Council of the
European Union

Brussels, 6 May 2024
(OR. en)

9097/24

Interinstitutional File:
2024/0012(NLE)

POLCOM 167
COMER 68
RELEX 547
DUAL USE 35
RECH 173
ENER 188
ENV 433

LEGISLATIVE ACTS AND OTHER INSTRUMENTS

Subject:	COUNCIL RECOMMENDATION on enhancing research security

COUNCIL RECOMMENDATION

of …

on enhancing research security

THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 292, in conjunction with Article 182(5) thereof,

Having regard to the proposal from the European Commission,

Whereas:

(1) Openness, international cooperation, and academic freedom are at the core of world-class research and innovation. Yet, with growing international tensions and the increasing geopolitical relevance of research and innovation, the Union's researchers and academics are increasingly exposed to risks to research security when cooperating internationally, resulting in European research and innovation being confronted with malign influence and being misused in ways that affect the Union's security or infringe upon Union values and fundamental rights as defined in the Treaty on European Union ('TEU') and in the Charter of Fundamental Rights of the European Union ('Charter'). It is therefore vital that the Union research and innovation sector is supported and empowered to address these risks. Precise and proportionate safeguarding measures are needed to keep international cooperation open and safe.

(2) The changing geopolitical context urgently requires a joint response from all Member States and the Commission to strengthen and exploit the research and innovation potential across the Union. Only collective efforts can ensure the enhancement of research security. This context also requires a rebalancing of international cooperation in research and innovation in the light of Union interests, values and principles to develop and safeguard the Union's open strategic autonomy[1], while pursuing a level-playing field and balanced reciprocal openness.

[1] Special meeting of the European Council (1 and 2 October 2020) – Conclusions, 13/20, paragraph 3.

(3) Open science ensures that scientific research is made as accessible as possible for the benefit of science, the economy and society as a whole. International cooperation in research and innovation is vital for finding solutions to pressing global challenges for the benefit of our societies and drives scientific excellence, while international mobility of research talent enriches scientific enquiry and is essential for fostering innovation and achieving scientific breakthroughs. Academic freedom implies that researchers are free to conduct their research and choose the research methods as well as their research partners from around the globe, taking into account that with academic freedom comes academic responsibility.

(4) Growing strategic competition and the return to power politics are leading to increasingly transactional international relations. This shift has resulted in threats that are diverse, unpredictable, and oftentimes hybrid[2]. Given the pivotal role of critical knowledge and technology for political, economic, intelligence and military pre-eminence, some of theUnion's competitors are increasingly advancing their capabilities in this respect or actively pursuing civil-military fusion strategies.

(5) Hybrid threats may affect all relevant sectors; however, owing to its openness, academic freedom, institutional autonomy and worldwide collaboration, the research and innovation sector is particularly vulnerable. Union-based researchers and innovators may be targeted to obtain state-of-the-art knowledge and technology, at times using methods that are deceptive and covert, or through outright theft or coercion, but more often exploiting seemingly bona fide international academic cooperation. Next to jeopardising security and welfare, hybrid threats could affect academic freedom and research integrity in the Union.

---

[2] Joint Framework on countering hybrid threats a European Union response, JOIN(2016)18.

(6) The research and innovation sector is thus navigating an increasingly challenging international context for collaborations, with the risk of undesirable transfer of critical knowledge and technology to third countries which might be used to strengthen these countries' military capabilities and intelligence services, affecting the security of the Union and its Member States, or for purposes that are in violation of Union values and fundamental rights. While not always legally prohibited, those collaborations can pose significant security and ethical concerns.

(7) In accordance with institutional autonomy and academic freedom, research performing organisations and research funding organisations are primarily responsible for developing and managing their international cooperation. Public authorities at all levels should consider providing them with assistance and support, empowering them to take informed decisions and to manage the risks to research security involved.

