The European Commission's Scientific Advice Mechanism

Johannes Klumpers
Head of Unit
Scientific Advice Mechanism

http://ec.europa.eu/research/sam/index.cfm

Source: www.kudelka.com.au

Why?

"..a focus on…making sure that Commission proposals and activities are based on sound scientific evidence and contribute best to our jobs and growth agenda"

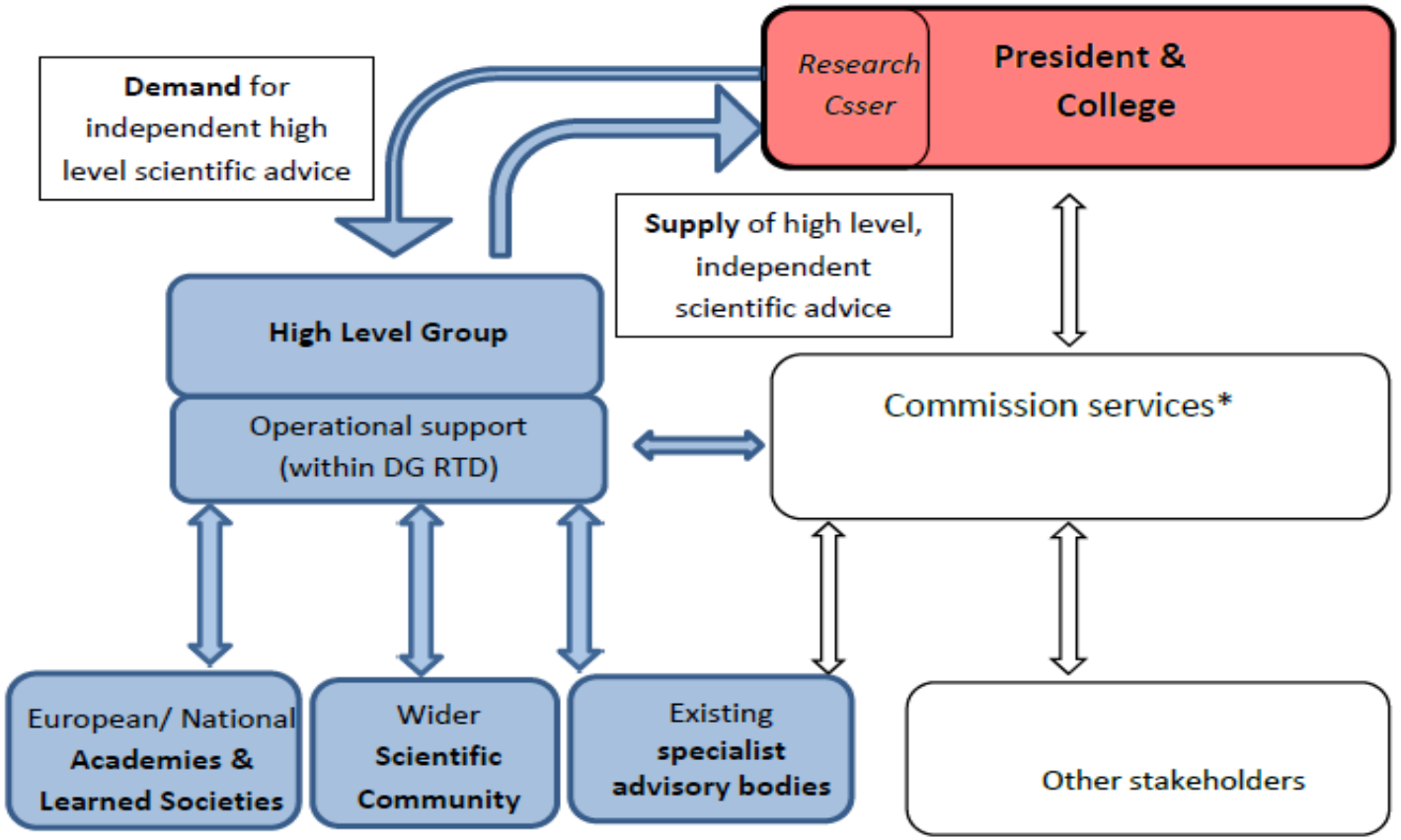
President Jean-Claude Juncker, in his mission letter to Carlos Moedas, 1 November 2014

"The new mechanism will provide high quality, timely, independent scientific advice to policy making… and will build upon the wealth of expertise available both in Europe and in the services of the European Commission".

Commissioner Moedas, Informal Competitiveness Council lunch, July 2015

How do we get there?

How?



