EU CIVILIAN TRAINING AREA
„HYBRID THREATS AND CYBER “
TRAINING REQUIREMENTS ANALYSIS

October 2020

Contents

INTRODUCTION

This Training Requirement Analysis (TRA) follows the guidelines and requirements of EUCTG Strategic Guidance on CSDP Civilian Training,[1] to provide an analysis of the EU Civilian Training area "Hybrid threats and cyber". The analysis was conducted in spring-summer 2020, and the full TRA was first presented to EEAS in October 2020.

The TRA has been put together by a consortium of: Estonian Academy of Security Sciences [consortium lead], Republic of Estonia Ministry of the Interior, Tallinn University of Technology, The European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA), European Security and Defence College, The European Centre of Excellence for Countering Hybrid Threats, and Ministry of the Interior of Austria.

Background

The rapid development of technology, including communication technology, over the past few decades has introduced a vast number of new vectors for communication and information exchange as well as changing work practices across the world. Networked computers and the growing number of devices with computing capacity are used for both work (e.g. accessing remote databases or sharing relevant documents) and leisure (e.g. reading newspapers and keeping up with friends).

Growing use of networked technology has also brought about new threats. Virtual cyberspace enables remote cyberattacks that can affect the whole network as well as having introduced new forms of criminal activity (i.e. cyber crime). Likewise, hybrid warfare[2] has found new means via exploitation of new technologies, e.g. online disinformation campaigns that make use of the borderless, more segregated, and less regulated information sphere that cybersphere provides. Again, networks and people can be susceptible to adverse and/or malicious activity either at work, or during leisure time.

The EU, Member States, EU institutions as well as EU Common Security and Defence Policy (CSDP) missions, including civilian missions to third countries, rely on a stable and well-functioning cybersphere for communication and information exchange as well as for providing essential services. Due to the threats intrinsic to this reliance upon the cybersphere, the EU as a whole and individual Member States have recognised the growing importance of building resilience against these new threats.

In this light, EU CSDP missions (civilian and military) are in an especially vulnerable situation when located in third countries. Whilst requiring technology, as well as networks, for work and communication, for example, (i) the cybersphere and IT-devices in the host country might not be subject to the same level of security monitoring and regulation as inside the EU; (ii) development of IT-infrastructure in the host country might be not as advanced (and so, secure) as in the EU; (iii) the

[1] Civilian Strategic Guidance 9898/19, 6 June 2019.

[2] As a terminological note, the TRA follows the same (consciously flexible) definition of hybrid threats, as proposed in the mini-concept, where adverse hybrid actions have the following features: "the mixture of coercive and subversive activity, conventional and unconventional methods (e.g. diplomatic, military, economic, technological, media, religious institutions etc.), which can be used in a coordinated manner by State or non-State actors to achieve specific political objectives, while remaining below the threshold of formally declared warfare " (EEAS Working Document (2020) 523, p.3).

host country might be subject to cyber or hybrid threats; (iv) the mission itself, both physically as well as virtually, might be subject to cyber or hybrid threats. Considering this new and developing threat landscape, there is also heightened attention to and recognition of the need enhance mission resilience and mission-members' awareness of the new emerging threats.[3]

Aim and scope

The aim of this Training Requirements Analysis is to identify the training required on the Civilian Capability Cluster "hybrid threat and cyber", map the currently available training and develop the Civilian Training Area High Level Learning Outcomes (CTALO), which should serve as a guiding framework for developing any new/further training courses for civilian CSDP mission members on "hybrid threats and cyber".

The scope of the Training Requirements Analysis is analysis of the EU policy framework on hybrid threats and cyber, analysis of relevant training available to civil mission members in how to conduct assignments and daily-life safely and without compromising their mission or their own individual wellbeing in respect to new technology subject to hybrid and cyber threats. The analysis provides CTALO for developing further training of the CSDP mission members to raise and harmonize their awareness on the 7 central "hybrid threats and cyber" themes: (I) General EU response to hybrid threats and cyber; (II) Safe use of work-related systems and devices in mission premises; (III) Safe use of personal devices outside mission premises; (IV) Situational awareness; (V) Hybrid threats; (VI) Cyber threats; (VII) Physical threats to it-systems etc.

This civilian CSDP missions Training Requirements Analysis is distinct from the previously submitted military CSDP missions "hybrid threats and cyber" Training Requirements Analysis. This approach was taken to: i) guarantee the focus on civilian mission specific training themes; ii) avoid confirmation bias by adopting the themes and results from military analysis; iii) enable identification of synergies after completion of both research projects.

TRA structure

The TRA has the following structure: The first section provides an analysis of the policy documents regarding "hybrid threats and cyber" with special focus on European Common Security and Defence Policy (CSDP), and the EU CSDP civilian missions and mission planning.

The second section maps and analyses training on "hybrid threats and cyber" currently (or shortly) available to EU CSDP civilian mission members.

The third section presents the results and analysis of an empirical qualitative research conducted in spring-summer 2020 among current CSDP civilian mission members, to assess their awareness of and training needs on 7 themes on "hybrid threats and cyber" identified as relevant to a CSDP civilian mission member by the consortium.

The final section presents the Civilian Training Area High Level Learning Outcomes (CTALO), which are developed according to 7 themes on "hybrid threats and cyber" identified as relevant to a CSDP civilian mission member by the consortium.

[3] For example: General Secretariat of the Council, 14305/18, 19 November 2018.

I POLICY DOCUMENT ANALYSIS

According to EUCTG Strategic Guidance on CSDP Civilian Training[4] and CCT Workplan for the Conduct of Training requirements analysis[5] a comprehensive study of EU policy and framework documents was performed aiming to identify policy areas relevant to CSDP missions' effective performance, especially in relation to the capability cluster "hybrid threats and cyber".

This chapter presents an overview of this study: First, summarising the most relevant EU documents (up to this moment) to CCT "hybrid threats and cyber" (Section 1). Second, presenting common themes as found in the documents. Third, putting forward recommendations or further attention and implementation of the documents with the perspective of their use at civilian CSDP missions as per the analysed documentation (EEAS for civilian mission training/planning).

The policy document summary is further divided into two sub-sections. Section 1.1. summarises key EU documents on cyberspace and cyberspace governance relevant to the CTR area "Hybrid threats and cyber". These documents introduce, define, and determine the EU wide approach to cyberspace and cyberspace governance, as well as approaches to and cooperation regarding hybrid threats. Additionally, these documents determine the response to cyber and hybrid incidents and the responsibilities that each individual Member State must undertake. Section 1.2. summarises EU documents (including research reports) explicitly covering the topics of hybrid threats and cyber in relation to CSDP missions including suggestions for improving pre-deployment training as well as enhancing cyber and hybrid threat capacity in the mission. Both sections summarise the documents by presenting the central themes which are relevant for CSDP missions.

This first set of documents (Section 1.1.) is important in so far as it articulates the core EU values of cyberspace, which are also carried across to CSDP missions in third countries. Likewise, the documents define standardisation of responses and information sharing protocols, set priorities for training, identify the EU institutions responsible when a cyber incident occurs, lay out cooperation needs with other international organisations and third countries, and so on. Given these points, awareness of these documents and central themes is important for all personnel related to the CSDP and related mission.

The second set of documents (Section 1.2.) presents detailed information concerning CSDP missions' resilience to and preparation for hybrid threats and cyber. Whilst the agreements and developments in relation to CSDP missions documented therein are also relevant to all mission members, details of the state of CSDP missions and further development is of extra importance to mission Senior-Management and hybrid threats and cyber experts.

[4] Civilian Strategic Guidance 9898/19, 6 June 2019.
[5] Brussels, 12 July 2019

1. DOCUMENT SUMMARY

1.1. EU POLICIES ADDRESSING HYBRID THREATS AND CYBER

Documents in this section date from 2010 onward and describe EU policies regarding: cyberspace; Single Market as enabled by cyberspace; the growing risks of hybrid threats and cybercrime and the responsibilities of the EU as a whole and Member States (from here onward, MS(s)) individually in respect to building and training resilience; the growing need for standardization of protocols and MS' focal points and/or institutions specialising on cybers security and hybrid threats; EU agreements with NATO for growing collaboration; and, how hybrid threat and cyber should be part of EU foreign policy, and also, part of EU external missions. This summary presents the key themes in EU's hybrid threat and cyber policy.

Document with special relevance to civilian CSDP missions include:

Council conclusions on Digital Agenda for Europe
3017th TRANSPORT, TELECOMMUNICATIONS AND ENERGY Council meeting
Brussels, 31 May 2010
Available at:
https://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/trans/114710.pdf)

The Council conclusion acknowledges the importance of the Digital Agenda for Europe, and recognises that wider use and more effective implementation and use of new technologies will improve the life of the European population as a whole, and enhance social and economic cohesion by providing more equal possibilities. So, Europe should put forward a unified effort to create a digital single market.

The adoption of the Digital Agenda, the Council recognises, however, requires a commitment at both EU and Member State level, to a coordinated action to improve the interoperability of IT-solutions and promote standardization. Additionally, all countries need to work together towards network safety, trust and confidence in cyberspace.

JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS
Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace 8th of February 2013, 6225/13
Available at: http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%206225%202013%20INIT

The Strategy clarifies the principles of EU and International cybersecurity policy, such as the growing vulnerability that open and free cyberspace provides to counties, communities, and citizens, and the need for protection of cyberspace from incidents, malicious activities and misuse as the number of online fraud victims is increasing. The strategy covers several important issues relevant to CSDP missions, such as developing cyber-defence policy and capabilities related to the framework of the Common Security and Defence Policy (CSDP). A key activity is developing the EU cyber-defence policy framework to protect networks within CSDP missions and operations, including dynamic risk management, improved threat analysis, and information sharing. Dialogue and coordination between civilian and military actors and international partners in order to avoid duplication is foreseen. Emphasis should be placed upon the exchange of good practices and information, on early warning,

incident response, risk assessment, awareness raising and training. Procedures to report incidents that may relate to crime, cyber espionage, or state-sponsored attacks, should be followed accordingly.

JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL
The EU's comprehensive approach to external conflict and crises 11.12.2013
Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52013JC0030&from=en

The joint communication addresses and draws out action to further employ EU's comprehensive approach to external conflict and crises.

Following the Treaty of Lisbon's coming into force and the new institutional context it created, the EU has both the increased potential and ambition to make its external action more consistent, effective and strategic. Whilst not new, the ideas and principles governing the comprehensive approach are yet to become systematic, guiding principles for EU external action across all areas, in particular in relation to conflict prevention and crisis resolution. The Joint Communication sets out the High Representative and Commissions' understanding of the EU's comprehensive approach to external conflicts and crises – to all stages of the conflict or other external crises - and fully committing to its joint application in the EU's external policy and action.

The key underlying principle in the comprehensive approach is the connection between security and development. Likewise, principles of having context-specific response; a shared responsivity of all EU actors in Brussels, in MS' and on the ground in third countries; and the full respect of different competences and respective added value of the EU's institutions and services, as well as of the MSs, also underpin this approach.

To further enhance the coherence and effectiveness of EU external policy and action in conflict and crisis situation, the steps included mandate that:

A shared analysis is developed. Actions toward which include: First, improving situational awareness and analysis capacity by better linking up the dedicated facilities in the EU institutions and services, also by providing access to EU institutions' and MSs' information and intelligence. Second, strengthening information-sharing among HQ in Brussels and in the field, including CSDP missions and operations. Third, developing a common methodology for conflict and crisis analysis, and using the analysis as a base for further discussion within relevant council bodied.

The different strengths and capacities of the EU are mobilised. The actions for this include confirmation that all relevant EU actors are involved and engaged in the analysis and the assessment of the conflict and crisis situation; strengthening operational cooperation among the various emergency response functions in the EU; and ensuring coherence between EU and MS's action.

The communication also emphasises the long-term perspective of the comprehensive approach. This demands close cooperation between internal and external action policies, additionally EU delegations in third countries should play a central role in delivering EU dialogue, action and support.

COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS

Internet Policy and Governance Europe's role in shaping the future of Internet Governance (Text with EEA relevance) (12th of Feb 2014)

Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52014DC0072

The communication proposes a basis for a common European vision for Internet governance to defend and promote democratic rights and clear multi-stakeholder governance structure.

The communication states that whilst over the 15 years the EU has helped to sustain and develop the Internet as a fundamental pillar of the Digital Single Market, recently there are conflicting visions on the future of the Internet and growing distrust in the Internet due to fear of cybercrime as well as revelations of large-scale surveillance programmes. Hence, the communication builds on strengthening the multi-stakeholder mode, focussing on the policy areas relevant to the complex Internet governance ecosystem. Also, the Commission is committed to building confidence in the Internet, including efforts to drastically reduce cybercrime. To rebuild confidence, the Commission will work with the Council and Parliament to achieve rapid adoption and implementation of key legislation, including reform of the data protection framework and Directive on network and information security. The European Commission will launch an in-depth review of risks at the international level of conflict of laws and assess how to solve such conflicts. Additional guideline development will also be carefully considered.

The Internet should remain open and inclusive, respecting human rights and protecting democracy. Yet, the Internet should be subject to the same laws as other areas of day-to day life. The network needs to have a resilient and transparent architecture to ensure the trust in the system. The Commission invites the Council and Parliament, relevant committees as well as MSs to agree on a common vision as highlighted in the Communication and defend it jointly.

Council Conclusions on Cyber Diplomacy (6122/15) 11th of February 2015

Available at: http://data.consilium.europa.eu/doc/document/ST-6122-2015-INIT/en/pdf

The Council Conclusion presents the common and comprehensive EU approach for cyber diplomacy at the global level.

The comprehensive approach to cyber diplomacy is to promote and protect EU values of democracy, rule of law, and human rights, and ensure that the behaviour on the Internet is not undermining these values. Also, European growth and competitiveness needs to be ensured by strengthening cybersecurity and improving cooperation in fighting cybercrime. Finally, the EU approach should contribute to mitigation of cybersecurity threats, conflict prevention, and greater stability in international relations through the use of diplomatic and legal instruments. Important to CSDP missions, the approach reiterates the importance of cyber capacity building in third countries, to support EU efforts to promote its core values, and enable the full economic and social potential of ICT, as well as developing resilient systems and mitigating cyber risks for EU.

To reach this goal, the EU and MSs are encouraged to make cyber capacity building part of a wider global approach in all cyberspace domains, including close cooperation with relevant EU agencies (e.g.

ENISA). That includes cooperation with international stakeholders in providing training and awareness-raising and using available financial instruments and programmes.

Joint communication to the European Parliament and the Council.
Joint Framework on countering hybrid threats a European Union response
6th of April 2016, JOIN (201) 18 final
Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016JC0018&from=en

The Joint Communication addresses changes in EU and neighbouring countries' security environment and underlines the need for mobilising EU instruments for countering hybrid threats and cyber.

The comprehensive approach to crisis Management considers deployment of CSDP tools and missions in order to assist third country partners in enhancing their capacities in strategic communication in countering hybrid threats. The approach foresees partners finding synergies between CSDP instruments and security (EUROPOL, FRONTEX, CEPOL, EUROJUST, INTERPOL etc) in accordance with their mandates by conducting Specific Actions such as a hybrid risk survey in neighbourhood regions

The Communication addresses CSDP by proposing engagement between civilian and military training; mentoring and advisory missions; contingency planning to identify signals of hybrid threats and strengthened early warning capabilities; and support in CBRN risk mitigation.

Increasing cooperation with third countries requires actions to enhance cyber-resilience and partners' abilities to detect and respond to cyber-attacks and cybercrime, so as to counter hybrid threats in third countries.

In conclusion, it should be mentioned that the focus of the Joint Framework Document lays on improving awareness. The need for enhanced resilience building in areas such as cybersecurity, critical infrastructure, and efforts to counter violent extremism and radicalisation is underlined. Additionally, the prevention of, response to, and recovery from hybrid threats in case of serious hybrid attack could be supported by common operational protocol (COP).

Communication from the commission to the European Parliament, the Council, The European Economic and Social Committee and the committee of the regions: Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry
5th of July 2016, COM (2016) 410 final
Available at: https://ec.europa.eu/digital-single-market/en/news/communication-strenghtening-europes-cyber-resilience-system-and-fostering-competitive-and

The Communication presents measures aiming to strengthen EUs cyber resilience and foster a competitive and innovative cybersecurity industry in Europe.

Despite EU efforts to mitigate cybersecurity risks to the EU Single Market, incidents occur daily, so also undermining trust in digital society. The Commission is looking for measures to further enhance the EU's cybersecurity resilience and incident response, and with that, help to achieve the Single Market ambition of ensuring economic growth and increasing employment.

To achieve the goal, there is a need for further commitment to addressing cybersecurity challenges faced by the single market, including in cooperation to ensure the response to cyber incidents, as well as supporting industrial capabilities in the field of cybersecurity. The NIS Directive will lead the way towards EU-level cooperation across MSs and help to further prepare for large-scale cyber crises. Relevant expertise in EU level is currently scattered, hence a further cooperation blueprint needs to be established and expertise further pooled into information hubs. Likewise, an advisory board should be established and an ENISA mandate assessed with the possibility to enhance that also.

Currently, ENISA, ECTEG, European cybercrime centres at Europol, as well as CEPOL, all have an important role in capacity-building support. Yet, there is a need to further develop civil-military cooperation and synergies in training and exercises between MSs, EEAS, ENISA and other relevant EU bodies, so as to increase the resilience and incident response capabilities of the EU. Likewise, the civ-mil synergies should look toward cyber defence product development.

Furthermore, to enhance EU cyber resilience steps required include: certification across the EU to be unified to make sure that the relevant products can be implemented in all MS; promotion of a security-by-design approach; and establishment of a contractual public private partnership (cPPP) to gather resources to deliver excellence in research and innovation.

DIRECTIVE (EU) 2016/1148 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.[6]

Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN

The EU Directive objective is to achieve a high common level security of network and information systems in the Union. The Directive sets the responsibilities for MSs to ensure the security of EU-wide networks and resilience to cyber incidents relating to essential services. It also establishes the roles of relevant EU institutions, as well as emphasising the need for further international cooperation to ensure the sustainability of essential services.

The Directive reiterates the vital role for network and information systems across EU, including their being essential for trade, due to which the functioning of these networks is crucial. Currently, MSs have very different levels of preparedness, constituting a security risk for all. To improve the situation, a Cooperation Group (including ENISA) should facilitate good policy practices as well as strategic cooperation across MSs regarding security of network and information systems. Additionally, there is a demand for standardization of security requirements.

The MSs need to adopt national strategies that see respective and proportionate measures put in place. This includes the need for MSs to establish what are their essential services, where responsibility for ensuring the essential services is on the (digital) service providers; put into place an institution and/or a focal point to communicate with the Cooperation Group; provide adequate and up to date information, including incident reports, to EU and other MSs; and ensure that competent authorities have the necessary power to assess and issue binding instructions to fix any identified shortcomings.

[6] This Directive is commonly referred to in other documents as the NIS Directive.

EU and NATO joint declaration 2016
8th of July 2016
Available at: https://www.consilium.europa.eu/media/21481/nato-eu-declaration-8-july-en-final.pdf

The joint declaration presents new cooperation avenues between the EU and NATO. As the two organisations face common challenges, it affirms the need for a further joint effort and ambition for cooperation in enhancing neighbours' and partners' stability. Enhancing stability includes supporting their sovereignty, territorial integrity, independence, and reform efforts.

To achieve this objective, there is an urgent need to boost abilities to counter hybrid threats, including working together on intelligence sharing between staff. Also, relevant to CSDP missions is the aim to expand coordination on cyber security and defence, including in the context of EU and NATO missions and operations, exercises, and on education and training. For that, more coordination on exercises, including on hybrid, should be sought. Cooperation in the areas of cyber and hybrid threats is considered a strategic priory and the speedy implementation of special importance.

Draft Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox") – Adoption (7th of June 2017)
Available at: http://data.consilium.europa.eu/doc/document/ST-9916-2017-INIT/en/pdf

The draft council conclusions announce the adoption of and development of a framework for diplomatic responses to malicious cyber activities.

The EU recognises that, despite the opportunities it represents, cyberspace also poses a growing challenge to EU external policy as well as to the EU and its MSs. Hence, ongoing EU cyber diplomacy engagements as well as coherence among EU cyber dialogue are of high relevance for resilience building, both in the EU and in third countries. To do that, the EU calls on the MSs, the European External Action Service (EEAS) and the Commission to give full effect to the development of a Framework for a joint EU diplomatic response to malicious cyber activities and reaffirm in this regard its commitment to continue the work on that framework in cooperation with the Commission, EEAS and other relevant parties by implementing guidelines, including preparatory practices and communication procedures, and testing them through appropriate exercises.

Annual Report on the Implementation of the Cyber Defence Policy Framework
19th of December 2017, 15870/17
Available at: https://data.consilium.europa.eu/doc/document/ST-15870-2017-INIT/en/pdf

The annual report provides an overview of the implementation of the EU Cyber Defence Policy Framework (CDPF) for the period November 2016 - December 2017.

The report refers to the need identified by the Council to reimplement the 2014 Cyber Defence Policy Framework and to update it so as to further integrate cyber security and defence into Common Security and Defence Policy (CSDP), and wider security and defence agenda. Additionally, further cooperation and development of cyber initiatives is necessary to develop adequate cyber capabilities in Europe. Regarding CSDP missions, the report points out that the concept for integrating cyber security in the planning and conduct of civilian CSDP missions was finalized in June 2017.

European Commission Recommendation of 13.9.2018 on Coordinated Response to Large Scale Cybersecurity Incidents and Crises, C(2017) 6100 finale

Available at: https://ec.europa.eu/transparency/regdoc/rep/3/2017/EN/C-2017-6100-F1-EN-MAIN-PART-1.PDF

The recommendations draw attention to the suggestion in the 2016 Communication "Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry" for a 'blueprint' for cooperation across various elements of the cyber ecosystem to increase preparedness. The Blueprint states that, in case the crisis entails an important external or Common Security and Defence Policy (CSDP) dimension, the European External Action Service (EEAS) Crisis Response Mechanism (CRM) will be activated.

EU Cyber Defence Policy Framework (2018 update)[7]
19th of November 2018, 14413/18

Available at: https://data.consilium.europa.eu/doc/document/ST-14413-2018-INIT/en/pdf

The updated CDPF aim is to further develop EU cyber defence policy by taking into account relevant developments in fora and policy areas since the initial implementation of CSPF (in 2014). It identifies cyber defence priority areas as well as clarifies responsibilities and competences of different parties involved.

Cyber security is a priority within EU Global Strategy, emphasising the need for protection from crises thorough strengthening the EU as a security community able to enact autonomously, as well as in partnership, however is necessary. These goals demand further cooperation in capability development, including promoting effectiveness and interoperability of the resulting civilian and military capabilities.

The updated CDPF places primary focus on developing cyber defence capabilities of the EU CSDP communication and information network, which means further assessment of vulnerabilities of the CSDP mission infrastructures as well as establishing relevant protection. To do so, EEAS, along with MSs, should further integrate cyber capabilities in CSDP missions and operation. Further actions include: EEAS' development of coherent IT security and policy guidelines, satisfaction of common cyber defence requirements for CSDP military and civilian missions; and promotion of threat information sharing to relevant EU institutions.

Further CSPF priorities include training and exercise and civ-mil and international cooperation; in particular this require updating the MSs cyber defence training of the CSDP chain of command and adequately addressing the cyber domain in exercises, as well as civil-military cooperation in the cyber field, to ensure coherent response.

[7] The EU Cyber Defence Policy Framework was first adopted by the Council in the 18th of November 2014. (Council document 15585/14, 18 November 2014.)

COUNCIL DECISION concerning restrictive measures against cyber-attacks threatening the Union or its Member States
14th of May 2019, 7299/19
Available at: https://data.consilium.europa.eu/doc/document/ST-7299-2019-INIT/en/pdf

On 14 May 2019, the Council established a framework allowing the EU to impose targeted restrictive measures to deter and respond to cyber-attacks that constitute an external threat to the EU or its member states. This includes cyber-attacks against third States or international organisations where restricted measures are considered necessary to achieve the objectives of the Common Foreign and Security Policy (CFSP).

Cyber-attacks falling within the scope of this new sanction regime are those which have significant impact and which:

- originate or are carried out from outside the EU, or
- use infrastructure outside the EU, or
- are carried out by persons or entities established or operating outside the EU, or
- are carried out with the support of person or entities operating outside the EU.

This framework allows the EU for the first time to impose sanctions on persons or entities that are responsible for or are associated with cyber-attacks or attempted cyber-attacks, who provide financial, technical or material support for such attacks, or who are involved in other ways.

Council Conclusions: Complementary efforts to enhance resilience and counter hybrid threats
10th of December 2019, 14972/19
Available at: https://data.consilium.europa.eu/doc/document/ST-14972-2019-INIT/en/pdf

The Conclusions sets priorities and guidelines for EU cooperation in the field of countering hybrid threats and enhancing resilience to these threats, building on the progress made in recent years.

The conclusions call for a comprehensive approach to security to counter hybrid threats, working across all relevant policy sectors in a more strategic, coordinated, and coherent way. It underlines the need to continue developing cooperation with international organisations and partner countries on enhancing resilience and countering hybrid threats, in particular EU-NATO cooperation and cooperation with countries in the EU's neighbourhood. The Council also stresses the importance of continuously improving the cooperation between national authorities, as well as EU institutions, bodies, and agencies, across the internal-external security nexus.

As regards countering disinformation, the Council recalls the importance of the continued implementation of the Action Plan Against Disinformation. It underlines the need for sufficient resources for the three Stratcom Task Forces (East, Western Balkans, South) of the European External Action Service and invites the EEAS to assess the needs and possibilities for reinforcing its strategic communication work in other geographical areas, such as sub-Saharan Africa. The Commission and the EEAS are also urged to further develop, together with the member states, the Rapid Alert System into a comprehensive platform for cooperation, coordination and information exchange for member states and EU institutions. As regards social media platforms, the Commission is invited to consider ways to further enhance the implementation of the Code of Practice on Disinformation, including possible enforcement mechanisms.

To enhance the security of EU information and communication networks and decision-making processes, the EU institutions, bodies, and agencies are invited to develop and implement a comprehensive set of measures for countering hybrid threats and other malicious activities.

COUNCIL DECISION (CFSP) 2020/1127 of 30 July 2020 amending Decision (CFSP) 2019/797 concerning restrictive measures against cyber-attacks threatening the Union or its Member States

Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32020D1127&from=EN

The Council amends the previous decision by describing targeted restrictive measures against cyber-attacks that have a significant effect and due to that poses an external threat to the Union of its Member States. These are vital instruments in responding to and deterring attacks and these measures are included in the cyber diplomacy toolbox. These measures can also be implemented when a serious attack against third States or international organisations occurs.

In this context, as a measure of response and prevention of malicious behaviour in cyberspace, six natural persons and three entities or bodies should be included in the list of natural and legal persons subject to restrictive measures. Those persons and entities or bodies are responsible for, provided support for, were involved in, facilitated, or attempted cyber-attacks, including the attempted cyber-attack against the OPCW and the cyber-attacks publicly known as 'WannaCry', 'NotPetya', and 'Operation Cloud Hopper'.

1.2. POLICY DOCUMENTS ADDRESSING HYBRID THREATS AND CYBER IN RELATION TO CSDP MISSIONS

Documents in this section provide an overview of the EU's and European External Action Service's approach to hybrid threats and cyber, especially in relation to CSDP civilian missions. This section also covers studies and reports documenting the need for further implementation of hybrid threat and cyber resilience measures in mission planning/throughout the mission structure as well as showing the initial results of this process.

Document with special relevance to civilian CSDP missions training on "hybrid threats and cyber" include:

European Union Agency for Network and Information Security (ENISA) study: Cybersecurity in the EU Common Security and Defence Policy (CSDP): Challenges and risks for the EU (Study EPRS/STOA/SER/16/214N) (May 2017)

Available at: http://publications.europa.eu/resource/cellar/2e35913c-1d03-11e8-ac73-01aa75ed71a1.0001.01/DOC_1

This is a study by the European Union Agency for Network and Information Security (ENISA) for the European Parliament's Science and Technology Options Assessment (STOA) Panel with the aim of identifying risks, challenges and opportunities for cyber-defence in the context of the EU CSDP.

The study focusses on three thematic areas: policies, capacity building, and the integration of cyber in the CSDP missions. The aim of the study is to provide suggestions, especially medium and long term, as to what could be done in cybersecurity for the CSDP. Considering the differing level of cyberactivity of MSs, varying threat levels, distinct priorities, and capacities, the study focusses on increasing coherence.

The study provides a list of action-points, following which is of special significance to CSDP missions: (i) the principle of security by design should be adopted in CSDP procurement equipment, while also addressing liability and supply chain integrity provisions; (ii) a capacity maturity model, such as the CMM (the Cybersecurity Capability Maturity Model), should be considered for developing and monitoring cybersecurity capacities in the context of the CSDP; (iii) the EU should ensure appropriate resources for cybersecurity capacity building and continue investing in cybersecurity, while at the same time supporting education, training and career path development; (iv) communication of information to EU-level mechanisms like the EU-INTCEN and the CSDP OHQs/MHQs should be further developed for a safer operational environment of CSDP missions; (v) cyberskills and capabilities at the operational layer should be further enhanced because they are essential for assessment of cyberthreats in CSDP missions.

The report further suggests that the CSDP missions should work out a necessary level of cybercapabilities relevant to any specific mission at the planning phase of the mission as well as the further mitigation measures at the operational layer of CSDP missions. Finally, there is a lack of international cooperation in the legal dimension regarding cybersecurity, and points out that the CSDP missions are in an especially vulnerable position in that regard, considering that the missions are taking place outside EU.

Draft list of Generic Civilian CSDP Tasks and Requirements
EEAS, 9th of February 2017, 6616/17

Available at: https://data.consilium.europa.eu/doc/document/ST-6166-2017-INIT/en/pdf

In November 2016, the EU Foreign and Defence ministers adopted Council conclusions, deciding on a new level of ambition and on key steps in the area of Security and Defence to deliver on the objectives of the Global Strategy. These conclusions were based on HR/VP Mogherini's Implementation Plan on Security and Defence. Specifically, on the Requirements list, the EEAS was tasked with taking forward the work to identify the required capabilities on the basis of the work on the List of generic civilian CSDP tasks and through a revision of the Civilian Capability Development Plan (CCDP).