(8) In recent years, discussions on strengthening research security have been ongoing in several Member States and at Union level, where various initiatives have been taken:

– in May 2021, the Commission published its communication on the Global approach to research and innovation, outlining a new European strategy for international research and innovation policy. The Council responded in September 2021 through the adoption of Council conclusions emphasising the Union and Member States commitment to strengthen measures for countering foreign interference;

– several safeguards were introduced in the Union's framework programme for research and innovation 2021-2027, Horizon Europe, giving effect to the Union's distinctive responsibility as one of Europe's largest research funders;

– in November 2021, the Council adopted the European Research Area (ERA) policy agenda 2022-2024 as part of its conclusions on Future governance of the ERA, in which tackling foreign interference is included in one of its priority actions;

– in January 2022, following up on its commitments stemming from both the Global approach and the ERA policy agenda, the Commission published its staff working document on tackling research and innovation foreign interference. Additionally, to facilitate peer learning among Member States, a mutual learning exercise took place throughout 2023;

– on 9 March 2022, the European Parliament adopted a resolution on foreign interference in all democratic processes in the Union, including disinformation, in which it calls for strengthening academic freedom, improving transparency of foreign funding as well as mapping and monitoring of foreign interference in the cultural, academic and religious spheres;

– in April 2022 , the Council adopted conclusions on a European strategy empowering higher education institutions for the future of Europe highlighting that deeper cooperation within the Union can be beneficial to support higher education institutions and equip researchers, trainers, students and staff with the necessary tools to deal with the challenges to fair global collaboration, such as inequity, foreign interference and obstacles to open science. The Council also stresses the need to promote an informed and independent understanding of third-country counterparts;

– on 10 June 2022, the Council adopted conclusions on principles and values for international cooperation in research and innovation, underlining the importance of risk management and security, and inviting the Commission and the Member States to develop further good practices;

– from a broader security and defence perspective, work is ongoing in the framework of the EU Security Union Strategy[3] as well as the Strategic Compass for Security and Defence, aiming at a shared assessment of threats and challenges and greater coherence in actions in the area of security and defence, including through the Union Hybrid Toolbox, that brings together different instruments to detect and respond to hybrid threats;

[3] COM(2020)605.

– in the domain of Union export control rules for dual-use goods and technology, the Regulation (EU) 2021/821 of the European Parliament and of the Council[4] is of significant importance to research security. To help research organisations, the Commission published in September 2021 a recommendation on compliance programmes for research involving dual-use items[5].

(9) The Commission and the High Representative adopted a joint communication on European Economic Security Strategy[6] which aims to ensure that the Union continues to benefit from economic openness, while minimising risks to its economic security. The Strategy proposes a three-pillar approach: promotion of the Union's economic base and competitiveness; protection against risks; and partnership with the broadest possible range of countries to address shared concerns and interests. In each of the pillars, research and innovation have a key role to play.

---

4 Regulation (EU) 2021/821 of the European Parliament and of the Council of 20 May 2021 setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items (OJ L 206, 11.6.2021, p. 1).

5 Commission Recommendation (EU) 2021/1700 of 15 September 2021 on internal compliance programmes for controls of research involving dual-use items under Regulation (EU) 2021/821 of the European Parliament and of the Council setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items (OJ L 338, 23.9.2021, p. 1).

6 JOIN(2023)20.

(10) Following that joint communication, the critical technology areas for the Union's economic security for further risk assessment with Member States were identified in Commission Recommendation (EU) 2023/2113[7]. Risk assessments have already been launched as a matter of priority on four of the 10 identified critical technology areas, namely advanced semiconductors, artificial intelligence, quantum and biotechnologies. The outcome of risk assessments, when finalised, could inform other potential measures to implement the European Economic Security Strategy, including measures to enhance research security.

(11) The joint communication on the European Economic Security Strategy furthermore announced that the Commission would propose measures to enhance research security by ensuring the use of the existing tools and identifying and addressing any remaining gaps, while preserving the openness of the research and innovation ecosystem. This recommendation is part of a package issued by the Commission in January 2024 as follow-up on the joint communication.

(12) In terms of gap identification referred to in the previous point, discussions with Member States and stakeholder organisations demonstrate an urgent need among policymakers and all other actors concerned for more conceptual clarity, a shared understanding of the issues at hand as well as of what constitutes a policy response that is both proportionate and effective.

---

[7] Commission Recommendation (EU) 2023/2113 of 3 October 2023 on critical technology areas for the EU's economic security for further risk assessment with Member States (OJ L, 2023/2113, 11.10.2023, ELI: http://data.europa.eu/eli/reco/2023/2113/oj).

