Strengthening the EU's Cyber Defence Capabilities

A new CEPS Task Force

PROSPECTUS – 05 March 2018

The security of cyberspace has gradually become a key priority both for the protection of critical infrastructure, as well as for military purposes. However, cyber defence is often at a structural disadvantage to attacks, especially those of a global or cross-border nature. In Europe, this is also due to the fragmented nature of defence strategies and capacities, unevenly confined in the hands of national governments. At the EU level, this becomes even clearer due to the ongoing integration of the Digital Single Market. With the growing degree of interconnectedness, an enhanced level of cooperation and coordination in the defence domain is required: otherwise, the least prepared countries might become an easy entry point for cyber-attackers (spies, thieves or terrorists) wishing to target the whole EU (so-called "weakest link" problem). The distributed nature of attacks also implies that more than one member state could be targeted by a single, large-scale cyberattack, as occurred in several circumstances (e.g. the Petya and Wannacry attacks last summer). In many cases, response coordination may be best achieved at supranational level, based on data collected throughout the territory of the EU and jointly analysed by a centralized authority and response team. The emergence of the Internet of Things is bringing along botnets, which bear the potential to create massive dysfunctions in both civilian critical infrastructures and military operations (e.g. drones).

Against this background, the cybersecurity landscape in Europe is very fragmented. Various initiatives have been undertaken to strengthen coordination, including a revision of the mandate of ENISA (the EU Agency for Network Security, in Greece); the creation of Computer Emergency Response Teams (CERTs) in each member state; and the adoption of the Network and Information Security (NIS) Directive, which creates an unprecedented set of information sharing obligations between private players and public authorities. There is a growing understanding that both cyber and hybrid defence require (i) more public-private trust and cooperation; (ii) enhanced coordination of response teams located at the national level; (iii) increased international dialogue and cooperation; and (iv) stepping-up Europe's ability to "detect, defend, and deter" as a single player, rather than through inter-governmental (voluntary) information sharing.

As a result, CEPS considers it very important to discuss measures to make stronger cyber defence capabilities in Europe. This is also timely as the EU's

Common Security and Defence Policy (CSDP) is developing further by setting up permanent structured cooperation (PESCO) between 23 member states.

This provides the upshot for a progressive framing of a common EU defence in specific areas of cyber threats. The PESCO goes hand-in-hand with renewed efforts to shape the regulatory and institutional framework of a single market for defence. Under the European Commission's European Defence Action Plan (more details here http://europa.eu/rapid/press-release_IP-16-4088_en.htm), EU funding has come online for co-financed R&D of prototypes developed by a minimum of 3 (in the future more) member states. Easy entry points are projects related to cyber and hybrid defence: the member states do not have sufficient capacities to counter cyber-attacks and are thus more readily motivated to cooperate at the EU level.

The European Commission, and in particular Vice-President Katainen, supports the idea of a CEPS TF that would provide input to the ongoing reflections on the EU contribution to cyber defence. This could include:

1. Identify short term measures which can be already done under the current institutional framework.
2. Developing a policy to enhance European cyber defence capabilities.
3. Identifying which capabilities should and could be developed in this framework (cyber teams to support MS, stress-tests for critical infrastructures).
4. If a new structure is set up, design a governance structure for a ECSA.
5. Roadmap for implementation of the institutional architecture.

Given the dual-use nature of cyber technologies and the hybrid nature of cyber threats, there is a need to integrate cybersecurity and defence within the Common Security and Defence Policy — and/or outside of it (i.e. based on a parallel legal act that caters for, e.g., the competitiveness of the Union's industry or the efficient execution of EU funded R&D) and to promote synergies between military and civilian efforts.

The goal of this TF would be to focus on building EU capabilities geared towards the detection, defence and deterrence of sophisticated cyber threats.

CEPS envisages the possibilities of taking ad hoc measures to create stronger cyber defence capabilities in the EU such as EU Crisis Emergency Response Teams (EU CERT) that can complement those of member states. Given the speed of cross-border traffic and attacks on the weakest links in a largely ungoverned cyberspace, the ECSA should do more than just coordination. It should get involved in data collection and forecasting, which in turn can inspire more effective deterrence/preparedness strategies. The actual response to cyberattacks should continue to be done (instantly) at the member state level, but whenever needed this should occur on the impulse and in the execution of an obligation emanating from the EU. Overall, effective prevention/early warning at EU level would require people, big data and artificial intelligence to study patterns. An ECSA will need to rely on national telecom providers, private networks and open internet sources. As such, the proposal raises questions

about sovereignty (i.e. attribution of competences to the EU) and subsidiarity (i.e. the most efficient and effective level of implementation).