The elaboration of a Capabilities Requirements List for the civilian dimension was initiated already upon adoption of the 2008 Civilian Headline Goal. At the time, however, this exercise led to a job description list rather than covering capability areas such as equipment, planning, logistics, mission support and command and control: all essential areas for effective civilian CSDP.

The draft list proposed identifies the requirements for each task, as well as assessing the capacity to satisfy these requirements.

The list identified the necessity for development regarding CIS, both practical (e.g. more technological solutions) as well as theoretical (e.g. cleared guidelines and regulations).

Integrating cyber security in the planning and conduct of Civilian CSDP missions. (Working document of the European External Action Service, 16th of June 2017, EEAS (2017) 773

The concept paper states that threats to Civilian CSDP missions originating from the cyber domain, are considered equally serious, as these can also threaten the safety of the personnel and undermine the whole operation. Effective measures for protection are urgently required, also as part of the EU's broader efforts to counter hybrid threats. Security measures against cyber threats are to be implemented to ensure the security of personnel, protection of often sensitive data and information assets, and the fulfilment of mission mandates. The aim is that CSDP mission have a capacity to protect themselves against cyber threats.

Counter to EU military missions, for civilian missions, the lead nation is not responsible for CSI used to meet requirements of interoperability and security, nor does CERT-EU systematically cover missions. Thus, civilian missions are more vulnerable and exposed to cyber threats. The nature of missions means that interoperability/interconnected instruments need to be ensured. Interoperability, however, poses security risks because the strength of the system relies on the security of every object attached to the system.

The aims of the plan are to integrate cyber security, including cyber intelligence reports, into planning and conducting civilian CSDP missions, to set the parameters of enhanced cybersecurity in civilian CSPD missions, and to promote a greater emphasis on cyber issues throughout the lifespan of a mission. For that, the strategic planner, operational planners, and Heads of mission should be able to identify areas of possible cyber-attack, liaise with experts regarding risk avoidance and mitigation, and take steps to ensure attack response capabilities

Up-to-date training is a key element in mitigating the risks of cyber security incidents enabled by human error and social engineering. Additionally, there should be dedicated exercises provided to all the CSDP structures for the purposes of practicing reacting to cyber threats. Due to the very distinct nature of CSDP missions, development of distinct training for mission staff should also be considered.

Civilian Capabilities Development Plan, EEAS (2018) 906, 4 September 2018
Available at: https://data.consilium.europa.eu/doc/document/ST-11807-2018-INIT/en/pdf

This Civilian Capability Development Plan (CCDP) is a second step in the process of strengthening civilian CSDP. The aim is to make civilian CSDP missions more flexible, whilst also enabling missions to support security threat tackling etc. Whilst initial capability priorities (police, rule of law, civilian administration and Security Sector Reform (SSR)) remain fully valid and relevant, due to the change in the contemporary threat landscape, the core categories need to be updated as well.

The emphasis of the plan include that: (i) there is a clear desire among member states to integrate needs of emerging from new security threats and challenges into these priorities (including, hybrid threats, cyber security etc.); (ii) developing civilian capabilities to meet national as well as agreed EU needs is a national responsibility; (iii) more systematic links between required skills, availability of training (both, at the Member States level and at the EU level, including CEPOL, and other EU agencies), and adaptability of the training curricula should be developed; (iv) For newly set security priorities, covered in mini-concepts, pilot projects should be set up in CSDP missions in co-operation with relevant agencies and services including civ-mil cooperation; (v) a mission-specific situational awareness platform (MSAP) should be set up in all theatres where civilian CSDP Missions are active,

and should consolidate already existing coordination and information-sharing structures; (vi) one CSDP mission assignment is providing (specialist level) support to countering hybrid threats and contributing to cyber security and strategic communication.

Conclusions of the Council and of the Representatives of the Governments of the Member States, meeting within the Council, on the establishment of a Civilian CSDP Compact General Secretariat of the Council, 19th of November 2018, 14305/18
Available at: https://www.consilium.europa.eu/media/37027/st14305-en18.pdf)

The Conclusion summarises the EM and MSs agreement to the Civilian CSDP Compact, which include strategic guidelines to more effective and joined up Civilian CSDP as well as action proposals for achieving these aims.[8] The Compact should be delivered as soon as possible, by early summer 2023 at the latest.

The conclusion recognises that worsening of the EU's strategic environment demands continued need to strengthen EU's role and capacity to act as a security provider through the CSDP, deploying both, civilian as well as military missions. EU is determined to make a qualitative as well as quantitative leap forward in civilian CSDP. But, as the operational capacity is drawing from the MSs, then, strengthening the civilian CSDP requires MSs to deploy required capabilities.

Regarding capability cluster "hybrid threats and cyber", the strengthened EU capacity to deploy civilian crisis management missions should, also, contribute to the EU wide response to tackle security challenges which include hybrid threats and cyber security, and significantly contribute to the resilience and security of partner countries with sustainable results. For this, EU and MSs commitment involves training experts pre- and in-mission in accordance with the CSDP Training Policy. Also, enhancing cooperation EU level training, especially specific training need in new security challenges, and seizing the opportunities offered by the recognise training provides.

Civilian CSDP Compact: Council conclusions
9th of December 2019, 14611/19
Available at: http://data.consilium.europa.eu/doc/document/ST-14611-2019-INIT/en/pdf?utm_source=dsms-auto&utm_medium=email&utm_campaign=Civilian+CSDP+Compact%3a+Council+adopts+conclusions

The Civilian Common Security and Defence Policy (CSDP) Compact reaffirms its commitment to making civilian CSDP more capable, more effective, more flexible and responsive, and more cohesive.

The conclusions highlight the significant contribution of civilian CSDP missions to international peace and stability as an essential part of the EU's integrated approach to external conflicts and crises. They also emphasise the need to strengthen the EU's role and capacity to act as a security provider through CSDP.

[8] For the summary of actions and commitments undertaken, see ANNEX 5: JOINT STAFF WORKING DOCUMENT Joint Action Plan Implementing the Civilian CSDP Compact (8962/19) (30 April 2019).

Following the first annual review conference (ARC) held on 14 November 2019 in Brussels, the Council welcomes the positive overall progress during the last year and the strong commitment by all stakeholders to fully deliver on the compact.

The Council endorses the waypoints identified at the ARC, which aim to contribute to the overall implementation of the Compact, ensuring cross-connections between the different areas. They also seek to promote close cooperation with relevant partners on a case-by-case basis.

The annual report of the Mission Support Platform 2019 14th of April 2020, (EEAS) WK3795/2020 INIT

The report is providing an annual overview of mission supports. Based on the EEAS working document "Concept for integrating cyber security into the planning and conduct of civilian CSDP missions" the MSP CIS team supported implementation of some of the recommendations.

The CPCC Cyber expert and some of the Mission's cyber experts actively participated in the CERT EU annual cyber security conference in November 2019. MSP is in direct contact with CERT-EU and regularly briefs CIS officers in the Mission.

The results of these meetings in 2019 included: (i)introduction of cyber security measures to the Operational Plan (OPLAN) in each mission; and, (ii) the nomination of a cyber focal point in all Missions with a view to enhancing the coordination of actions at the mission level, CPSS, and the EEAS Security Operation Centre.

MSO CIS has also provided support for use of the Inter Institutional Framework Contract for Cyber Security. The procurement process for standard cyber defence basic equipment in the Warehouse II has been completed and the related equipment is now available to the Mission.

In 2019, the MSO CIS team succeeded in covering all civilian CDP Missions by basic CERT-EU services. (Total of 4 – 2 added in 2019 – Missions are under special agreement with CERT EU, enrolled to advanced CERT-EU services of network surveillance, penetration testing and incident handling.)

Training activities were suggested through to missions by the ESDC Training course portfolio, with a view to increasing an in-house cyber security culture.

Working document: Mini-concept on civilian CSDP support to countering hybrid threats 20th of May 2020, (EEAS 8077/20)[9]

The EEAS developed mini-concept introduces a specific concept for civilian CSDP – hybrid threat – stemming from the new security environment. The mini-concept would determine necessary new training, cooperation with relevant EU institutions, changes in mission protocol and processes etc. The concept deals with the priority area of identifying, reacting to, and building resilience against hybrid threats in the context of civilian CSDP missions. It builds on ongoing efforts to increase resilience to

[9] This mini-concept is not adopted yet. The current summary is written based on the working document of EEAS (EEAS 8077/20) presented to the Delegations on the 20th of May 2020. The CCT of EU Civilian Training Area "Hybrid threats and cyber" has been advising EEAS during the mini-concept development.

hybrid threats both for the missions themselves and in support of the host States, and suggests ways to improve resilience against these challenges

While definitions of hybrid threats vary and need to remain flexible to respond to their evolving nature, this mini-concept aims to address the following main features of adverse hybrid actions: the mixture of coercive and subversive activity, conventional and unconventional methods (e.g. diplomatic, military, economic, technological, media, religious institutions etc.), which can be used in a coordinated manner by State or non-State actors to achieve specific political objectives, while remaining below the threshold of formally declared warfare.

All civilian CSDP missions can build on ongoing EU efforts aimed at countering hybrid threats, including those undertaken by the EU Hybrid Fusion Cell, the EEAS Strategic Communication Task Forces, and through hybrid risk surveys.

Increased efforts to counter hybrid threats against civilian CSDP missions involve training on hybrid threats to improve resilience, increasing situational awareness and preparedness to protect the mission, as well as the mission's increased role regarding overall EU situational awareness on hybrid threats. Moreover, the mission should be prepared in such a way as to help to increase host states' resilience against hybrid threats, which can include conducting a hybrid risk survey and ensuring strategic advice, help in countering disinformation, as well as being able to provide training to the host state.

2. ANALYSIS OF HYBRID THREATS AND CYBER POLICY AND LEGAL FRAMEWORK IN CONNECTION WITH CSDP MISSIONS

2.1. FINDINGS

I. These documents provide a wide range of awareness that cyberspace is a distinct borderless sphere, due to which all actors engaged in it and every state/institution connected to it are subject to the possible threats.

II. The documents focus on changes in threat landscape, including describing that threats can also emerge in a non-conventional way e.g. the disinformation campaigns etc. With that, it is possible to detect s growing attention to the concept 'hybrid threat' in the documents[10].

III. There is growing attention to cyber and hybrid threats in EU policy documents including emphasis on the need to raise awareness and the need to put relevant measures in place (e.g. staff training; introduction of relevant units; more cooperation among MS and relevant institution etc.), and to be able to respond to these new and quickly developing forms of threat.

IV. There are EU wide agreements in place, as well as with other international institutions e.g. NATO, to cooperate and support each other to tackle these new threats.

V. The documents state that there is a developed draft of a 'blueprint' for institutional cooperation regarding cybersecurity, but as of this moment this does not seem to be implemented.

VI. Some direct action is expected of the EEAS regarding CSDP missions so as to incorporate assessment/awareness of new threats into mission planning, as well as to enhance preparedness of mission members to tackle these threats in-mission and to provide relevant support for the host state.[11]
    a. Regarding relevant training, it is expected that the MSs will provide that training or provide a greater proportion of that.
    b. There is a need to further assess the relevant training needs regarding emerging new threats and to find relevant training opportunities (including training already provided by relevant institutions e.g. ESDC, CEPOL etc.).[12]

VII. Whilst there are agreed actions for CSDP missions to raise mission-specific awareness and build resilience to new threats e.g. 'mini-concepts', implementation of these actions have started only relatively recently. Due to that, there is not a 'cyber' 'mini-concept' with the specific focussing on CSDP missions developed just yet.

[10] Whilst non-conventional threats that are associated with hybrid warfare are not (all) new in nature e.g. disinformation campaigns or economic influencing, it is in the light of several incidents from 2000 onward (e.g. Russian Federation invasion of Crime in March 2014) that have forced to pay further attention to "hybrid warfare" as well as build EU and EU CSDP missions' resilience against these threats.

[11] In 2017 EEAS put together a report/working document *EEAS (2017) 773: Integrating cyber security in the planning and conduct of Civilian CSDP missions* detailing suggestions for how cyber threat prevention and training should be incorporated into future mission planning. The 2020 report *WK3795/2020 INIT: (EEAS) The annual report of the Mission Support Platform 2019* indicates that some of these suggestions have been implemented, e.g. some mission cyber experts have been participating in CERT EU conferences; all OPLANS have introduced cybersecurity measures; all missions have a nominated cyber focal point, etc.

[12] *WK3795/2020 INIT: (EEAS) The annual report of the Mission Support Platform 2019* suggests Missions training activities through ESDC training portfolio to cultivate in-house cyber security culture.

2.2. RECOMMENTATIONS

The document summary and analysis shows EU's growing awareness and pro-active response to hybrid threats and cyber, both in relation to EU internal as well as external policies and regulations. Likewise, documents are generally well developed and largely address CSDP missions' needs.

According to analysis and findings, the following recommendations aiming to enhance effectiveness of CSDP mission members' performance are provided:

- As relevant policy documents cover the core EU values and approach to hybrid threats and cyber and propose tools as training to the relevant EU institutions for cyber incident response, respective parts of EU policy and strategy documents should be integrated in mission members' training.

- Due to constantly evolving nature of hybrid threats and cyber, to ensure timely information exchange with CSDP missions, mission members should receive updates and access to relevant documents in a timely manner.

- To make sure that the EU policies and strategies are continuing to address CSDP missions' needs, the CSDP missions' senior management should be involved in EU hybrid threats and cyber policy and strategy development.

- To ensure the movement and awareness of relevant information to CSDP missions, the EU policy and strategy documents implementation in CSDP missions should be monitored. Likewise, feedback about identified obstacles and gaps should be systematically gathered to modify the process, where necessary.

- Cyber security issues are well addressed in EU policy documents whilst hybrid threats, including their definition, have not been fully covered. Addressing this gap should enable common efforts to attend to the constantly evolving phenomena of hybrid threats and their varying nature, and so addressal in respective policy documents

II AVAILABLE TRAINING ANALYSIS

According to EUCTG Strategic Guidance on CSDP Civilian Training[13] a study of training available was performed aiming to identify training relevant to civilian CSDP missions' effective performance, especially in relation to the capability cluster "hybrid threats and cyber".

The mapping of existing training opportunities was conducted in accordance with the principles set in paragraph 18 in EUCTG Strategic Guidance on CSDP Civilian Training[14], which state that "the EUCTG should ensure that CSDP training activities and training opportunities respect the EU principles of incisiveness and transparency and are open to all EU MS". Considering that a lot of training that is provided in MSs is not open to all EU MS, for example, due to nature of institutions, where the training is provided e.g. part of a degree course[15], or due to the language in which the training is provided, then, the training mapping is only addressing EU institutions that provide relevant training.

Due to no relevant and recent data available mapping the existing training standards and opportunities on "Hybrid threats and cyber" in MS or other international organisations, the CCT conducted a questionnaire survey addressing relevant institutions.[16] According to the survey results, a list of available training on "Hybrid threats and cyber" was formed (See: ANNEX 1).

1. AVAILABLE TRAINING SURVEY

1.1. SURVEY DESIGN

Questionnaire design

- The questionnaire mapping relevant training available on "Hybrid threats and cyber" was modelled according to the template provided in the Annex 2, EUCTG Strategic Guidance on CSDP Civilian Training. [17] (Questionnaire template, see: ANNEX 2).

Questionnaire distribution

- The questionnaire was distributed via email on the 24th of March 2020; the responses were collected until the 26th of June 2020.
- Taking the accessibility of the training as an essential feature of the training available, relevant institutions were identified and the questionnaire was sent to 4: European Security and Defence College (ESDC), European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE), The European Union Agency for Law Enforcement Training (CEPOL), Crisis Management Centre Finland (CMC Finland).

[13] Civilian Strategic Guidance 9898/19, 6 June 2019.
[14] Civilian Strategic Guidance 9898/19, 6 June 2019, p. 7.
[15] To test the availability criteria, a questionnaire was also sent to Tallinn University of Technology (TalTech), a consortium member. The response confirmed that they are not providing any relevant training outside from a degree course. So, the further mapping of training did not engage with state specific institutions, which might provide relevant training, but where training is not accessible to CSDP mission members.
[16] Civilian Strategic Guidance 9898/19, 6 June 2019, p. 27.
[17] Civilian Strategic Guidance 9898/19, 6 June 2019, p. 29-30.

1.2. SURVEY RESULTS

Training provided in relevant institutions:

- CMC Finland does not provide any relevant training;
- Hybrid CoE has so far only run one course on hybrid threats, which explicitly focuses on election intervention. (This course has been held in several countries worldwide [See: Annex 1, p. 108-109]).
- CEPOL reported 13 cyber-themed courses.
- ESDC reported a wide variety of training (jointly with other institutions) available both on cyber and on hybrid threats.

2. ANALYSIS

The nature of available training:

I. The cyber-themed training available at CEPOL is only aimed at expert level civil servants (especially law-enforcement officials) whose job is related to cybercrime prevention, detection and investigation, or cybercrime cases/trials.
    a. For example, CEPOL offers training in cyber-forensics, digital evidence management etc. [See: Annex 1, p. 103-106.]
II. Hybrid CoE has only developed/delivered training on 'Prevention of election interference' for election officials.
III. ESDC and Hybrid CoE have jointly developed 6 e-learning courses, which introduce hybrid threats.
IV. ESDC outlines a very wide-ranging training programme, key features of which are:
    a. Several cyber-themed courses are under development with partner organisations. These courses combine e-learning and stationary learning. Considering the Coronavirus pandemic, the mode of course might change in the near future.
    b. The majority of courses, developed with partner organisations, are only at the stage of planning or running pilot courses. So, the content of the courses can still be moderated/changed?.
    c. The cyber-themed courses are not just developed for civilian officials, but both civilian as well as military officials are considered as target participants. As a result, there is a lack of trainings explicitly targeted to civilian officials.
    d. The courses are aimed at mid-ranking and senior officials, not all officials. Hence, there is a gap at the level of basic training for low-ranked officials.
V. ESDC has developed independent e-leaning courses, [European Security and Defence College (ESDC) - AKU (Autonomous knowledge units)], which also introduce European policy documents and crisis management. These e-learning courses are aimed at both military and civilian officials. With that there is in-built synergy between the military and civilian training available.

Overview of available training:

I. Currently there is a lack of training available for and targeted at civilian officials that would introduce hybrid and cyber threats. Moreover, the available civil-servant oriented training is primarily for experts and specialists whose role is immediately related to hybrid and cyber threats, or, to senior officials whose responsibility is to coordinate the work of hybrid and cyber threat specialists.
II. Currently there are significantly more courses available on cyber than on hybrid threats.
III. Currently there is a lack of training explicitly developed for and targeted to civilian officials/civilian mission members. E.g. the ESDC training available is meant for both military as well as civilian officials.

3. RECOMMENDATIONS

The available training analysis shows that whilst the training areas/capability cluster of "hybrid threats and cyber" is still relatively new and constantly in development, there is a growing number of training possibilities available and in development in this capability cluster. Likewise, the analysis shows that the number of training course available and accessible to CSDP civilian mission members, including e-learning courses with a remote access, is also increasing.

According to the analysis and findings, the following recommendations aimed at enhancing the effectiveness of CSDP mission members' performance are offered:

- To ensure that the amount of training available on hybrid threats matches that available on cyber, further attention should be paid to planning and providing future training.

- To ensure that there is sufficient cyber training for all rankings of civilian mission members available, more training should be provided and made available to basic level/non-experts.

- To ensure sufficient training explicitly targeted to civilian CSDP members is available, there should be further attention paid to planning and providing future training. Training already in place could also be adapted to explicitly address civilian CSDP mission member's needs.

- To ensure that the training available at different institutions is compatible and fits the CSDP civilian mission requirements, further attention should be paid to standardization of the target audience, content, and level of training provided (e.g. using EQF/SCF/SQF qualification standard when developing the training, including training level identification).
- To ensure the movement and awareness of relevant information to CSDP missions, the available training information flow and training participation in CSDP missions should be monitored. Likewise, feedback upon identified obstacles and gaps should be systematically gathered to modify the process where necessary.

III TRAINING NEEDS ANALYSIS

According to EUCTG Strategic Guidance on CSDP Civilian Training, to effectively conduct the TRA, a task analysis and environmental scan[18] should be conducted. To meet this requirement, mission members' self-assessment survey of training received and needed in the 7 central "hybrid threats and cyber" themes: (I) General EU response to hybrid threats and cyber; (II) Safe use of work-related systems and devices in mission premises; (III) Safe use of personal devices outside mission premises; (IV) Situational awareness; (V) Hybrid threats; (VI) Cyber threats; (VII) Physical threats to it-systems etc. was conducted.

1. CSDP MISSION MEMBER'S TRAINING SURVEY

To identify the training requirements at the specific civilian training area cluster "hybrid threats and cyber" a questionnaire study with relevant mission members was conducted.

Hybrid threats and cyber knowledge is relevant for all the missions' members because, a) they are using technology in their daily work; b) they are using technology in their private life daily; c) the host country (as any country) is reliant on functioning of digital technology, but also net neutrality and good will of other countries, for well-functioning society. Thus, the aim of the survey is to map the training required for all mission members, including IT-specialists or senior management of the mission.

1.1. SURVEY DESIGN

Pilot study

To identify the initial awareness of the hybrid threats and cyber themes among CSDP mission members, a pilot survey was conducted in December 2019-January 2020 among Estonian CSDP missions' members. There survey was distributed to 29 persons, and the filled in questionnaire was received from 15.

The questionnaire asked about pre-deployment training, in-mission training as well as asked for further recommendations/ identification of further relevant training on hybrid threats and cyber.

Participants responded not receiving any pre-deployment training on the topics of hybrid threats and cyber. Some had received general training on hybrid threats in-mission. Leading-experts reported on participating in 2-day training on assessment and management of cyber risks, most of participants said to have received in-mission training on cyber. .

In the light of varying awareness/knowledge as well as training received, respondents generally welcomed the initiative to provide training on these topics, as overall threat awareness is relevant to all the mission members.

The pilot study identified the initial gap in the training regarding hybrid threats and cyber, especially on hybrid threats.

[18] Civilian Strategic Guidance 9898/19, 6 June 2019, p.26.

Questionnaire development

The questionnaire identifying the requirements for training of civilian mission members on 'hybrid threats and cyber' was developed by the cyber and hybrid threat consortium members (Estonian Academy of Security Sciences, Republic of Estonia Ministry of the Interior, EU and Foreign Relations Department, Tallinn University of Technology, The European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA), European Security and Defence College, The European Centre of Excellence for Countering Hybrid Threats, Ministry of the Interior of Austria) from January to March 2020. All the themes identified in the questionnaire are taken by the consortium to be highly relevant for mission members. Awareness of identified cyber and hybrid threats, including understanding of relevant protocols/EU policy documents etc. that are relevant to senior management and expert level, should ensure the safety of the missions and its' members as well as competent/confident reaction to potential situations/security risks & breaches. The questionnaire was liaised with the CCT focal point from EEAS and it was confirmed in late-March 2020.

Questionnaire structure

The questionnaire (See: ANNEX 3) questions are divided into 7 sections, each addressing a specific cluster of themes. The clusters are: 1) General EU response to hybrid threats and cyber; 2) Safe use of work-related systems and devices in mission premises; 3) Safe use of personal devices outside mission premises; 4) Situational awareness; 5) Hybrid threats; 6) Cyber threats; 7) Physical threats to it-systems etc.

The questions and answers in the questionnaire are divided into two:

- First (e.g. Question 1), the respondent is asked to assess their own knowledge and/or awareness on a specific topic/issue presented to them, according to a scale (yes - advanced understanding/ yes - good understanding/ yes - some understanding/ no – no understanding) or a yes – I have knowledge and/or awareness /no – I do not have knowledge and/or awareness answers. The respondents are also given a chance to further specify the rationale for their answer.

- Second (e.g. Question 1.1), the respondent is asked to assess, whether the topic/issue covered by the question is – in their opinion – relevant knowledge to a CSDP mission member. Again, the respondent is given a chance to further explain the rationale for their answer.

- Additionally, at the end of the questionnaire, the respondent is provided the possibility to provide additional comments regarding training needs on the hybrid threats and/or cyber, if these are not covered in the questionnaire.)

Questionnaire distribution

The questionnaire was made available to all missions by EEAS via GoogleForms between 1st of April to 2nd of June 2020.[19] Due to the COVID-19 pandemic, this was later than the original date for distribution (March), in respect to that delay the response time for this questionnaire was also extended until the period from the 20th of May until the 2nd of June.

[19] One mission (EUMM Georgia) encountered technical difficulties accessing the questionnaire and distributed some of the filled in questionnaires via e-mail as .docx documents. One mission (EUAM Ukraine) did not respond to the online questionnaire and was directly approached by the CCT in June 2020. Filled in questionnaires from that mission were received on the 13th of July 2020.

1.2. CSDP MISSION MEMBER'S SURVEY RESULTS DATA

1.2.1. RESPONSE DATA

1.2.1.1. Number of respondents

Total 82 filled in questionnaires were received.

62 questionnaires were filled in online using GoogleForms;
20 questionnaires (10 from EUMM Georgia; and, 10 from EUAM Ukraine) were filled in offline as .docx documents and forwarded via e-mail.

1.2.1.2. Break-down of questionnaires received by mission

EUAM-Iraq – 1 questionnaire;
EUBAM-Libya – 1 questionnaire;
EULEX (Kosovo) – 2 questionnaires;
EUCAP Sahel Niger – 7 questionnaires;
EUCAP Sahel MALI – 7 questionnaires;
EUCAP Somalia – 8 questionnaires;
EUAM Ukraine – 10 questionnaires;
EUMM Georgia – 43 questionnaires.
Mission information not provided on the questionnaire – 3 questionnaires.

1.2.1.3. Respondent profile

- 35 respondents out of 82 reported their role at the mission.[20] I.e. Less than half of the respondents identified their exact role/unit at the mission in the questionnaire. Considering that even the respondents reporting their role carried out distinct roles/were part of different units, it can be presumed that the sample is varied and that knowledge from different ranking mission operatives has been represented.

- Questionnaire respondents providing information about their role were primarily in mid- and senior- managerial positions and/or related to cyber/situational awareness and the training related to that.

- For some missions, only explicitly senior-management/ cyber & hybrid threat related mission members responded. E.g. EUAM Iraq – questionnaire answered by HoM, EUBAM-Libya – questionnaire answered by OP assessment Adviser of training; EULEX (Kosovo) questionnaires answered by a ISO (Information Security Officer) and a Cyber security analyst & Incident Responder.

[20] Breakdown: Head of Mission (HoM) - 1; Acting director/Head of Mission (HoM) – 1; Chief of Staff (COS) – 5; Chief of Staff Office – 1; Executive Officer (HoM's office) – 1; Acting Head of Operations – 1; Deputy head of Field Office – 1; Deputy Team Leader, ABL – 1; Mission HQ – 1; MSD (Mission Support Department) Communication and Information Systems (CIS) – 3; Cyber security analyst and Incident Responder - 1; MAC (Mission Analytical Capability) – 1; Security department (INFOSEC) – 1; Security and Duty of Care Department/Security Unit – 1; Duty of Care and Security Department/Security Unit – 1; CT– 1; ISO – 1; Coordination Unit – 1; Project Cell – 1; Planning and Evaluation Department (PED) – 1 +1; PED Department/Reporting Unit – 1; Political unit – 1; HR unit – 1; Monitor – 1; Monitor/Operation Officer – 1; CP – 1; Operations Assessment Adviser-Training - 1; Field Officer (FO) – 1.

1.2.2. METHODOLOGY AND LIMITATION

1.2.2.1. Analysis methodology

- The questionnaire responses provide data for qualitative and not quantitative analysis. I.e. due to differing support level between missions, mission mandates, and the situation of host countries, the survey presents understanding and awareness amongst mission operatives of the hybrid threat and cyber themes that the consortium has already identified as relevant for CSDP members. It does not provide statistical evidence or analysis of whether the mission members find specific issues relevant or not.

- Some explanations provided by respondents are grouped under the labels + and - . These indicate respondents´ own view/tonality in the comment, not whether the points raised are positive or negative from the viewpoint of the training needs analysis.

- All answers to thematic question clusters (7) are summarised individually following the summary of responses.

- An independent/distinct summary of common themes is provided at the end of each cluster.

- An independent/distinct summary of common themes emerging in additional comments is provided in the last sub-chapter of this section.

1.2.2.2. Survey analysis limitations

- The response rate may have suffered due to a shift to remote working arrangements from March 2020 in response to the ongoing Covid-19 pandemic.

- Missions participating in the survey have different OPSEC protocols/ actions. For some missions, cyber and hybrid threats are recognised and closely monitored and relevant reports are being provided or a distinct unit is part of the mission (e.g. Georgia, Ukraine; also, new mission to CAR[21]). The same level of attention may have not been paid to cyber and hybrid threats as a constitutive part of other missions. These differences may also account for differences across missions in respondent's recognition of hybrid threats and cyber as a significant threat to the specific mission/to their mission.

- Missions participating in the survey are operating in distinct countries in which the threat landscape and level can vary significantly. These differences may also account for differences across missions in respondent's recognition of hybrid threats and cyber as a significant threat to the specific mission/to their mission.

- Some missions are currently contributing to the hybrid threat and cyber resilience building. Due to that some respondents may have different attitudes and insight into the help provided to host country than other mission members.

[21]Mini-concept on civilian CSDP support to countering hybrid threats (EEAS 8077/20), p.4.

- There is a significant difference between the amount of responses received from the EUMM Georgia and other missions. Out of the 82 respondents, 43 reported that they from the EUMM Georgia i.e. 52% of the respondents. Considering that EUMM Georgia mission members have a heightened awareness of hybrid and cyber threats, as well as specific protocols for responding to these in place, it may be that the levels of awareness indicated in responses from this mission and so a significant part of the survey is? not indicative of levels of awareness in other missions.

