

The President

Mr Radosław Sikorski
Mr David McAllister
Mr Arnaud Danjean
Mr Michael Gahler

D 303479 01.07.2021

Dear colleagues,

Thank you very much for your letter of 11 March regarding the threat of espionage in the European Parliament and the measures in place to mitigate it, especially in the context of the present geopolitical landscape.

I fully share your concerns linked to the geopolitical tensions currently characterising international relations. I am aware that EU Institutions and agencies are more than ever targets of hostile intelligence gathering, disinformation and cyber-attacks, including influence operations and attempts to cultivate EU staff by foreign state and non-state actors. Let me assure you that Parliament has already taken important steps in this regards and will further increase its resilience and preparedness.

The Secretary-General of the Parliament - in coordination with the Secretaries-General of the Commission, of the Council and of the External Action Service - recently mandated its services to reinforce cooperation specifically with respect to hybrid threats.

Moreover, Parliament's ICT Systems Security Board has adopted in 2019 an Information and Communication Technology Systems Security Policy which is fully aligned with the Bureau decision on cybersecurity of September 2015 and the Cybersecurity Strategy of the European Union. It defines the guiding principles for a cybersecurity policy in the EU and internationally. The competent services in the Secretariat organise regular cybersecurity trainings and awareness raising activities. Also, as first in class, Parliament's legal and financial services have developed a cybersecurity-sensitive equipment policy which assists authorising officers in drafting technical specifications and exploiting the tools of the Financial Regulation to avoid the acquisition of connected devices that may be used by hostile actors to interfere or disrupt Parliament's activities.

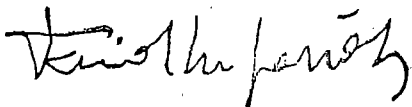
With regard to ensuring personnel security, I would like to inform you that there are procedures applied by Parliament's services to carry out screening protocols with the collaboration of the competent authorities in Member States prior to the hiring of personnel from different categories. Besides, and in order to have access to EU Classified Information (EUCI), staff from the Secretariat and from political groups must obtain a Personal Security Clearance (PSC) granted on basis of a vetting certificate provided from the National Security Authorities (NSA) of their respective Member States.

Additionally, the Secretary-General adopted an information security policy in June 2020, which includes practical guidance on the secure management of sensitive information. Finally, an agreement with the Belgian host state authorities allows security checks to be performed on staff members of Parliament's service providers with access to our premises.

The Secretary-General, in his capacity as Security Authority of the European Parliament, maintains a dedicated capability - with the relevant expertise - in the Business Continuity Management Unit, to coordinate and implement the necessary measures fostering resilience, countering hybrid threats, including malicious acts of cyberattacks and espionage.

I hope that the information provided is useful for you. I invited the Secretary-General to continue his efforts of protecting Parliament against interference and disruption of Parliamentary work by malicious actors.

Yours sincerely,

A handwritten signature in black ink, appearing to read 'David Maria SASSOLI', with a stylized flourish at the end.

David Maria SASSOLI