(13) An increasing number of Member States have developed or are in the process of developing policies aimed at enhancing research security. While those efforts generally contribute to raising awareness and boosting resilience, to be truly effective , the development and implementation of safeguards should be consistently applied at all levels, including Union, national, regional as well as at the level of research performing organisations and research funding organisations. Union level coordination and Commission support for capacity building and exchange of practices are therefore needed to protect the integrity of the ERA, while respecting the competences of Member States for going further, for example by developing regulatory frameworks.

(14) It is important that hybrid threats affecting the research and innovation ecosystem are structurally assessed, enhancing situational awareness among policymakers by relying on the Single Intelligence Analysis Capacity, in particular the Hybrid Fusion Cell, and taking into account the work of the European Centre of Excellence for Countering Hybrid Threats as well as the European Union Agency for Cybersecurity and the European Cybercrime Centre set up by EUROPOL in relation to cybersecurity threats.

(15) Taking into account that a significant share of research and innovation takes place in the private sector, it should be stressed that, while the risks to which companies are exposed may be similar, their nature, needs and capacities differ from those of research performing organisations.

(16) Due attention should be paid to the policy experience of Member States and key international partners, while emphasising that an approach that suits the unique European context should be formulated. Good practices are, for example, shared through the Multilateral Dialogue on values and principles for international cooperation in research and innovation, as part of association negotiations and Joint Science and Technology Steering committee meetings in the context of international science and technology agreements, as well as in multilateral fora, such as G7, and relevant multilateral export control arrangements.

(17) Research security is a concern that is gaining increasing attention, and the ongoing debate on the risks involved and how to best manage them is intensifying. Consequently, there is a need to further raise awareness, promote and facilitate peer learning between Member States and relevant stakeholder organisations, as well as contribute to a learning approach that is both flexible and agile.

(18) For the purpose of this recommendation:

(1) 'Research security' refers to anticipating and managing risks related to: (a) the undesirable transfer of critical knowledge and technology that may affect the security of the Union and its Member States, for instance if channelled to military or intelligence purposes in third countries; (b) malign influence on research where research can be instrumentalised by or from third countries in order to inter alia create disinformation or incite self-censorship among students and researchers infringing academic freedom and research integrity in the Union; (c) ethical or integrity violations, where knowledge and technologies are used to suppress, infringe on or undermine Union values and fundamental rights, as defined in the Treaties.

(2) ‘Research and innovation sector’ refers to all research performing organisations , including higher education institutions as far as they perform research, research funding organisations and research infrastructures across the Union, as well as all other actors in the Union’s research and innovation ecosystem. While elements of this recommendation can be equally relevant to companies, engagement with private sector actors to address their research security is needed.

(3) ‘Research performing organisation’ means any non-profit organisation that performs scientific research.

(4) ‘International cooperation’ refers to cooperation of research performing organisations and research funding organisations established in the Union or individual researchers funded by those organisations, on the one hand, with entities, including companies, established outside the Union or individual researchers funded by those entities, on the other hand. Cooperation with research performing organisations and companies established in the Union but owned or controlled from outside the Union should be considered on the basis of a risk appraisal.

(5) ‘Risk appraisal’ refers to a process in relation to international research and innovation cooperation in which a combination of main risk factors is taken into consideration. The combination of those factors determines the risk level. The key elements to be assessed can be grouped in four categories: a) the risk profile of the Union-based organisation entering into the international cooperation: consider the organisation’s strengths and vulnerabilities, including financial dependencies, relevant to the research project; b) the research and innovation domain in which the international cooperation is to take place: consider whether the project focusses on research domains involving critical knowledge and technology, methodologies, data or research infrastructures considered particularly sensitive from a security or Union values and fundamental rights perspective; c) the risk profile of the third country where the international partner is based or from where it is owned or controlled (for example, whether the country is subject to restrictive measures or whether it has a flawed rule of law or human rights protection track record, an aggressive civil-military fusion strategy or limited academic freedom); d) the risk profile of the international partner organisation, namely – to perform due diligence on the organisation to be cooperated with to determine inter alia whether it is subject to restrictive measures or has links to the military, the affiliations of the researchers or of staff involved, as well as the partner’s intentions regarding the end-use or application of the research results.