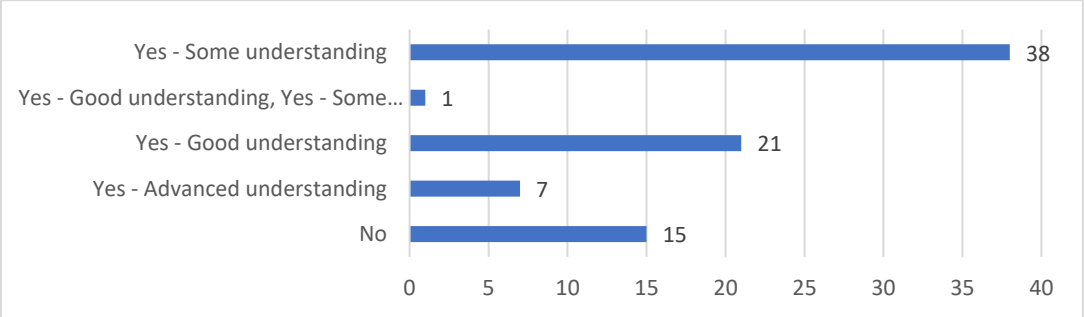
1.3. CSDP MISSION MEMBER'S TRAINING SURVEY RESULTS

1.3.1. CLUSTER I: GENERAL EU RESPONSE TO HYBRID THREATS AND CYBER

1.3.1.1. SUMMARY OF REPONSES

Q1: I am able to outline EU policy documents on tackling new security challenges, including those linked to hybrid threats.

No. of responses per choice:



Summary of explanations for level of understanding given per choice:

No understanding:

- Not part of individual mission assignment; absence of official communications or information; no training received.

Some understanding:

+ Previous civil and military mission experience; common-sense.

- Lack of access to relevant documents; novelty of topic hybrid threats; not part of individual mission assignment.

Good understanding:

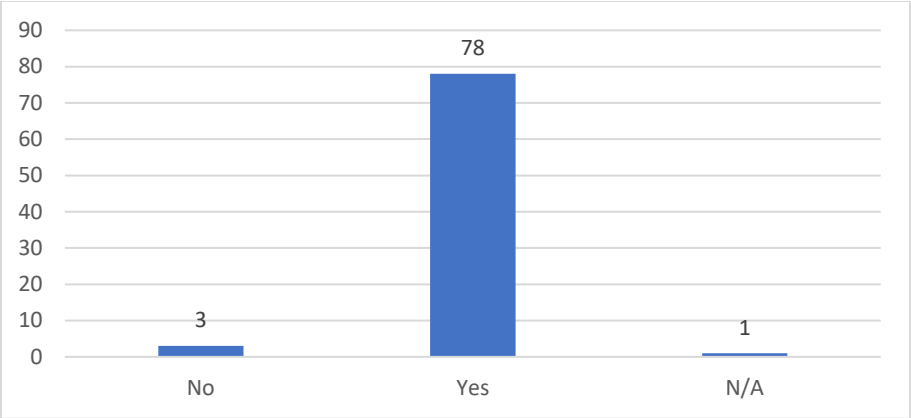
+ Part of previous role held; previous mission experience; and/or part of current role.

Advanced understanding:

+ Personal ability and interest; prior understanding; and/or part of current role.

Q 1.1: Do you think you need this knowledge as a CSDP mission member?

No. of responses per choice:



Summary of explanations given per choice:

Yes:

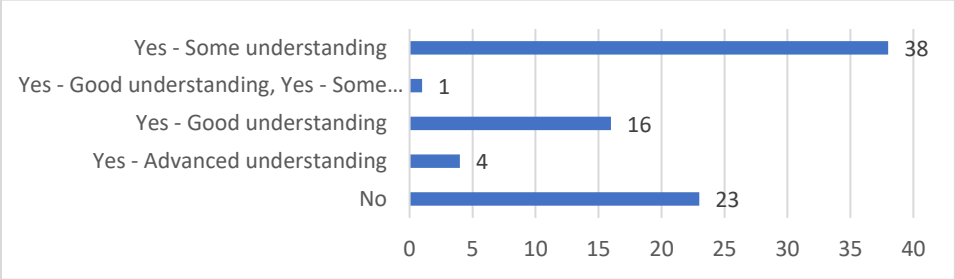
Relevant for recognition of new threats in respect to CSDP missions as well as the host state; for effectively responding to situations; conducting tasks safely; handling information and documents.

No:

Not relevant to all mission members or only broad understanding required.

Q 2: I am able to describe the overall strategic framework for EU initiatives on cybersecurity and cybercrime.

No. of responses per choice:



Summary of explanations given per choice:

No understanding:

- No relevant training; not relevant to field of speciality no relevant information shared within mission context.

Some understanding:

+ Basic understanding via specific role/job; some theoretical or general knowledge of topic.

- Primarily not field of work so no knowledge of specific frameworks; outdated information and/or documentation; lack of regularly updates on relevant (EU) policy documents.

Good/some understanding (single respondent):

+/- Knowledge in cybersecurity via role/job; less knowledge in cybercrime.

Good understanding:

+ General, if not expert, level of understanding; previous job/role related knowledge; awareness of specific policy documents; knowledge of how to access relevant documents; general awareness of policies as necessary in host nation.

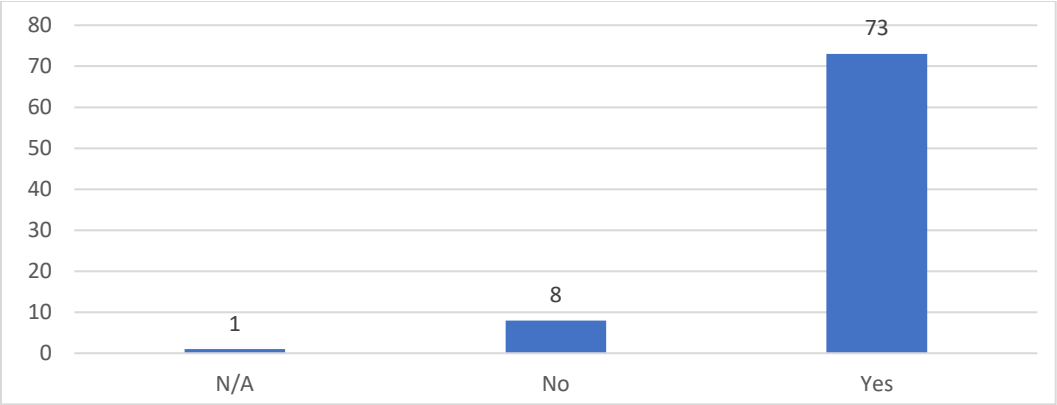
Advanced understanding (single respondent):

+ Involved in policy making.

N.B. One respondent (advanced) indicated that they were involved in the policy making.

Q 2.1 Do you think you need this knowledge as a CSDP mission member?

No. of responses per choice:



Summary of explanations given per choice:

Yes:

+ Mission work involves computer/IT work, so knowledge is immediately relevant; relevant to job roles; recognition of growing threat levels; mission may be target for cyber-attack; relevant to EU mandate under which missions operate.

- Necessary given policy trends, but overemphasised; relevant but lack of training; need for refresh on current frameworks.

No:

Job/role does not demand specialist knowledge; only relevant when risk of espionage is high.

1.3.1.2. ANALYSIS

CLUSTER I: GENERAL EU RESPONSE TO HYBRID THREATS AND CYBER

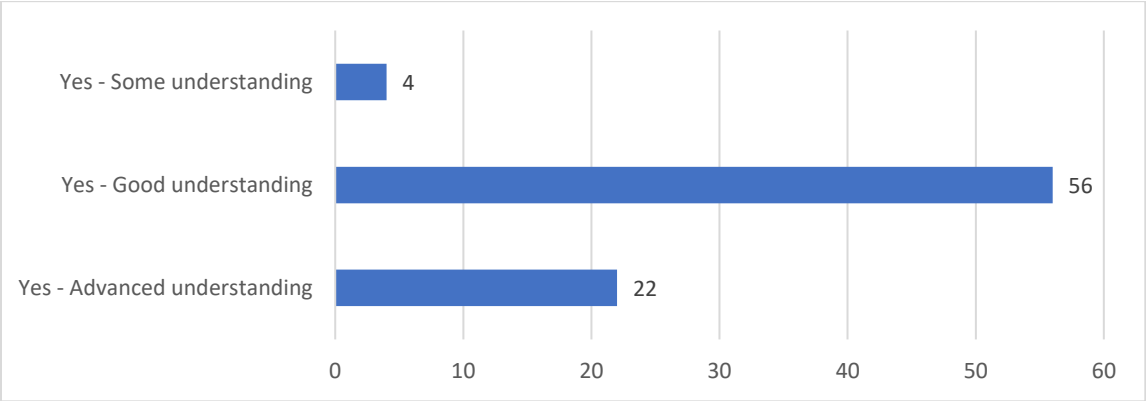
I. In general, respondents who state that they have some/good/or advanced knowledge of the 'GENERAL EU RESPONSE TO HYBRID THREATS AND CYBER' do not refer to the relevant EU policy documents and offer only vague explanations of the source of their purported understanding of the issues.
II. Respondents who state that they have good or advanced knowledge frequently cite previous experience or career work as the source of this knowledge.
III. Along similar lines to (II) a number of respondents suggest that their knowledge comes from a personal interest in the area, not from any training received.
IV. Most respondents indicated that knowledge/understanding referred to in this cluster is relevant to the mission. However, in line with (I-III), respondents frequently emphasised the need for more or further training in the area; especially refresher training on developments to frameworks, new threats, and hybrid threats.
V. Explanations for a lack of knowledge included:
    a. Lack of access to relevant documents
    b. Access only to outdated documents and material
    c. Lack of training
    d. The respondent's view that the knowledge/understanding in question was not relevant to their particular job or role on the mission
VI. Differences in level of understanding as well as attitudes towards the relevance of knowledge of the 'GENERAL EU RESPONSE TO HYBRID THREATS AND CYBER' to mission members, to some degree track the respondent's role or job with the context of the mission.

1.3.2. CLUSTER II: SAFE USE OF WORK-RELATED SYSTEMS AND DEVICES IN MISSION PREMISES

1.3.2.1. SUMMARY OF REPONSES

Q 3: How familiar am I with mission rules, guidelines and/or procedures on handling and use of hardware; digital communication related issues (e-mail, chats), software and applications (e.g. WhatsApp and other applications)?

No. of responses per choice:



Summary of explanations given per choice:

Some understanding:

+ Common-sense; discussions with mission security analysts.

- (Implied, lack of official training.)

Good understanding:

+ Knowledge of relevant SOPs; MAC activities and documents provide relevant support; part of mission preparation; part of CIS or relevant team; information received in remote work period since March 2020.

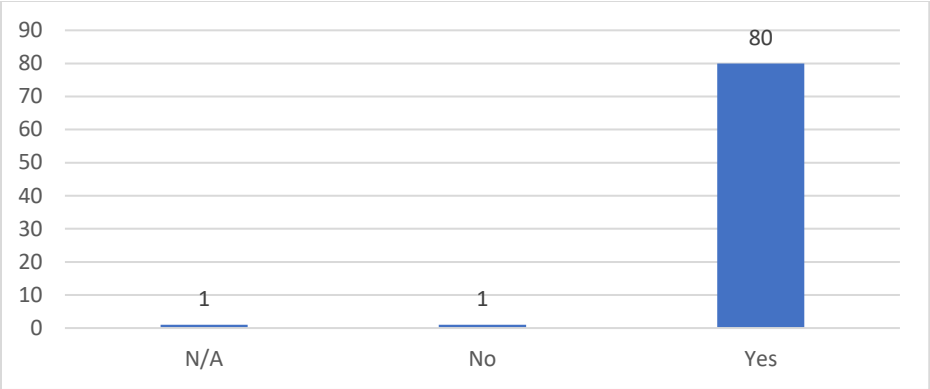
- Lack of clarity in policy considering shifts in approved communication channels.

Advanced understanding:

+ Well briefed by mission CIS; regular updates received; currently or formerly part of CIS or relevant team; aware of mission SOPs.

Q 3.1 Do you think you need this knowledge as a CSDP mission member?

No. of responses per choice:



Summary of explanations given per choice:

Yes:

Matter of OP security; risks are relevant to mission's day-to-day assignments; general security risks; increased relevant to missions current remote-work status; necessary to prevent leaks of sensitive information (mission-specific and personal); necessary to mission integrity; job/role.

No (single respondent):

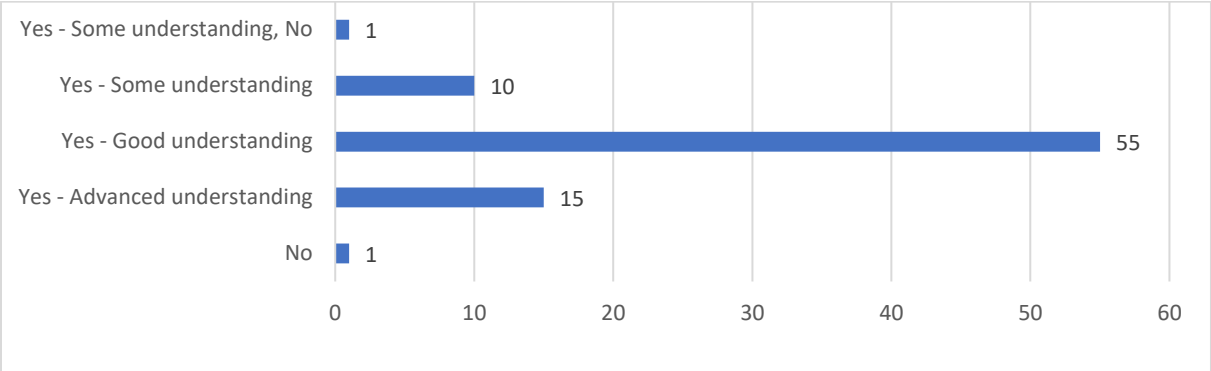
No explanation provided.

N/A (single respondent):

No explanation provided.

Q 4. I am familiar with EU rules, Mission guidelines and/or procedures on secure use of mission related IT-systems

No. of responses per choice:



Summary of explanations given per choice:

No understanding:

- No relevant information received.

No/Some understanding:

+ Common sense.

Some understanding:

+ Implementation of basic guidelines if priority to MAC.

- Not part of specific role/duties.

Good understanding:

+ Rules to check and follow on day-to-day basis are clear; part of role/job – including updating knowledge, implementing rules on system; training received; information from CyberCell; awareness of mission rules; necessary to prevent cyber/hybrid rules.

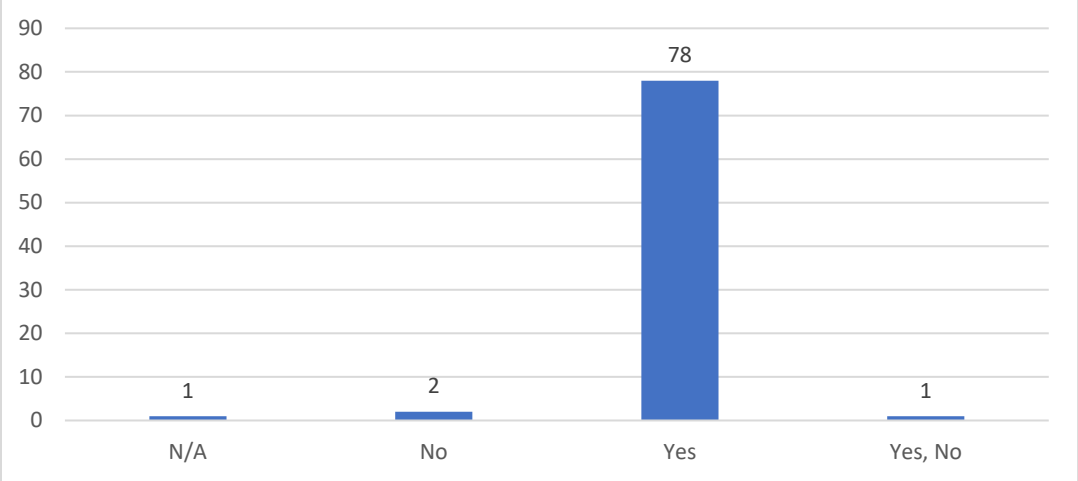
- Lack of awareness of EU roles; SOP needs to be updated in response to latest threats.

Advanced understanding:

+ Well covered in the training/mission preparation; independent interest in field; current role is in IT; previous job/roles; SOP on CIS.

Q 4.1: Do you think you need this knowledge as a CSDP mission member?

No. of responses per choice:



Summary of explanations given per choice:

No:

SOP on CIS already in place on mission (both respondents part of EUAM Ukraine).

Yes:

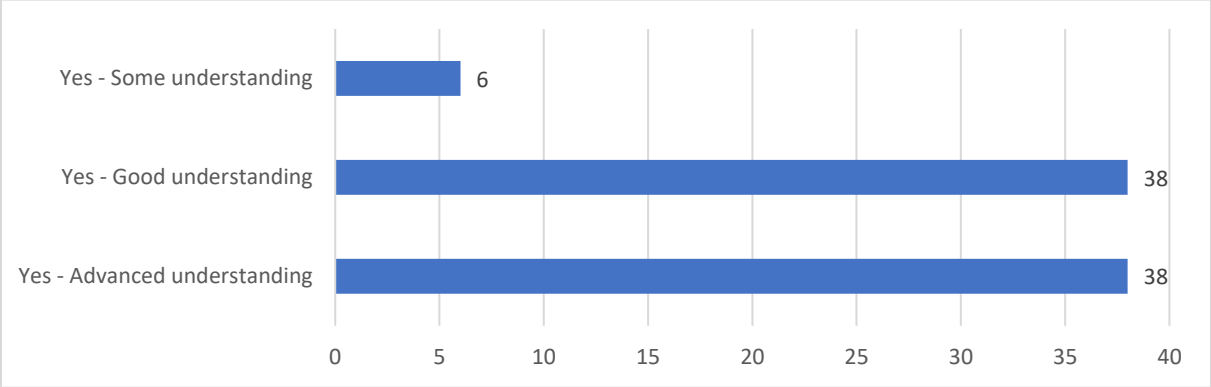
Necessary to minimise risk of cyber-attacks; ensure communication and data protection; maintain mission IT system security; prevent leaks of personal and mission information; safely conduct day-to-day assignments. Relevant to job/role/duties.

Additional comments:

Update/refresher training every two/three years would be useful.

Q5: I am familiar with EU/Mission rules and procedures on handling official, sensitive and/or classified (secret, confidential, restricted) information/documents available to me on the mission

No. of responses per choice:



Summary of explanations given per choice:

Some understanding:

+ General awareness of rules (though not relevant to current job/roles); need to know the difference between classified/secret/confidential/restricted documents.

Good understanding:

+ Necessary for level of security clearance; rules clearly reported; good training; awareness of relevant documents; updates received.

- Understanding limited to level of security clearance; would need further training if in new assignment/role.

Additional comment: General problem of exchanging classified information with EUDEL and the EUSR due to lack of access to RUE[22] and ARES[23].

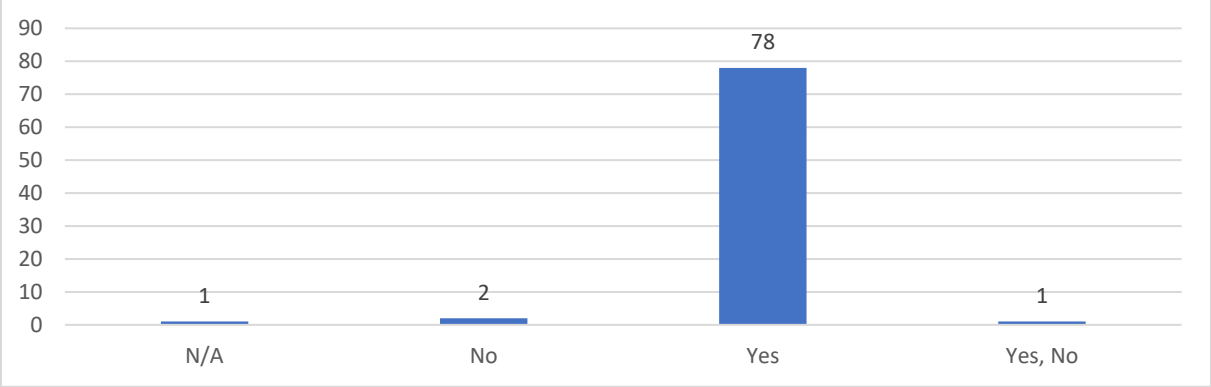
Advanced understanding:

+ Formal training (national and mission specific) is mandatory; part of mission work; part of host country specific work; previous roles/missions; security clearance level.

[22] RUE – Restreint UE (EU restricted documents)
[23] ARES – Advanced REcords System (electronic document management system)

Q 5.1: Do you think you need this knowledge as a CSDP mission member?

No. of responses per choice:



Summary of explanations given per choice:

No:

+ Sufficient training already received.

Yes/No:

- Further training in relation to hybrid threats needed.

Yes:

+ Vital to understand overall importance of OPSEC, misuse of documents can compromise entire mission; general mission members require general knowledge; specific jobs/roles call for specialist knowledge; necessary for day-to-day work with classified documents.

- Colleagues do not follow rules closely; incidents due to failure to following protocol have been reported previously.

1.3.2.2. ANALYSIS

CLUSTER II: SAFE USE OF WORK-RELATED SYSTEMS AND DEVICES IN MISSION PREMISES

I. All respondents reported some, good, or advanced understanding when it comes to familiarity with mission rules, guidelines and/or procedures on handling and use of hardware; digital communication related issues and also when it comes to the safe use of mission related IT-systems.

II. Respondents were primarily of the attitude that knowledge of the relevant procedures for handling hardware and usage of communication devices is relevant to their status as mission members and to mission security in general.

III. All respondents indicated that they have at least some, but primarily good or advanced understanding of the protocols for handling specifically sensitive/classified data.

IV. Relevant to (II and III), and despite (I), a common theme in the longer answers, was concern that data in general (i.e. including personal as well as sensitive/classified data) is not currently handled with sufficient care and rigour and that protocols need to be followed more closely. In line with this:
    a. One respondent pointed particularly to the use of informal communication channels by mission members (e.g. WhatsApp) and the lack of official communication channels apart from e-mail, as areas for concern.
    b. One respondent pointed to the continuous change of accepted forms of mission communication and a lack of clarity as a result of that as a source of the shortcomings in mission security.
        i. Relevant to b. prior civilian or military experience, as opposed to current training for the role in the mission in question, was commonly cited as a source of knowledge.

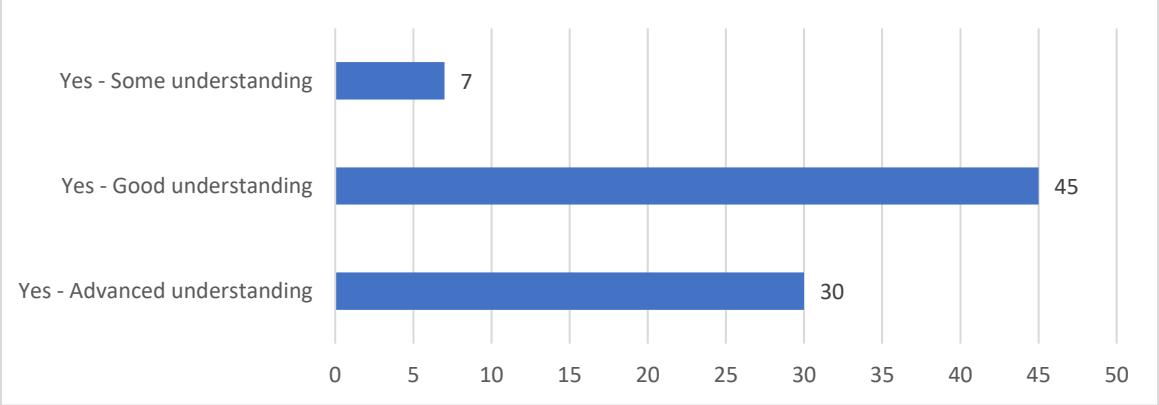
V. A number of respondents, especially from EUAM Ukraine, whilst stating that their awareness of cyber-security issues in this area was sufficient for their role on the mission, cited the move to remote/online work since March 2020 as the source of this awareness. This would appear to indicate a lack of awareness prior to the special circumstances giving rise to that period (i.e. changes to work patterns as a result of the Coronavirus pandemic).

1.3.3. CLUSTER III: SAFE USE OF PERSONAL DEVICES OUTSIDE MISSION PREMISES

1.3.3.1. SUMMARY OF REPONSES

Q 6: How competent am I regarding the use of hardware, digital communication related issues (e-mail, chats, social media), software and applications (e.g. WhatsApp and other applications) outside the mission premises (e.g. at home)?

No. of responses per choice:



Summary of explanations given per choice:

Some understanding:

+ General understanding; need to distinguish between personal and job-related technology use.

- No special technical skills.

Good understanding:

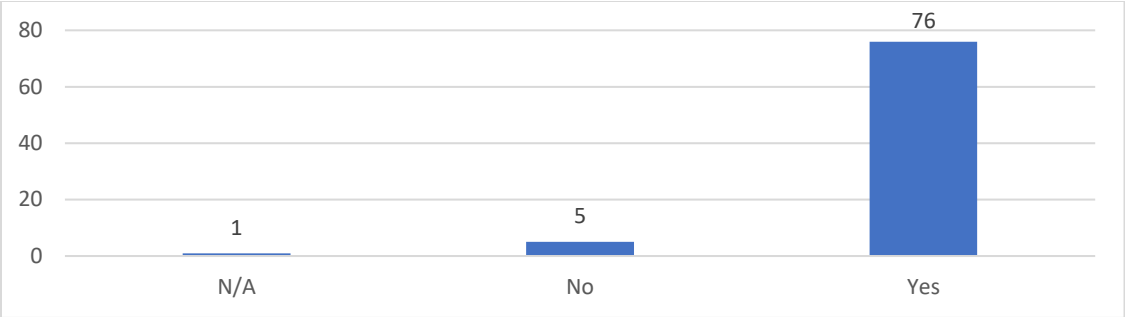
+ Job/role related; IT specialist; training received; increased attention due to period of remote working since March 2020; need to distinguish between personal and job-related technology use.

Advanced understanding:

+ Specific to job/role as part of CIS team; personal interest in IT and information security; previous higher-education; additional guidance received due to period of remote working since March 2-2-; need to distinguish between personal and job-related technology use.

Q 6.1: Do you think you need this knowledge as a CSDP mission member?

No. of responses per choice:



Summary of explanations given per choice:

No:

Not necessary as CSDP member; should be permitted to use preferred technology/devices; not necessary even if additional information would be useful.

Yes:

Necessary given shift to remote working since March 2020; knowledge also useful beyond current situation. Necessary to protect mission and mission sensitive information; to safely use informal communication channels.

N/A (single respondent):

No explanation provided

1.3.3.2. ANALYSIS

CLUSTER III: SAFE USE OF PERSONAL DEVICES OUTSIDE MISSION PREMISES

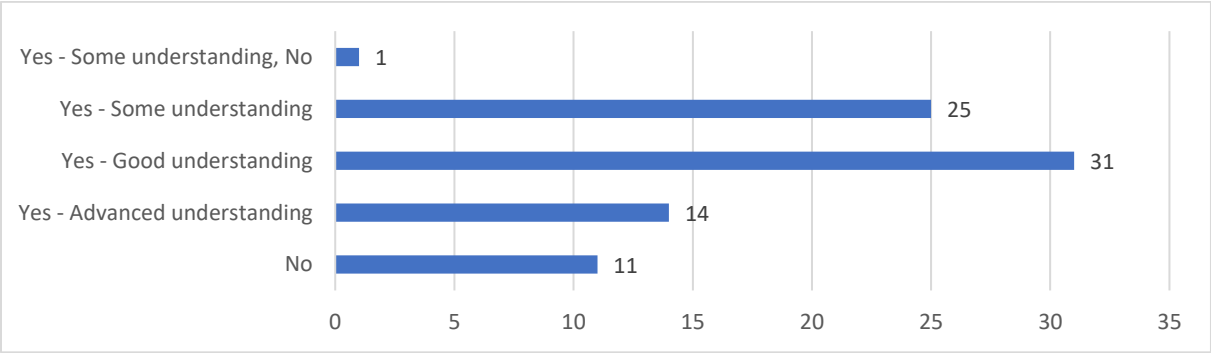
I. All respondents indicated at least some, but primarily good or advanced understanding of the 'SAFE USE OF PERSONAL DEVICES OUTSIDE MISSION PREMISES'.
II. A common theme amongst longer answers was the need to distinguish between personal and job-related technology use.
III. Whilst the majority of respondents indicated that knowledge in this area is relevant to their status as a CSDP mission member, and for protecting the mission and mission sensitive information, a common theme in longer answers was that this had become the case since the shift to remote working post-March 2020.
IV. Additionally, respondents who reported good or advanced understanding of this area, cited personal interest, prior education or career based experience, or specific role in the mission as the source of this understanding. This would appear to indicate that despite attitudes towards the relevance of this area (see III) there are significant differences in understanding across the cohort.

1.3.4. CLUSTER IV: SITUATIONAL AWARENESS

1.3.4.1. SUMMARY OF REPONSES

Q 7: I am able to describe the content of regular /periodical updates about the mission environment, in relation with possible cyber/hybrid threats, specific to the country/area that I am in

No. of responses per choice:



Summary of explanations given per choice:

No understanding:

- No updates received; cyber- hybrid-threats not covered in updates; lack of sufficient training; respondent is not an expert; no updates on mission-specific cyber- hybrid-threats.

Some/No understanding:

No explanation given.

Some understanding:

+ Awareness of situation in mission host state; updates received; personally keeping up to date on developments in area.

- Not relevant to mission; not part of relevant security issues. Updates on recent/new threats do not explain general significance.