CEPS suggest to concentrate the work of the TF on what many observers consider the most critical cyber threats, including (but not limited to) 'Collection Operations' (trolls used to influence election or create social tensions) and 'Intrusions to Hold Target at Risk' (i.e., network intrusions to develop offensive capabilities against future targets, such as the attack on power grid in Ukraine in 2015).

CEPS is well placed to convene and support an authoritative group of stakeholders (see e.g. the Task Force on 'More Union in European Defence' chaired by Javier Solana; as well as the ongoing Task Force on Software Vulnerability in the European Union). Our Task Forces will comprise political, policy, business and thought leaders and will rely on a research backbone provided by CEPS.

European Commission Vice President Katainen has expressed interest for the launch of the CEPS Task Force in his visit to CEPS in January 2018, and is willing receive the first copy of its report later this year.

The CEPS Task Force plans to structure its works in four meetings:

1. Threat assessment and stocktaking (26 March 2018)
2. EU value added (25 April 2018)
3. Legal and institutional recommendations (23 May 2018)
4. Official presentation of the Task Force Report (June 2018)

Issues to consider:

- Legal confines in and complementarities between the military (CSDP > TEU) and civilian (single market, R&D, humanitarian > TFEU) spheres.
- Transformation of European network security authority (ENISA) and budget.
- NIS directive on facilitating information sharing and coordination (cf. COM of 13/09/2017).
- The US experience: one authority and backup network. Should the EU create a European secure network for critical (information) infrastructure, such as the U.S. FirstNet?
- Should Cyber Defence function as part of the EDA, or should it go beyond a merely inter-governmental approach?
- Strengthening the EU-NATO cooperation.
- Cyber defence training & education.

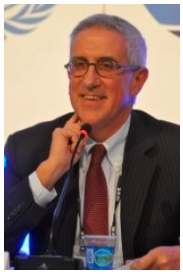
Chair of the Task Force

Jaap de Hoop Scheffer is a retired Dutch politician of the Christian Democratic Appeal (CDA). He served as the 11th Secretary General of NATO from 5 January 2004 until 1 August 2009. He previously served as a Member of the House of Representatives from 3 June 1986 until 23 May 2002, and became the Parliamentary leader of the Christian Democratic Appeal in the House of Representatives of the Netherlands and CDA Party leader on 27 March 1997. He resigned as Minister of Foreign Affairs on 3 December 2003, when he was selected as the next Secretary General of NATO, he served as Secretary General from 5 January 2004 until 1 August 2009. After his term as Secretary General of NATO ended, De Hoop Scheffer became a professor at the Leiden University sitting in the Pieter Kooijmans Chair. He also teaches at Leiden University College.

CEPS Rapporteurs:

Steven Blockmans is a senior research fellow and the head of the 'EU foreign policy' and 'politics and institutions' units of CEPS. He has published widely on the institutional structures for EU external action, the Union's role in global governance, norm promotion absorption, the EU enlargement policy, relations with neighbouring countries, Common Foreign and Security Policy, Common Security and Defence Policy, trade, development, and humanitarian aid. Steven is a Professor of EU External Relations Law and Governance at the University of Amsterdam (part-time) and one of the founding members of the Centre for the Law of EU External Relations (CLEER). Steven holds a PhD in law from Leiden University, where he worked as a lecturer from 1998 until 2002.

Hrant Kostanyan is a Researcher at CEPS, a Senior Key Expert at the College of Europe Natolin and an Adjunct Professor at Vesalius College. His research focuses on EU institutions and decision-making, primarily on the European External Action Service (EEAS), the European Neighbourhood Policy (ENP) and the EU's relations with Eastern Neighbours and Russia. He has worked as a senior expert in a number of the EU projects related to reforming public administration, communications, the European Neighbourhood Policy, the Eastern Partnership and Russia.



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. 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.

Andrea Renda is a Senior Research Fellow and Head of Regulatory Policy at CEPS. He currently holds the Chair in Digital innovation at the College of Europe in Bruges (Belgium). He is a non-resident fellow at the Kenan Institute for Ethics at Duke University. Over the past two decades, Andrea has provided academic advice to several institutions, including the European Commission, the European Parliament, the OECD, the World Bank and several national governments around the world. An internationally recognized expert in regulation, evidence-based policymaking, and the impact of new technologies on policymaking both in developed and developing countries, in 2017 Andrea became member of the ESIR (Economic and Societal Impacts for Research) expert group of the European Commission. He holds a Ph.D. degree in Law and Economics awarded by the Erasmus University of Rotterdam.

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 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.