European Union
EXTERNAL ACTION

European Union Military Staff

Official document of the European External Action Service

of 15/09/2021

EEAS Reference	**EEAS(2021) 706 REV4**
Distribution marking/ Classification	**LIMITE**
From **To**	**European Union Military Staff (EUMS)** **European Union Military Committee (EUMC)** **CSDP/PSDC; EUMC**
Title / Subject	**European Union Military Vision and Strategy on Cyberspace as a Domain of Operations**
[Ref. prev. doc.]	

AO: LtCDR Jerome DAEMS Tel. 02 584 57 28
EUMS CIS& CD Directorate / Policy & Requirements Branch

Delegations will find attached the EU Military Vision and Strategy on Cyberspace as a Domain of Operations, which was agreed by the EUMC on 15 September 2021, subsequent to a silence procedure.

European Union
EXTERNAL ACTION

European Union Military Staff

Official document of the European External Action Service

15 September 2021

European Union
Military Vision and Strategy
on
Cyberspace as a Domain of Operations

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

INTRODUCTION

1. The European Union's (EU) firm commitment to implement the agreed EU Level of Ambition (LoA) in response to external conflicts and crises is executed through the EU Common Security and Defence Policy (CSDP). CSDP is an integral element of the EU's Common Foreign and Security Policy (CFSP) within the framework of the European Union Global Strategy (Ref. A) in the area of security and defence. In order to enhance EU capabilities to act as a global security provider, to ensure strategic autonomy, and to strengthen capabilities needed to cooperate with partners and engage across all operational domains, EU CSDP must embrace all the relevant aspects to military operations and missions, including the challenges of cyberspace.

2. Within the EU Cyber Defence Policy Framework (CDPF) 2018 Update (Ref. J) EU Member States acknowledged that cyberspace is the fifth domain of operations, alongside the domains of land, sea, air, and space. Therefore, the framework provides guidance to develop EU Cyber Defence (CD) policy further and supports the development of CD capabilities of EU Member States (EU MSs) as well as increasing the level of protection of EU security and defence infrastructures against cyber threats. The framework further outlines that the successful implementation of CSDP is increasingly depending on uninterrupted access to and secure use of cyberspace, and thus requires robust and resilient operational capabilities in cyberspace. Thus, the full implementation of cyberspace as the fifth domain of operations and the effective integration of this operational domain into EU CSDP military operations and missions constitute a key element of success. Furthermore, with the approval of Strategic Implementation Plan for the Digitalisation of the EU Forces[1], it has been recognized that one of the key factors on which the success of military operations and missions will depend is the freedom of action (FoA) in cyberspace. EU Forces must integrate cyberspace into a coordinated crosscutting domain approach in order to contribute to the joint operational factors[2].

3. The availability of cyber resilient networks and systems and the availability, confidentiality and integrity of the data stored, transferred and processed by them, regardless of their military or civilian origin, are vital for the security of the EU within as well as beyond its borders. This also applies to the security of EU CSDP military operations and missions conducted by the EU to ensure peace and stability in the wider region and globally, as highlighted in the EU Global Strategy. It is therefore essential to be able to count at all times on robust digital service providers which will continue to be strengthened by the implementation of the directive on the Security of Networks and Information Systems in the Union (NIS Directive) (Ref. B) as far as possible and where appropriate.

[1] ST. 9058/20 dated 24 June 2020. The document states that EU Forces to be made available to the EU by Troop Contributing Nations (TCN) and/or international organisations are to meet the requirements of the EU-led military operations and missions, including the EU HQs and C2 structures.
[2] The factors are Forces, Environment, Time and Information.

4. State and Non-State actors are increasingly aiming to meet their geopolitical goals not only through conventional means and tools like military force, but also especially through the exploration of the cyberspace by all available means. The Joint Communication to the European Parliament and the Council on EU's Cybersecurity Strategy for the Digital Decade, JOIN (2020) 18 final (Ref. Q), reemphasizes that the use of cyberspace as a domain of warfare is now widely acknowledged. Consequently, to protect and defend EU CSDP military operations and missions, which become more and more exposed to these fatal risks, the EU must improve substantially and vigorously its CD capabilities. This EU Military Vision and Strategy is to lead the way in this effort.

AIM AND SCOPE

AIM

5. This document sets the framework conditions and describes the ends, ways and means needed to use cyberspace as a domain of operations in support of EU CSDP military operations and missions.

6. Furthermore, it aims to integrate cyberspace into all aspects of EU CSDP military operations and missions, by researching and developing the capabilities required at the appropriate levels of authority, permanently or on purpose for an operation or mission.

7. Lastly, the document intends to raise awareness and understanding of cyberspace, being a crosscutting domain. It does so by driving all activities to implement the required cultural shifts, enhanced processes, capability developments, organizational adaptations, and cyber skills.

SCOPE

8. This EU Military Vision and Strategy addresses all military elements of the EU CSDP cyberspace, within the scope of EU CSDP policies and the EU Cyber Defence Policy Framework (CDPF). It takes into account the interlocking of civil and military elements of CSDP through civil and military CSDP operations or missions often conducted in a mutually supportive and integrated setting in line with the EU Integrated Approach (IA) to crisis management. Furthermore, it underlines the continuous need to defend the military information systems of EU, permanent and ad hoc, within or outside of the EU territory.

9. The main emphasis of this document is on military operations and missions outside of the territory of the EU, in accordance with the Treaty on European Union (TEU) (Articles 42 and 43). However, it does also apply to all elements of EU CSDP that are located within the EU territory, such as Headquarters (HQ), Communication and Information Systems (CIS) infrastructures and digital service providers which contribute to the planning, execution and (reach-back) support of EU CSDP military operations and missions. It further reflects the required coherence with EU MS

national assets and other national contributions supporting EU CSDP military operations and missions, understanding that the employment, protection and defence of these assets is a national responsibility and prerogative.