(6) ‘Critical knowledge and technology’ refers to knowledge and technology, including know-how, in emerging and disruptive areas and in domains that are key to economic competitiveness, social welfare and the security of the Union and its Member States and in which, consequently,overdependency on third countries is undesirable, taking into account the dynamic nature of research security and evolving risks. That includes but is not limited to research and innovation with dual-use potential.

(7) ‘Third countries’ refers to all non-Union countries.

HEREBY RECOMMENDS THAT MEMBER STATES AND THE EUROPEAN COMMISSION:

1. Take into account the following principles for responsible internationalisation when designing and implementing policy actions to enhance research security:

   (a) continue to promote and defend academic freedom and institutional autonomy, taking into account that research performing organisations are primarily responsible for their international research and innovation cooperation;

   (b) continue to promote and encourage international cooperation in research and innovation that is both open and secure, in line with the principle 'as open as possible, as closed as necessary', ensuring that research outputs are findable, accessible, interoperable and reusable (FAIR), with due consideration to applicable restrictions, including security concerns;

   (c) ensure proportionality of measures: where safeguards are introduced, these should not go beyond what is necessary to mitigate the risks at stake and avoid any unnecessary administrative burden. The objective is to manage rather than to avoid risk;

   (d) steer research security measures to safeguard economic security, as well as Union and national security, and defending and promoting Union values and fundamental rights, academic freedom and research integrity, while avoiding protectionism and political instrumentalisation of research and innovation;

(e) promote self-governance in the research and innovation sector, within the applicable regulatory framework, empowering its actors to take informed decisions, underscoring the societal responsibilities of research performing organisations, taking into account that with academic freedom comes academic responsibility;

(f) adopt a whole-of-government approach, which brings together relevant expertise and skills, ensures a comprehensive approach to research security and fosters coherence of governmental actions and messaging towards the research and innovation sector, including necessary steps to upskill and reskill the relevant workforce;

(g) while pursuing a risk-based approach, adopt policies that are country-agnostic, identifying and addressing risks to research security wherever they emanate from, as that is the best guarantee that a balanced approach to opportunities and risks in the research and innovation cooperation is maintained and that evolving developments in the threat landscape, including the emergence of new threat actors, are not overlooked;

(h) ensure that every effort is made to avoid all forms of direct as well as indirect discrimination and stigmatisation of groups or individuals that could occur as an unintended consequence of safeguarding measures and ensure the full respect of fundamental rights as enshrined in the Charter;

(i) acknowledge the dynamic nature of research security shaped by new insights, evolving risks and geopolitical context, which requires a learning approach with periodical reviews and updates being carried out to ensure that research security policies and related capacity building efforts remain up-to-date, effective and proportionate, and in line with the above mentioned principles.

RECOMMENDS THAT MEMBER STATES, with full regard to subsidiarity, proportionality, institutional autonomy and academic freedom, and in accordance with Member States' national specificities, different starting points, and their exclusive competence regarding national security, without prejudice to the possibility for Member States to go further:

2. Work towards developing and implementing a coherent set of policy actions to enhance research security, making best use of the elements listed in this section.

3. Engage in dialogue with the research and innovation sector with a view to defining responsibilities and roles and developing a national approach, if not already in place, for example through guidelines or a list of relevant measures and initiatives to boost research security with a clear process for implementation, while considering Commission guidance and available tools for support.

4. Where relevant, create a new or reinforce an existing support structure or service, to help actors in the research and innovation sector to deal with risks related to international cooperation in research and innovation. Bringing together cross-sectoral expertise and skills, such a support structure or service could provide information and advice that research performing and funding organisations can use to makeinformed decisions, weighing opportunities and risks of a prospective international cooperation as well as other services for which the research and innovation sector has a clear need, including awareness raising activities and training courses.

5. Strengthen the evidence base for research security policymaking, through analysis of the threat landscape, including from a cybersecurity perspective.

6. Facilitate information exchange between research performing organisations and research funding organisations on the one hand and intelligence agencies on the other hand, for example through classified and non-classified briefings or dedicated liaison officers.

7. Develop or reinforce cross-sectoral cooperation within government, notably bringing together policy-makers responsible for higher education, research and innovation, trade, foreign affairs, intelligence and security.

8. Gain insight into the resilience of the sector as well as the effectiveness and proportionality of the applicable research security policies, including through regular resilience testing and incident simulations, considering where appropriate the support of the Commission.