Good understanding:

+ Updates from CyberCell or MAC or CERT-EU; personal interest in area; prior knowledge; writing reports is part of job/role; updating system is part of job/role.

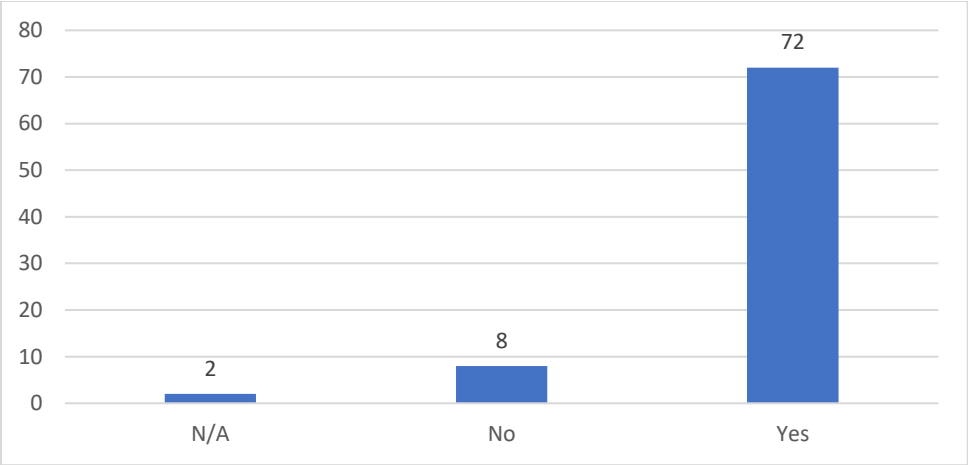
Advanced understanding:

+ Part of role; personal interest/effort; clear updates are received.

- Updates are limited in number.

Q 7.1: Do you think you need this knowledge as a CSDP mission member?

No. of responses per choice:



Summary of explanations given per choice:

No:

Not relevant to job/role or area of expertise; global awareness of current/possible threats is important, but no further training required; terminology in area is too complex.

Yes:

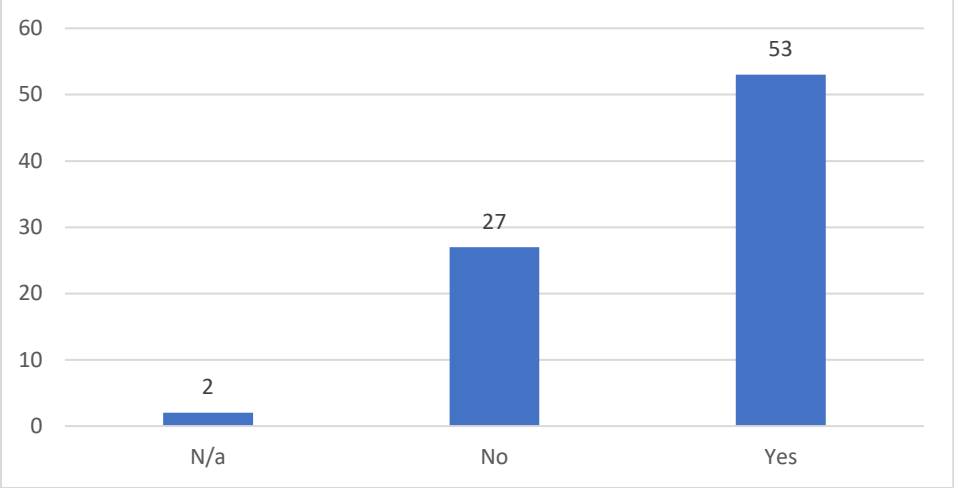
+ Relevant to specific job/role; mission members should understand and be aware of threats in mission environment/host state; key to proper mission-specific coordination with host state; useful for mitigating mission risks; prevention of mission member vulnerability.

- Missions are too slow to adapt to changing threats in host states

N.B. One of the N/A respondents indicated that they were unsure about the relevance.

Q 8: According to my opinion, the regularity of those newsletter/up-dates is sufficient and timely

No. of responses per choice:



Summary of explanations given per choice:

No:

- Updates are not regular; have received too few or no updates; updates are sufficient but not timely; lack of understanding of areas covered; lack of information sharing between relevant EU institutions and other missions; updates are not sufficiently focused; updates are not timely; updates are too technical.

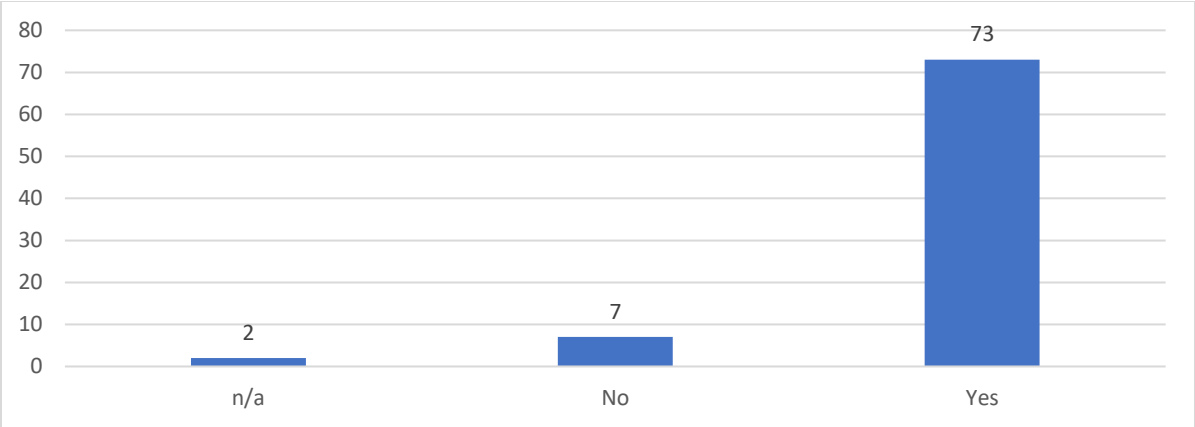
Yes:

+ Regular reports from relevant department received; training received every 6 months in FO; part of respondent's job/role; seems sufficient but respondent is not a specialist; seems sufficient due to lack of recent incidents.

- Recent updates have been information but do not pay sufficient attention to hybrid threats aside from disinformation and cyber-security; regularity of newsletter depends on the threat level.

Q 8.1: Do you think you need this knowledge as a CSDP mission member?

No. of responses per choice:



Summary of explanations given per choice:

No:

In-principle important information, but not relevant to all mission members in same depth. Lack of interest in topic. Current knowledge is sufficient.

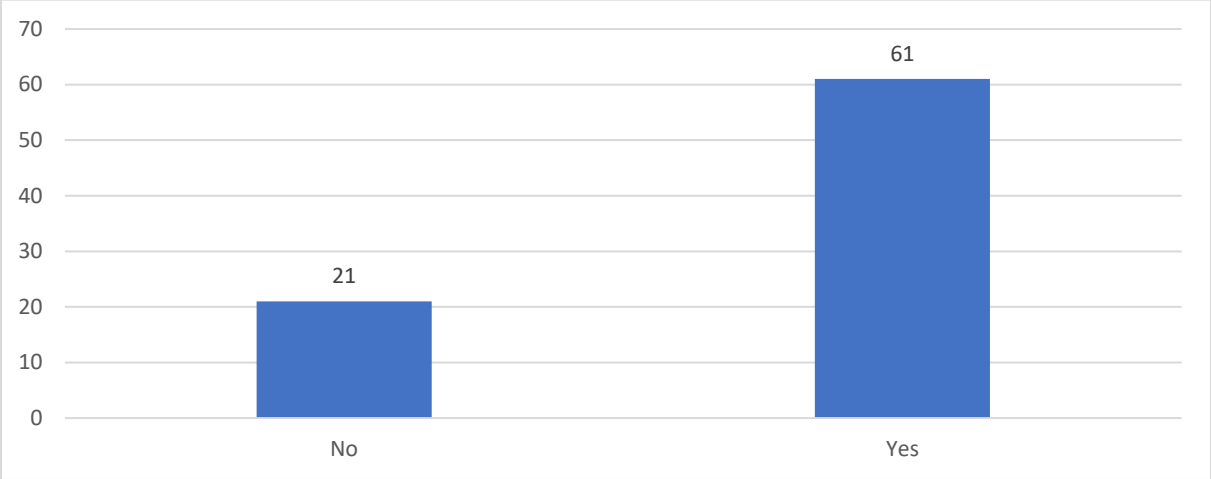
Yes:

+ Enhanced awareness is necessary; awareness of threats in environment is necessary; knowledge of wider context in host nation/region is necessary; relevant to IT security; relevant to all missions; updates can enhance overall security level.

- Insufficient number/depth of updates; information should provide more detail on situation in host nation; reports could be more accessible.

Q 9: According to my knowledge, hybrid threats and cyber security are currently recognised as issues for the host State of the Mission

No. of responses per choice:



Summary of explanations given per choice:

No:

Main threat in host nation is terrorism, hybrid- and cyber-threats are not priority; not relevant in host nation; host country not advanced enough for proper response to threats even if present; threats are more likely to be to mission than to state.

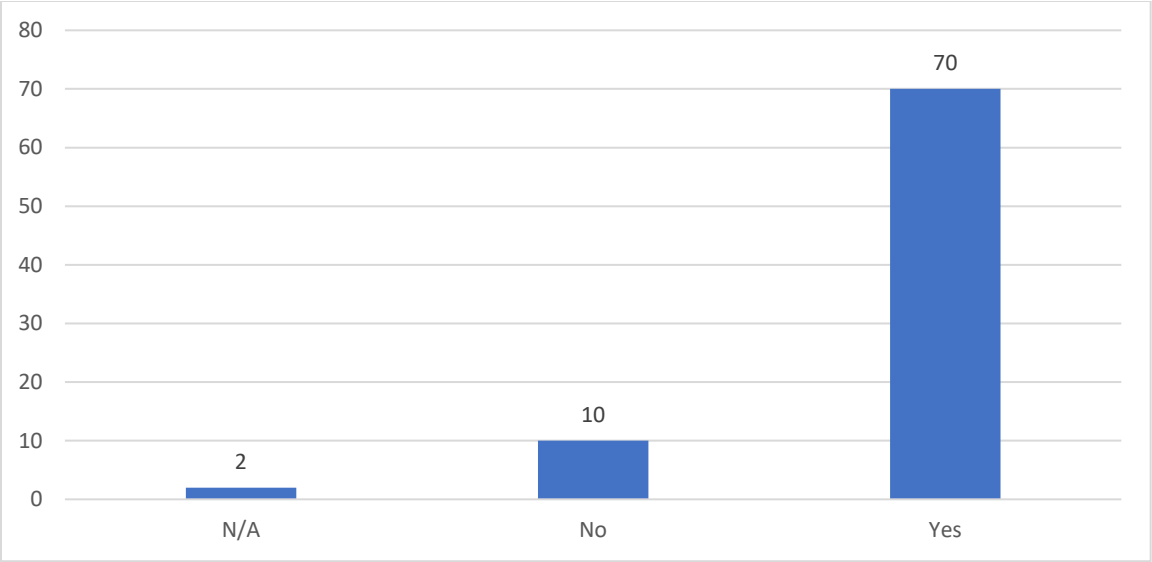
Yes:

+ Host country has a strategy paper in place; host nation is aware and has relevant institutions in place; mission has analyst in place;

- Implementing strategy paper is not priority of host nation; threats are recognised but host state lacks resources to respond; relevant measures may be in place, but little awareness in mission.

Q 9.1: Do you think you need this knowledge as a CSDP mission member?

No. of responses per choice:



Summary of explanations given per choice:

No:

Not relevant to area of expertise; following government action/politics in host state is not relevant to job/role.

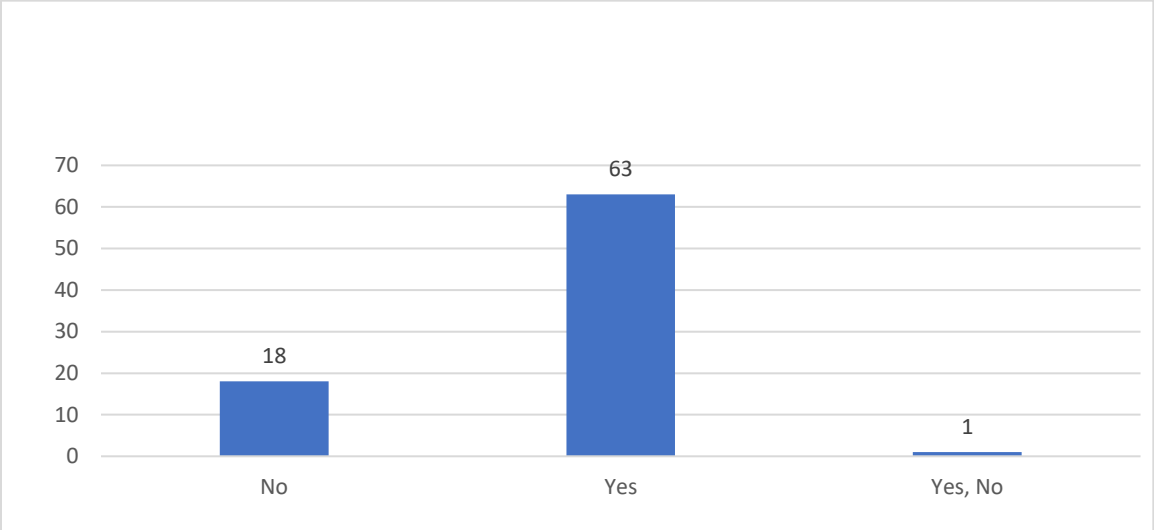
Yes:

+ Relevant to current job/role; relevant background knowledge even if not related to job/role; host nation has been subject to hybrid attacks in past; necessary to understand the operating environment/host nation; mission aims include assessing host states capability to respond to hybrid threats; up-to-date awareness of threats is relevant for strategic response, recovery, etc.

- Further training required, especially for protection of mission/personal data and information.

Q 10: I believe the host State will be interested in receiving Mission support in this area (training, advice etc.)

No. of responses per choice:



Summary of explanations given per choice:

No:

Host state has other priorities; outside of mission mandate; host state already able to respond to threats; EU provides support through other institutions.

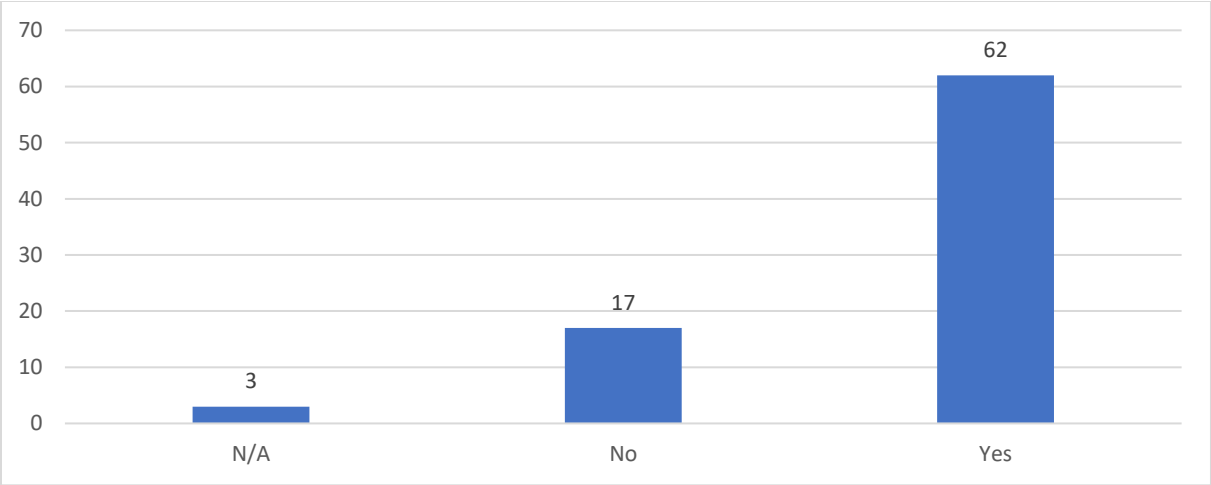
Yes:

+ Hose state should have capacity to recognise threats; nation state is open to EU support in all areas.

- Respondent believes mission support is relevant, but host state has different properties. Host state would be interested, but support should come from EU delegation or is already provided by NATO. Host state would be interested but mission requires further pre-training, re-structuring of agenda/mandate.

Q 10.1: Do you think you need this knowledge as a CSDP mission member?

No. of responses per choice:



Summary of explanations given per choice:

No:

Not relevant to respondent's area of expertise; not relevant to job/role; not relevant to mission mandate; mission does not have resources to provide support.

Yes:

Would increase efficiency of respondent's work; necessary part of understanding operative environment; relevant to compliance work; relevant to specific job/role; useful to establish relevant contacts; generally relevant to mission in host state.

1.3.4.2. ANALYSIS

CLUSTER IV: SITUATIONAL AWARENESS

I. Answers to the questions in the cluster on 'SITUATIONAL AWARENESS' indicate notable differences in knowledge across difference missions, e.g. a large number of respondents from Georgia and Ukraine indicated a higher level of understanding of hybrid threats and familiarity with threat analysis, whereas some respondents from other missions (e.g. Somalia) reported a lack of reports on specific hybrid or cyber threats.

II. Reflecting (I) some respondents indicated concerns with the lack of reports/ updates on threats from outside of the specific mission context (i.e. reports on the global situation, or on other missions).

III. Related to (II), respondents indicated concern that there is a deficit of information on threats to the host-country as a whole that respondents felt would be relevant to mission success.

    a. More specifically, one respondent voiced concerns with the capability on-mission to respond to new or changing threats arising in the mission context vis-à-vis the host country.

    b. Additionally, a common theme in longer answers was that more could be done to inform the host-countries of cyber/hybrid threats – though this would require additional training for mission members.

IV. Concerning more specifically in-mission understanding, respondents indicated concerns that reports are too technical and so in-accessible to general mission members – whilst at the same time most respondents were of the opinion that such information is relevant to mission security.

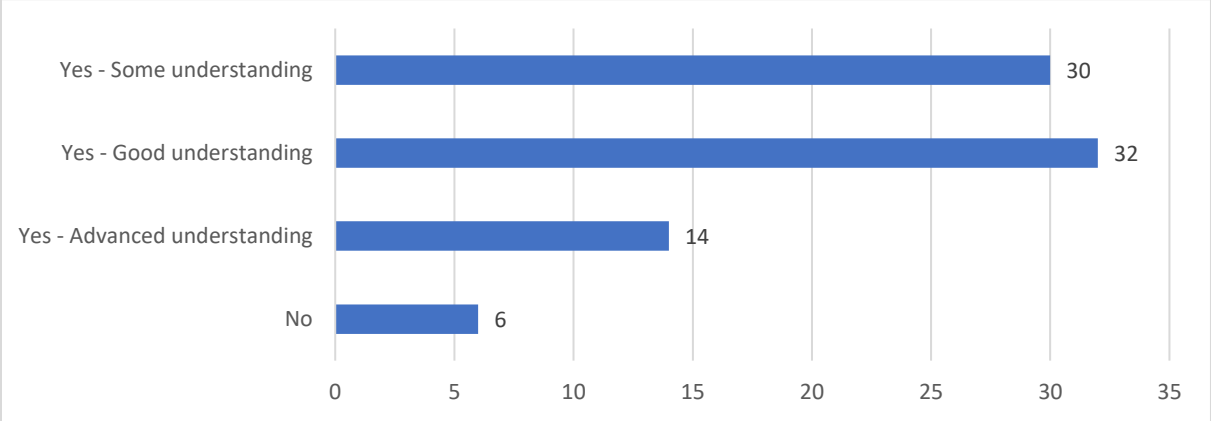
V. Related to (IV) frequently given explanation of higher levels of understanding (i.e. good/advanced) were prior job/career experience, personal interest, and the need for such understanding as a part of the respondent's specific role/job on the current mission.

1.3.5. CLUSTER V: HYBRID THREATS

1.3.5.1. SUMMARY OF REPONSES

Q 11: I am able to outline the main characteristics of a hybrid threat

No. of responses per choice:



Summary of explanations given per choice:

No understanding:

- No training received/no advanced training received.

Some understanding:

+ Some training; personal research via internet.

- Not enough training; lack of common approach to training on hybrid threats; would benefit from briefings on mission specific hybrid threats.

Good understanding:

+ Attendance of seminars and meetings; CyberCell reminders; relevant briefs; part of job/role.

- Local hybrid threat group established, but not providing expert level training; opportunity to develop understanding limited to those with specific job/roles.

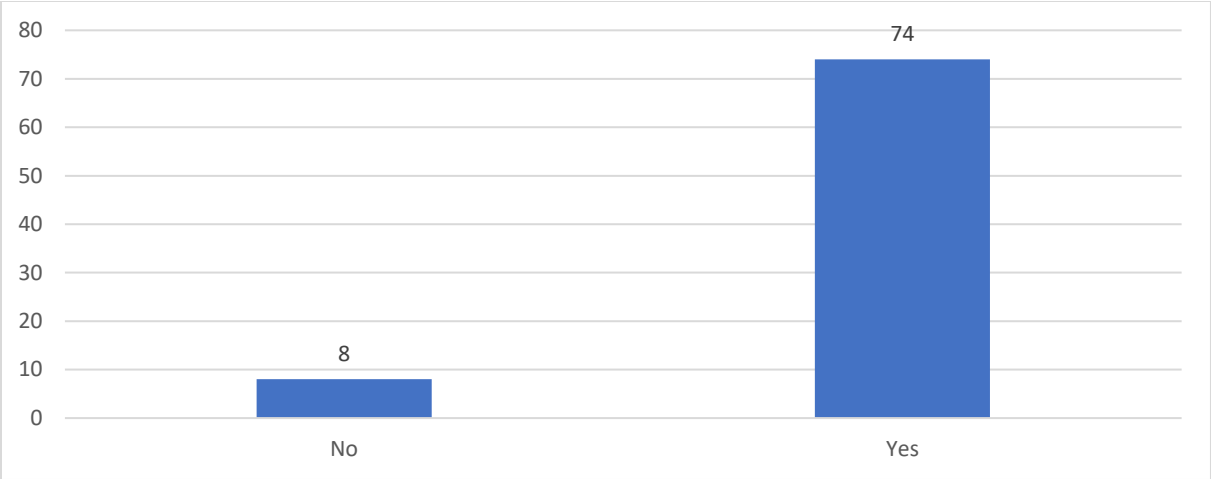
N.B. One respondent suggested that whilst the term 'hybrid threat' is new, they have prior training on/understanding of this kind of threat.

Advanced understanding:

+ Previous job/role/post; current posting (esp. Ukraine/Georgia; personal interest.

Q 11.1: Do you think you need this knowledge as a CSDP mission member?

No. of responses per choice:



Summary of explanations given per choice:

No:

Not all mission members need specialist knowledge, though there is a strong need for mandatory basic training and awareness briefing.

Yes:

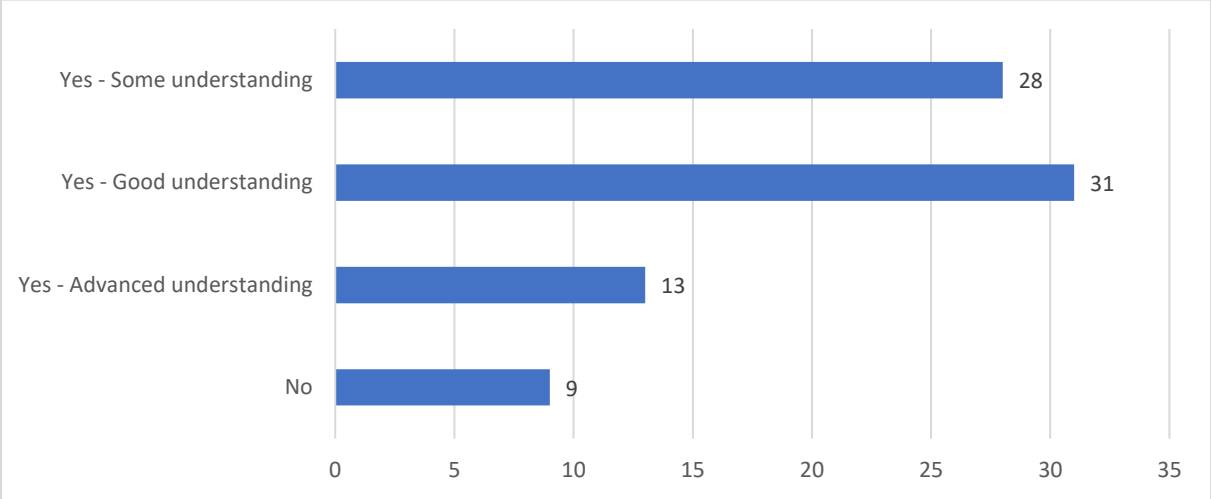
+ Important for understanding broader context of mission; basic example driven training is important for awareness of relevant threats; required to effectively carry out specific jobs/roles; adapting to changing threat environment; expectation for training.

- Mission specific training/briefing is important but prior general training is not helpful.

N.B. General emphasis on need only for basic knowledge.

Q 12: I am able to describe different kinds of hybrid threats and the different ways in which they can occur

No. of responses per choice:



Summary of explanations given per choice:

No understanding:

- No training received; no advanced training received.

Some understanding:

+ Prior understanding; understanding acquired through job/role.

- No in-depth understanding; lack of training; more training required to be fully competent.

Good understanding:

+ Attendance of relevant seminars/work-groups; CyberCell reports; part of current job/role; prior experience and understanding; mission specific reports; training received.

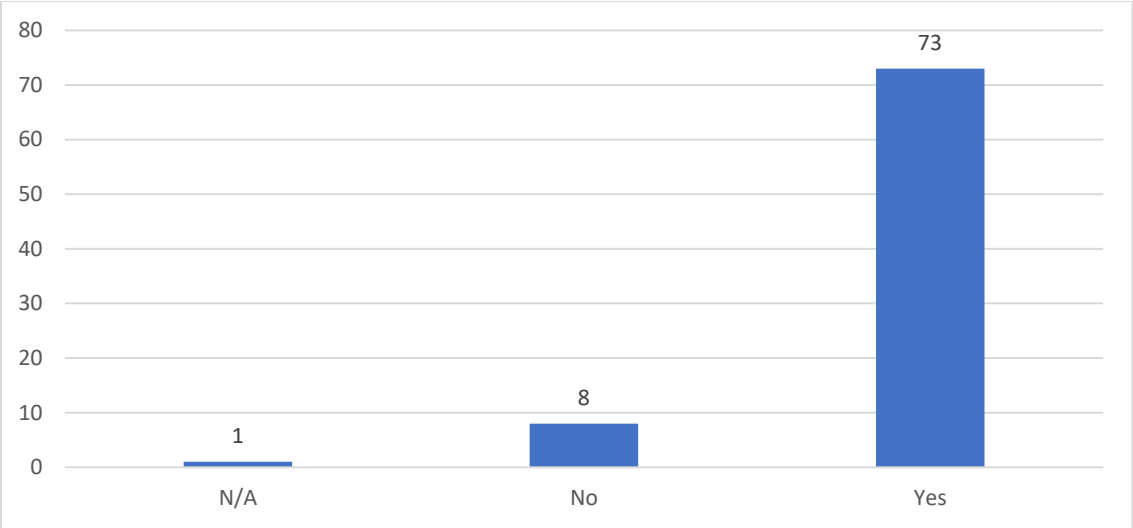
Advanced understanding:

+ Part of job/role; prior experience and training.

N.B One respondent stated that they under stood the concept but were of the view that it confuses war and peace time.

Q 12.1: Do you think you need this knowledge as a CSDP mission member?

No. of responses per choice:



Summary of explanations given per choice:

No:

Not relevant to job/role; expertise in area not required; greater emphasis when developing OPSEC is required but discrete training in area is not.

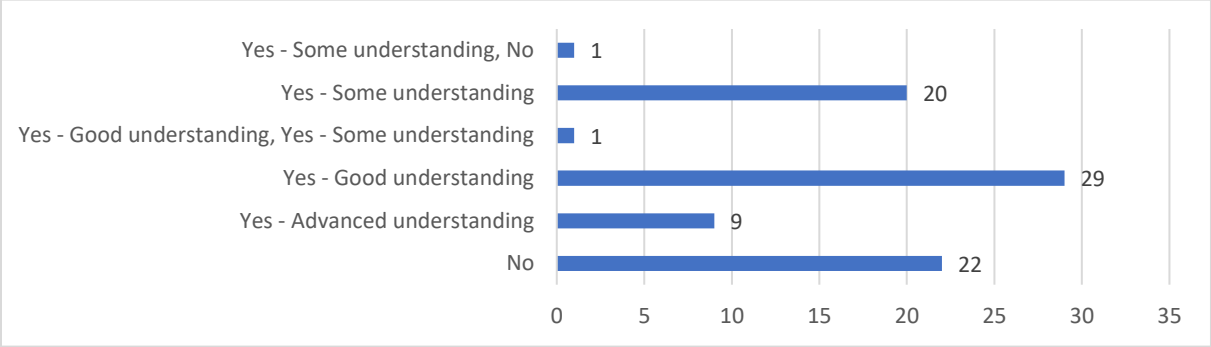
Yes:

Awareness would help accomplish task/job; help to react/adapt to changing situations; would contribute to situational awareness in host-nation; necessary for protection of IT systems; necessary for general mission security; relevant to all mission jobs/roles.

- Lack of training in area at the moment.

Q 13: I am able to assess any location specific information made available to me for the potential of hybrid threats

No. of responses per choice:



Summary of explanations given per choice:

No understanding:

- Do not understand question; no training received; no advanced training received; cannot easily access location specific information.

Some/no understanding:

+ Would be important to develop training opportunities in matter.

Some understanding:

+ Some units of CyberCell and ISO have expertise already; part of job/role; keeping up to date on location-specific information from other mission briefs (i.e. EUAM).

- More training required; more updates required.

Some/good understanding:

+ Information is available but access/understanding is time-consuming.

