Task Force

SOFTWARE VULNERABILITY DISCLOSURE IN EUROPE

Prospectus for CEPS Task Force

Chair: **Marietje Schaake**, Member of European Parliament

Content

Background

For decades, the issue of SW vulnerability disclosure has been the subject of broad debate in the information security arena. Recent events, however, have created a new sense of urgency on this issue. The ransomware attacks from Wannacry took advantage of a vulnerability in Microsoft software discovered by the National Security Agency (NSA) and leaked by a group of hackers called Shadow Brokers. Such incidents focus critical attention on the widespread activity of stockpiling vulnerabilities by national intelligence agencies around the world. Moreover, with the development of the Internet of Things (IoT) and billions of devices connected to the internet, the attack surface is becoming broader and the impact of vulnerabilities will be even greater, thereby increasing the risks to critical infrastructure.

'Vulnerability disclosure' is the process by which someone shares information about a security vulnerability so that it can be mitigated or fixed. Particularly critical are the zero-day vulnerabilities, which are undisclosed software vulnerabilities that hackers can exploit to adversely affect computer programmes, data, additional computers or a network – and for which patches or mitigation do not yet exist. The way to handle this process has generated four types of vulnerability disclosure: full disclosure, responsible disclosure, coordinated vulnerability disclosure and no disclosure. While full disclosure consists of a public release of all the details of the vulnerabilities, quite often without any mitigation measures to protect users, the no disclosure approach represents a way for governments or

vendors to acquire vulnerabilities for exploitation or advantage at a later stage. Both the responsible disclosure and the coordinated vulnerability disclosure aim at sharing vulnerabilities information with vendors, but they differ on the degree of the coordination process to protect users. Discussants at a recent CEPS cyber event in Brussels emphasised the importance of introducing a coordinated vulnerability disclosure (CVD) process in Europe, in which finders– individuals or organisations that identify a potential vulnerability in a product or online service – share vulnerability information with vendors, and stakeholders focus on ways to protect users.

EU member states have only begun the practical implementation of this process. The Dutch government is leading the way with a Coordinated Vulnerability Disclosure Initiative, through the Global Forum on Cyber Expertise. The French agency ASSI is also actively participating. Other countries like Italy are catching up in this process through the initiative of the Digital Transformation Team. There is a real need for better harmonisation of vulnerabilities disclosure and handling the process at the national level. The policy framework that is already developed, however, may also need to be updated in view of future technologies such as the Internet of Things. The Joint Research Centre of the European Commission has extensively studied these issues and is suggesting that research should be the main driver for vulnerabilities discovery, while the creation of an EU pilot vulnerability management centre, serving as a test-bed platform, could act as an independent third party in this process. This role could be played by ENISA, which should have a stronger and more focused function in European cybersecurity policy, under the new Cybersecurity Strategies to be announced in the autumn.

But there is quite a lot of ground yet to be covered, especially for the role that governments should play in resolving the dilemma between disclosing zero-day vulnerabilities and retaining them for intelligence purposes. Only recently has the US government created a vulnerability equity process (VEP), which focuses on explaining how the government determines whether to release or retain a zero-day vulnerability through a structured policy process.

The CEPS Task Force on SW Vulnerability Disclosure in Europe will look at key aspects of the debate on this issue with the purpose of defining guideline to harmonize the process of Coordinated Vulnerability Disclosure (CVD) in Europe and to outline specific principles for member states to follow in developing a European vulnerability equity process (VEP) with clear priority given to reporting vulnerabilities to vendors.

Schedule and Content of Meetings

Meeting 1: **Coordinated Vulnerability Disclosure**

The first meeting will be focused on the overall agenda of the Task force and in particular on the discussion of the Coordinated Vulnerability disclosure in Europe. The following issues will be addressed:

- Status of the debate and best practices on SW vulnerability disclosure in each EU Country (government and private sector practices)
- EC Joint Research Centre proposal
- Implementation of ISO Standards
- Analysis of the most critical issues: collection of vulnerabilities, etc.
- SW Vulnerability disclosure and IoT
- Takeaways for a European Proposal

Kick-off date: 27 September 2017

Meeting 2: Equity Vulnerability Process (EVP)

The second meeting will be focused on the discussion on how to frame in Europe a Vulnerability Equity Process. The following issues will be addressed:

- Status of the debate in the EU Countries
- Analysis of the US Experience and the Patch Act
- EVP: geopolitical asymmetries
- Takeaways for a European Proposal

Proposed date: end of November/ early December 2017

Meeting 3: Final Presentation of the Task Force Report

During this meeting, the main conclusions and policy recommendations of the Task force will be illustrated and discussed with a high level panel of speakers from EU and national institutions, industry and academia.

