2020.

Joining the Task Force

Participation in the Task Force is subject to a fee to cover the research and organizational expenses. CEPS Corporate Members are entitled to receive a significant discount. Discounted fees will be considered for non-members if they decide to become a member of CEPS.

The fee covers:

- The research carried out by CEPS for the purpose of this Task Force
- Organisational, catering and other costs of all meetings
- Web access and documentation
- Launch of the final report in Brussels in a public event to maximise exposure
- Press release and communications management
- Printing and editing costs of the final report
- Distribution of the final report to key stakeholders in industry and policy-making
- Three printed copies of the final report per member (mailing included)

The fee does not cover travel and accommodation costs for Task Force members to attend the meetings.

Upon request, CEPS will mail additional copies of the final report to members, at their expense. The final report will be launched at a public event in Brussels, open to the press, with the presence of high-level policy-makers. Additional launch events in other European capitals may be organized, if sponsored by members of the Task Force.

Fee Structure (+21% VAT if applicable)	
CEPS Corporate Members	€ 1,500
Non-Members–Large corporations	€ 5,000
Non-Members – SMEs	€ 500
Academics and civil society	€ 300 [upon request]
European Institutions & Agencies	Free of charge [upon request]

To join the Task Force, please fill in the application form on the next page. If you have any questions do not hesitate to contact us:

Lorenzo Pupillo
Associate Senior Research Fellow
Head of the Cybersecurity@CEPS Initiative
Tel. +32 2 229 39 61
E-mail: lorenzo.pupillo@ceps.eu

REGISTRATION FORM

Artificial Intelligence and Cybersecurity: Technology ,Governance and Policy Challenges

Person attending the meetings			
Title:	First name:		Last name:
Job title:			
E-mail:		Telephone:	
Company / Institution			
Company / Institution name:			
Postal address:			
	Postcode:	City:	Country:
Contact Person:			
E-mail:		Telephone:	
Billing information			
Tax register number (VAT for Europe):			
Your reference, Customer Purchase Order No. or Cost Code N:			
Department:			
Postal address:			
	Postcode:	City:	Country:
Contact person:			

CEPS members – check the applicable fee (+21% VAT)

☐	CEPS Corporate Member | EUR 1,500

Non-members - check the applicable box (+21% VAT)

☐	Full Fee | EUR 5,000	☐	My company is interested in becoming a member of CEPS*

Date:	**Signature:**

Return to: Ada Modzelewska | ada.modzelewska@ceps.eu | + 32.2.229.39.75 | Centre for European Policy Studies | 1 Place du Congrès | 1000 Brussels | Belgium

More information: If you would like to become a member or need more information, please contact Lorenzo Pupillo, Associate Senior Research Fellow at lorenzo.pupillo@ceps.eu

*Discounted fees for this Task Force will be considered for non-members if they decide to become member of CEPS

ANNEX

Principles and Guidelines for CEPS Task Forces

This Annex offers guidance to prospective Task Force members and other interested parties in understanding the functioning of a CEPS Task Force and the process of drafting a Task Force report. Task Forces are processes of structured dialogue among industry representatives, policy-makers, consumers and NGOs, who are brought together over several meetings. Task Force reports are the final output of the research carried out independently by CEPS in the context of the Task Force.

Participants in a Task Force

- ✓ Members are for-profit entities, membership organisations or NGOs which participate in a Task Force and contribute to its expenses by paying a fee.
- ✓ Rapporteurs are CEPS researchers who organise the Task Force, conduct the research independently and draft the final report.
- ✓ Chair is an expert appointed by CEPS to steer the dialogue during the meetings and advise as to the general conduct of the activities of the Task Force.
- ✓ Observers are any policymakers or stakeholders who are invited to attend the Task Force meetings and provide oral and written input.

Objectives of a Task Force report

- ✓ Task Force reports are meant to contribute to policy debates by presenting a balanced set of arguments, based on the members' views, available data and literature.
- ✓ Reports seek to provide readers with a constructive basis for discussion. Conversely, they do not seek to advance a single position or misrepresent the complexity of any subject matter.
- ✓ Task Force reports also fulfil an educational purpose, and are therefore drafted in a manner that is easy to understand, without jargon, and with any technical terminology fully defined.

The role of the Task Force members

- ✓ Member contributions may take the form of participation in informal debate or a formal presentation in the course of the meetings, or a written submission.
- ✓ Input from members is encouraged and will be made available to all members, if it is to be used for the final report.
- ✓ Members represent their institutions but are asked to provide input as experts.
- ✓ Members are given ample opportunity to review the Task Force report before it is published, as detailed below.

Drafting of conclusions and recommendations

- ✓ Task Force reports feature a set of conclusions. To draft these conclusions, rapporteurs will summarise members' views. Wherever members' views do not lead to clear conclusions, general phrasing will be employed.
- ✓ Task Force reports feature a set of policy recommendations. These recommendations are meant to reflect members' views.
  - For a recommendation to be featured in the report, there needs to be 'consensus' or 'broad agreement' among Task Force members. Consensus does not however mean unanimity or full agreement as to every aspect of a given recommendation.
  - Where 'consensus' co-exists with a significant minority view, the report will feature this minority view next to the relevant recommendation.
  - Where there is no 'consensus' but several contradictory views, the report will feature all these views and either refrain from making any recommendation or simply advise policy-makers to clarify the given subject matter.
  - In all cases, the report will seek to identify the points where there is some form of agreement, for instance a common understanding of facts or opinions.
- ✓ Both conclusions and policy recommendations will be summarised at the beginning of the report in the form of an 'executive summary'.
- ✓ Members will be given ample opportunity to review the text of both conclusions and recommendations.

Drafting of the main text

- ✓ In the main text, rapporteurs detail the results of the research carried out independently in the framework of the Task Force. This part of the report will refer to the discussions during the task force meetings but also to available data and literature.
- ✓ Members' views are not simply presented as such but are also put into context. Wherever there is fundamental disagreement, the rapporteurs will ensure that all views are presented in a clear and fair manner.
- ✓ Scientific literature may be cited in this part of the report. Members are not purported to endorse any reference to this literature. A general disclaimer is inserted to clarify this aspect.
- ✓ The conclusions for each section will be clearly presented –and highlighted if appropriate. For the drafting of these conclusions please refer to the section above.

Use of data

- ✓ Task Force reports feature data that are considered both relevant and accurate by the rapporteurs.
- ✓ Task Force members are encouraged to contribute with any data or propose any sources they may consider relevant.
- ✓ Members may question either the relevance or accuracy of any given data. After consultation with other Task Force members, rapporteurs may decide either to exclude this data or to mention these concerns in the main body of the text.

Sample structure of a Task Force report

1. Editorial information
2. Disclaimer (see example below)
3. Executive summary
4. Outline
5. Main text
6. Summary of conclusions
7. References
8. Annexes, if any
9. List of participants

Sample disclaimer

"This report is based on the discussions in the CEPS Task Force on Innovation and Entrepreneurship, which met on five separate occasions in 2015. The policy recommendations offered at the beginning of this report reflect a general consensus reached by Task Force members, although not every member agrees with every aspect of each recommendation. A list of members, observers and invited guests of the Task Force can be found in Annex 3. The members were given the opportunity to comment on the draft final report, but its contents may only be attributed to the rapporteurs."