* Including the Joint Research Centre which provides in-house scientific support

Learning from others

Eight ways to improve expert advice

Sutherland, Burgman; Nature, 15 Oct 2015

- Use groups
- Choose members carefully
- Don't be starstruck
- Avoid homogeneity
- Don't be bullied

Science Advice to Governments: Diverse systems, common challenges

Wilsdon, Allen, Paulavets; The Guardian Aug 2014

- Distinguish between 'Science for Policy' and 'Policy for Science'
- Improve quality through multi- and inter-disciplinary expertise

Learning from experience

We also need a fundamental review of the way European institutions access and use scientific advice. In the next Commission I want to set up a Chief Scientific Advisor who has the power to deliver proactive, scientific advice throughout all stages of policy development and delivery. This will reflect the central importance I attach to Research and Innovation.

José Manuel Barroso, 18 September 2009

European Commission

Avoiding duplication & adding value

EFSA explains **risk assessment**

Caffeine

- What is **caffeine**?
- How does the **body process** caffeine?
- What are the **risks**?
- Why did EFSA carry out its **risk assessment**?
- What does the assessment **cover**?
- **How much** caffeine do we consume?
- How much caffeine is it **safe** to consume?
- **How much caffeine** is there in…
- Does caffeine have an **adverse effect** when consumed with other constituents of "energy drinks" and/or with alcohol?

What is **caffeine**?

Caffeine is a naturally occurring chemical compound found in plant constituents such as coffee and cocoa beans, tea leaves, guarana berries and the kola nut, and has a long history of human consumption. It is added to a variety of foods, such as baked pastries, ice creams, sweets, and cola drinks. Caffeine is also found in so-called energy drinks, alongside other ingredients such as taurine, and D-glucurono-γ-lactone. It is also present in combination with *p*-synephrine in a number of food supplements that are marketed for weight loss and sports performance. Some medicines and cosmetics contain caffeine.

When consumed by humans, caffeine stimulates the central nervous system, and in moderate doses increases alertness and reduces sleepiness.

Caffeine is also found in so-called energy drinks, alongside other ingredients such as taurine, and D-glucurono-γ-lactone.

How does the **body process** caffeine?

Taken orally, caffeine is absorbed rapidly and completely by the human body. The stimulatory effects may begin 15 to 30 minutes after ingestion and last a number of hours. In adults the half-life of caffeine – the time it takes for the body to eliminate 50% of the caffeine – varies widely, depending on factors such as age, body weight, pregnancy status, medication intake and liver health. In healthy adults, the average half-life is approximately four hours, with a range of two to eight hours.

What are the **risks?**

Short-term adverse effects on adults and children can include issues related to the central nervous system such as interrupted sleep, anxiety and behavioural changes. In the longer term, excessive caffeine consumption has been linked to cardiovascular problems and, in pregnant women, stunted foetus development.

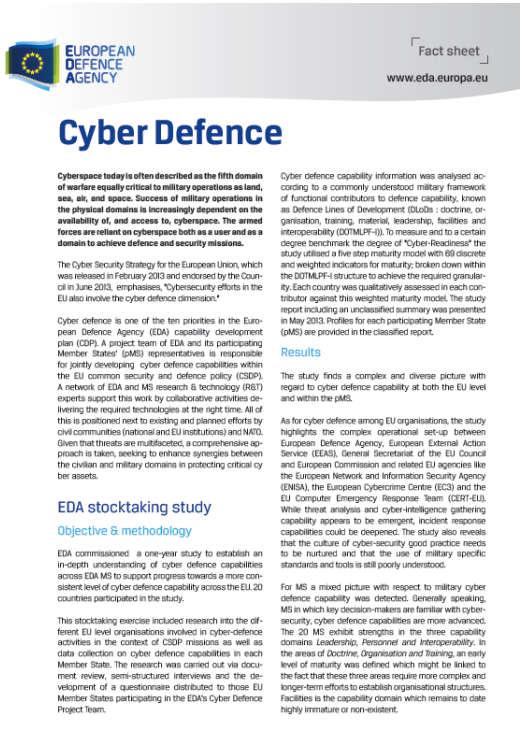
efsa
European Food Safety Authority

ecdc

SCIENTIFIC ADVICE

Expert Opinion on the public health needs of irregular migrants, refugees or asylum seekers across the EU's southern and south-eastern borders

www.ecdc.europa.eu



EUROPEAN DEFENCE AGENCY

Fact sheet

www.eda.europa.eu

Cyber Defence

Cyberspace today is often described as the fifth domain of warfare equally critical to military operations as land, sea, air, and space. Success of military operations in the physical domains is increasingly dependent on the availability of, and access to, cyberspace. The armed forces are reliant on cyberspace both as a user and as a domain to achieve defence and security missions.

The Cyber Security Strategy for the European Union, which was released in February 2013 and endorsed by the Council in June 2013, emphasises, "Cybersecurity efforts in the EU also involve the cyber defence dimension."