Proposed Date: Beginning of 2018.

Team and Methodology

Chair of the Task Force

Marietje Schaake, Member of European Parliament

The Task force will be chaired by Marietje Schaake. She has been serving as a Member of the European Parliament for the Dutch Democratic Party (D66) with the Alliance of Liberals and Democrats for Europe (ALDE) political group since 2009. She serves on the International Trade committee and is the spokesperson for the ALDE Group on the Transatlantic Trade and Investment Partnership (TTIP).

Ms Schaake also serves on the committee on Foreign Affairs and the subcommittee on Human Rights. She is the founder of the European Parliament Intergroup on the Digital Agenda for Europe. Furthermore, Marietje Schaake is the Vice-President of the US Delegation and serves on the Iran Delegation and the Delegation for the Arab peninsula. She is a Member of the Global Commission on the Stability of Cyberspace and is a Young Global Leader and a Member of the Global Future Council on Future of Digital Economy and Society with the WEF.

The Research Group

Coordinator

Lorenzo Pupillo, Associate Senior Research Fellow, CEPS

Dr. Lorenzo Pupillo is an Associate Senior Research Fellow and Head of the Cybersecurity@CEPS Initiative. Before joining CEPS, he served as an Executive Director in the Public & Regulatory Affairs Unit of Telecom Italia developing the company' global public policies for Internet, Cyber-Security, Next Generation Networks. He also managed Telecom Italia's relations with the OECD, the ITU and other international associations and organizations. Previously, Dr. Pupillo held a variety of senior positions in the Strategy, Business Development and Learning Services divisions of Telecom Italia. He is an economist by training and has worked in many areas of telecommunications demand and regulatory analysis, publishing four books on Internet Policy and many papers in applied econometrics and industrial organization. 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 he worked as senior economist for governmental institutions. Dr. Pupillo is also an affiliated researcher at Columbia Institute for Tele Information at Columbia Business School and serves on numerous scientific and advisory boards around the globe. 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.

Rapporteurs

Afonso Ferreira, Directeur de Recherche CNRS

Afonso Ferreira, PhD, is Directeur de Recherche with the French CNRS and currently working at the Institut de Recherche en Informatique de Toulouse (IRIT) in the area of Cybersecurity. He has over thirty years of experience 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 60 Technical Program Committees for international events and is an editorial board member for international scientific journals.

From 2011 until 2017, Dr Ferreira was seconded to the European Commission as an expert in the areas of cybersecurity, future and emerging technologies, and foresight. While dealing with policy making and operations, his main achievements were the following. In 2015-2017 he designed, negotiated, procured, and implemented the EU Connecting Europe Facility programme in the area of cybersecurity (circa Euro 20 Million). Prior to that he managed the stakeholders' platform *Secure ICT: Research and Innovation* (120 experts) and coordinated their establishment of the European Strategic Agenda for Research and Innovation in cybersecurity, released late 2015. He also assisted in the management of the evaluation and renewal of the mandate of the European Agency for Network and Information Security (ENISA) to be proposed in 2017. In addition to his in-depth knowledge of European Union policies and programmes, Dr Ferreira specialises in Cybersecurity, Foresight, Innovation Policy, Collective Intelligence, and on the impact of the Digital Revolution on growth and jobs.

Gianluca Varisco, Cybersecurity Expert, Italian Digital Transformation Team.

Gianluca Varisco currently works for the Digital Transformation Team, within the Italian Government, focusing on assessing and improving cybersecurity infrastructures, processes and practices of those digital platforms and web sites coordinated by the Digital Transformation Team or other PA departments.

Gianluca previously held engineering roles at Rocket Internet, Red Hat, Lastminute.com Group, PrivateWave.

Romain Bosc, Research Assistant, CEPS

Romain Bosc is a Research Assistant within the CEPS Regulatory Policy Unit, where he works mainly on digital and related regulatory policies. He organises thematic events for the CEPS Digital Forum, a platform that gathers numerous stakeholders active in the digital economy, forward-looking ICT policy in Europe, the United-States and other regions. Recently, he was actively involved in exploring the impacts of the copyright reform, and in analysing the different attempts to regulate Internet platforms and e-commerce, or in exploring the economic, legal and societal implications coming along with the 'hyper-connected society'.