Good understanding:

+ Part of job/role; reports available; location-specific information available; personal interest in topic

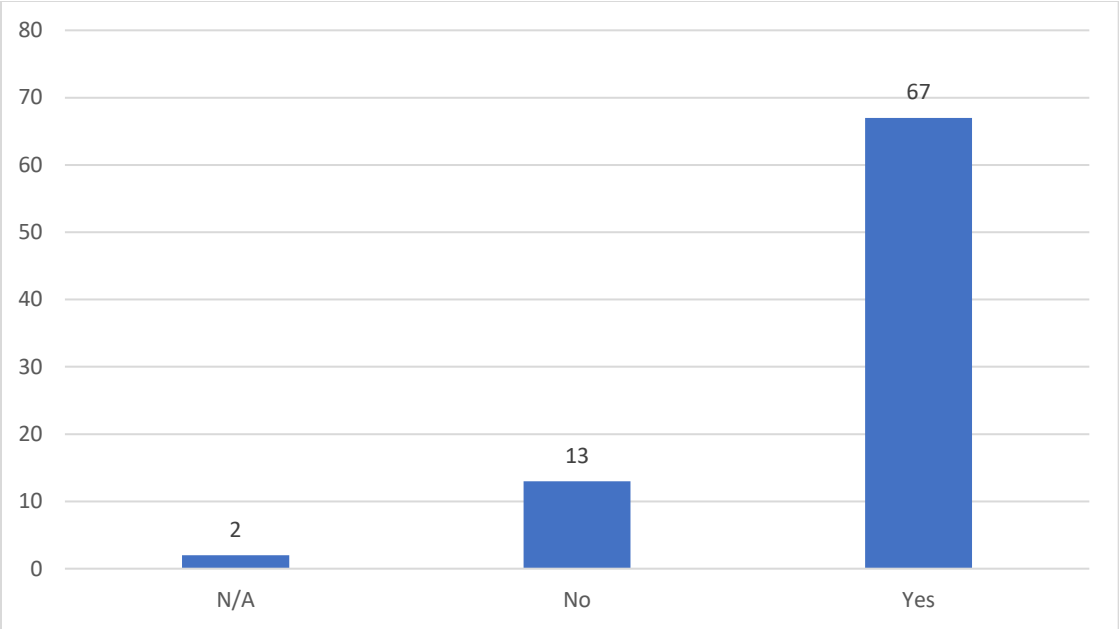
- Good understanding but lack of time to assess relevant threats.

Advanced understanding:

+ Extensive prior and ongoing experience; access to relevant information and reports; high importance to mission location.

Q 13.1: Do you think you need this knowledge as a CSDP mission member?

No. of responses per choice:



Summary of explanations given per choice:

No:

Expertise not required for job/role; training only required for specific specialists; would be more helpful if built into OPSEC.

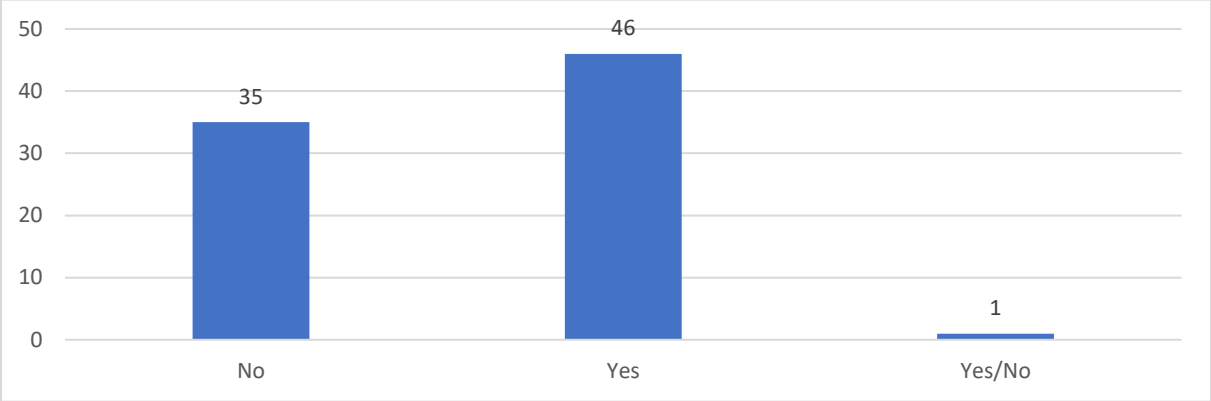
Yes:

+ Necessary to accomplish job/role; would enhance personal portfolio; crucial for mission security; necessary for proper awareness of mission situation; useful for responding to changing situations; useful when filing reports.

- Further training is required.

Q 14: Does any location specific information made available to me specifically refer to hybrid threats or potential hybrid threats in the mission area?

No. of responses per choice:



Summary of explanations given per choice:

No:

Information not received; information is not relevant in location or stage of mission; do not have training to assess whether information is received; information received only covers typical threats (e.g. spam, phishing); information is received from local and EU partners but specifically concerning hybrid-threats; information is acquired via internet/news not from official reports.

Yes/No

Information is received sometimes but not on all missions.

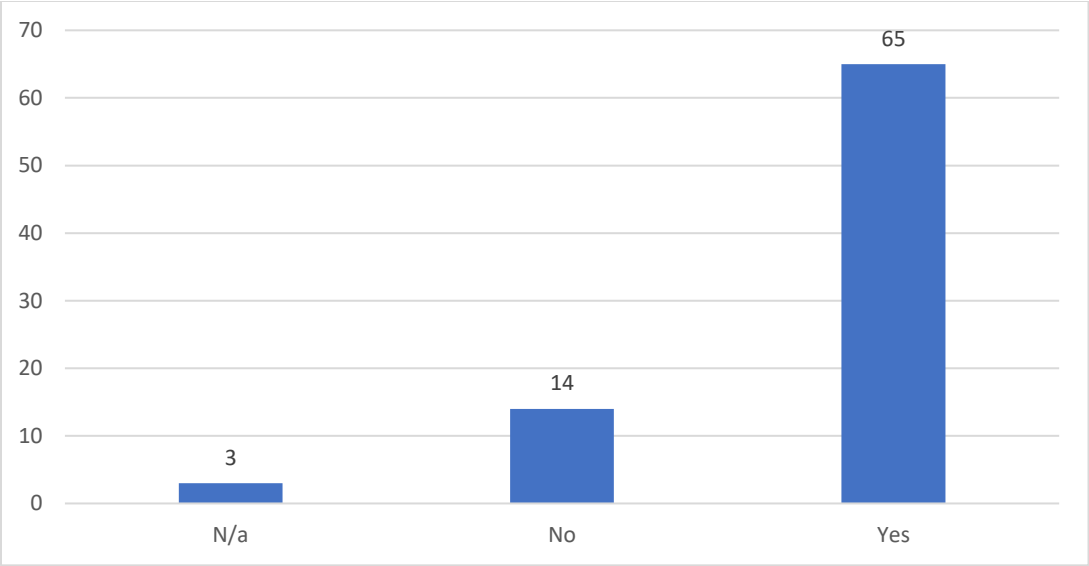
Yes:

+ MAC unit deals with this information; working on hybrid-threats; part of job/role; press office updates; mission area specific reports; hybrid-threat report in development.

- Information received but limited; common-sense to assess local situation; indirect awareness via other reports.

Q 14.1: Do you think you need this knowledge as a CSDP mission member?

No. of responses per choice:



Summary of explanations given per choice:

No:

Too specialist to be relevant to host-state; should be part of OPSEC development; only relevant to specific jobs/roles.

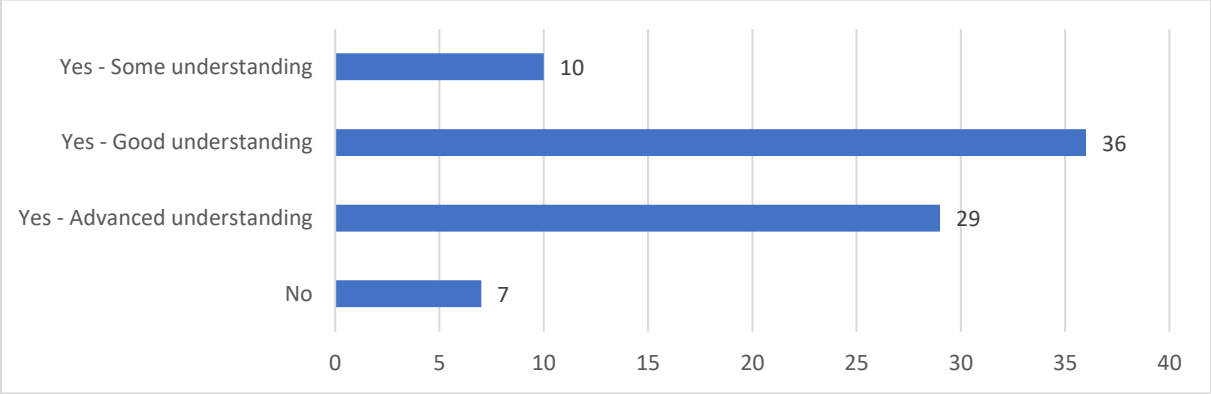
Yes:

+ Basic knowledge would be useful; necessary to protect mission/mission security; useful for raising situational awareness; relevant to specific host-states; improves capacity to respond to changing situations.

- Necessary, but more effective information exchanged required; could be better methods of sharing information between institutions; information gap between mission and EU institutions.

Q15: I am familiar with the procedures on who to contact (in the Mission/in Brussels) in case of evidence or suspicion of a hybrid threat incident that has already occurred

No. of responses per choice:



Summary of explanations given per choice:

No understanding:

- No awareness of procedure; first contact would be line-manager or experts in mission HQ.

Some understanding:

+ Aware of mission specific procedures; independently updating understanding.

- Not aware of procedures in EU institutions.

Good understanding:

+ Part of job/role; have received clear instructions/training; procedures already in place; aware of first stage of procedures, i.e. contacting mission security; follow SOP.

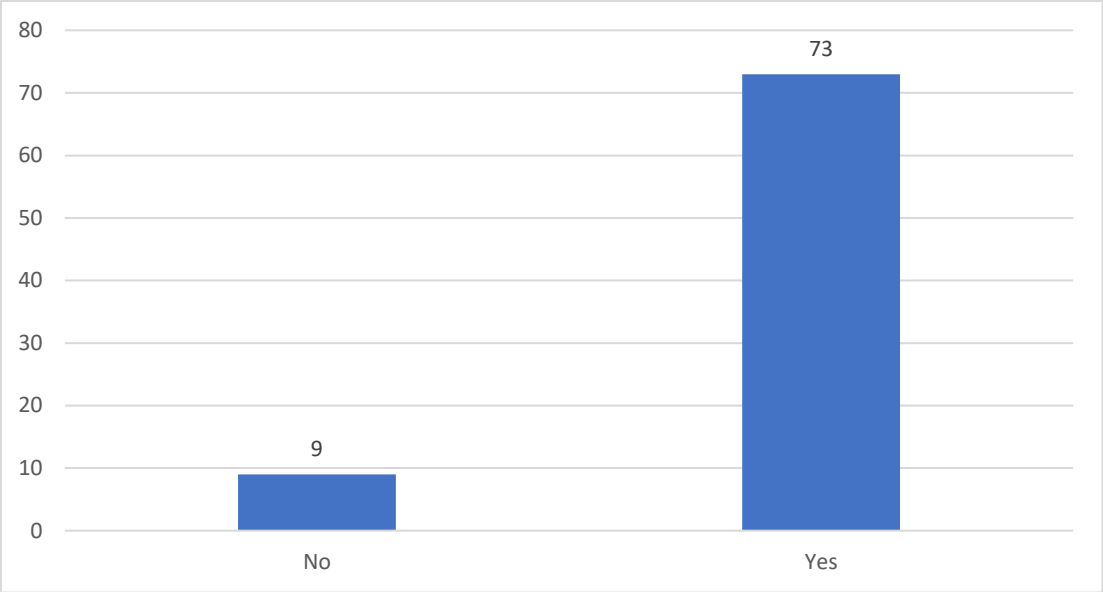
- Aware of main points of contact but cyber-threat procedures need improving; more clarity on procedures would be useful.

Advanced understanding:

+ Clear understanding of procedures and reporting hierarchy; CyberCell provides reminders on procedures; all staff is well-informed; mission specific organisational structure in place; following CIS/SOP; part of job/role.

Q 15.1: Do you think you need this knowledge as a CSDP mission member?

No. of responses per choice:



Summary of explanations given per choice:

No:

No new training required, mission members already informed; structure for response already in place; only specialists should contact EU.

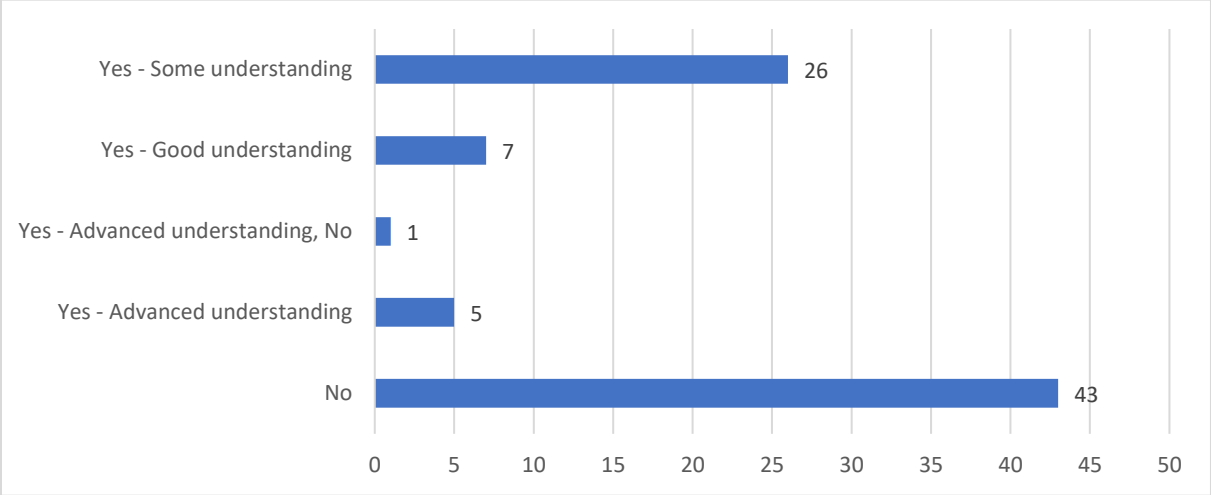
Yes:

+ Yes, protocols are already known; training is useful to respond to threats effectively; enhances reporting; part of job/role; necessary for mission security.

- Roles could be more clearly delineated; structures are overly mission-specific.

Q 16: I am well aware of main activities performed by EU Hybrid Fusion Cell, the Hybrid Centre of Excellence (CoE), EEAS Strategic Communication Task Forces and/or related hybrid risk surveys

No. of responses per choice:



Summary of explanations given per choice:

No understanding:

- Not part of job/role; information overload; not crucial information for roles in general; can be briefed by specialists if necessary; no training; not aware of/see no need for higher-level institutional knowledge.

Advanced/no understanding:

- no training received.

Some understanding:

+ ongoing learning; have attended meetings of specialised task force.

- little knowledge about specific institutions; more training required; better information sharing needed; would like to improve awareness; would be interested in possibilities to collaborate; information does not reach all staff.

Good understanding:

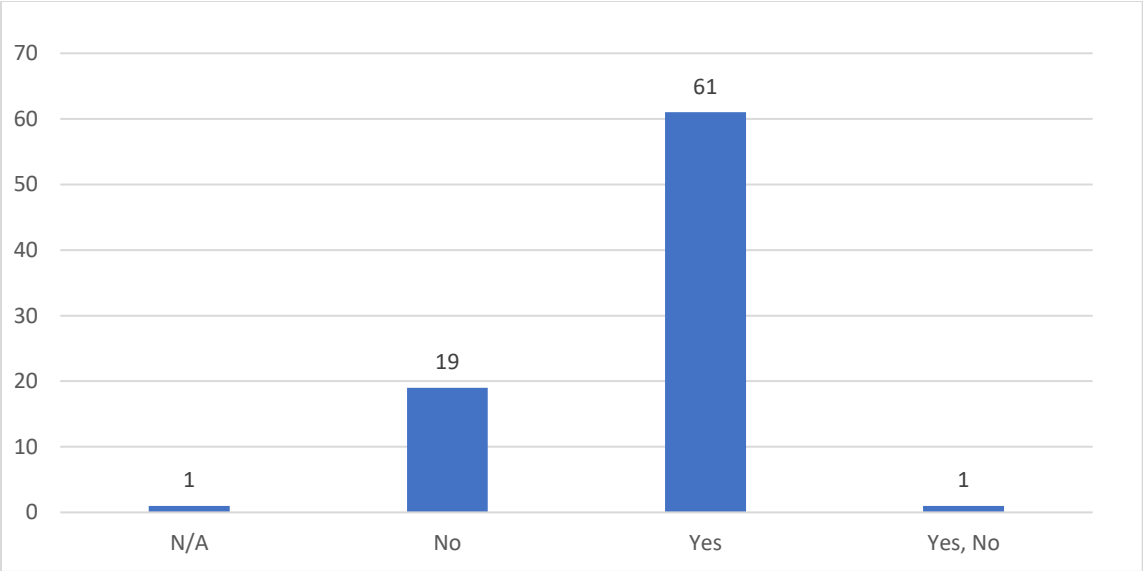
+ Part of job/role; receive relevant reports; personal interest; has enough awareness to explain to others.

Advanced understanding:

+ Prior experience; personal interest; information provided by relevant EU institutions.

Q 16.1: Do you think you need this knowledge as a CSDP mission member?

No. of responses per choice:



Summary of explanations given per choice:

No:

Not necessary for job/role; relevant only for specific jobs/roles; not interested; need to have basic understanding before advanced is relevant.

Yes:

+ Only basic level needed; important to mission integrity and security; mission should receive all possible help.

- Opportunities for cooperation would be useful; more training is required; only relevant to some jobs/roles; job related information would be useful; would be useful to know more about training offered by these institutions – only short review needed.

Yes/No (single respondent):

No explanation provided

N/A (single respondent):

No explanation provided

1.3.5.2. ANALYSIS

CLUSTER V: HYBRID THREATS

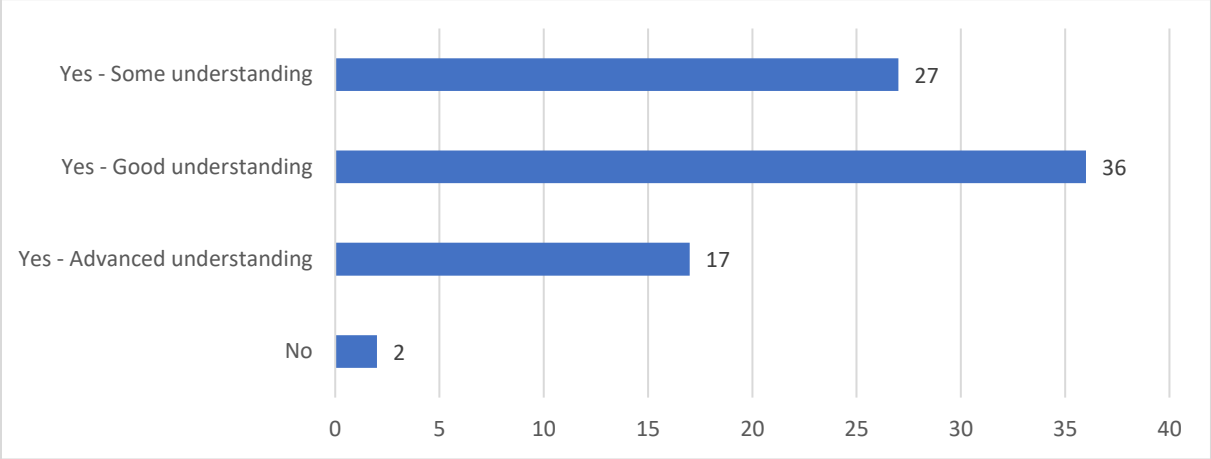
I. Answers to longer questions indicated that knowledge/understanding is closely related to respondents' specific jobs/roles within the mission.
II. Frequently given explanations of higher levels of understanding (i.e. good/advanced) were prior job/career experience, personal interest, and the need for such understanding as a part of the respondent's specific role/job on the current mission.
III. A repeated theme amongst those with levels of knowledge/understanding below advanced was the disparity in the availability of training between specialist mission members and general mission members (with more training available to specialists).
IV. Related to (II) respondents frequently indicated their being unaware of relevant EU institutions and training provided by those institutions.
V. Most respondents indicated that knowledge of hybrid threats is relevant to mission members, frequently cited reasons for this were the need to protect mission security and mission integrity.
VI. Despite (V) a number of respondents indicated some familiarity with protocols for reporting hybrid-threats and suggested that knowledge of these protocols is sufficient knowledge of hybrid threats for non-specialist mission members.
VII. Related to (IV) nearly half of respondents indicated that even mission specific information does not refer to hybrid-threats in general or in the specific mission context. The implication of this would appear to be a shortfall in the ability of mission members to identify or recognise relevant threats when they arise.
VIII. A common theme in longer answers was the suggestion that issues pointed at (V) would best be addressed through embedding relevant training and information in OPSEC.

1.3.6. CLUSTER VI: CYBER THREATS

1.3.6.1. SUMMARY OF REPONSES

Q 17. I am able to explain the definition of ”a cyber threat”

No. of responses per choice:



Summary of explanations given per choice:

No understanding:

No training received.

Some understanding:

+ Some knowledge, but not an IT professional.

- No specific training received; not sure of difference between cyber-crime and cyber-threat.

Good understanding:

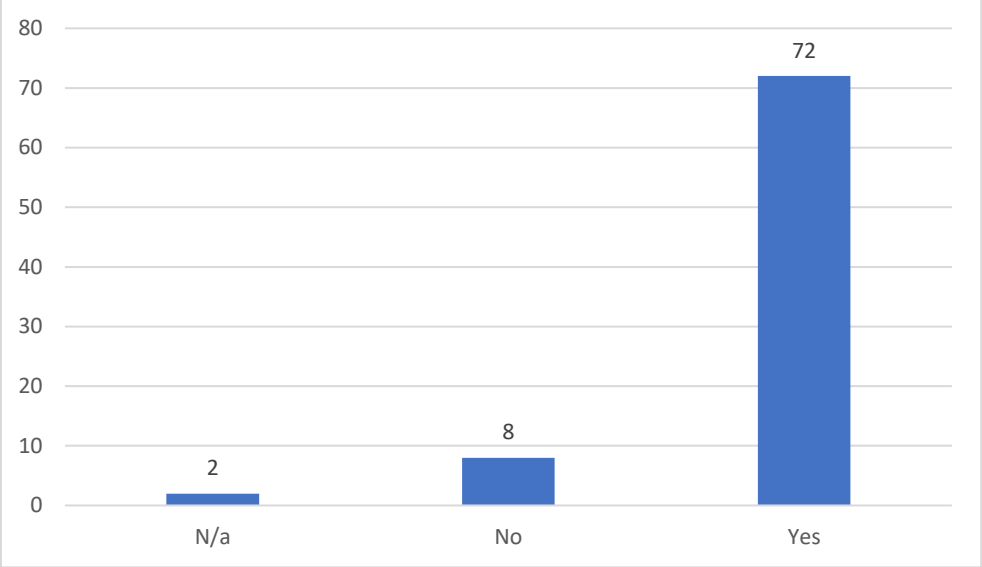
+ Knowledge but not technical knowledge of cyber-threats; prior experience/professional background; useful information provided as part of mission brief; ongoing learning; training received; regular updates received on mission.

Advanced understanding:

+ Professional background/prior experience; part of current job/role; prior training.

Q 17.1: Do you think you need this knowledge as a CSDP mission member?

No. of responses per choice:



Summary of explanations given per choice:

No:

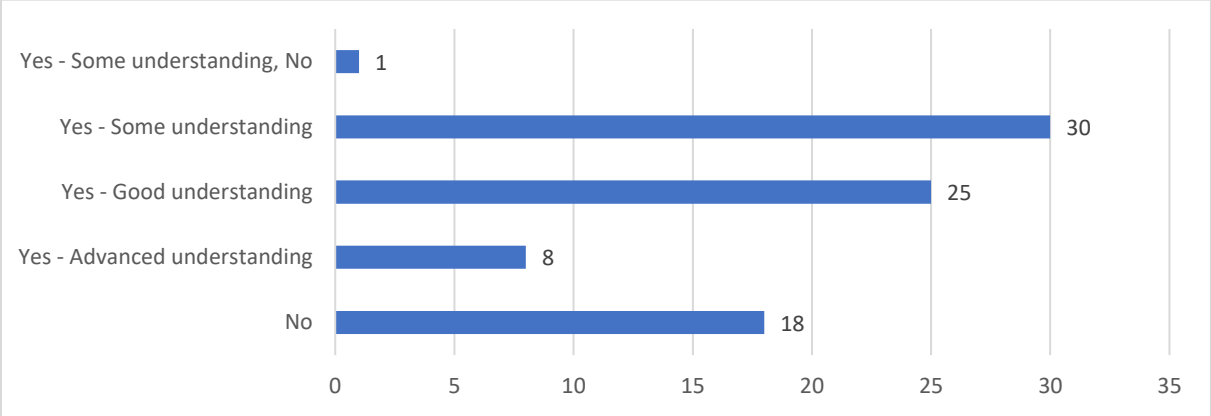
Non-expert members require only practical, not theoretical, understanding; theoretical understanding not relevant to current job/role; should be embedded in OPSEC.

Yes:

Part of job/role; relevant to situation in host-state; to prevent risky personal behaviour; necessary for security/integrity of mission; cyber-threats are a threat to mission; necessary for identification of threats; every mission member should have basic knowledge at the least; mission hardware and data security are important; training should be provided; necessary for situational understanding of cyber-threats.

Q 18. I am able to list the different, most common types of cyber threats described in EU policy documents

No. of responses per choice:



Summary of explanations given per choice:

No understanding:

- Not relevant to job/role; no information received; no information received that is not mission-specific; not enough training; not aware of any relevant EU policy documents.

Some understanding:

+ Common-sense; ongoing learning.

- No specific training; not relevant to job/role; aware of cyber-threats but not EU policy.

Good understanding:

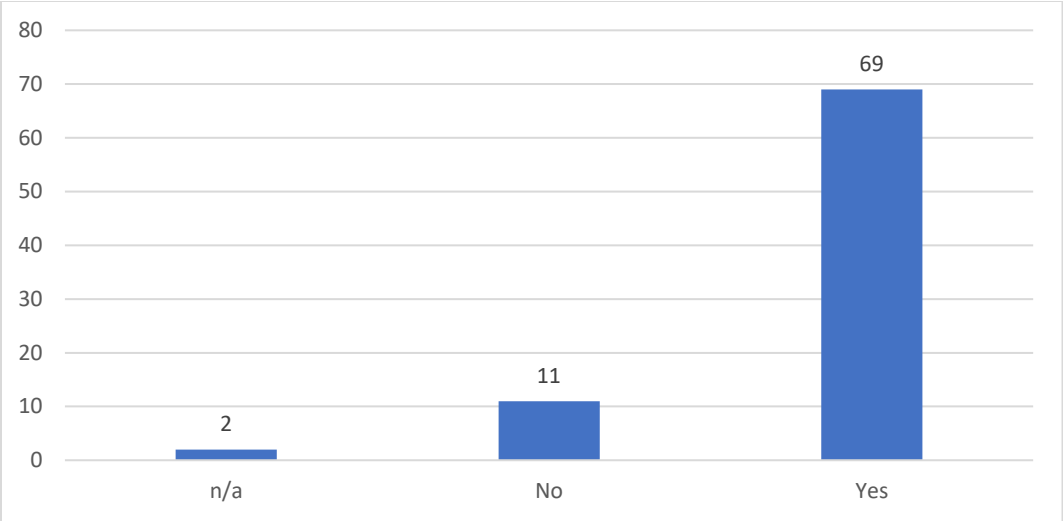
+ Prior experience/professional background; on-mission training.

Advanced understanding:

+ Extensive prior experience/professional background; general awareness; received relevant training.

Q 18.1: Do you think you need this knowledge as a CSDP mission member?

No. of responses per choice:



Summary of explanations given per choice:

No:

Non-necessary knowledge; not relevant to specific job/role; too theoretical.

Yes:

+ Awareness of threats in host-state is relevant or necessary; necessary to minimize risks to mission; part of job/role; useful to distinguish between kinds of threat; all EU policies are important to mission.

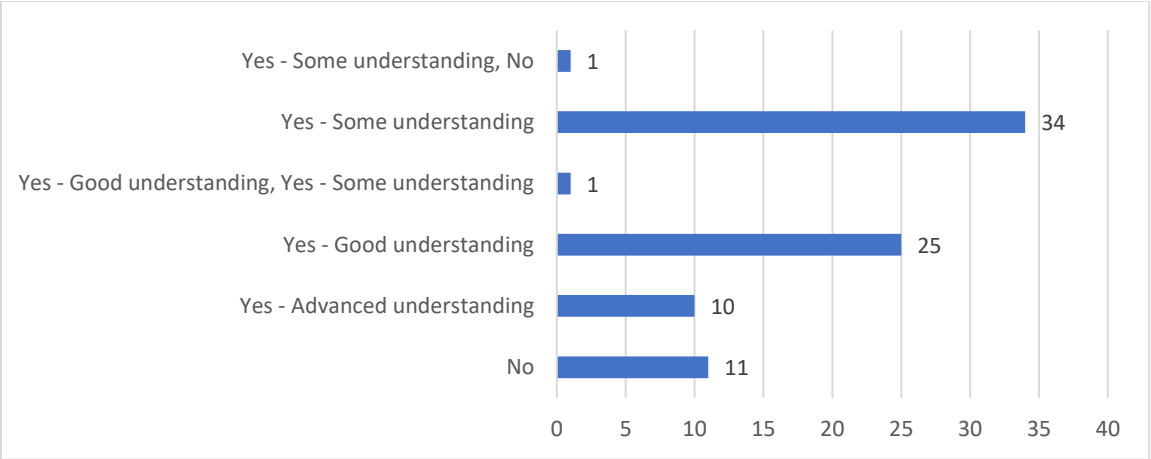
- Theoretical knowledge may not be necessary; reoccurring refreshing needed, but not necessarily formal training; general awareness is necessary, but not in-depth knowledge.