10. Furthermore, it acknowledges that attribution of cyber-attacks in and through cyberspace remains a political responsibility assumed at national level or through a consensus in EU.

11. This EU military vision and strategy takes appropriate cognizance of the Joint Communication to the European Parliament and the Council on EU's Cybersecurity Strategy for the Digital Decade, JOIN (2020) 18 final (Ref. Q), the Council conclusions on the Implementation of the Joint Declaration (Ref P). Furthermore, the Commission Recommendation on Coordinated Response to Large Scale Cybersecurity Incidents and Crises – Blueprint (Ref. H), the Network and Information Systems Security (NIS) Directive (Ref. B), and the Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities (Ref. F) are reflected were needed.

12. Due to its overarching nature, it sets the framework conditions for the development of additionally required EU military concepts, plans, policies, and standards, and the revision of existing documents.

OPPORTUNITIES AND CHALLENGES OF CYBERSPACE

13. Cyberspace interconnects a large variety of entities, which may be employed to maximize and multiply effects in other domains. This interconnected nature of cyberspace, together with the rapid digitalization of military platforms and weapon systems, developments of advanced technologies create a constantly shifting terrain, which makes present and future operational environments volatile, uncertain, complex and even more ambiguous.

14. Adding to this complexity and thereby increasing cybersecurity risks, the quickly expanding Internet of Things (IoT), with millions of ICT solutions and services embedded and functioning in various Operational Technology (OT)[3] in support of human needs, has become a factor also to be considered in EU CSDP military operations and missions.

15. The emergence of new innovative technologies, featured by the duality of their use and thus subsequently increasing application within operational context will offer unmatched opportunities but also may be used against the EU. In particular, faster and smarter networks will play a central role in achieving the digital transformation of the EU, with 5G and further generations having the potential to enable and support a wide range of applications and functions. Artificial Intelligence (AI)

[3] Interconnected systems and data analytics, Supervisory Control and Data Acquisition (SCADA), Industrial Control Systems (ICS), Industrial Internet of Things (IIoT) and smart sensors. OT is the hardware and software that keeps things, for instance critical infrastructures running.

enhanced capabilities will open unprecedented opportunities but also open new attack vectors in cyberspace. Quantum computing and other cutting-edge technologies will lead to opportunities and challenges not yet fully visible. This will create new cybersecurity threats and opportunities on top of the existing ones, which need to be anticipated and managed to prevent unacceptable risks.

16. EU CSDP military operations and missions' reliance on digital Commercial Off-The-Shelf (COTS) solutions also represents a risk factor, e.g. through obsolete hard- and soft-ware in military systems without sufficient cybersecurity support or technological backdoors deliberately created for covert cyber operations. Therefore, special attention must be paid to supply chains[4] for cyber related technologies and products in order to ensure a better understanding of the related cyber risks and how to mitigate them.

17. Along with this goes an increasing tendency by potential adversaries to exploit the opportunities and developments in the cyber domain to take full advantage of the widespread availability of advanced ICT.

18. EU objectives in military CSDP are put at risk significantly through strategically planned, well-resourced, and covertly executed cyber-attacks aimed to gain strategic impact without EU detection (and thereby without the chance to apply effective counter-measures). Thus, the EU must understand and recognize that its organizations, headquarters, forces and supporting elements are constantly tested and under attack.

19. These attacks undermining not only military mission success, but more importantly diplomatic, economic, and also social cohesion of the entirety of all relevant stakeholders to a mission, often span over more than one operation/mission, civil or military, affect EU institutions and/or EU MS installations as well as military forces in an EU CSDP operation or mission.

20. Exploiting the opportunities of cyberspace for EU CSDP will further increase the need for skilled personnel for ICT management, administration and security and will therefore exacerbate the human resource challenge the EU faces.

21. It is therefore essential to understand that the manifold opportunities of cyberspace correspond with the related challenges, and risks, with all entities in cyberspace potential targets, and that the vulnerability of EU CSDP military operations and missions in cyberspace directly relate to their dependence upon cyberspace.

22. Cyberspace Operations (CO) are often conducted long before the use of lethal means. This offers new opportunities for crisis response below the threshold of military conflict but also adds to the challenges of dealing with crisis response, in particular in hybrid scenarios, where Cyberspace Operations have become a common feature.

[4] Cf SolarWinds hack. The original cause of the incident was a supply chain weakness. The integrity and security of supply chains is critical.

CYBERSPACE AS A DOMAIN OF OPERATIONS

23. To establish cyberspace fully as the fifth domain of operations, crosscutting through the other domains of operations, the understanding of the interdependencies of this domain with the other domains and the subsequent and consistent implementation of the required cultural shifts, enhanced processes, capability developments, organizational adaptations, and cyber skills, are essential. Potential adversaries often operate in cyberspace, which fundamentally changes the operational environment.

