Briefing
STOA Options Brief

Cybersecurity in the EU Common Security and Defence Policy (CSDP) – Challenges and risks for the EU

The purpose of this policy option brief is to provide the Members of the European Parliament with foresight policy options regarding the enhancement of cybersecurity in the context of Common Security and Defence Policy (CSDP). The policy options are based on the STOA study 'Cybersecurity in the EU Common Security and Defence Policy (CSDP) - Challenges and risks for the EU', which was concluded in May 2017.

As a first pre-requisite for any options proposed in this options brief, it is strongly suggested that the EU Cyber Defence Policy Framework action items identified in the study should be appropriately supported by resources. An overview of these action items is provided in Annex A of the study, their successful implementation being essential to the improvement of cybersecurity in the CSDP. The authors of the study also suggest the use of a capacity maturity model in order to monitor cybersecurity capacity building in the context of the CSDP.

Further to the above, the study proposes additional options based on the following five high-level objectives:

1. Maintenance of coherent cyber policies and strategies across the EU
2. Promotion of the cybersecurity culture
3. Development of cyber-skills through education and training
4. Enhancement of the legal and regulatory frameworks
5. Development of standards, organisation and capabilities.

In the next sections of this brief, these options are analysed and translated into more specific proposals and possible actions.

Policy objective 1: Maintenance of coherent cyber policies and strategies across the EU

Coherence is a major challenge for EU policies regarding cybersecurity. Coherence of policies and strategies should be assured, not only within the CSDP administration, but also across all EU institutions and bodies. CSDP considerations should also be taken into account by EU level cyber stakeholders (institutions, agencies and other bodies) for the coordination and planning of current and future cyber capacities.

Enhance cyber incident response for CSDP

- Develop mechanisms to enhance cooperation regarding information exchange and best practices between EU Member States' military and civilian computer security incident response teams (CSIRTs).
- Pilot the establishment of a cybersecurity rapid response team (RRT) for CSDP missions.
- Plan the development of a computer security incident response team for CSDP classified and unclassified networks.
- Develop cyber standard operating procedures ensuring compatibility between civil and military incident response.

Protect critical infrastructures used by CSDP structures

- Develop policies for critical infrastructure cyber-risk assessment for CSDP headquarters (HQs) and missions.
- Provide the necessary instruments to support Member States and hosting countries of CSDP missions for the cyber protection of critical infrastructure used by CSDP missions.

Enhance EU crisis management processes

- Support the development of the pan European cyber-crisis management system based on the CSIRT Network, established by the directive on security of network and information systems (NIS Directive).
- Develop policies for coordination of efforts between civilian and military structures during cyber-crises.

Improve cyber-defence in CSDP

- Consider cyber-defence as an operational task for CSDP missions and include cyber-defence considerations in CSDP operational planning processes.
- Provide adequate resources for the development CSDP cyber-defence capabilities.
- Sponsor synergies for capabilities development with civilian research and development programmes.
- Develop further collaboration between CSDP operational HQs, other EU cyber stakeholders (e.g. ENISA, EC3) and strategic allies (i.e. NATO) at the operational level.

Improve cyber-resilience of CSDP systems and processes

- Support the interoperability of cyber capabilities of EU and Member State IT systems and services used in CSDP missions (e.g. cryptography).
- Agree on a common set of security measures for cyber-resilience of the EU and Members State IT systems used in CSDP missions.
- Define and agree on specific levels of services for all EU and Member State IT systems used in CSDP.

Policy objective 2: Promotion of cyber-culture

The human factor and the importance of responsible behaviour in the cyber domain is often overlooked in favour of building new technical capabilities. It is a fact, though, that an overwhelming percentage of successful cyber-attacks are due to human error. Moreover, communities at national, EU and international level should invest in building trust in mechanisms against cyber-threats and confidence in emerging technologies such as social media and the internet of things. Promoting a responsible cyber-culture should receive a higher priority in Europe's efforts to achieve a safer cyber-space, including in CSDP.

Promote a cybersecurity mind-set for CSDP

- Establish cybersecurity awareness campaigns for CSDP command structures.
- Establish an information-sharing network between EU agencies, bodies and institutions.

Build trust and confidence

- Establish a minimum level of trust required in the CSDP context between:
    - EU bodies, institutions and Member States.
    - EU and international organisations (e.g. NATO, Organization for Security Co-operation in Europe (OSCE), United Nations (UN).
    - EU and third countries hosting CSDP missions.
- Sponsor confidence-building measures between:
    - EU bodies, institutions and Member States.
    - EU and international organisations (e.g. NATO, OSCE, UN).
    - EU and third countries hosting CSDP missions.

Protect the identity and privacy of CSDP staff

- Develop measures to safeguard the privacy of CSDP staff according to the General Data Protection Regulation (GDPR).
- Develop measures to protect the identity of CSDP staff during missions.
- Develop awareness campaigns for CSDP staff on privacy, data and identity protection.

Consider advanced uses of social media for CSDP

- Develop policies on social media usage for CSDP staff.
- Leverage social media to the benefit of CSDP missions (trust building, promotion, social feedback).
- Strengthen the use of social media open source intelligence for CSDP missions.

Policy objective 3: Development of cyber-skills through education and training

Development of cyber-skills should be a continuous process. The continuous evolution of cyber-threats requires up-to-date personnel to handle today's sophisticated cyber-capabilities. In the CSDP context, education and training should be viewed not only as a development of cyber-competencies but also as another aspect of operational training.