N/A:

No explanation provided.

Q 19. I am able to outline the most commonly used methods of cyberattack

No. of responses per choice:



Summary of explanations given per choice:

No understanding:

- Not relevant to job/role; no training received; insufficient training received; anti-virus software is sufficient.

Some/no understanding:

- Not relevant to job/role.

Some understanding:

+ Local intel services provide threat information; informal sources of information (i.e. media); aware of EUROPOL reports; knowledge of recent security updates; anti-virus is sufficient.

- No specific training received; more information/training required.

Good understanding:

+ Professional background/prior training; ongoing learning; information supplied on-mission; regular updates from mission CIS.

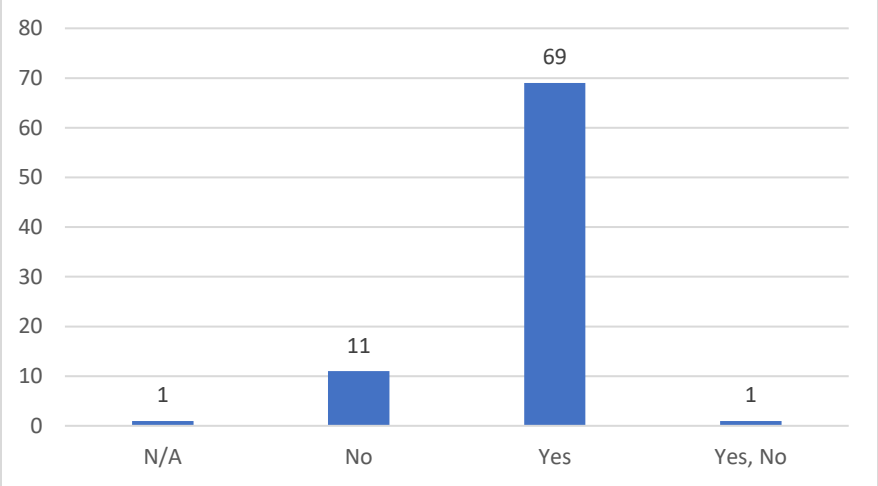
- More specialised training would be useful.

Advanced understanding:

+ Information is everywhere/common-sense; higher-level certification in area; acquired technical and legal knowledge in area prior to mission.

Q 19.1: Do you think you need this knowledge as a CSDP mission member?

No. of responses per choice:



Summary of explanations given per choice:

No:

Sufficient awareness already; training in threats to IT users in general would be sufficient.

Yes/No (single respondent):

No explanation provided.

Yes:

+ Important for understanding cyber-crime events; necessary to minimize possible threats and risks; necessary to secure/work with information; important for mission safety/mission member safety; contributes to situational awareness on mission; part of job/role.

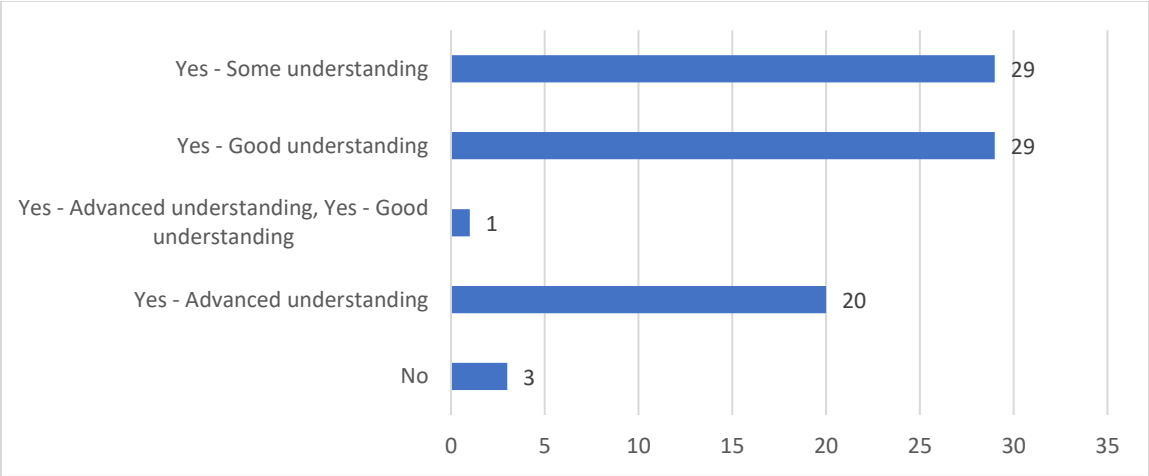
- Training is needed, not sufficient knowledge; part of job/role but more training for detecting responding to threats; more attention in OPSEC needed; practical knowledge more important than theoretical knowledge.

N/A (single respondent):

No explanation provided.

Q 20. When I can identify a cyber threat, I know how to react

No. of responses per choice:



Summary of explanations given per choice:

No understanding:

- Not sure.

Some understanding:

+ Would ask specialists on mission; would inform line-manager/supervisor; follow SOP.

- No specific training; no information available.

Good understanding:

+ CyberCell campaigns; would approach relevant units; follow POC; ongoing learning; experienced colleagues; procedures in place; training received.

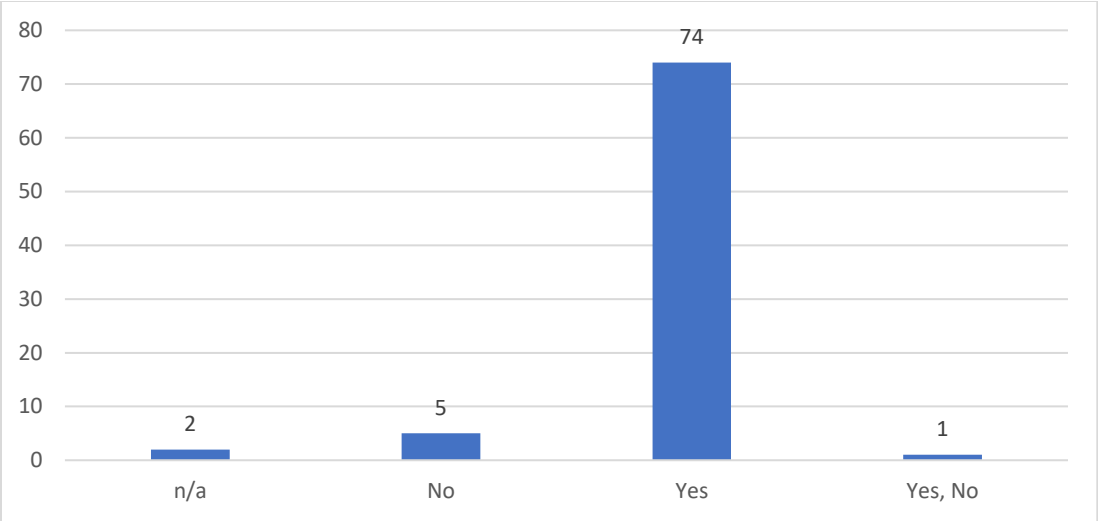
Advanced understanding:

+ Would unplug laptop, inform IT officer; CyberCell reporting procedure in place; general IT security policies are relevant; part of job/role.

- Able to identify attack, but not sufficient understanding to respond whilst attack is ongoing; aware of protocol but would be important to improve communication lines with relevant EU institutions.

Q 20.1: Do you think you need this knowledge as a CSDP mission member?

No. of responses per choice:



Summary of explanations given per choice:

No:

Common understanding of who to contact, no need for further training.

Yes/No (single respondent):

No explanation provided.

Yes:

+ Necessary to protect integrity/security of mission; necessary for recognising risk; relevant to specific job/roles; part of following SOP; part of standard protocols.

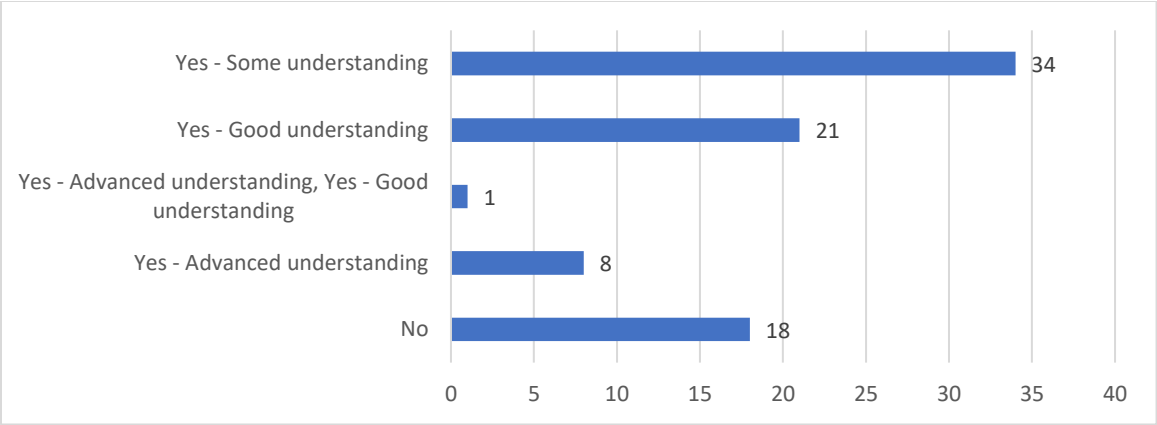
- Common-sense/basic understanding is sufficient; relevant, should be part of standard operating procedures; training required; could be part of OPSEC already; knowledge should be improved at all levels.

N/A (single respondent):

No explanation provided.

Q 21. I am familiar with tools/equipment for preventing cyber incidents

No. of responses per choice:



Summary of explanations given per choice:

No understanding:

- Not relevant to role/job; no specific training received; no familiarity with relevant issues.

Some understanding:

+ Some information has been shared; ISO level is part of job/role; received updates from CIS; basic understanding of anti-virus software; aware of various methods.

- Basic understanding would be useful.

Good understanding:

+ Tools/information provided as part of mission; ongoing learning; general awareness of tools employed on mission; part of job/role.

- Good understanding, but no always mindful of specific threats.

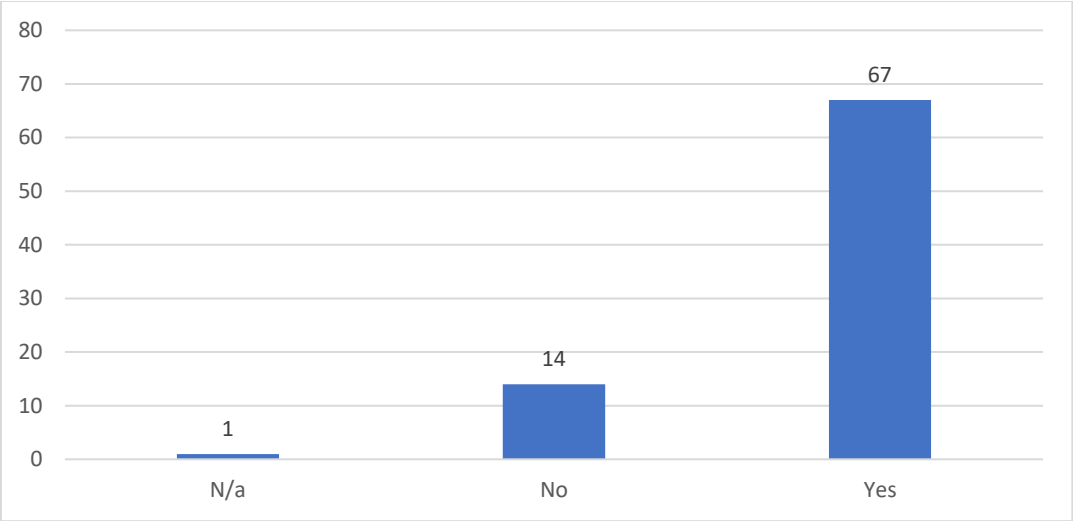
Advanced understanding:

+ Already use a number of tools regularly as part of job/role.

N.B. A number of respondents list relevant tools/institutions, but give no explanation of how they acquired 'advanced understanding'.

Q 21.1: Do you think you need this knowledge as a CSDP mission member?

No. of responses per choice:



Summary of explanations given per choice:

No:

Not relevant for general job/roles; only basic knowledge is necessary for non-specialist mission members; too technical/too complicated.

Yes:

+ More important for specialist mission-members, but basic level is important for all; important for mission security/integrity and mission members; part of job/role.

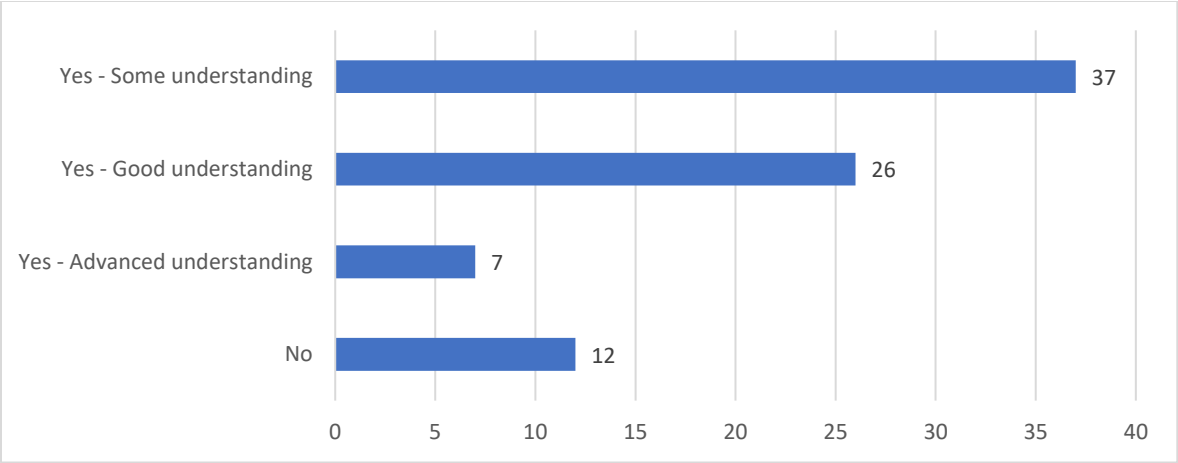
- Better training would be useful to prevent incidents; updates on new developments in area would be useful.

N/A (single respondent):

No explanation provided

Q 22. How familiar am I with risk mitigation actions to cope with cyber threats?

No. of responses per choice:



Summary of explanations given per choice:

No understanding:

- No information received; not relevant to job/role; sufficient to keep software up-to-date.

Some understanding:

+ Information received from ISO; part of job/role; aware of appropriate standards for online behaviour.

- Not sufficient training; only basic understanding provided

Good understanding:

+ Understanding from general use of technology; professional background/prior experience; on-mission training; updating documents part of current job/role; new information received as part of job/role.

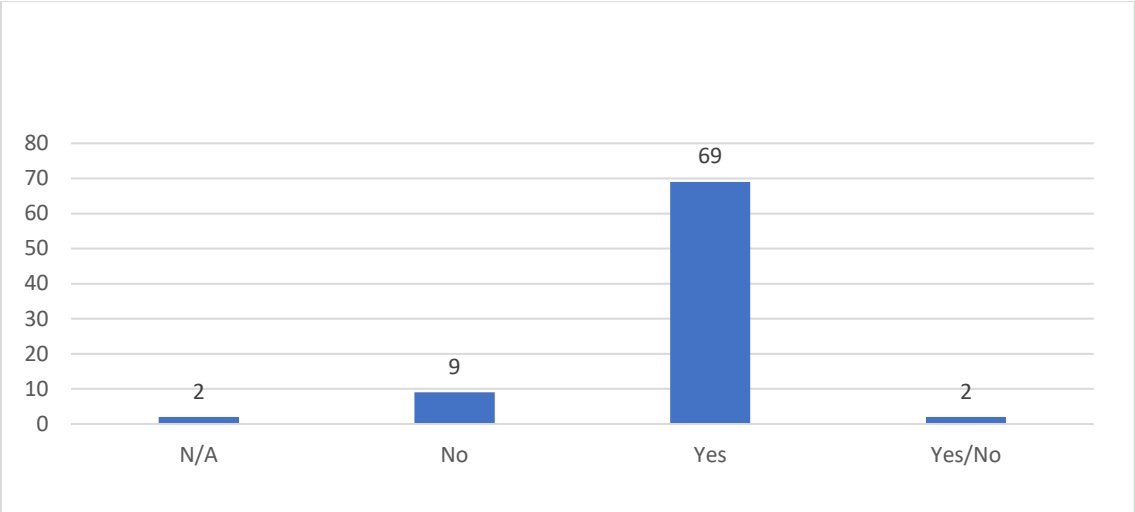
- Reminders would be important to maintain vigilance against threats; fundamental area which all mission members should receive more training on.

Advanced understanding:

+ Part of current job/role.

Q 22.1: Do you think you need this knowledge as a CSDP mission member?

No. of responses per choice:



Summary of explanations given per choice:

No:

Only necessary for specialist members of mission; not related to current job/role.

Yes:

+ Important for mission protection, but basic level/common-sense approach is sufficient; relevant to current job/role; useful to respond to threats/attack; important to all internet users on-mission.

- Further training would be important for risk-mitigation; could be part of OPSEC.

Yes/No (single respondent):

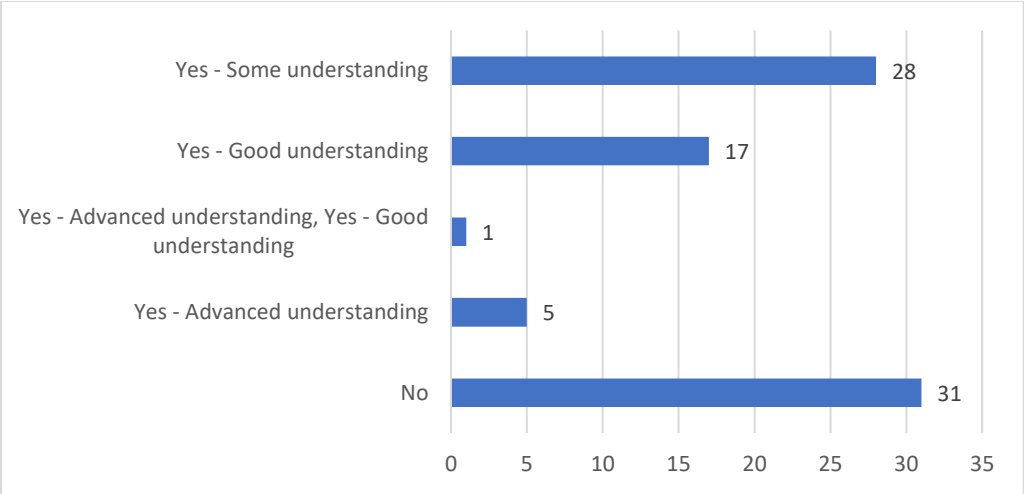
No explanation provided

N/A

More important to specialist mission members.

Q 23. How familiar am I with the management of a cyber incident?

No. of responses per choice:



Summary of explanations given per choice:

No understanding:

- No information received; no specific training received; not part of job/role, CIS and ISO specialists should deal with it; too technical to grasp.

Some understanding:

- Have not participated in managing a cyber-incident, but has read about it; have partially been involved in process; knowledge only of basics. More information/training needed.

+ Part of job/role.

Good understanding:

+ Part of job/role.

Good understanding/ Advanced understanding:

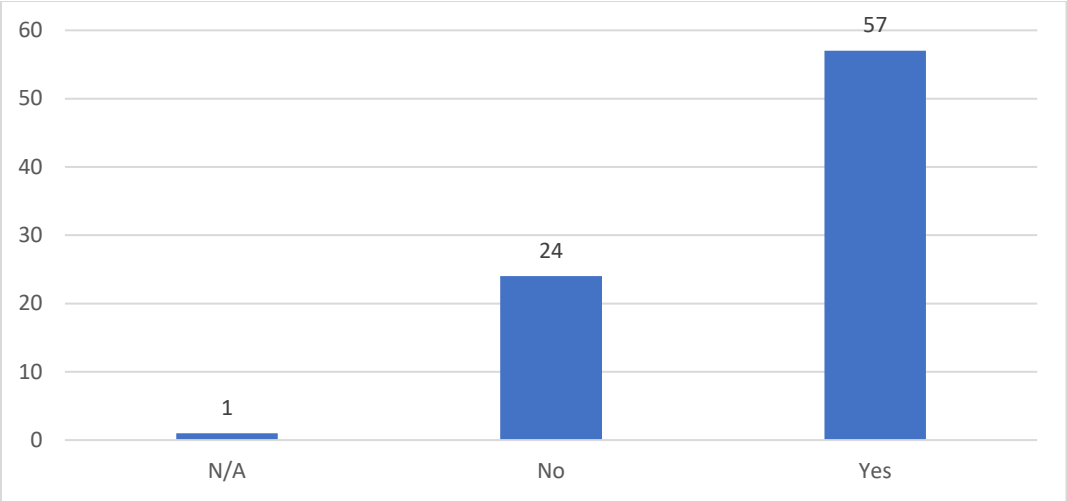
No explanation provided

Advanced understanding:

+ Part of job/role.

Q 23.1: Do you think you need this knowledge as a CSDP mission member?

No. of responses per choice:



Summary of explanations given per choice:

No:

Knowledge of reporting process is necessary, technical knowledge and ability to respond is not necessary for non-specialists.

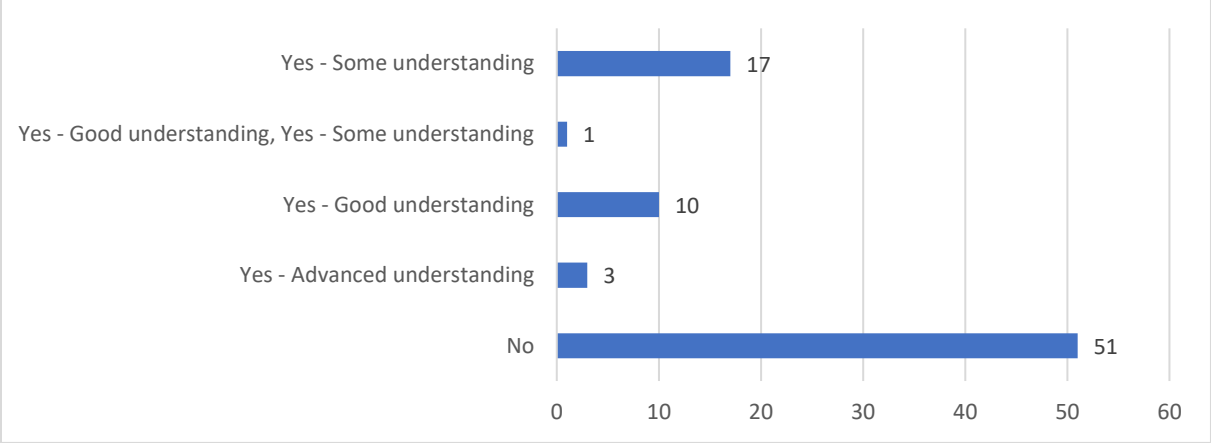
Yes:

Basic knowledge is required; knowledge is necessary to manage any cyber-incident, but training should reflect specific position held on mission; knowledge is necessary to prevent initial damage of cyber-incident, i.e. before specialists are able to respond; part of job/role;

- More training required, some lack any knowledge/awareness.

Q 24. I know the procedures to recover essential systems for the mission after a cyber incident

No. of responses per choice:



Summary of explanations given per choice:

No understanding:

- Knowledge is too technical for general mission members; not related to job/role, nor skills required by job/role; only necessary for specialist mission members; awareness of reporting process is sufficient.

Some understanding:

+ Theoretical knowledge, but no experience; part of job/role, so knowledge is regularly updated.

Good understanding:

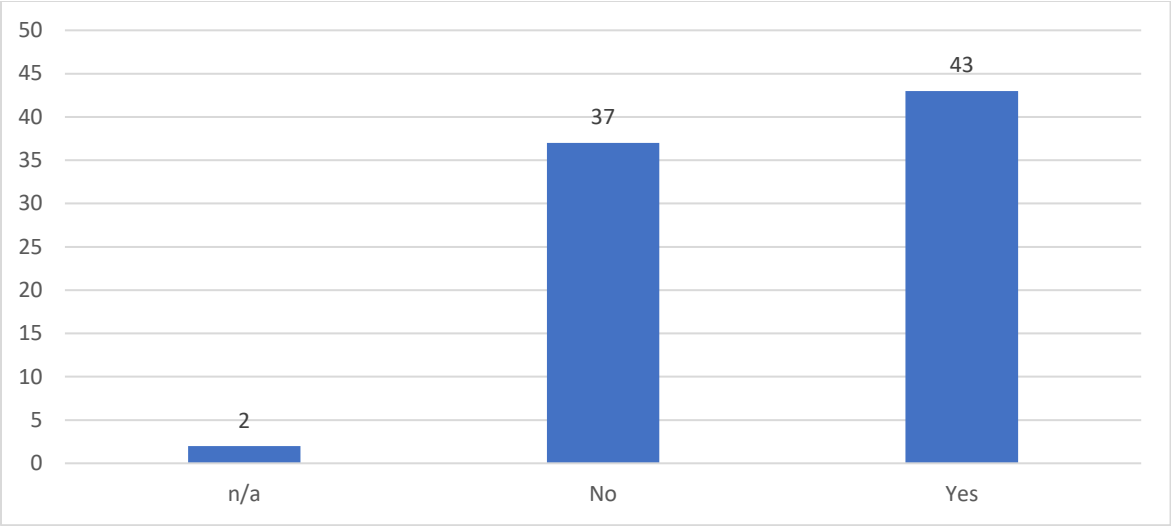
+ Part of job/role; mission CyberCell provided information/training; specific procedures in place.

Advanced understanding:

+ Developing and implementing incident management and recovery procedures.

Q 24.1: Do you think you need this knowledge as a CSDP mission member?

No. of responses per choice:



Summary of explanations given per choice:

No:

Work is too specialist; not required for job/role; training only required for specialists; knowledge of reporting/support procedures is sufficient.

Yes:

Basic knowledge would be useful, especially to recognise what falls into their domain and to coordinate with others.; if training is accessible/user-friendly, would be beneficial; important for protecting mission to be able to recover systems; part of job/role, so necessary to keep knowledge up-to-date.

1.3.6.2. ANALYSIS

CLUSTER VI: CYBER THREATS

I. In general, the majority of respondents indicated that knowledge of Cyber Threats in all areas was relevant to mission members. Notably, however, almost a third of respondents indicate that they did not think knowledge of how to manage incidents was relevant to non-specialist mission members and half of respondents indicated that they did not think knowledge of how to recover systems was relevant to non-specialists.

II. Despite (I), higher (good/advanced) levels of knowledge or understanding in the relevant areas largely tracked prior experience, personal interest, and current mission role.

III. Common themes in answers on all areas of knowledge in this cluster were that basic knowledge is enough for non-specialist mission members, and where knowledge is relevant practical knowledge or understanding would be of significantly greater value than theoretical understanding of the relevant areas.

IV. In general respondents appeared to recognise the importance of the various areas of knowledge relevant to Cyber Threats for protecting mission security and integrity, as well as for protecting personal and sensitive information vis-à-vis the mission, members of the mission, and host countries.

V. As with other clusters, several respondents expressed the opinion that training in Cyber Threats could or should be part of OPSEC.

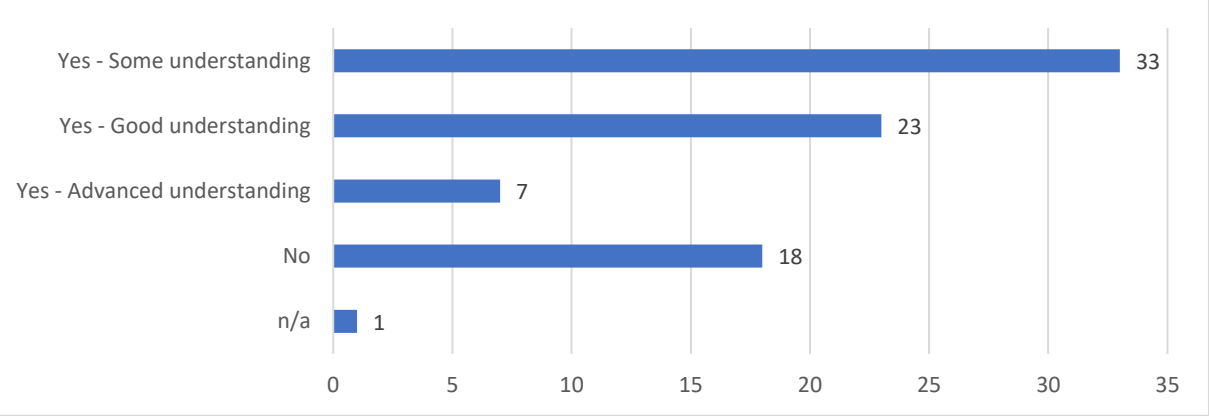
VI. Worryingly, a small number of respondents indicated that they believe in place anti-virus software is sufficient defence against cyber threats.

1.3.7. CLUSTER VII: PHYSICAL THREATS TO IT-SYSTEMS ETC.

1.3.7.1. SUMMARY OF REPONSES

Q 25. I am able to identify the most commonly recognised physical threats and vulnerabilities that could affect/damage the IT system/data storage units that are essential to the mission

No. of responses per choice:



Summary of explanations given per choice:

No understanding:

- Not part of job/role, specialist knowledge; role of CIS or ISO; no information/training received.

Some understanding:

+ Common-sense applies; specialist area, but useful for senior management to be aware of; aware of basics; SOP on CIS; personal research.