Cyber defence is one of the ten priorities in the European Defence Agency (EDA) capability development plan (CDP). A project team of EDA and its participating Member States' (pMS) representatives is responsible for jointly developing cyber defence capabilities within the EU common security and defence policy (CSDP). A network of EDA and MS research & technology (R&T) experts support this work by collaborative activities delivering the required technologies at the right time. All of this is positioned next to existing and planned efforts by civil communities (national and EU institutions) and NATO. Given that threats are multifaceted, a comprehensive approach is taken, seeking to enhance synergies between the civilian and military domains in protecting critical cyber assets.

EDA stocktaking study

Objective & methodology

EDA commissioned a one-year study to establish an in-depth understanding of cyber defence capabilities across EDA MS to support progress towards a more consistent level of cyber defence capability across the EU. 20 countries participated in the study.

This stocktaking exercise included research into the different EU level organisations involved in cyber-defence activities in the context of CSDP missions as well as data collection on cyber defence capabilities in each Member State. The research was carried out via document review, semi-structured interviews and the development of a questionnaire distributed to those EU Member States participating in the EDA's Cyber Defence Project Team.

Cyber defence capability information was analysed according to a commonly understood military framework of functional contributors to defence capability, known as Defence Lines of Development (DLoDs : doctrine, organisation, training, material, leadership, facilities and interoperability (DOTMLPF-I)). To measure and to a certain degree benchmark the degree of "Cyber-Readiness" the study utilised a five step maturity model with 69 discrete and weighted indicators for maturity; broken down within the DOTMLPF-I structure to achieve the required granularity. Each country was qualitatively assessed in each contributor against this weighted maturity model. The study report including an unclassified summary was presented in May 2013. Profiles for each participating Member State (pMS) are provided in the classified report.

Results

The study finds a complex and diverse picture with regard to cyber defence capability at both the EU level and within the pMS.

As for cyber defence among EU organisations, the study highlights the complex operational set-up between European Defence Agency, European External Action Service (EEAS), General Secretariat of the EU Council and European Commission and related EU agencies like the European Network and Information Security Agency (ENISA), the European Cybercrime Centre (EC3) and the EU Computer Emergency Response Team (CERT-EU). While threat analysis and cyber-intelligence gathering capability appears to be emergent, incident response capabilities could be deepened. The study also reveals that the culture of cyber-security good practice needs to be nurtured and that the use of military specific standards and tools is still poorly understood.

For MS a mixed picture with respect to military cyber defence capability was detected. Generally speaking, MS in which key decision-makers are familiar with cyber-security, cyber defence capabilities are more advanced. The 20 MS exhibit strengths in the three capability domains *Leadership, Personnel and Interoperability*. In the areas of *Doctrine, Organisation and Training*, an early level of maturity was defined which might be linked to the fact that these three areas require more complex and longer-term efforts to establish organisational structures. Facilities is the capability domain which remains to date highly immature or non-existent.

Trickier questions?

Internal organisational

Ensure synergy

Ensure buy-in

- President's priority
- Close working relationship in college and at services level
- JRC
- EU-ANSA

External organisational

Go beyond the HLG

- HLG - Academies and other science advice providers - MS

Scope

- Long, medium, short
- Critical to EU policy development or legislation
- Pro-active

Communications

- Under development: relations with scientific community, civil society

Whom?

Professor Janusz M. Bujnicki
Head of the Laboratory of Bioinformatics and Protein Engineering, International Institute of Molecular and Cell Biology, Warsaw

Professor Elvira Fortunato
Professor, Materials Science Department of the Faculty of Science and Technology, NOVA University, Lisbon

Professor Rolf-Dieter Heuer
Director-General, European Organization for Nuclear Research (CERN)

Professor Pearl Dykstra
Professor of Sociology, Erasmus University, Rotterdam

Professor Julia Slingo
Chief Scientist, Met Office, Exeter

Cédric Villani
Director, Henri Poincaré Institute, Paris

Professor Henrik C. Wegener
Executive Vice President, Chief Academic Officer and Provost, Technical University of Denmark

What?

- ***RESPONSIVE**:*
  - *Provide independent scientific advice to EU policy and legislation (not duplicating existing advice)*
- ***PROACTIVE:***
  - *Identify policies where advice required*
  - *Recommend improvements to interaction between policy and advice*

First meeting, 29th January 2016

- Closing the gap between light duty vehicles real world CO2 emissions and laboratory testing
  - ✓October 2016
- Cybersecurity
  - ✓Longer term
- Rules for procedure

Ongoing / Next steps (provisional)

- JRC Ispra – 4 March
- 2nd meeting 17 March; 3rd ESOF 24-27 July; 4th 29-30 INGSA September; 5th November.