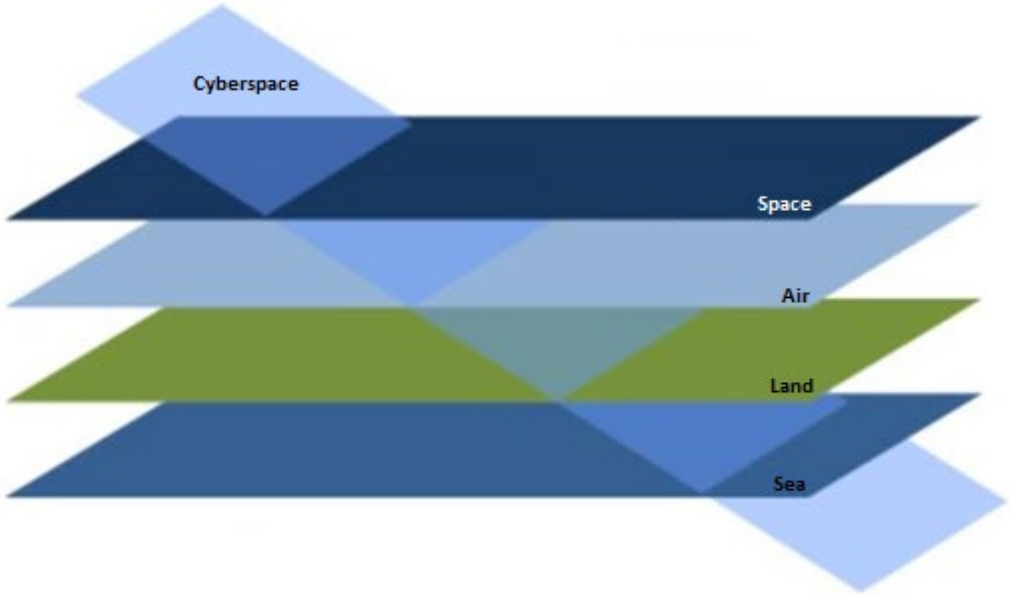

Figure 1:

Cyberspace domain of operations and substrate of Space, Air, Land and Sea

24. With military platforms and weapon systems of all domains and communication and information systems (CIS) closely connected and interacting through cyberspace, commanders of EU CSDP military operations and missions are increasingly dependent on the confidentiality, the integrity and the availability of military networks and systems and associated data and information to ensure information assurance as a prerequisite for mission assurance.

25. Thus, freedom of action across cyberspace plays a decisive role for EU CSDP military operations and missions' success. However, information assurance is considered to be under continual stress, with potential adversaries continuously

testing EU CSDP Command and Control (C2) capabilities, networks and systems and related CD capabilities.

26. Furthermore, lines between civilian and military security blur, especially in cyberspace, and even more so where adversarial state and non-state actors use cyberspace to exert influence, project power and disrupt EU interests in CSDP.

27. The digitalization of the battlefields, with cyberspace as a domain of operations, which by its very nature cannot be limited in geographic terms, leads to new challenges for EU military commanders to establish and maintain information assurance and achieve decision superiority as a critical enabler for mission assurance. Consequently, their recognition of the battlefield must fundamentally change and the planning for and the implementation of EU CSDP CO needs to consider the implications of cyberspace for all other domains, while anticipating the effect on and the dependencies from the civil elements of CSDP.

28. Therefore, cyberspace, which comprises of the distinct but interrelated physical layer, logical layer and cognitive layer, cannot be considered independently but is one facet of the triad: cyberspace, electromagnetic environment and cognitive Environment.

29. A new look at the digitalized battlefields of today is required as well as a forward-looking anticipation of the battlefields of the future and a review of EU CSDP CO. In this context, opportunities and limitations for the prevention of cyber-attacks and for the conduct of defensive operations need to be explored and respective capabilities implemented, in order to be ahead of potential adversaries and to protect EU military operations and missions in cyberspace.

30. Finally, to achieve unity of effort, technical and procedural interoperability and improved effectiveness in the provision of persistent levels of readiness and resilience in the cyber domain, stronger efforts in the harmonization and standardization, and where applicable, the centralization of EU military CSDP cyberspace capabilities, wherever possible, is required.

VISION *(ENDS)*

31. Ahead of all other considerations, the international law, including the UN Charter in its entirety, international humanitarian law, international human rights law, and the law of armed conflict apply in cyberspace. In that regard, these laws and the established principles of necessity, distinction and proportionality bind all EU CSDP military operations and missions stakeholders. Furthermore, commanders are to conduct any action in cyberspace in accordance with the operation mandate, and under commonly agreed Rules of Engagement (RoE).

32. To use cyberspace as domain of operations in EU CSDP, all stakeholders, in particular all EU institutions, bodies and agencies, EU Framework Nations[5], EU MS and EU partners involved in EU military CSDP operations and missions contribute in their respective area of responsibility. In order to ensure a comprehensive perspective to this challenge, the European Union's military vision for cyberspace as a domain of operations is tri-fold:

    A. The EU is able to accomplish its objectives[6] in the cyberspace domain as effectively as it does in the other domains in order to execute EU CSDP military operations and missions.

    B. The EU has effectively integrated cyberspace into EU CSDP military operations and missions planning and conduct, established an effective and consistent cyber resilience and cyber deterrence against potential adversaries, including international cooperation with partners[7] in support of CD of EU military CSDP.

    C. The EU, in line with its integrated, cross-domain approach to EU crisis management, has achieved effective civil-military synergies in EU CSDP, reflecting the close interlocking of civilian and military CSDP Operations and Missions, the dual-use nature of cyber tools and technologies as well as the blurring of lines between civilian cybersecurity and military CD.

STRATEGY

33. This European Union's military strategy aims to establish and empower the prerequisite capacities and capabilities in order to implement and use cyberspace as a domain of operations in support of EU military CSDP, acknowledging implications for all other domains of operations.

[5] See EU Framework Nation Concept (Ref. K)
[6] See EU Global Strategy and related Council Conclusions
[7] In an inclusive way for all EU MSs.

CONCEPT *(WAYS)*

34. To implement the EU's military vision for cyberspace as a domain of operations, seven complementary ways are required, which can only be achieved through a unified effort of all stakeholders in EU CSDP:

A. Ensure the achievement of the EU's strategic objectives in CSDP military operations and missions, through effective and interoperable cyberspace capabilities, and through appropriate organizations and personnel capable of handling the full range of cyber threats.

B. Integrate cyberspace as a domain of operations into EU CSDP military operations and missions, through the mainstreaming of cyberspace aspects into the full scale of EU crisis prevention and management, in particular by providing situational awareness, early warning, advance and crisis response planning, while strengthening the EU autonomous analysis capacity in order to better inform the decision-making processes.

C. Protect and defend cyberspace of EU CSDP military operations and missions, through the building and maintaining of effective cyber resilience of networks and systems.