- No training received; unsure of what counts as a physical threat;

Good understanding:

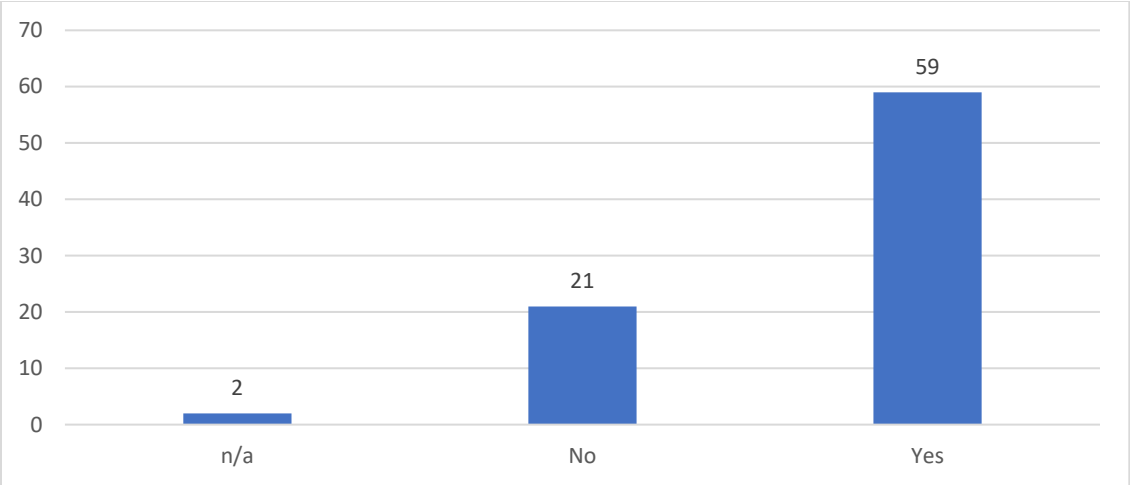
+ Part of job/role; received training; general understanding.

Advanced understanding:

+ Part of job/role to mitigate risk levels.

Q 25.1: Do you think you need this knowledge as a CSDP mission member?

No. of responses per choice:



Summary of explanations given per choice:

No:

Not necessary for non-specialist mission members; basic knowledge of what not to do is sufficient, pro-active response is a specialist area.

Yes:

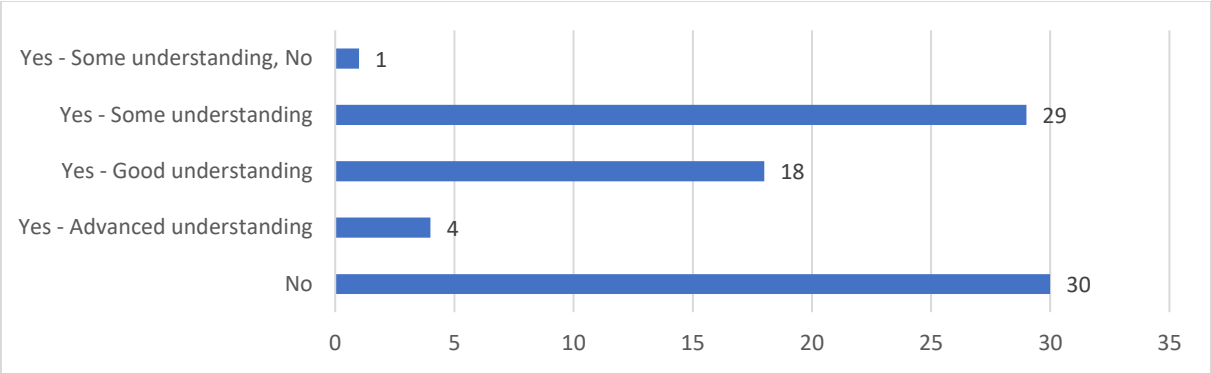
Necessary to raise awareness of risks involved in mission; general understanding of risks is necessary for overall mission security; necessary for specific job/role; preparedness is always valuable; relevant to personal security.

N/A (single respondent):

No explanation provided

Q 26. I am able to describe the tools normally used to create or trigger a cyber/hybrid threat

No. of responses per choice:



Summary of explanations given per choice:

No understanding:

- Not part of job/role; no information/training received; insufficient training received; necessary only for CIS and ISO.

Some/no understanding:

+ Aware of existence of viruses/malware etc.

Some understanding

+ Part of job/role; experience on mission; professional background.

- Less able to explain cyber threats than hybrid threats; more training would be useful; a better understanding from a political perspective, rather than theoretical would be useful.

Good understanding:

+ Good understanding of hybrid-threats; personal interest; part of job/role; awareness of most common tools used.

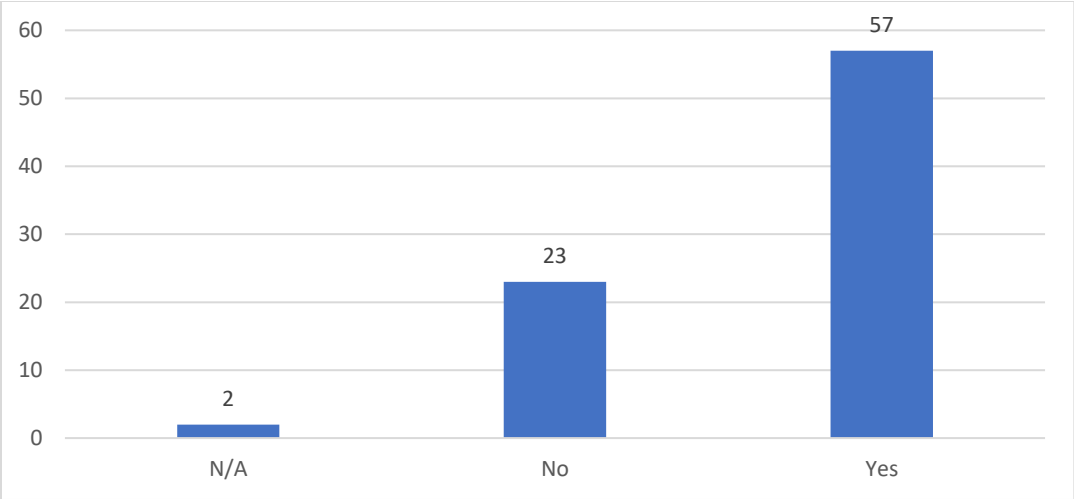
- Less knowledge of cyber-threats, than hybrid-threats; limited knowledge of hybrid-threats.

Advanced understanding:

+ Part of job/role to mitigate cyber and hybrid threats and deploy specific counter-measures.

Q 26.1: Do you think you need this knowledge as a CSDP mission member?

No. of responses per choice:



Summary of explanations given per choice:

No:

Lack of interest; knowledge for specialised personnel only; unsure if it is part of job/role.

N/A:

Unsure.

Yes:

Common-sense applies; awareness raising is important; would contribute to overall mission security; training via simulations would be useful; part of job/role.

- Yes, but only basic understanding is necessary.

1.3.7.2. ANALYSIS

CLUSTER VII: PHYSICAL THREATS TO IT-SYSTEMS ETC.

I. A significant number of respondents (around 1/4 on each) indicated that they had no understanding of physical threats to IT or relevant tools used to create or trigger a hybrid threat. Similar numbers of respondents indicated for each question that knowledge/understanding in these areas was not relevant to non-specialist mission members.
II. As with other clusters, understanding level appears to track prior experience and/or respondents having specialist role relevant to area in question.
III. A common theme amongst respondents was that general knowledge or common-sense would be sufficient for non-specialist mission members in both areas.
IV. Amongst those who expressed that knowledge in these areas would be relevant at least one expressed the opinion that the cohort as a whole would require ongoing training in the relevant areas
V. One respondent expressed the opinion that knowledge, specifically of tool used to generate hybrid threats, would be more valuable from a political perspective than theoretical.

1.4. GENERAL THEMES IN SURVEY ACROSS ALL CLUSTERS

I. Understanding level in all themes often appears to track prior experience and/or respondents having specialist role relevant to area in question.
II. Respondents on all questions frequently indicated that they were of the view that knowledge/understanding in the relevant areas was necessary only for specialist members.
III. Common explanations for a lack of knowledge in all clusters included:
    a. Lack of access to relevant documents/EU policies;
    b. Lack of awareness of relevant institutions;
    c. Lack of training;
    d. The respondent's view that the knowledge/understanding in question was not relevant to their particular job or role on the mission.
IV. A common theme amongst those who did indicate that training would be useful for all mission members was that practical training would be of greater value than purely theoretical training.
V. In general, whilst some respondents indicated that receiving updates on relevant fields and threats in all clusters is important, this was far from a common theme in answers given. Relatedly, amongst the reoccurring themes across all clusters was that general knowledge or common-sense were sufficient for non-specialist members.
VI. Taken together these themes may indicate a significant area of concern in respect to mission members knowledge of and awareness of the rapidly changing nature of cyber and hybrid threats and the need for missions to have the capability to respond to these changes.
VII. Though rarely explicitly expressed, answers to questions in all clusters suggest an underlying lack of familiarity with, or full grasp of, the concept of hybrid threats.
VIII. It is worth pointing out that at a number of points in the survey respondents indicated that they had either newly acquired relevant knowledge/understanding, or else brought it up to a sufficient standard, only in the period of remote working since March 2020 put in place in response to the Covid-19 pandemic.

1.5. GENERAL THEMES AND ADDITIONAL COMMENTS ON THE QUESTIONNAIRE

This section summarises the common themes and training needs identified additional comments offered in response to the final question of the questionnaire, which asks: ***Please describe any other specific topic and express your personal need for training on hybrid threats and/or cyber, not provided in the questionnaire.*** (For a full list of the answers provided, see: ANNEX 4)

General overview:

I. Initiatives to provide training and/or further training on hybrid threats and cyber would be well received and welcome.
II. Some respondents consider knowledge of hybrid threats and cyber as covered in the questionnaire to be too specialist and suggest that relevant training need be provided for specialists only.
III. Some respondents were interested in acquiring more knowledge/further training on theoretical themes e.g. policy documents.
IV. Some respondents were only interested in receiving more practical knowledge.

Suggested themes and topics of training:

- An introductory online course, introducing the different layers/different aspects of these new threats.

- Training on disinformation and Strategic Communication.

- Training on fake news and how to detect fake news.

- Information security training, especially on processes and tools, to harmonize knowledge of the whole mission and standardize modes of action.

- A general awareness course for all mission members would be useful as current training is only directed to CIS experts and senior-management.

- Further training upon the relevant policy documents would be especially welcomed.

- Training for hybrid threats specialists: identification/assessment of hybrid threats through foresight approaches, especially horizons scanning and scenarios pathways.

Other themes:

- More attention to personal smartphone security is suggested. One possibility suggested is to develop an opensource and secure version of smartphone software standard for all mission members, e.g. GraopheneOS.

- Missions should recruit more hybrid threat experts, ideally for every Field Office. Additionally, subject matter experts should be doubled, as there should be more trainings for new mission members.

- More attention to presenting IT-related communication clear and easy to understand manner is needed. Especially, considering that (i) IT uses a lot of specialist language; and, (ii) recipients of the communications are not usually native speakers.

- Generally, CSDP, EU and EU MSs should provide more training on hybrid threats and cyber, both for those people employed by the CSDP, UE, MS, and for the general populous.

- Cooperation between security departments and CIS could be developed. (Counter-intelligence, using the TESSOc framework would be a good model for this.)

- More training should be provided to senior-management to ensure that they are sufficiently aware of and attentive to possible new threats. A separate training package should be developed for CIS specialist/technical staff and the senior-management.

1.6. RECOMMENTATIONS

As per analysis of the empirical survey, prior training has been received and an overall awareness among the CSDP civilian mission members is present regarding the 7 central "hybrid threats and cyber" themes: (I) General EU response to hybrid threats and cyber; (II) Safe use of work-related systems and devices in mission premises; (III) Safe use of personal devices outside mission premises; (IV) Situational awareness; (V) Hybrid threats; (VI) Cyber threats; (VII) Physical threats to IT-systems etc. As the analysis shows, however, the level of awareness varies and the respondents themselves repeatedly brought out the need for further training in these areas, especially in relation to the continuously changing and developing nature of the threats.

According to the above analysis and findings, the following recommendations aiming to enhance effectiveness of CSDP mission members' performance are offered:

- To harmonize the training on "hybrid threats and cyber" provided to CSDP civilian mission members, a training curriculum and training courses in accordance with that curriculum should be developed according to Civilian Training Area High Level Learning Outcomes (CTALO).

- To address the difference in training requirements of mission members, it is important to follow the division of expertise level identified in the CTALO, when developing the training.

- To address the mission members' interest in receiving practical rather than theoretical training, practical implementation of the training should be considered when developing training.

- To address the continuously changing natures of "hybrid threat and cyber", further attention should be paid to providing continuing education to mission members who previously received pre-deployment or basic training past a relevant amount of time.

- To ensure that mission members' training needs are met, training needs should be systematically monitored using feedback analysis that would enable identification of possible obstacles and gaps and timely updates of the course and respectively, curriculum.

IV CIVILIAN TRAINING AREA HIGH LEVEL LEARNING OUTCOMES (CTALO)

Capability cluster Hybrid threats and cyber

HLLO

Upon completion of this course the leaner will be able to

Learning levels Learning Areas	Basic	Advanced	Expert/Specialist
GENERAL EU RESPONSE TO HYBRID THREATS AND CYBER			
Knowledge (K)	-outline EU policy documents on tackling new security challenges, including those linked to hybrid threats;	- describe the aim, policy and implementation mechanism of EU policy and strategy on tackling new security challenges in relation to hybrid threats and cyber in context of CSDP missions;	-explain the significance of EU policy and strategy documents on tackling new security challenges, including those linked to hybrid threats, and their relevance to Mission activities; -describe the role of CSDP Missions in contributing to the implementation of EU policy and strategy in relation to tackling hybrid threats and cyber
Skills (S)		-identify links between EU strategy and policy documents related to tackling hybrid threats and cyber crime in relation to Missions' activites	-propose measures for implementation of relevant parts of EU strategy and policy documents related to tackling hybrid threats and cyber crime in personal performance of Mission members;
Autonomy/responsibility (A/R)			-take responsibiity for proposing any updates to EU policy and strategy

			documents related to tackling hybrid threats and cyber crime
SAFE USE OF WORK-RELATED SYSTEMS AND DEVICES IN MISSION PREMISES			
K	-list Mission rules, guidelines and/or procedures on safe and secure handling and use of Mission related information, documents, IT-systems, hard- and software, applications, digital communication related issues and information/documents available on the Mission,	-describe risks related to inappropriate handling and use of Mission-related IT-systems, official, sensitive and/or classified (secret, confidential, restricted) information/documents, hardware and digital communication tools and applications;	
S		- in simulated environment, select safe and secure procedures for handling and use of Mission-related IT-systems, information/documents, and digital communication tools and applications;	- assess Mission rules, guidelines and/or procedures on handling and use of hardware; digital communication related issues (e-mail, chats), software and applications (e.g. WhatsApp and other applications) on secure use of Mission related IT-systems by proposing any adjustments or amendments ensuring safe and secure use of IT-systems and tools ; - identify challenges and shortcomings related to the safe and secure handling of official, sensitive and/or classified (secret, confidential, restricted) information/documents via IT support, justifying any actions to be taken on the Mission in context of

			handling and use of hardware, software and applications
A/R			-take responsibility for proposing amendments to EU and Mission rules, guidelines and/or procedures on handling and use of documents, IT-systems, hard- and software, applications ; digital communication related issues (e-mail, chats), by justifying any action to be taken;
SAFE USE OF PERSONAL DEVICES OUTSIDE MISSION PREMISES			
K	- outline the procedures regarding the use of hardware, digital communication related issues such as e-mail, chats, social media, software and applications, e.g. WhatsApp and other applications outside the Mission premises (e.g. at home)	-assess the potential of risk related to the use of hardware, digital communication related issues (e-mail, chats, social media), software and applications (e.g. WhatsApp and other applications) outside the Mission premises (e.g. in buidings of host country authorities, at home)	
S		-in simulated environment, select safe and secure hard- and software, digital communication related tools and applications outside the Mission premises (e.g. at home)	-identify challenges and risks related to safe and secure use of hardware, digital communication related issues (e-mail, chats, social media), software and applications (e.g. WhatsApp and other applications) outside the Mission premises (e.g. at home)
A/R			-take responsibility for proposing measures for upgrading procedures related to safe and secure use of hardware, digital communication related issues (e-mail, chats, social media), software and applications

			(e.g. WhatsApp and other applications) outside the Mission premises (e.g. at home)
SITUATIONAL AWARENESS			
K	- describe the role of regular /periodical updates about the Mission environment, in relation with possible cyber/hybrid threats, specific to the country/area of the Mission;	-explain how hybrid threats and cyber can affect the situation in the host State and on the Mission based on regular/periodical updates about the Mission;	
S		-report findings indicating hybrid threats and/or cyber according to agreed communication line	-identify situations and information related to hybrid threats and cyber to be reflected in Missions' regular/periodical updates basing on simulated case scenario;
A/R			-critically evaluate a broad range of hybrid threats and cyber as issues for the host State of the Mission in terms of the impact to security, economy and international relations of the host State of the Mission and EU by proposing countermeasures; - propose measures enabling Mission support to host State in countering hybrid threats and cyber
HYBRID THREATS			
K	-outline the main characteristics of a hybrid threat;	-explain the relevance of location specific information related to	-outline the main tasks and activities performed by EU Hybrid Fusion Cell, the Hybrid Centre of Excellence

	-describe different kinds of hybrid threats and the different ways in which they can occur; -describe the procedures on who to contact (on the Mission) in case of evidence or suspicion of a hybrid threat incident that has already occurred;	hybrid threats in relation to decision making process in the Mission area; -explain the procedures on who to contact (in the Mission/in Brussels) in case of evidence or suspicion of a hybrid threat incident that has already occurred;	(CoE), EEAS Strategic Communication Task Forces and/or related hybrid risk surveys -define wide range of procedures on who to contact (in the Mission/in Brussels) in case of evidence or suspicion of a hybrid threat incident that has already occurred;
S		-basing on simulated case scenario, assess any location specific information available for the potential of hybrid threats in context of decision making process;	- basing on simulated scenario, identify different kinds of hybrid threats by assessing any location specific information available for the potential of hybrid threats by justifying any action to be taken;
A/R			-in a simulated environment, take responsibility for proposing actions for identification and referring a hybrid threat using agreed and established communication channels and procedures
CYBER THREATS			
K	-describe most common types of cyber threats included in EU policy documents; -outline the most commonly used methods of cyberattack;	-explain the definition of a "cyber threat" -list the different types of cyber threats, including those provided in EU policy documents; -outline the methods of cyberattack;	-explain a broad range of EU policy documents related to cyber threats in context of CSDP Missions' activities; - explain the tools and methods for preventing cyber incidents and risk mitigation actions in context of CSDP Missions' activities;

S		-in a simulated environment, select response options/tools/equipment for preventing cyber threat according to EU and Mission procedures	-basing on case scenario, plan actions to counter cyberattacks, mitigate risks and manage cyber incidents including in relation to the recovery of essential systems for the Mission after a cyber incident; -assess tools/equipment for preventing cyber incidents by proposing measures for upgrading existing tools/equipment; -analyse risk mitigation actions to cope with cyber threats and incidents in compliance with data protection rules; -establish procedures to recover essential systems for the Mission after a cyber incident
A/R	-		-take responsibility for coordinating actions related to prevention, management and recovery of essential systems for the Mission in case of cyber incident in line with established procedures
PHYSICAL THREATS TO IT-SYSTEMS ETC.			
K	-describe the most commonly recognised physical threats and vulnerabilities that could affect/damage the IT system/data	-describe the tools normally used to create or trigger a cyber/hybrid threat;	-explain a range of recognised physical threats and vulnerabilities that could affect/damage the IT

	storage units that are essential to the Mission;		system/data storage units that are essential to the Mission; -describe the tools normally used to affect/damage the IT system/data storage units or create or trigger a cyber/hybrid threat;
S		- in a simulated environment, select measures enabling an identification and dismantling of physical threats and vulnerabilities that could affect/damage the IT system/data storage units that are essential to the Mission;	-identify physical threats and vulnerabilities that could affect/damage the IT system/data storage units that are essential to the Mission by justifying any action to be taken; - ensure permanent use of the tools for minimising cyber/hybrid threat; -propose risk mitigation measures.
A/R			-basing on case scenario, take responsibility for coordinating activities aiming at reducing physical threats and vulnerabilities that could affect/damage the IT system/data storage units that are essential to the Mission.

REFERENCES

(IN ALPHAPETHICAL ORDER)

- *Annual Report of Politico-Military Group (PMG) 15870/17 of 19 December 201 7on the Implementation of the Cyber Defence Policy Framework.* [Online]. [Accessed: 15 September 2020]. Available from: https://data.consilium.europa.eu/doc/document/ST-15870-2017-INIT/en/pdf

- *Joint Communication JOIN (2013) 30 final of 11 December 2013 on The EU's comprehensive approach to external conflict and crises.* [Online]. [Accessed: 15 September 2020]. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52013JC0030&from=en

- *Joint Communication JOIN (201) 18 final of 6 April 2016 on Joint Framework on countering hybrid threats a European Union response.* [Online]. [Accessed: 15 September 2020]. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016JC0018&from=en

- *Joint declaration of 8 July 2016 on EU and NATO.* [Online]. [Accessed: 15 September 2020]. Available from: https://www.consilium.europa.eu/media/21481/nato-eu-declaration-8-july-en-final.pdf

- *Civilian Strategic Guidance 9898/19 of 6 June 2019 on EUCTG Strategic Guidance on CSDP Civilian Training.*

- *Commission Communication COM (2014) 72 final of 12 February 2014 on Internet Policy and Governance Europe's role in shaping the future of Internet Governance. (Text with EEA relevance).* [Online]. [Accessed: 15 September 2020]. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52014DC0072

- *Commission Communication COM (2016) 410 final of 5 July 2016 on Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry.* [Online]. [Accessed: 15 September 2020]. Available from: https://ec.europa.eu/digital-single-market/en/news/communication-strenghtening-europes-cyber-resilience-system-and-fostering-competitive-and

- *Commission Recommendation C (2017) 6100 final of 13 September 2018 on Coordinated Response to Large Scale Cybersecurity Incidents and Crises.* [Online]. [Accessed: 15 September 2020]. Available from: https://ec.europa.eu/transparency/regdoc/rep/3/2017/EN/C-2017-6100-F1-EN-MAIN-PART-1.PDF

- *Council and the Representatives of the Governments of the Member States Conclusion 14305/18 of 19 November 2018 on the establishment of a Civilian CSDP Compact.*

- *General Secretariat of the Council.* [Online]. [Accessed: 15 September 2020]. Available from*:* https://www.consilium.europa.eu/media/37027/st14305-en18.pdf)

- *Council Conclusions of 31 May 2010 on Digital Agenda for Europe 3017th Transport, Telecommunications and Energy Council meeting.* [Online]. [Accessed: 15 September 2020]. Available from: https://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/trans/114710.pdf)

- *Council Conclusions (6122/15) of 11 of February 2015 on Cyber Diplomacy.* [Online]. [Accessed: 15 September 2020]. Available from: http://data.consilium.europa.eu/doc/document/ST-6122-2015-INIT/en/pdf

- *Council Conclusions 9916/17 of 7 June 2017 on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox") [Draft]. [*Online]. [Accessed: 15 September 2020]. Available from: http://data.consilium.europa.eu/doc/document/ST-9916-2017-INIT/en/pdf

- *Council Conclusion 14972/19 of 10 December 2019 on Complementary efforts to enhance resilience and counter hybrid threats.* [Online]. [Accessed: 15 September 2020]. Available from: https://data.consilium.europa.eu/doc/document/ST-14972-2019-INIT/en/pdf

- *Council Decision 7299/19 of 14 May 2019 on concerning restrictive measures against cyber-attacks threatening the Union or its Member States*. [Online]. [Accessed: 15 September 2020]. Available from: https://data.consilium.europa.eu/doc/document/ST-7299-2019-INIT/en/pdf

- *Council Decision (CFSP) 2020/1127 of 30 July 2020 on amending Decision (CFSP) 2019/797 concerning restrictive measures against cyber-attacks threatening the Union or its Member States.* [Online]. [Accessed: 15 September 2020]. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32020D1127&from=EN

- *EEAS Plan EEAS (2018) 906 of 4 September 2018 on Civilian Capabilities Development.* [Online]. [Accessed: 15 September 2020]. Available from*:* https://data.consilium.europa.eu/doc/document/ST-11807-2018-INIT/en/pdf

- *EEAS Working Document 6166/17 of 9 February 2017 on Draft list of Generic Civilian CSDP Tasks and Requirements.* [Online]. [Accessed: 15 September 2020]. Available from: https://data.consilium.europa.eu/doc/document/ST-6166-2017-INIT/en/pdf

- *EEAS Working Document EEAS (2017) 773 of 16 June 2017 on Integrating cyber security in the planning and conduct of Civilian CSDP missions.*

- *EEAS Working Document (EEAS 8077/20) of 20 May 2020 on Mini-concept on civilian CSDP support to countering hybrid threats.*

- *EU Directive* 2016/1148 *of 6 July 2016 on measures for a high common level of security of network and information systems across the Union.* [Online]. [Accessed: 15 September 2020]. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN

- *General Secretariat of the Council policy framework 14413/18 of 19 November 2018 on EU Defence Policy (2018 update).* [Online]. [Accessed: 15 September 2020]. Available from: https://data.consilium.europa.eu/doc/document/ST-14413-2018-INIT/en/pdf

- Trimintzios, P., Chatzichristos, G., Portesi, S., Drogkaris, P., Palkmets,L., Liveri, D. and Dufkova, A. (2017). *European Union Agency for Network and Information Security (ENISA) study: Cybersecurity in the EU Common Security and Defence Policy (CSDP): Challenges and risks for the EU.* European Parliamentary Research Service Scientific Foresight Unit (STOA): Brussels. [Online]. [Accessed: 15 September 2020]. Available from: https://www.europarl.europa.eu/RegData/etudes/STUD/2017/603175/EPRS_STU(2017)603175_EN.pdf

ANNEX 1: LIST OF AVAILABLE TRAINING

EU CIVILIAN TRAINING AREA: HYBRID THREATS AND CYBER - LIST OF AVAILABLE TRAINING OPPORTUNITIES

COURSES ON CYBER

	COURSE	PROVIDER	LEARNING LEVEL	TARGET GROUP	DELIVERY METHOD	NOTES
1.	Challenges of EU Cyber Security	European Security and Defence College (ESDC)	EQF/SQF - 6 and 7	Middle-ranking to senior officials (Civ-Mil)	Residential & e-learning	
2.	Cyber Security/Defence Training Programme	ESDC	EQF/SQF - 6 and 7	Middle-ranking to senior officials (Civ-Mil)	Residential & e-learning	
3.	Infrastructures in the Context of Digitization	ESDC	EQF/SQF - 6 and 7	Middle-ranking to senior officials (Civ-Mil)	Residential & e-learning	
4.	Cybersecurity basics for non-experts	ESDC	EQF/SQF - 6 and 7	Middle-ranking to senior officials (Civ-Mil)	Residential & e-learning	
5.	Cybersecurity Organisational and Defensive Capabilities	ESDC	EQF/SQF - 6 and 7	Middle-ranking to senior officials (Civ-Mil)	Residential & e-learning	
6.	Information Security Management and ICT security	ESDC	EQF/SQF - 6 and 7	Middle-ranking to senior officials (Civ-Mil)	Residential & e-learning	
7.	The role of the EU cyber ecosystem in the global cyber security stability	ESDC	EQF/SQF - 6 and 7	Middle-ranking to senior officials (Civ-Mil)	Residential & e-learning	

8.	Civil-Military Dimension of Cyberattacks	ESDC	EQF/SQF - 6 and 7	Middle-ranking to senior officials (Civ-Mil)	Residential & e-learning	
9.	Cyber Diplomacy	ESDC	EQF/SQF - 6 and 7	Middle-ranking to senior officials (Civ-Mil)	Residential & e-learning	
10.	Cyber Defence policy on national and international levels	ESDC	EQF/SQF - 6 and 7	Middle-ranking to senior officials (Civ-Mil)	Residential & e-learning	
11.	Cybersecurity and smart city: challenges for residents, visitors and businesses	ESDC	EQF/SQF - 6 and 7	Middle-ranking to senior officials (Civ-Mil)	Residential & e-learning	
12.	Cyber Threat Intelligence and Information Sharing using MISP	ESDC	EQF/SQF - 6 and 7	Middle-ranking to senior officials (Civ-Mil)	Residential & e-learning	
13.	AKU 104b Information Security Management Implementation Course Part 1_v1.1	European Security and Defence College (ESDC) – AKU (Autonomous knowledge units)			e-learning	
14.	AKU 104c Information Security Management Implementation Course Part 2_v1.1	ESDC – AKU			e-learning	
15.	AKU 104c Information Security Management Implementation Course Part 3_v1.1	ESDC – AKU			e-learning	
16.	AKU 105 Cyber Situational awareness for senior decision makers	ESDC – AKU		Senior officials	e-learning	
17.	Open source intelligence (OSINT) and IT solutions. (1st)	CEPOL	Expert level/specialised training	OPERATIONS STAFF - Law enforcements analysts, officers who have some experience of High-Tech crime	Residential	

				investigations or are about to be appointed as network investigators or IT forensic analysts, and prosecutors working in cyber-Investigations.		
18.	Open source intelligence (OSINT) and IT solutions. (2nd)	CEPOL	Expert level/specialised training	OPERATIONS STAFF - Law enforcements analysts, officers who have some experience of High-Tech crime investigations or are about to be appointed as network investigators or IT forensic analysts, and prosecutors working in cyber-Investigations.	Residential	
19.	Darkweb and cryptocurrencies	CEPOL	Expert level/specialised training	OPERATIONS STAFF - LE officials and prosecutors dealing with Darkweb and VCs, in cybercrime but also other relevant crime areas (e.g. online trafficking of firearms, drugs, payment card credentials).	Residential	
20.	Conducting forensic searches in various IT devices	CEPOL	Expert level/specialised training	OPERATIONS STAFF- Forensic experts with advanced professional experience on investigating IT devices.	Residential	
21.	Cybercrime - advanced Windows file systems forensics	CEPOL	Expert level/specialised training	OPERATIONS STAFF - Computer forensics practitioners who need to improve file systems knowledge in order to supervise forensic analysis and provide explanation at court.	Residential	