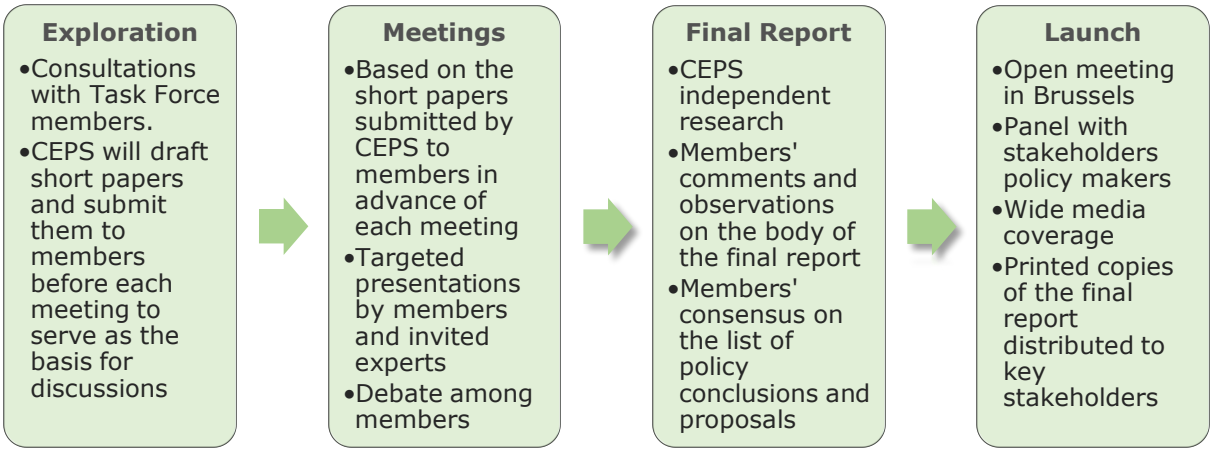
Graduated in Political Science (BA, Université Saint-Louis) and International Relations (MA, Université Libre de Bruxelles), Romain complemented his multidisciplinary background with various trainings and professional experiences in EU affairs. Prior to joining CEPS, Romain accomplished a traineeship at the European Commission DG CNECT, where he worked on international collaboration

in ICT research & innovation, including the transatlantic dialogue on the information society and various regulatory matters, such as cybersecurity and data protection, ICT standardisation and copyright issues, as well as Internet Governance policy.

Advisors

- Ross Anderson, Cambridge University
- Michael Daniel, Cyber Threat Alliance
- Allan Friedman, NTIA
- Andriani Ferti, Karatzas & Partners Law Firm
- Trey Herr, Belfer Center, Harvard University
- Demosthenes Ikonomou, ENISA
- Tim Watson, University of Warwick

Methodology



See the Annex for background information of the functioning of CEPS Task Forces.

Joining the Task Force

Participation in the Task Force is subject to a fee to cover the research and organisational 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 chair is serving in her independent capacity, and has not received any type of compensation from CEPS or from any of the participants in the task force for her role in chairing the CEPS taskforce

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 organised, if sponsored by members of the Task Force.

Fee Structure (+21% VAT if applicable)	
CEPS Corporate Members	€ 1,000
Non-Members	€ 2,500
Academics	€ 500 [upon request]
Policy-makers	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
Tel. +32 2 229 39 68
E-mail: lorenzo.pupillo@ceps.eu

Diana Musteata
Corporate and External Relations
Tel: +32 (0) 2 229 39 34
E-mail: diana.musteata@ceps.eu

Romain Bosc
Research Assistant
Tel: +32 (0)2 229 39 23
Email: romain.bosc@ceps.eu

Anne-Marie Boudou
Conference & Membership Coordinator
Tel:+32 (0) 2 229 39 12
E-mail:amboudou@ceps.eu

REGISTRATION FORM
Software Vulnerability Disclosure in Europe

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 1,000		
Non-members - check the applicable box (+21% VAT)			
☐	Full Fee | EUR 2,500	☐	My company is interested in becoming a member of CEPS*
Date:		**Signature:**	

Return to: Anne-Marie Boudou | amboudou@ceps.eu | +32 2 229 39 12 | 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 +32 2 229 3968 or *Diana Musteata* Corporate and External Relations, at diana.musteata@ceps.eu or +32 2 229 39 34.

*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 or outside experts 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."

About CEPS – Centre for European Policy Studies

Founded in Brussels in 1983, the Centre for European Policy Studies (CEPS) is among the most experienced and authoritative think tanks operating in the European Union today. CEPS serves as a leading forum for debate on EU affairs, and its most distinguishing feature lies in its strong in-house research capacity, complemented by an extensive network of partner institutes throughout the world.

CEPS' funding is obtained from a variety of sources, including membership fees, project research, foundation grants, conferences fees, publication sales and an annual grant from the European Commission.

www.ceps.eu

Place du Congrès 1 | 1000 Brussels | Tel: + 32 2 229 39 11