D. Ensure effective and consistent cyber deterrence against potential adversaries of EU CSDP military operations and missions, through the coordinated and prioritized establishment, employment and communication of effective EU cyber defence capabilities, in line with the Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities.

E. Ensure EU military CSDP unity of effort in cyberspace, through effective civil-military relationships and synergies in line with the integrated cross-domain approach to EU crisis management.

F. Strengthen the sustainability and interoperability of EU CSDP military operations and missions in cyberspace, through a deepened cooperation with international partners in the development, sharing and mutually supportive employment of cyberspace capabilities, in particular with NATO. Any cooperation has to respect the inclusiveness of all EU MSs and the decision-making autonomy principle of the EU.

G. Ensure EU state of the art cyberspace capabilities (for CO as well as for CD), resilience and sovereignty through joint, combined and coordinated research and development of technologies to encounter cyber threats.

CAPABILITIES AND CAPACITIES *(MEANS)*

35. To implement and use cyberspace as a domain of operations, a comprehensive set of means is required. These means are mutually supportive and closely interlocked capabilities, which contribute to the building of required capacities. Several of the means contribute to more than one of the seven ways and therefore are not directly linked to specific ones.

36. The sum of entire means of this strategy, and not one or a few in isolation, and all implemented in a coordinated fashion, will contribute to a more stable and secure cyberspace in the context of EU CSDP military operations and missions.

A. Cyberspace Cultural Adoption

37. First is the recognition that adversary behavior in cyberspace is intentionally set below the threshold of armed aggression and that it often aims to achieve strategic effects. To implement the required cultural shifts for success in EU CSDP cyberspace it is essential to establish a broader acceptance that EU CSDP stakeholders must be prepared to continuously adapt and respond to the evolving cyber threat landscape. There is no true "end-state" – there is a new situation and a new threat out there every day.

38. It is therefore essential to understand adversarial cyberspace operations for what they are – generally well thought out campaigns seeking to degrade or even suppress EU capacities and actions in CSDP, while avoiding significant EU reaction and to be seen as an important trigger and hence step forward in the EU thinking the cyberspace. Consequently, new approaches are required to operate purposefully and safely in cyberspace. These approaches notably emphasize the linking of resiliency, defensive actions and, in this context, to deter potential opponents in a seamless strategic and operational framework. They require the development of appropriate processes and capabilities to ensure rapid and targeted response, with due consideration of the EU cyber diplomacy toolbox.

39. Success in each of these elements flows from having the initiative to anticipate where critical EU vulnerabilities lie. Hence, through the application of resiliency and defensive actions and if possible through cyber deterrence in combination with technological advantage (i.e. R&T of future technologies) against adversarial actors, it is foreseen to reduce the potential threat of opening EU vulnerabilities. Herewith, EU is capable to encounter adversarial actions by blunting and mitigating those before affecting EU military networks and systems. It is therefore the implementation

of these components of the strategy, which will lead to a more stable and secure EU CSDP cyberspace.

40. The imposing challenge for EU CSDP leadership is to take clear ownership of these required cultural shifts and to implement and enforce strategies to guide this effort so that it creates and sustains the required effects at all levels (political, strategic, operational, tactical).

B. Implementation of Cyberspace Operations (CO) Capabilities

41. EU institutions, bodies and agencies, EU Framework Nations, EU MS and EU partners involved in military CSDP operations and missions and EU commanders need to establish an EU military CSDP capability coordination and transition instrument to coordinate and expedite the implementation of existing as well as newly researched and developed CO capabilities. Such capabilities, identified through EU Capability Development Process (including EU Headline Goal Process HLGP)), which development is facilitated by the European Defence Fund (EDF) or the Permanent Structured Cooperation (PESCO) cyber projects, need to be quickly reflected in EU concepts and fielded in operations and missions[8], including effective operational testing and training. The Nations on voluntary basis will provide capabilities associated with CO.

C. Integration of Cyberspace into Advance and Crisis Planning

42. EU MS, EU institutions, bodies and agencies, EU Framework Nations and EU partners involved in military CSDP operations and missions and EU commanders are obliged to conceptually integrate cyberspace implications in CSDP crisis response planning, including the establishment of a cyber-threat early warning mechanism.

43. Those cyberspace implications are of a strictly defensive nature but require a proactive approach with an emphasis on early detection capabilities and timely information exchange in order to anticipate intentions of adversaries and prevent damages or limit the impact of potential cyber-attacks.

D. Cyber Defence Management & Evaluation Regime

44. EU MS, EU institutions, bodies and agencies, EU Framework Nations and EU partners involved in military CSDP operations and missions as well as EU commanders need to establish a standardized and consistent cyber risk management organization and process, including a systematic assessment of system vulnerabilities, attack vectors and entry points for cyber-attacks and cyber incidents. This includes the definition of security levels and the implementation of the required technical and organizational security measures to mitigate these

[8] Cyber capabilities in support of EU CSDP military operations and missions would need to be assessed for eligibility for European Peace Facility (EPF) funding.

challenges and encompasses the establishment of an evaluation regime for HQs CD organizations[9] to determine and promote the fulfilment of these requirements.

E. NIS Directive for the Military Domain

45. EU CSDP military operations and missions' stakeholders will improve the cooperation with the European Union Agency for Network and Information Security (ENISA) in accordance with ENISA's mandate.

46. An analysis is required to ensure the needs-based appreciation of the revised Directive on the Security of Network and Information Systems (the "NIS Directive") in the military field, taking into account the specific framework conditions of EU CSDP military operations and missions.

47. Although it is primarily designed to build resilience by improving national civilian cybersecurity capabilities and fostering better cooperation between EU MSs, core components of this EU-wide cybersecurity law are suitable to improve the cyber resilience and responsiveness of EU CSDP military operations and missions. The implementation of the NIS Directive therefore plays a key role in stepping up both operational cooperation and crisis management across the EU, including CSDP.