9. Pay specific attention to international cooperation in domains involving critical knowledge and technology, including those identified by the Commission Recommendation (EU) 2023/2113, and to the outcomes of such collective risk assessments.

10. In order to ensure compliance with the applicable Union export control rules for dual-use items and the restrictive measures adopted pursuant to Article 29 TEU and Articles 207 and 215 of the Treaty on the Functioning of the European Union, take national measures on intangible technology transfer, as well as to strengthen the implementation and enforcement of restrictive measures with relevance for research and innovation.

11. Proactively contribute to the Union's one-stop-shop platform on tackling research and innovation foreign interference by sharing tools and resources developed through public funding with the aim of facilitating the cross-border uptake of these tools and resources and of delivering them in a user-friendly, accessible and secure manner.

12. Engage with the private sector to develop guidance for companies involved in research and innovation, including for research-intensive start-ups, spin-offs and small and medium sized companies. In this regard, attention should be drawn to the existing rules, including those on the control of exports of dual-use items, the screening of foreign investments as well as the ongoing work on the monitoring of outbound investments.

13. Consider, where relevant, and based on risk-assessment, the application of the measures contained in this recommendation to international cooperation activities related to researchers' mobility.

Role of research funding organisations

14. Engage with research funding organisations to encourage them to ensure that:

(a) research security is an integral part of the application process that takes into account the different factors jointly defining the risk profile of the project. The objective is to encourage beneficiaries to considerthe context in which the research and innovation cooperation takes place and which reasons and (hidden) agendas could play a role, ensuring potential risks and threats are identified up front;

(b) research projects selected for funding that raise concerns undergo a risk appraisal proportionate to their risk profile, resulting in agreeing on appropriate risk management while ensuring that the time-to-grant is not unnecessarily delayed, and avoiding any unnecessary administrative burden;

(c) whenever entering into research partnership agreements with foreign entities, including through Memoranda of Understanding, consider possible risks related to international cooperation and include key framework conditions, such as respect for Union values and fundamental rights, academic freedom, reciprocity and arrangements on intellectual asset management, including the dissemination and exploitation of results, licensing or transfer of results and spin-off creation, and provide for an exit strategy to be in place in the event that the conditions of the agreements are not complied with;

(d) when applying safeguarding measures in national funding programmes, those applied in relevant Union funding programmes are taken into consideration;

(e) applicants seek assurance from prospective partners, for projects with a high risk profile, for example through a partnership agreement, taking into account key framework conditions such as those listed in 15(c);

(f) adequate expertise and skills are available within the funding organisation to address research security concerns and that research security is integrated in existing monitoring and evaluation measures, including keeping track of incidents, and taking timely and credible measures in the event of non-compliance.

Support for research performing organisations

15. Encourage and support research performing organisations to:

(a) engage in information exchange, peer learning, development of tools and guidelines and incident reporting among peers, as well as to consider resource pooling to make best use of scarce and scattered resources and expertise;

(b) implement internal risk management procedures in a systematic manner, including through risk appraisal, conducting due diligence on prospective partners and escalation to higher levels of internal decision-making in the event of issues that raise concern, while avoiding any unnecessary administrative burden;

(c) when entering into research partnership agreements with foreign entities, including through Memoranda of Understanding, consider possible risks related to the international cooperation and include key framework conditions, such as respect for Union values and fundamental rights, academic freedom, reciprocity and arrangements on intellectual assets management, including the dissemination and exploitation of results, licensing or transfer of results and spin-off creation, and provide for an exit strategy to be in place in the event that the conditions of the agreements are not complied with;

(d) assess risks related to foreign government-sponsored talent programmes in research and innovation, notably focusing on any undesirable obligations imposed on their beneficiaries, and guarantee that foreign government-sponsored on-campus providers of courses and trainings abide by the host institution's mission and rules;

(e) invest in dedicated in-house research security expertise and skills, assign research security responsibility at the appropriate organisational levels and invest in cyber hygiene and in creating a culture in which openness and security are in balance;

(f) facilitate access to training programmes, including online courses, for new and existing research staff , as well as develop education and training programmes aimed at training security advisers and other relevant actors and at training recruiters and staff dealing with internationalisation to check and detect, as part of a structural vetting process, elements that raise concern in applications for research positions, especially those in research domains involving critical knowledge and technology;