22.	Cross border exchange of e-evidence	CEPOL	Expert level/specialised training	OPERATIONS STAFF - Head of Operations, Deputy Head of Operations, Head of Component, Head of Unit X, Deputy Head of Unit X, Head of Field Office, Deputy Head of Field Office, Head of Regional Coordination/Outreach Unit, Deputy Head of Regional Coordination/Outreach Unit, Head of Project Cell/Project Manager, Head of Training Unit, Justice Adviser, Legal Adviser (Operations), Senior Adviser/Expert, Adviser/Expert, Human Rights Adviser, Gender Adviser, Project Management Officer, Programme Officer, Coordination and Cooperation Officer, Monitor, Operational Officer, Training Officer, BSE Policy Support Officer	Residential	
23.	Digital forensic investigators training	CEPOL	Expert level/specialised training	OPERATIONS STAFF - Law enforcement officials who have experience of High-Tech crime investigations or are about to be appointed as network investigators or IT forensic analysts.	Residential	
24.	Cyber Intelligence	CEPOL	Expert level/specialised training	OPERATIONS STAFF Law enforcement officials working in the field of cyber intelligence at the operational	Residential	

				and technical level, and prosecutors working in cyber-investigations.		
25.	Malware Investigations	CEPOL	Expert level/specialised training	OPERATIONS STAFF Law Enforcement Investigators who have a good knowledge of Computer Networking and the Microsoft Windows OS architecture.	Residential	
26.	Live Data Forensics	CEPOL	Expert level/specialised training	OPERATIONS STAFF Law Enforcement Investigators who have a good knowledge of Computer Networking and the Microsoft Windows OS architecture.	Residential	
27.	Mac Forensics	CEPOL	Expert level/specialised training	OPERATIONS STAFF Law Enforcement investigator involved in computer forensics with at least 1 year experience of computer forensics	Residential	
28.	Linux Forensics	CEPOL	Expert level/specialised training	OPERATIONS STAFF Law Enforcement investigator involved with computer forensics which must have been working with computer forensics for at least 1 year.	Residential	
29.	First responders and cyber forensics	CEPOL	Expert level/specialised training	OPERATIONS STAFF Law enforcement officials – IT crime first responders (first responders in cases of cyber-attacks).	Residential	

COURSES ON HYBRID THREATS

	COURSE	PROVIDER	LEARNING LEVEL	TARGET GROUP	DELIVERY METHOD	NOTES
1.	EU facing "hybrid threats" challenges	European Security and Defence College (ESDC)	EQF/SQF - 6 and 7	Middle-ranking to senior officials (Civ-Mil)	Residential & e-learning	
2.	The Challenges of securing Maritime Areas	ESDC	Advanced/specialised training	Civilian and military personnel (incl. police) from EU Member States, EU institutions/agencies.	Residential & e-learning	
3.	Advanced Course for Political Advisors in EU Missions and Operations	ESDC	Advanced/specialised training	Personnel working in political advisory positions/departments in national capitals, EU institutions, EU agencies as well as in EU missions and operations.	Residential & e-learning	
4.	EU Energy security: implications fot the CSDP	ESDC	Advanced/specialised training	Civilian and military personnel (incl. police) from EU Member States, EU institutions/agencies.	Residential	2020 course held online
5.	Regional seminars on security and defence	ESDC				
	E.g. *CSDP Seminar (Bi-regional Security and Defence Seminar) EU-South America and Mexico*	ESDC	Basic training/ Orientation Course	Civilians, Military, Police (Participants should be senior-level officials, preferable representing both Ministry of Foreign Affairs, Ministry of Defence and the police forces/services from the	Residential & e-learning	

				respective participant country.)		
6.	AKU 106a Hybrid-CoE Adversarial Behaviour	European Security and Defence College (ESDC) - AKU (Autonomous knowledge units) (Course developed by Hybrid CoE)			e-learning	
7.	AKU 106b Hybrid-CoE The Landscape of Hybrid Threats	ESDC - AKU (Course developed by Hybrid CoE)			e-learning	
8.	AKU 106c Hybrid-CoE: The changing security environment (HS2)	ESDC - AKU (Course developed by Hybrid CoE)			e-learning	
9.	AKU 106d Hybrid-CoE Introduction to Hybrid Deterrence	ESDC - AKU (Course developed by Hybrid CoE)			e-learning	
10.	AKU 106e Hybrid-CoE: Hybrid Warfare (JS)	ESDC - AKU (Course developed by Hybrid CoE)			e-learning	
11.	AKU 106f Hybrid-CoE: Hybrid Threats & Maritime Security (JS)	ESDC - AKU (Course developed by Hybrid CoE)			e-learning	
12.	Prevention of election interference	Hybrid CoE		Practitioners	Residential	Courses held up to date: a. Canada (January 2019, two trainings), around 105 practitioners b. Lithuania (February 2019), 40 practitioners c. Finland (March 2019), 35 practitioners d. Poland (April 2019) 50 practitioners

						e. EU RAS (only exercise April 2019) 30+ practitioners f. Montenegro (January 2020) 40 practitioners

COURSES WHICH COVER SOME ELEMENTS OF CYBER AND/OR HYBRID

	COURSE	PROVIDER	LEARNING LEVEL	TARGET GROUP	DELIVERY METHOD	NOTES
1.	CSDP High Level Course (HLC) (e.g. 2020-2021 JEAN REY - 4 modules)	European Security and Defence College (ESDC)		senior experts (mil-civ); incl. diplomats and police officers, who work in key positions or have a clear potential to achieve leadership posts particular CFSP/CSDP. Suitable academics, members of NGOs and the business community may be invited to participate	Residential and e-learning	.
2.	CSDP orientation course	ESDC		Nominated participants from civilian and military personnel from EU Member States, EU Institutions and Agencies, working the field of CSFP/CSDP (1 person per country, or more upon availability.)	Residential	
3.	AKU 01 - History and Context of ESDP/CSDP Development	European Security and Defence College (ESDC) – AKU (Autonomous knowledge units)			e-learning	
4.	AKU 02 - The European Global Strategy (EUGS)	ESDC – AKU			e-learning	

5.	AKU 03 - Role of EU Institutions in the field of CFSP/ CSDP	ESDC – AKU			e-learning	
6.	AKU4 - CSDP Crisis Management Structures and the Chain of Command	ESDC – AKU			e-learning	
7.	AKU6 - CSDP Decision Shaping/Making	ESDC – AKU			e-learning	
8.	AKU 07 - Impact of Lisbon Treaty on CSDP	ESDC – AKU			e-learning	
9.	AKU 11A - Gender and the UNSCR 1325 women, peace and security agenda	ESDC – AKU			e-learning	
10.	AKU 11B - Gender aspects in missions and operations	ESDC – AKU			e-learning	
11.	AKU 15 - European Armaments Cooperation (EAC)	ESDC – AKU			e-learning	
12.	AKU16 - An introduction to the Protection of Civilians (PoC) v.2	ESDC – AKU			e-learning	
13.	AKU 17 - Fragility and Crisis Management	ESDC – AKU			e-learning	
14.	AKU 21- Intercultural Competence	ESDC – AKU			e-learning	
15.	AKU 25 - The EU's Mutual Assistance Clause	ESDC – AKU			e-learning	
16.	AKU 34: PM2 - The EC's Project Management Methodology	ESDC – AKU			e-learning	
17.	AKU 200 Conflicts and crisis management - The EU as a global actor (Gorgio Porzio Adviser of CivOpsCrd)	ESDC – AKU			e-learning	

18.	AKU 300: Intercultural Competence in Civilian Crisis Management	ESDC – AKU			e-learning	

ANNEX 2: TRAINING PROVIDER QUESTIONNAIRE - TEMPLATE

EU CIVILIAN TRAINING GROUP (EUCTG) CIVILIAN COORDINATOR FOR TRAINING (CCT) QUESTIONNOAIRE TO HYBRID THREATS AND CYBER TRAINING PROVIDERS FOR TRAINING REQUIREMENT ANALYSIS (TRA)

EU Civilian Training Area: Hybrid threats and cyber

This questionnaire is aiming to identify and map **Hybrid threats and cyber training** already provided by different Training Providers (like CoE for Countering Hybrid threats, CMC Finland, ESDC etc), for personnel to be deployed at CSDP missions. There is another questionnaire to CSDP missions aiming to identify CSDP mission members' current level of knowledge on hybrid threats and cyber, and their future training requirements and needs in this field.

Both questionnaires will be analyzed to find possible gaps and the need for CSDP mission members' training. As an outcome of analysis, High Level Learning Outcomes for training will be developed to provide Hybrid threats and cyber-related competencies to personnel deployed at missions.

The deadline for answers is 15 April 2020.

Training provider	
Organization and Country	
Type of organisation (Law Enforcement Agency, Training Institution, NGO, MFA, MoI etc.)	
POC for the questionnaire Name/Department/Unit	
Telephone number	
E-mail address	

1. What training do you provide **on Hybrid threats and/or cyber (please specify)** in support of EU External Action (CSDP missions personnel)? Please specify the below details for each course:

a) Training audience (reference is CDSP mission organization).
Please, find Minimum Essential Qualifications and Experience for the position[24]:

- **OFFICES OF THE HEAD OF MISSION AND THE CHIEF OF STAFF**

*Head of Mission**,** Deputy Head of Mission, Chief of Staff, Special Adviser to the Head of Mission, Personal Assistant to the Head of Mission, Head of Coordination and Cooperation Unit, Head of Planning, Analysis, Evaluation and Reporting Unit, Head of Internal Investigations Unit, Head of Press and Public Information Office, Senior Mission Security Officer, Deputy Senior Mission Security Officer, Mission Security Operations Room Manager, Senior Political Adviser, Political Adviser, Mission Analytical Capability Analyst, Reporting Officer ,Senior Reporting Officer, Planning and Evaluation Officer, Lessons Learnt/Best Practices Officer, Press and Public Information Officer, Liaison and Coordination Officer, Mission Security Officer, Mission Security Analyst, Information Security Officer*).

- **OPERATIONS STAFF**

Head of Operations, Deputy Head of Operations, Head of Component, Head of Unit X, Deputy Head of Unit X, Head of Field Office, Deputy Head of Field Office, Head of Regional Coordination/Outreach Unit, Deputy Head of Regional Coordination/Outreach Unit, Head of Project Cell/Project Manager, Head of Training Unit, Justice Adviser, Legal Adviser (Operations), Senior Adviser/Expert, Adviser/Expert, Human Rights Adviser, Gender Adviser, Project Management Officer, Programme Officer, Coordination and Cooperation Officer, Monitor, Operational Officer, Training Officer, BSE Policy Support Officer

- **MISSION SUPPORT STAFF**

Head of Mission Support Department, Head of Technical Services, Head of Finance, Head of Procurement, Head of Human Resources, Head of Logistics, Head of Communication & Information Systems, Legal Adviser (MSD), Finance Officer, Accounting Officer, Procurement Officer, Human Resources Officer, Administrative Officer, Records Management Assistant, Communication & Information Systems Officer, Logistics Officer, Transport Officer, Building Management Officer, Engineer, Logistics Assistant, Medical Adviser, Nurse, BSE Human Resources and Administrative Officer.

- **OTHER** (please specify)

b) Name of the course

c) Is this course part of a broader training program (for example specialized course, professional development)? If yes, please specify.

[24] *Common Security and Defence Policy of the European Union: Force Generation Handbook* 2017 European Union External Action, pp. 7 - 8. (Annex 1)

d) Training language

e) Mode of delivery
   - residential
   - e-learning
   - distance
   - blended
   - other, please specify

f) Training methodology and pedagogical approach

g) Course duration (credit units, days, hours)

h) Course frequency

i) Number of participants

j) Course aim

k) Course learning objectives

l) EQF/SQF level (please specify)

m) Course content

n) How many seats do you offer for foreign participants?

If convenient, please attach the course syllabus.

2. Are you aware of additional training requirements/needs related to Hybrid threats and/or cyber in EU External Action (especially targeted to CSDP mission personnel)? Please specify.

3. Do you have any additional comments/recommendations on training requirements related to Hybrid threats and/or cyber?

1. Head of Mission / Operations

Function	Person Profile	Level EQF[2]	Minimum Years of University Degree[3]	Minimum Years of Professional Experience	Minimum Years of Management Experience
Deputy Head of Mission	Person responsible for supporting HoM in leading the Mission, including deputising.	7	4	12	5 Snr.
Chief of Staff	Person responsible for exercising day-to-day co-ordination of all the Mission's units at its Headquarters	7	4	10	5 Snr.
Head of Operations / Deputy Head of Operations	Person responsible for implementation of Mission mandate through delivering all Lines of Operation. Oversees two or more Components. Likely to be managing 20-50+ persons.	7	4	10	5
Head of Component / Deputy Head of Component	Person responsible for implementation of one Line of Operation. Oversees two or more Units. Likely to be managing 10-20+ persons.	7	4	10	5
Senior Mission Security Officer	Person responsible for ensuring the security of the Mission, and its staff members, through drafting and implementing the Mission Security Plan. Likely to be managing 8-30+ staff.	6	3	8	3[5]
Head of Unit / Deputy Head of Unit	Person responsible for implementation of one part of one Line of Operation (or the same part of several LOs). Likely to be managing 2-10 persons.	7	4	7	3
Senior Adviser / Expert / Officer /Analyst Team Leader	Person responsible for advising and/or mentoring a senior local counterpart (e.g. Director General of Police, Minister of Justice/Interior) or senior Mission leader (e.g. HoM). May also coordinate/manage 2-5 persons[4].	7	4	6	3[5]
Adviser / Expert / Analyst	Person responsible for advising and/or mentoring local counterparts either at mid-level or ground level, or senior Mission leader on matters such as legislative drafting, border management, customs policy, community policing etc. No managerial responsibilities.	6	3	5	0
Officer	Person responsible for conducting a task as required e.g. reporting, lessons learned, planning, evaluating, monitoring, etc. No managerial responsibilities.	6	3	4	0
Monitor	Person conducting monitoring tasks. No managerial responsibilities.	6	3	3	0
Assistant	Person providing secretarial support to senior management. No managerial responsibilities.	n/a	0	3	0

[2] European Qualifications Framework
[3] Or, where applicable, Police/Military rank equivalent. See individual Job Descriptions for details.
[4] On occasion, this person may manage a programme and up to 10/12 persons, on par with a Head of Unit.
[5] Only for positions with managerial responsibilities.

2. Mission Support

Function	Person Profile	Level EQF[6]	Minimum Years of University Degree[7]	Minimum Years of Professional Experience	Minimum Years of Management Experience
Head of Mission Support Department	Person responsible for supporting HoM in all administrative matters. Responsible for managing all the administrative and technical units in the Mission.	7	4	10	5
Head of Technical Services	Person responsible for managing all technical units. Likely to be managing 10-50 staff	7	4	7	3
Head of Unit (Finance, Procurement, Human Resources, Logistics, CIS)	Person responsible for managing one administrative or technical unit. Likely to be managing 2-20 staff	7	4	7	3
Legal Adviser	Person responsible for providing legal advice to the H/MSD and HoM. May manage 3-5 lawyers.	7	4	5	3[8]
Medical Adviser	Doctor skilled in General Practice; may also manage 2-10 persons	7	4	5	3[8]
Officer	Person responsible for conducting a task as required e.g. procurement, recruitment, finance, administration etc. No managerial responsibilities.	6	3	4	0
Engineer	Person trained and skilled in the design, construction, and use of engines or machines, or in any of various branches of engineering.	6	4	4	0
Nurse	Nurse skilled in General Practice. No managerial responsibilities.	6	3 (where applicable)	4	0
Assistant	Person responsible for assisting mission support functions (ex. Transportation, warehouse, logistics, etc., financial)	n/a	0	3	0

NOTA BENE:

Mission mandates are structured according to Lines of Operation. Therefore we have more closely aligned the functional roles with full Lines of Operation (senior management), sub-sections of Lines of Operation (middle management) or individual tasks associated with Lines of Operation (officers/advisers).

By 'Senior Management' experience we understand a person who has held a strategic level management position in either their home country or internationally, with a strong track record of political or institutional change.

[6] European Qualifications Framework
[7] Or, where applicable, equivalent military/police education/training or rank: see individual Job Descriptions for details.
[8] Only for positions with managerial responsibilities.

EU CIVILIAN TRAINING GROUP (EUCTG) CIVILIAN COORDINATOR FOR TRAINING (CCT)

Estonian Academy for Security Sciences, Internal Security Institute

QUESTIONNAIRE TO CSDP MISSIONS FOR TRAINING REQUIREMENT ANALYSIS (TRA)

EU Civilian Training Area: Hybrid threats and cyber

This questionnaire is developed with the aim to identify training needs of CSDP mission members in Hybrid threats and cyber.

Answers to this questionnaire will be consolidated and analysed in order to determine possible gaps in Hybrid threats and cyber training. As an outcome of the analysis, a training programme for CSDP mission members' in Hybrid threats and cyber will be developed.

This questionnaire consists of **26 questions/statements** and it is anonymous. Information about the Point of Contact for the questionnaire is requested only in case of the need for clarification of answers.

While providing your answers, please assess your current knowledge and select between "**advanced", "good", "some"** and **"no"** knowledge. In addition, there are some

questions/statements aiming to identify your opinion on defined specific situations, for example, regarding the availability and regularity of surveys/reports provided to the mission, including on hybrid threats and cyber. You can answer those questions/statements by marking **"yes" or "no".** Also, we ask you to give **explanations and additional comments**, including on specific topics not covered by this questionnaire. Your contribution will facilitate the development of a substantial training programme which meets CSDP missions' training requirements and promotes capacity building in hybrid threats and cyber.

Kindly note, that the deadline for submission of the questionnaire is 15 May 2020.

On behalf of Hybrid threats and cyber Team, we wish you success in answering questions/statements!

Please identify yourself	
CSDP mission	
POC for the questionnaire/ Name/Department/Unit	
E-mail address	
Telephone number	

QUESTIONS

		Please assess your knowledge and understanding in the following areas below					**DO YOU THINK YOU NEED THIS KNOWLEDGE AS A CSDP MISSION MEMBER?**		
	Question/ statement	**Yes** **Advanced** understanding	**Yes** **Good** Understanding	**Yes** **Some** understanding	**No**	**Explain your answer**	**Yes**	**No**	**Explain your answer**
GENERAL EU RESPONSE TO HYBRID THREATS AND CYBER									
1.	I am able to outline EU policy documents on tackling new security challenges, including those linked to hybrid threats								
2.	I am able to describe the overall strategic framework for EU initiatives on cybersecurity and cybercrime								
SAFE USE OF WORK-RELATED SYSTEMS AND DEVICES IN MISSION PREMISES									

3.	How familiar am I with mission rules, guidelines and/or procedures on handling and use of hardware; digital communication related issues (e-mail, chats), software and applications (e.g. WhatsApp and other applications)?								
4.	I am familiar with EU rules, Mission guidelines and/or procedures on secure use of mission related IT-systems								
5.	I am familiar with EU/Mission rules and procedures on handling official, sensitive and/or classified								

	(secret, confidential, restricted) information/documents available to me on the mission								
SAFE USE OF PERSONAL DEVICES OUTSIDE MISSION PREMISES									
6.	How competent am I regarding the use of hardware, digital communication related issues (e-mail, chats, social media), software and applications (e.g. WhatsApp and other applications) outside the mission premises (e.g. at home)?								
SITUATIONAL AWARENESS									
7.	I am able to describe the content of regular /periodical updates about								

	the mission environment, in relation with possible cyber/hybrid threats, specific to the country/area that I am in								
8.	According to my opinion, the regularity of those newsletter/up-dates is sufficient and timely		----------						
9.	According to my knowledge, hybrid threats and cyber security are currently recognised as issues for the host State of the Mission		----------						
10.	I believe the host State will be interested in receiving Mission support in this area		----------						

	(training, advice etc.)							
HYBRID THREATS								
11.	I am able to outline the main characteristics of a hybrid threat							
12.	I am able to describe different kinds of hybrid threats and the different ways in which they can occur							
13.	I am able to assess any location specific information made available to me for the potential of hybrid threats							
14.	Does any location specific information made available to me specifically refer to hybrid threats or		----------					

	potential hybrid threats in the mission area?								
15.	I am familiar with the procedures on who to contact (in the Mission/in Brussels) in case of evidence or suspicion of a hybrid threat incident that has already occurred								
16.	I am well aware of main activities performed by EU Hybrid Fusion Cell, the Hybrid Centre of Excellence (CoE), EEAS Strategic Communication Task Forces and/or related hybrid risk surveys								
CYBER THREATS									

17.	I am able to explain the definition of ”a cyber threat”								
18.	I am able to list the different, most common types of cyber threats included in EU policy documents								
19.	I am able to outline the most commonly used methods of cyberattack								
20.	When I can identify a cyber threat, I know how to react								
21.	I am familiar with tools/equipment for preventing cyber incidents								
22.	How familiar am I with risk mitigation actions to cope with cyber threats?								
23.	How familiar am I with the								

	management of a cyber incident?								
24.	I know the procedures to recover essential systems for the mission after a cyber incident								
PHYSICAL THREATS TO IT-SYSTEMS ETC.									
25.	I am able to identify the most commonly recognised physical threats and vulnerabilities that could affect/damage the IT system/data storage units that are essential to the mission								
26.	I am able to describe the tools normally used to create or trigger a cyber/hybrid threat								

Please describe any other specific topic and express your personal need for training on hybrid threats and/or cyber, not provided in the questionnaire.

Thank you for your answers!

ANNEX 4: QUESTIONNAIRE – FULL LIST OF ADDITIONAL COMMENTS

FULL LIST OF RESPONSES TO THE QUESTIONAIRE QUESTION:

Please describe any other specific topic and express your personal need for training on hybrid threats and/or cyber, not provided in the questionnaire:

- Smartphone security, availability of hardened (opensoure) versions of android (such as GraopheneOS) for those who are interested in their privacy -- although I would personally make it a standard for all mission phones.
- I think it is an important topic, but also requires lots of technical expertise that most mission members don't have. It is important that there is one expert in each mission that is specifically in charge of this thematic area and briefs others regularly and gives practical advice on how to recognize these threats and how to protect from them.
- ON LINE COURSE COULD BE INTERESTING WITH VARIOUS LEVELS TO GET ACUSTOMED TO THAT KIND OF THREATS
- Disinformation/strategic communication is very important issue/threat for EUMM Georgia.
- As member of the mission working group on hybrid threats it would be useful to receive specialized training on: identification/assessment of hybrid threats through foresight approaches, especially horizons scanning and scenarios pathways.
- As CSDP Mission member working at the INFOSEC unit, I feel the need for specific training in this area, especially in the standardization of processes and tools taking into account the different backgrounds and professional experiences of the elements that make up the mission units involved in these matters and which leads to an amalgamation of intentions that rarely lead to an effective prevention.
- It is important that teaching and information is explained so it can be understood by non-professionals. IT technical language is a little bit like medical language which is hard enough as it is but becomes even harder when communicated in a second language thus for communication to have effect there should be a focus on making sure it is understandable
- the use of fake news and how to understand it's fake.
- All topics mentioned in the questionnaire
- Our Mission needs to recruit hybrid threat experts for each and every Field Office that can anticipate, recognize and analyze such threats. Subject matter experts will also need to double as a trainers of incoming staff that will also need to begin to shift their focus on non-conventional threats.
- I think CSDP and the EU and EU member states as a whole should educate its epmloyees and citizens much more about hybrid and cyber threats. There could be some kind of education on CSDP missions level introduced - some emails in SECNET explaining this subject.
- I would like to express my delight about the initiative to explore the need of further education on this topic in European community and I am truly interested to receive such kind of training.
- I think training in cyber security, hybrid threats and disinformation would be extremely valuable in my position
- The topic is more for CIS officers and top management in the mission, regarding hybrid (cyber) threat I have attended only one presentation and so I need another presentation or the training would be welcomed. In my opinion preventions tools (in Opennet, Secnet, whats

app, emails) against Hybrid cyber threat are established sufficiently, only is needed to keep the rules (with spam, to empty trash, logout when leaving PC, etc) and the basic training for monitors to know what to do and to whom to contact (which competent person) in case of cyber threat.

- There is a Big need for developing something between security department (basis security) and CIS (security of info systems). Counter intelligence, using the TESSOc framework which has been used for years within NATO for securing big structures would be a good option for counter hybrids and cyber.
- Organisationally speaking, the people in charge of this within the Mission should have a position in between CIS and Security.
- I use to say: everything has to be fitted for each with a strong common basis and objectives.
- I believe that trainings and/or e-learning courses should be made available for those Mission members who have an interest in exploring this domain in detail.
- Considering that the Hybrid Threats might undermine or harm the targeted organisations also by influencing its decision-making, I believe it might be useful the consolidation of preparedness also on senior management level. Therefore, the Training Requirements Analysis might result in creation of a dedicated training package for technical staff and another one for senior management.
- No, I have no need for additional trainings which were not mentioned in the questionnaire.
- I have very little knowledge in this field and would benefit from training/own research in most mentioned areas especially regarding policy guidelines.
- I believe a short introduction on the meaning of Hybrid threat is sufficient (15 minutes), most topics are covered under other specific trainings related to the topic (e.g. EUCI briefings, CIS).
- In my opinion, there is no need to have a separate Hybrid threat course for all MM. Such course training should only be available for the experts in each department.
- I am interested of basic training on hybrid or cyber threats. It should contain more practical aspects than theory on EU policies.
- These topics are too far from area of responsibility. I am not an expert on the field and it is too complicated to me.
- I am cyber professional and I can answer positively most of the questions. I would be happy to receive training as update on some topics.
- I am normal internet user and some of the questions ate too complicated for me.
- I am more familiar with the overall EU policies and am not aware of the technical aspects. My knowledge is more theoretical.

ANNEX 5: SUMMARY OF JOINT ACTION PLAN IMPLEMENTING THE CIVILIAN CSDP COMPACT

JOINT STAFF WORKING DOCUMENT Joint Action Plan Implementing the Civilian CSDP Compact (8962/19) (30.04.2019)

Available at: https://data.consilium.europa.eu/doc/document/ST-8962-2019-INIT/en/pdf

The Civilian CSDP Compact (doc. 14305/18, dated 19 November 2018) is a key strategic document, with the objective of strengthening the civilian dimension of the Common Security and Defence Policy (CSDP). It provides guidelines and commitments that are to be further undertaken by the Council and the Member States and that would lead to a more capable civilian CSDP with greater EU connection.

Implementation will take place in MSs through a National implementation plan, and at the EU level through the Joint Action plan by EEAS and Commission services in accordance with relevant responsibilities.

This working document provides further commentary on commitments, as well as suggesting concrete actions for implementing the Civilian CSDP Compact (doc. 14305/18, dated 19 November 2018) that should be undertaken by the EEAS and Commission service and which should support full implementation of the Compact by early summer 2023 at the latest.

The following commitments and suggested actions are especially relevant, considering this TRA:

- Commitment 1, which refers to making civilian CSDP more capable, suggests increasing contributions to civilian CSDP to be included in training. Members states are committed to this and a consolidated National Implementation Plan has already been circulated as a template for setting the level of training. Additionally, EEAS could provide further support for sharing best practices, and monitoring the overall process.

- Commitment 4 emphasises the need to develop mission support capabilities (e.g. security, IT, medical care and communication) and generic capability needs (e.g. reporting, strategic communication and management skills), so as to undertake the full range of civilian crisis management missions. Beyond national commitments, it is suggested that there should be greater focus on analysing the training needs of missions. In that respect, mini-concepts can be helpful in identifying capability needs, in particular related to a wider EU response to tackling security challenges.

- Commitment 5 sees national expert pre- and in-mission training in accordance with the CSDP Training Policy. EU CTG can enhance the cooperation EU-level in training, including specific training needs due to new security challenges. The CTG will promote effective use of the training already provided by including both the European Security and Defence College (ESDC) and CEPOL. (EEAS, meanwhile, will develop guidelines for in-mission training).

- Commitment 7 focusses on the capability of nations to provide formed units to be deployed where relevant, as well as to provide training where relevant.

- Commitment 17, which contributes to a more cohesive civilian CSDP, highlights the need to strengthen shared analysis and situational awareness with relevant EU actors. The aim is to promote a greater number of shared risk and conflict assessments that build on and reinforce existing EU tools so as to enable timely and relevant responses. The key action at EU level is for the EEAS to share relevant mission analytical production to other relevant EU institutions.

- Commitment 18 focusses on implementing a more integrated approach to programming and implementation of crisis response actions. Civilian CSDP missions, other CFSP actors and development actors, should seek synergies and implement action in a coordinated plan. For this, joint analysis and shared assessment are key. In this light, one of the key actions is for the EEAS, the Commission services and EU Member States, to further reinforce the implementation of the relevant elements of the EU's Integrated Approach to external conflicts and crises for CSDP.

- Commitment 20 refers to promotion of further cooperation and synergy creation between civilian CSDP missions, Commission services and JHA actors, building upon the uniqueness of all these roles and adding value from strategic planning to operational conduct and information sharing. Key actions at the EU level to promote the synergies are for the EEAS to develop the 'mini-concepts' as well as to develop and implement a proposal for CSDP-JAH cooperation.

- Commitment 21 aims to ensure the operational output of such CSDP-JHA cooperation by considering and mandating appropriate suitable new lines of operation for pilot projects in new or ongoing CSDP missions. These pilot projects should also emerge from the 'mini-concepts' in line with the Council's three priorities of the Level of Ambition: focussing on building and strengthening the capacity of partners to prevent conflict, building peace and addressing pre- and post-crisis needs, and implementation in line with crisis management procedures. In that respect, the EEAS should find suitable opportunities to launch pilot activities and possible future civilian CSDP missions.