F. Strong EU Cyberspace Skills Base

48. Effective response to cyber threats against EU CSDP military operations and missions relies on the individual skills of the cyberspace personnel and on ensuring a common EU CSDP cyberspace situational awareness. There is a strong Education, Training and Exercise (ETE) dimension to both civilian cybersecurity and military CD since military and civilian missions are often interlinked and interdependent and conducted in neighboring geographic areas.

49. Therefore, EU Cyberspace ETE must be developed at all levels, starting from regular training of a cyberspace personnel, additional cybersecurity training for all ICT specialists, specialized training for the existing CO capabilities and new specific and harmonized cybersecurity curricula. Herewith interoperability and resilience of EU CSDP operations and missions, both civilian and military, will increase significantly.

50. EU cyberspace ETE should not be limited to IT professionals only. The aim is to mainstream ETE in curricula for other areas, such as operations planning and conduct, system engineering, information management, legal, as well as for sector-specific education tracks. Furthermore, more skilled/trained personnel is required to ensure the required level of administration, maintenance and security due to the

[9] Mainly comprising of an active Cyber Defence Cell (CDC) within the HQs standing organization, led by the J3, providing advice and expertise on all cyber defence matters to the OpCdr, and a generally dormant Cyber Working Group (CWG) with representatives from all branches of the HQ. The CWG may be convened in case of large cyber events/incidents to mitigate the on-going threats, with the support of the CDC.

increased complexity of cyberspace generating a growing demand for a stronger engagement with academia.

51. The latter applies particularly to military leaders and decision makers that – apart from their domain of operation – require strong cyber skills to be able to appropriately assess and incorporate cyber effects. Military leaders as well as decision makers should therefore be aware of cyber domain implications in their area of responsibility.

52. EU Cyberspace ETE efforts need to be better utilized and coordinated, thus enhancing the educational quality delivered. In particular, training courses and exercises with a special focus on military strategic and operational aspects of cyberspace need to be provided regularly (e.g. Exercise Cyber Phalanx).

53. Furthermore, the principle of pooling and sharing must be utilized to the most extent possible, across the civil-military domains and across organizational boundaries, including international partners, in particular with NATO, in an inclusive way for all EU MSs, ensuring interoperability and mutual support.

54. Therefore, an EU Cyberspace ETE coordination capability needs to be established to ensure the required unity of effort. This capability shall encompass all relevant EU institutions, bodies and agencies, HQs and EU MS education and training installations, which provide services in support of EU CSDP.

G. Information Sharing

55. A critical component of CO is information sharing of relevant and timely threat analysis information from a variety of open and classified sources in an evolving threat environment, within and across all operations/missions, both civil and military. The building and continuation of a robust/reliable network of trusted entities and individuals is paramount. Hence, HQs conduct CO effectively and align operational intent and actions as required, allowing their EU commanders to gain or maintain an advantageous position and decision superiority against offensive actions in cyberspace and to provide CD capabilities for their operation/mission. Therefore, in order to effectively share and fuse cyber-specific information and relevant inputs from other sources such as intelligence, a permanent and federated cyber information sharing and fusion framework, together with applicable processes, procedures and technical capabilities, is required.

56. Coordination with and use/integration from already existing capabilities developed for the same purpose must be considered at all times in order to save resources.

H. Cyberspace Situational Awareness and Situational Understanding (CSASU)

57. The EU Cyber Defence Policy Framework provides guidance on cyberspace situational awareness, but requires further developing to CSASU in order to reflect all aspects of the cyber threat.

58. A rapid and shared understanding of cyber threats and incidents as they unfold is a prerequisite of CSASU. This requires a commonly recognized Cyber Defence Operational Picture (CDOP), which visualizes the key factors within the cyberspace affecting the CSDP mission or operation supporting military planning and execution. This entails assuring that appropriate processes are in place to share and process accurate cyberspace situational awareness information and quickly inform commanders and staff about cyber incidents or on-going cyber-attacks.

59. This information needs to be exchanged across all EU CSDP operations/missions and made available to all levels of command – tailored as required. Therefore, this information exchange requires the effective involvement of all relevant actors – EU institutions, bodies and agencies, EU HQs and forces, as well as EU MS – at strategic, operational and tactical levels, with the main emphasis on push instead of pull of information and the ability to quickly assess the impact on the operations/missions and to react accordingly.

I. Cyber Resilience

60. Cyber resilience is critical to preserving the EU's capability to conduct CSDP operations and missions and to maintain freedom of actions and decisions and linked to intelligence on cyber capabilities of potential adversaries. Strong cyber resilience requires a fast and effective response to cyber threats and incidents at any given point in time.

61. This calls for robust structures and procedures in order to mitigate impacts and to promote trust in the ability to respond effectively to cyber threats and incidents and mutually assist partners in cyberspace. It also requires a more comprehensive, cross-policy approach to building cyber resilience and cyber strategic autonomy, understanding that the EU needs to advance its own technological capabilities and capacities in the cyber domain.

62. The focus of cyber resilience must expand from information assurance to the wider perspective of mission assurance, to be able to understand how EU CSDP military operations and missions rely on cyberspace, including framework and HQs' host nation infrastructure, reach-back capabilities and supporting functions.

63. EU Framework Nations, involved EU institutions, bodies and agencies and EU commanders must establish a coordinated operation and mission mapping, joint planning and risk management as well as a common recognized CDOP to improve cyber resilience and maintain mission assurance, including C2.

64. Furthermore, standardized certification of security services and products according to common evaluation criteria will improve a sound supply of security products and services for EU military CSDP. These are key points to foster cyber resilience as well as interoperability of systems, forces, and EU MS.