(g) ensure in scientific publications and all other forms of dissemination of research results full transparency of funding sources and affiliations of research staff, avoiding that foreign dependencies and conflicts of interest or commitment affect the quality and content of the research;

(h) introduce compartmentalisation, both physical and virtual, guaranteeing that for areas, such as labs and research infrastructure, data and systems that are particularly sensitive, access is granted on a strict need-to-know basis, and that, for online systems, robust cybersecurity arrangements are in place;

(i) assess risks related to equipment, laboratories and research infrastructure sponsored by or acquired from entities established in or controlled by third countries, notably focusing on any undesirable obligations imposed on hosting organisations;

(j) ensure that all forms of discrimination and stigmatisation, both direct and indirect, are prevented, that individual safety is protected, with particular attention to coercion of diaspora by the state of origin and other forms of malign influence, which could give rise to self-censorship and may have security implications for foreign researchers, doctoral candidates and students involved, and that incidents are reported.

RECOMMENDS THE COMMISSION TO:

16. Make full use of the open method of coordination, notably the ERA governance structures, and support the implementation of this recommendation by raising awareness, facilitating and promoting peer learning, enabling capacity building as well as facilitating consistency of policies; incorporate the content of this reccommendation also in the agendas of relevant strategic platforms and boards.

17. Develop and maintain a Union one-stop-shop platform on tackling research and innovation foreign interference, which aims to consolidate all pertinent data, tools, reports, and other resources developed at Union, national, regional, organisational level, or outside the Union, while ensuring that they are presented in a manner that is both user-friendly, accessible and secure.

18. Support the collection of evidence for policy making in research security and bring together relevant expertise from Member States and stakeholders, as well as explore and assess options for more structural support in this respect, such as through a European centre of expertise on research security, taking into account existing structures and linking it to the one-stop-shop platform, furthermore additional functionalities to support Member States and the research and innovation sector could be added in due time.

19. Enhance, in cooperation with the High Representative of the Union for Foreign Affairs and Security Policy, situational awareness among policymakers by structurally assessing hybrid threats affecting the research and innovation ecosystem.

20. Develop a resilience testing methodology for research performing organisations that can be used on a voluntary basis by Member States with their research performing organisations.

21. Continue its work, in co-creation with the Member States and with involvement of the stakeholders, on assessing risks of critical technologies, as well as engage in a dialogue to ensure information sharing and consistency of approach regarding risk appraisal and research security safeguards in national funding programmes and those in relevant Union funding programmes.

22. Develop tools and resources, both country-agnostic and country-specific, to support research performing organisations to perform due diligence into prospective third country partners.

23. Organise, together with Union-level stakeholder organisations, a biennial flagship event on research security, aimed at sharing information and solution-oriented exchanges.

24. Prepare interpretative guidance, where necessary, on the development of risk appraisal procedures as well as on the application of relevant Union legislation. This applies in particular to export control rules, notably the intangible transfer of technology, the visa requirements for foreign researchers, as well as the interpretation of certain open science and intellectual asset management requirements from a research security perspective.

25. Engage with the research and innovation sector and the Member States to assess how best to increase transparency of research funding sources and affiliations of researchers.

26. Strengthen the dialogue and cooperation with international partners on research security through exchanging information and experience, sharing best practices and seeking ways to align safeguarding measures as well as take into consideration the option of bringing about a common Union voice on the topic in multilateral fora.

Monitoring progress

27. The Commission is invited to monitor the progress made in implementing this recommendation in a transparent way and based on clear indicators, in close cooperation with the Member States and after consulting the stakeholders concerned, using the ERA policy platform, and to report to the Council every two years, as part of its biennial reporting on the Global Approach to Research and Innovation and its existing reporting on the Research and Innovation Framework Programme.

28. In light of the urgently needed joint response, Member States are invited to implement this recommendation and to share with the Commission information on their national approach (referred to in recommendation 3 to the Member States), as input for the aforementioned monitoring and reporting activities by the Commission.

29. After in-depth assessment and in light of the future evolution of the geopolitical situation, further steps and measures can be proposed.

Done at Brussels, …

For the Council
The President