Develop further cyber-competencies

- Consider the development of an EU-wide cyber-defence education and training framework providing training standards career paths and certification requirements for cyber-duties at the operational, technical and tactical levels of CSDP structures.
- Develop cybersecurity training paths/requirements for cyber-duties for CSDP HQs.
- Make use of technical training opportunities offered by EU agencies and institutions.
- Explore NATO's cyber-defence education and training opportunities and synergies for CSDP operational planners.

Introduce cyber into exercises and operations

- Integrate cyber into existing operational exercises (planning, execution, evaluation, lessons learned).
- Consider the involvement of CSDP operational HQs in future pan-European cybersecurity exercises (such as Cyber Europe).

Policy objective 4: Enhancement of the legal and regulatory frameworks

Enhance cybersecurity legislation

- Future revisions of the NIS Directive should include CSDP considerations.
- Provide the operational commanders/directors with legal support for cyber-defence options during CSDP missions.

Coordinate law enforcement for cyber-crime

- Enhance collaboration of CSDP administration with cyber-crime authorities within and beyond the EU borders, for law enforcement challenges in the CSDP context, attribution information and cyber-crime related incidents.
- Stimulate CSDP staff awareness about cyber-crime threats in general, as well as in the context of CSDP missions.

Develop cyber-norms and confidence-building measures

- Provide CSDP inputs to EU-wide discussions and initiatives on the development of cyber-norms.
- Support confidence-building measures for cyber-intelligence sharing between relevant EU stakeholders.

Promote international cooperation on legal issues

- Engage in a discussion on attribution and cyber-intelligence information exchange with international organisations defining a set of minimum requirements.
- Promote dialogue between EU bodies and institutions and international organisations on legal challenges related to cyber-conflicts.
- Consider legal issues for the inclusion of cyber considerations in agreements between the EU and third countries hosting CSDP missions.

Promote private-public sector cooperation

- Enhance the regulatory frameworks for cooperation between the private sector and CSDP HQs for the delivery of cybersecurity services.

Policy objective 5: Development of standards, organisation and capabilities

This option relates to developing those technical capabilities and the required supporting mechanisms to enhance cybersecurity. Standards and capabilities mainly concern the operational and technical level, while the organisational measures concern the whole of CSDP administration.

Develop/adopt common standards

- Produce/adopt common cybersecurity standards in the EU area for classified and unclassified networks.
- Adopt a common cyber-taxonomy for CSDP.
- Produce and adopt specific cybersecurity standards/requirements for military systems (C4ISR) used in CSDP missions.
- Include CSDP considerations in the EU ICT standardisation processes.

Improve cyber-defence organisation in CSDP

- Regularly monitor cybersecurity capacity building in the context of the CSDP using a capacity maturity model, such as the Cyber Security Capability Maturity Model (CMM).
- Develop a permanent cyber-defence organisational structure within CSDP.

Enhance the cyber-defence capabilities for CSDP

- Establish a cyber-threat assessment capability.
- Establish a cyber-resilience assessment capability for CSDP HQs.
- Develop a technical cyber-intelligence capability.
- Integrate the cyber-threat landscape into CSDP missions' common operational picture (COP).
- Develop well-defined cyber-defence perimeters for classified and unclassified networks (centrally managed, monitored and protected).
- Develop a collaboration capability between military CSIRTs and the CSIRT Network.

Conclusions

Ongoing EU work stemming from the EU Cyber Defence Policy Framework action items should be supported and shaped with the appropriate resources. Their successful implementation is essential to the improvement of cybersecurity in EU CSDP.

Measuring progress and maturity is essential for the efficient allocation of resources. Therefore, the authors propose the **use of a capacity maturity model**, such as the Cyber Security Capability Maturity Model (CMM), in order to monitor the cybersecurity capabilities of the CSDP.

Coherence is a major challenge for EU policies on cybersecurity. **Policy and strategy coherency** should be assured not only within the EU CSDP administration but also across all EU institutions and bodies.

An overwhelming percentage of successful cyber-attacks are due to the human factor rather than technical issues. **Promoting a responsible cyber-culture** should receive a higher priority in Europe's efforts to achieve a safer cyber-space, including CSDP. Another key element concerning the maturity of CSDP cybersecurity is trust. The study proposes the **fostering of as many trust-building activities** between stakeholders as possible, from events, workshops and exercises to partnerships and common projects.

The continuous evolution of cyber-threats requires up-to-date personnel to handle the increasingly sophisticated cyber-challenges. The **development of cyber-skills** in the CSDP context should be a continuous process integrated with operational training.

Finally, it is recommended that a **permanent cyber-defence administration for CSDP** should be developed and funds invested in **technical capabilities** based on **common standards and cyber-taxonomy across the EU.**

This document is based on a STOA study on 'Cybersecurity in the EU Common Security and Defence Policy (CSDP) – Challenges and risks for the EU' (PE 603.175) published in May 2017. The study was carried out by the European Union Agency for Network and Information Security (ENISA) at the request of the Science and Technology Options Assessment (STOA) Panel and managed by the Scientific Foresight Unit (STOA), within the Directorate-General for Parliamentary Research Services (DG EPRS) of the European Parliament. Authors: Panagiotis Trimintzios, Georgios Chatzichristos. STOA administrator responsible: Zsolt G. Pataki. The study can be found at http://www.europarl.europa.eu/stoa/.