J. Protection and Defence of Military Networks and Systems

65. Static and deployable military networks and systems as well as supporting CD assets are essential for mission assurance. They need to be protected and defended in a federated and fully coordinated manner. Therefore, the existing EU MilCERT cooperation must be fostered and effectively used to protect static and deployable EU military networks and systems.

66. Furthermore, it is vital to setup and maintain Cyber Rapid Response Teams (CRRTs)[10], which are on standby to assist - on request - EU CSDP military operations and missions HQs and forces, in the handling of cyber threats and incidents. The use of these CRRTs has therefore to be considered at an early stage of the Force generation process.

K. Military Organizational Structures

67. C2 of EU CSDP military operations and missions, in or through cyberspace, requires an appropriate organizational structure, adequately reflecting CD requirements. To support such C2, a standing and centralized EU military cyber coordination element needs to be established.

68. The establishment of this coordination element and a closer cooperation in EU CSDP CD all relevant actors will also contribute to improved EU-level cyber situational awareness. It will further create direct and substantial benefit to all EU CSDP military operations and missions.

69. The new coordination element must therefore be able to merge and analyze information from various sources out of cyberspace and related domains allowing appropriate decision making, well orchestrated and timely response and actions in case of cyber incident or attack.

70. Furthermore, it is essential to implement adequate organizational adaptations in all EU HQs to ensure cyber related assessments and decision support capabilities to the respective military CSDP operations and missions.

L. Interoperability

71. In promoting technical and procedural interoperability between EU military CSDP organizations and all EU MSs as well as between the EU and partners (in particular with NATO) in the cyber domain special consideration has to be given to develop and provide cyber resilient capabilities in line with the multi-national Federated Mission Networking (FMN) Framework Initiative[11].

[10] CRRTs includes, but is not limited to, the "Cyber Rapid Response Teams and Mutual Assistance in Cyber Security", initiated within PESCO framework.

[11] The implementation of FMN in EU military CSDP is carried out with full respect of the principles of inclusiveness and the decision-making autonomy of the EU and under the condition that all EU MSs can join a CSDP operation/mission and operate implemented CIS as agreed.

72. The FMN framework provides the multinational agreed standards for the rapid and interoperable instantiation of CIS operations and missions' networks, to solve interoperability challenges and to enable the rapid provision of cyber resilient CIS services in support of CSDP. This is of particular importance in EU military CSDP, with its non-fixed C2 structures and different CIS solutions for each operation or mission with an increasing complexity of their interconnections and increasing interaction with non-EU partners.

73. To ensure this, all CSDP networks need to be fully FMN-compliant. The simultaneous activation and build-up of Operations Headquarters (OHQ)/Mission Headquarters (MHQ), Force Headquarters (FHQ) and, if applicable, Component Command Headquarters (CCHQs), in a multinational environment will, with regards to reducing deployment times and ensuring functional communication channels based on defined and tested standards, mandate the adoption of the FMN approach.

74. The implementation of FMN for current and future EU CSDP military operations and missions also involves setting common security standards amongst all operation and mission participants, enabling cooperative CD activities and establishing trust between them to allow effective and secure interconnection and information sharing.

M. Cyber Deterrence

75. The dissuasive effect of a credible cyber deterrence is an important element of CD. Cyber deterrence complements cyber resilience and cyber response to hostile activities and includes two ways to deter by denying perceived benefits and by imposing costs on the adversary. Both approaches are based on the core principle of changing the calculus of the adversary.

76. Improved capabilities and capacities, standardized procedures for detection and investigation as well as effective CD capabilities and mechanisms, where applicable embedded into the established EU diplomatic response framework to malicious cyber activities, need to be developed and implemented. These are prerequisites to establish an effective and credible cyber deterrence framework for EU CSDP military operations and missions.

N. Cyber Incident Reporting and Response

77. Capability to report and respond to cyber incident must be developed to deny the adversary the ability to succeed in offensive CO targeting at own forces' military networks and systems, and to contain the damage. This must be achieved through the establishment of the combination of a standardized and comprehensive ICT service management and a cooperation framework of static and deployable security operation capabilities across all EU CSDP military operations and missions. This will allow the linking of and the coordinated response to related incidents in EU military CSDP and the mitigation of the impact of similar future incidents.

O. Cyberspace Personnel

78. With the majority of cyber incidents caused by human error – intentional or not – there is a strong human factor at play in CO. Furthermore, all personnel, from soldiers and sailors up to the highest commanders, are digital actors due to the increasingly pervasive digitalization. Thus, cybersecurity is everyone's responsibility and "cyber culture" becomes a fundamental part of everyone's training and education. EU institutions, bodies and agencies and EU MS therefore are to invest in developing sufficient personnel resources for EU CSDP military operations and missions, which understand the implications of cyberspace and take responsibility each in its individual role.

79. Despite the growing importance of AI and the potential utilization of AI enabled systems and applications, the need to provide sufficient human resources to operate and defend military networks and systems will prevail and may even further increase. This condition must be reflected when initiating and implementing tailored efforts to enable cyberspace personnel to be prepared to defend against cyber threats. Reflecting the required cultural shifts and educational and training needs, building and sustaining a pool of cyber skilled personnel for EU military CSDP is paramount.

P. Cooperation with International Partners

80. The EU Cyber Defence Policy Framework provides guidance on cooperation with relevant international partners that should be further developed.

81. With EU CSDP military operations and missions conducted in the wider region and depending on host nation acceptance and support, a stronger cooperation with these nations and other international partners of matching interest in cyberspace is of utmost importance.

82. In view of the single set of forces paradigm and taking note that a majority of EU MSs are equally NATO nations, and that EU and NATO share strategic concerns regarding cyber, the deepening of the cooperation in cyberspace between the EU and NATO is of great importance, while respecting the inclusiveness of all EU MSs. This cooperation is essential for the effective implementation of cyberspace as a domain of operations in EU military CSDP and is carried out in a synergetic manner and in full respect for the decision-making autonomy of the two organizations.

Q. Military Conceptual Framework

83. The existing military conceptual framework for EU CSDP military operations and missions requires a comprehensive and profound review and update to provide sufficient guidance for the establishment and use of cyberspace as a domain of operations. When necessary, new military concepts will be developed as part of the EU Conceptual Development Implementation Programme (CDIP). In the implementation of this task, compatibility with NATO concepts and doctrine should be sought to the maximum extent possible in a mutually reinforcing manner. This,

in particular, includes guidance on how cyberspace will be considered within the Operations Planning Process (OPP).

R. Civil-Military Cooperation and Harmonization

84. EU CSDP civil and military operations and missions, both, significantly rely on technological solutions and critical infrastructures, which depend on each other or are inter-connected, with many of them identical for both[12]. Furthermore, military operations and missions may complement and provide security to civilian missions, in line with the Integrated Approach (IA). In addition, several CSDP assets, including HQs, depend on EU MS national critical infrastructures, which may be provided by civil and military service providers, alike.

85. The anticipated increase of information flow across civil-military boundaries of EU CSDP in the framework of IA and the need to protect geographically connected or closely intertwined civil and military operations and missions creates the necessity to harmonize civilian and military elements of cyberspace wherever feasible as well as to strengthen civil-military synergies in cybersecurity and CD.

86. Despite the necessary separation between civil and military areas of responsibility, a permanent cooperation function between both domains is required to ensure unity of effort in cybersecurity and CD, such as sharing common cyber threat knowledge and preparing response options in a coordinated manner.

S. Collaboration with industry, academia and the cybersecurity Market in EU

87. Industry, academia and the cybersecurity Market in EU play significant roles in maintaining and evolving a rapidly changing cyberspace, in innovative cybersecurity capacity building and in providing latest information and communication technologies and associated services to the military. Therefore, a strong collaboration with these significant EU players in cyberspace ensures that the EU remains up to date on leading-edge developments and provides the required strategic insight for effective and sustainable EU military CSDP. Further, opportunities for collaboration with e.g. the European Cybersecurity Competence Centre or the European Cyber Security Organisation (ECSO) has to be examined and utilized, where appropriate.

T. Research and Technology

88. EU research and technology development in particular on the use of new technologies associated with cyberspace must be focused to support the above-mentioned ways and means and be harmonized among EU MS and EU institutions, bodies and agencies. In this context, best use should be made of existing and emerging military Cyber Research Agendas and their Technology Building Blocks, as well as of funding opportunities through the Research Window of the European

[12] Dual use of ICT

Defence Fund (EDF). Cooperation with partners, including NATO, in a reciprocal manner, should be increased and further support these efforts.

U. Capability Development

89. To support EU military CSDP effectively, the EU should foster interoperability between the civilian cybersecurity initiatives, and the cyber defence initiatives under the PESCO projects, the European Defence Fund (EDF), the Coordinated Annual Review on Defence (CARD) and the Capability Development Plan (CDP). In particular, the EU should make use of the next phase of PESCO to encourage greater coherence between Member States' approaches in cyberspace, promoting interoperability and supporting EU capability development.

IMPLEMENTATION

90. To support the implementation of this EU military vision and strategy a set of terms and definitions is included which shall assist in the establishment of a common perspective on the use of cyberspace as a domain of operations in EU CSDP military operations and missions. It is therefore important to understand that these terms and definitions apply to EU CSDP military operations and missions only and do not intend to question or override MS national terms and definitions.

91. In order to ensure political control and strategic direction in the implementation of the EU military vision and strategy the EU Military Staff (EUMS) shall report to the EU Military Committee (EUMC) at regular intervals and the Chairman of the EUMC may update the Political and Security Committee (PSC) at his discretion or at the request of EU MS.

92. The EUMS shall also report to the Annual Report on the Implementation of the EU Cyber Defence Policy Framework.

CONCLUSIONS

93. This document provides overarching direction and guidance for the implementation of cyberspace as a domain of operations in EU CSDP military operations and missions. It underlines the need to harmonize civilian and military elements of CSDP when and where feasible. By establishing an integrated, cross-domain approach to EU CSDP military operations and missions, the EU ensures that it will accomplish the agreed EU Level of Ambition in response to conflicts and crises.

94. The EU decisions on policy, personnel, organizations associated to cyberspace and the approach to use it as depicted in this document will have implications for many years to come and will demand significant but inevitable efforts in support of EU CSDP and to CSDP Troop Contributing Nations.

95. The focused and coordinated development of capabilities described in this document will enable the building of the required capacities for cyberspace, both mid and long term.

96. However, the urgent need for unified action, without further delay and coordinated between EU MSs and EU entities, bodies and agencies, cannot be emphasized enough. Only a united and coordinated effort by all military and civilian stakeholders of EU CSDP, as well as close cooperation with partners, will ensure cohesion and achievement of the vision's objectives.

97. Furthermore, it should be noted that the cost to mitigate the described deficiencies are expected to rise with each additional delay, both in terms of resources and in terms of operational costs.

ANNEXES

A. References

B. Terms and definitions

C. Abbreviations

ANNEX A

REFERENCES

A. Global Strategy for the European Union's Foreign and Security Policy (EUGS), 29 June 2016

B. Directive (EU) 2016/1148 of the European Parliament and of the Council concerning measures for a high common level of security of network and information systems across the Union (NIS Directive), 6 July 2016

C. Council Conclusions on implementing the EU Global Strategy in the area of Security and Defence (14149/16), 14 November 2016

D. Implementation Plan on Security and Defence (14392/16), 14 November 2016

E. Council Conclusions on Security and Defence in the context of the EU Global Strategy (13978/18), 19 November 2018

F. Council conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox"), ST 10474 2017 INIT, 19 June 2017

G. Joint Communication to the European Parliament and the Council – Resilience, Deterrence and Defence: Building a strong cybersecurity for the EU (JOIN (2017) 450 Final), 13 September 2017

H. Commission Recommendation on Coordinated Response to Large Scale Cybersecurity Incidents and Crises (BLUEPRINT), C(2017) 6100 Final, 13 September 2017

I. Council Conclusions on the Integrated Approach to External Conflict and Crises (5413/18), 22 January 2018

J. EU Cyber Defence Policy Framework (2018 Update) (14413/18), 19 November 2018

K. EU Framework Nation Concept EEAS(2015) 1317 REV 6

L. EUMS CIS & CD Status Report & Action Plan, EEAS (2019) 697, 24 June 2019

M. EU Narrative on European Security and Defence (WK 7994/2019 REV1), 14 October 2019

N. European Union Concept for EU-led military operations and missions (14779/19), 3 December 2019

O. Council Conclusions on the significance of 5 G to the European Union Economy and the need to mitigate security risks linked to 5G (14517/19), 3 December 2019

P. Council conclusions on the Implementation of the Joint Declaration by the President of the European Council, the President of the European Commission and the Secretary General of the North Atlantic Treaty Organization, (6 December 2016, 15283/16; 5 December 2017, 14802/17; 8 June 2018, 9849/18).

Q. Joint Communication to the European Parliament and the Council – EU's Cybersecurity Strategy for the Digital Decade (JOIN (2020) 18 Final), 16 December 2020

R. EU Requirements Catalogue 2019 (RC19) (EU-C), Doc. 12773/19, 15 October 2019

ANNEX B

TERMS AND DEFINITIONS

Cyberspace

The virtual global and common domain within the information environment consisting of all interconnected and interdependent networks of global, organisational and national information infrastructure, based on the Internet and telecommunications networks, to be extended by other networks, computer systems and embedded processors, and containing also stand-alone systems and networks.

Cyberspace Domain of Operations

The global operational domain cutting through and being a substrate of all others, encompassing all cyberspace related information, information operations and strategic communications, and consisting of all interconnected information technology, communication networks, and included systems, which process, store or transmit information, separated or independent.

Cyber Defence (CD)

One of the cybersecurity dimensions (mostly seen as the military dimension, but comprising both military and civilian approaches). It may also be considered as measures to defend critical systems and information in order to achieve cybersecurity. Cyber defence comprises all technical and non-technical measures to improve resilience of ICT-based systems (such as CIS, C2 and any weapon or sensor systems) supporting MS' defence and national security interests, and to prevent, detect, react to and recover from a Cyber Attack on these systems.

Cyber Deterrence

Cyber Deterrence in the context of EU military CSDP is the ability to persuade continuously any cyber attacker that targeting EU CSDP military operations and missions in or through cyberspace will cost the attacker more than the gains expected. It encompasses all measures along the full spectrum of EU CSDP instruments.

Cyberspace Operations (CO)

Operation aimed to retain freedom of manoeuvre in cyberspace / in the cyber domain to accomplish operational objectives, deny freedom of action to adversaries, and enable other operational activities.

Cyber Resilience (CR)

The ability to continuously deliver the intended outcome despite adverse cyber events, in particular the capacity of an organization to face events (incident or attack), resist a failure or cyberattack and recover its previous condition after the incident.

Cyberspace Situational Awareness and situational understanding (CSASU)

The level of perception and understanding of all environmental elements and events, with respect to time or space and the projection of their status after some variable has changed, that allow making rational decisions and actions in cyberspace.

Information Assurance

Also defined as protection of information systems against unauthorized access to or modification of information, whether in storage, processing, or transit, and against the denial of service to authorized users, including those measures necessary to detect, document, and counter such threats.

Mission Assurance (MA)

A process to protect or ensure the continued function and resilience of capabilities and assets, including personnel, equipment, facilities, networks, information and information systems, infrastructure, and supply chains, critical to the execution of EU CSDP mission-essential functions in any operating environment or condition. It emphasizes the operational impact of cyberspace incidents and attacks.

ANNEX C

ABBREVIATIONS

ACRONYM	ABBREVIATED WORD
AI	Artificial Intelligence
CD	Cyber Defence
CDIP	Conceptual Development Implementation Programme
CDOP	Cyber Defence Operational Picture
CDPF	Cyber Defence Policy Framework
CCHQs	Component Command Headquarters
CERT	Computer Emergency Response Team
CFSP	Common Foreign and Security Policy
CIS	Communications and Information Systems
CO	Cyberspace Operations
COTS	Commercial Off-The-Shelf
CRM	Crisis Response Mechanism
CS	Communication Systems
CSASU	Cyber Situational Awareness and Situational Understanding
C2	Command and Control
DCO	Defensive Cyberspace Operations
EEAS	European External Action Service
ENISA	European Union Agency for Network and Information Security

ETE	Education, Training and Exercise
EUMC	European Union Military Committee
EUMS	European Union Military Staff
EU OPSWAN	EU Operational Wide Area Network
FHQ	Force Headquarters
EU MHQ	EU Mission Headquarters
FMN	Federated Mission Networking
HLGP	Headline Goal Process
HQ	Headquarters
IA	Integrated Approach
ICT	Information Communication Technology
IoT	Internet of Things
IT	Information Technology
LoA	Level of Ambition
MHQ	Mission Headquarters
MilCERT	Military Computer Emergency Response Team
MPCC	Military Planning and Conduct Capability
MS	Member States
NIS	Network and Information Systems
OCO	Offensive Cyberspace Operations
OHQ	Operation Headquarters
OpCdr	Operation Commander
OT	Operational Technology
PESCO	Permanent Structured Cooperation

PSC	Political and Security Committee
RM	Risk Management
RoE	Rules of Engagement
R&T	Research and Technology
SOP	Standing / Standard Operating Procedure
TCN	Troop Contributing Nations
TEU	Treaty on European Union