Council of the European Union

Brussels, 14 July 2017
(OR. en)

11256/17

LIMITE

COPS 245
POLMIL 85
EUMC 95
CIVCOM 134
CSDP/PSDC 427
IPCR 8

NOTE

From:	Politico-Military Group
To:	Political and Security Committee
Subject:	Exercise Instructions (EXINST) for the EU PACE17 Parallel and Coordinated Exercise with NATO CMX17

Delegations will find attached the Exercise Instructions (EXINST) for the EU PACE17 Parallel and Coordinated Exercise with NATO CMX17, as agreed by the Politico-Military Group on 13 July 2017.

———————————

EU PACE17

PARALLEL AND COORDINATED EXERCISE WITH NATO CMX17

Exercise Instructions

(EXINST)

FOREWORD

1. The EXINST contains all the basic information and instructions for the Training Audience (TA) and participants concerning the conduct of EU PACE17 as foreseen in the EXSPEC (Exercise Specifications).

2. EU PACE17 is an event driven exercise coordinated with and conducted in parallel to NATO CMX17. Only the EU storyline will be depicted in this document as NATO's CMX17 is classified and is releasable only to EU institutions.

3. The events required to drive the whole exercise will be injected in a timely way by DISTAFF during the lead in and the conduct phases.

4. The EXINST will be distributed to the TA, the exercise participants as well as DISTAFF before the start of the exercise (STARTEX).

5. This EXINST is structured in two sections:
   - Section I – Organisation.
   - Section II – Exercise Scenario.

6. Section I deals with all real life issues and includes a detailed description of the conduct phase as well as of all involved participants. Furthermore, it covers all "administrative" issues needed by the TA and by the participants of EU PACE17 to successfully execute the exercise.

7. Section II contains information regarding the exercise scenario which can be released to the TA and participants before the start of the conduct phase.

_____

SECTION I

ORGANISATION

A. GENERAL

1. The Council approved **on 6 December 2016 the Common Set of Proposals** to implement the Joint Declaration, signed in Warsaw on 8 July 2016 by the leaders of the institutions of the EU and NATO which i.a. stipulates that EU and NATO should step up their "coordination on exercises, including on hybrid, by developing as the first step Parallel and Coordinated Exercises for 2017 and 2018". As a follow-up, EU and NATO have agreed the modalities for the implementation of Parallel and Coordinated Exercises (PACE) for 2017 and 2018. The PACE concept was endorsed by NATO's COEC in December and was noted by PSC on 9 February.

2. According to the PACE concept, NATO will take the lead in 2017 with their CMX-17 whereas the EU will lead in 2018. Within this framework, each organisation will define its own aims, scope and objectives, while the non-leading organisation will draw elements from the leading organisation's exercise. These exercises will allow testing coordinated procedures focusing each organisation's Operational Protocols for Countering Hybrid Threats (EU and NATO respective Playbooks). It has also been agreed that each organisation will identify its own lessons and formulate recommendations that will be shared with the other organisation to the extent possible.

3. The PACE17 Exercise Specifications (EXSPEC), define i.a. the aim, scope, objectives and the TA. For the ease of reference, the most important issues are summarised in this chapter.

4. The exercise is named **EU Parallel and Coordinated Exercise 2017** (EU PACE17). It is a so-called comprehensive and combined exercise with a focus on Crisis management and response in a hybrid threats environment. The EU PACE17 will be conducted in accordance with the provisions of the EU Exercise Policy framework, and in full respect of the principles of inclusiveness, reciprocity and decision-making autonomy of the EU.

5. The EU PACE17 will **start on 01 Sept**. and **end on 11 Oct**. 2017 (ENDEX). It will consist of a lead-in phase from 01 to 27 Sept and a conduct phase from 28 Sept. (STARTEX) to 11 Oct. The conduct phase is split into EU storylines roll-out (28 Sept to 04 Oct.) and a staff-to-staff play with NATO (04 to 11 Oct.).

6. Official Scheduling the Exercise (OSE) is the HR/VP Ms. Federica Mogherini.

7. Officials Conducting the Exercise (OCE):
   – DSG Pedro Serrano (EEAS)
   – DSG Ilze Juhansone (Commission)
   – DG Leonardo Schiavo (Council)

8. Officials with Primary Responsibility (OPR):
   – Lead OPR: Tom Robbert (EEAS and lead OPR)
   – OPR: Marie-Ange Balbinot (COM)
   – OPR: Tarik Meziani (Council)

9. The participants (i.e. training audience and DISTAFF) are:

   EEAS:
   The HR/VP. All relevant EEAS services as appropriate, in particular: PRISM; INTCEN; EUMS; CMPD; CPCC; SECPOL; DGBA.IBS; SG. AFFGEN.1 (Stratcom); relevant geographical desks.

   Commission: Commissioners. All relevant Commission services as appropriate, in particular: SG; DG COMM/SPP; DG HOME; DG ECHO; DG GROW; DG ENER; DG CNECT; DG SANTE; HR/D.S; JRC.

   Council: Presidency of the Council of the EU. PSC, EUMC as appropriate. Relevant services of the General Secretariat of the Council, incl. the Directorate General Foreign Affairs, Enlargement, Civil Protection, in particular the IPCR team.

Relevant **EU Agencies** and **CERT-EU**.

10. The **aim** of the exercise is to improve and enhance, in a safe environment, the EU-NATO cooperation at staff-to-staff level using the EU Operational protocol for countering hybrid threats (EU Playbook), in the framework of the PACE concept.

11. In accordance with the EU Protocol for Countering Hybrid Threats (EU Playbook), as well as the EU exercise policy framework, the crisis scenario will be designed to cover – to the extent possible – the following strands: situational awareness; strategic communications; cybersecurity; crisis prevention and response.

12. The **overarching objectives** are to:
     - test the interaction between the existing crisis management arrangements run by Commission services, the General Secretariat of the Council and the EEAS, in particular secured exchange of information.
     - interact with NATO at staff to staff level, and
     - identify modalities to synchronize the two organisations crisis response activities in particular in a hybrid context including aggressive actions by state actors.

13. The specific objectives are:
     - SITUATIONAL AWARENESS**:** At the technical level, use the EU Hybrid Fusion Cell to trigger an EU response according to the EU Playbook in order to test the EU preparedness to respond to a hybrid threat scenario.
     - CRISIS RESPONSE: Test the EU Playbook at operational level by informing and preparing advice to the hierarchy on the management of a major threat and crisis with a predominant hybrid component, particularly testing the interaction and interoperability of the EU crisis management arrangements (notably the EEAS Crisis Response System, the Commission ARGUS, and the EU IPCR).
     - STRATCOM: Exercise EU public communication aiming at EU-NATO coordination of their media work in a threat and crisis situation.

- <u>CYBER:</u> Test Cybersecurity incident coordination at the EU level, especially the analysis of multiple Cybersecurity events including possible cyber constraints.
- To trigger discussions within the Council (PSC, EUMC) with a view to adopt possible measures in response to specific EU storyline events.
- To exchange classified information within and between EU institutions involved in the exercise and test the exchange of classified information between EU and NATO at Staff-to-Staff level.
- To integrate the gender perspective into analysis, planning and the decision- making process.
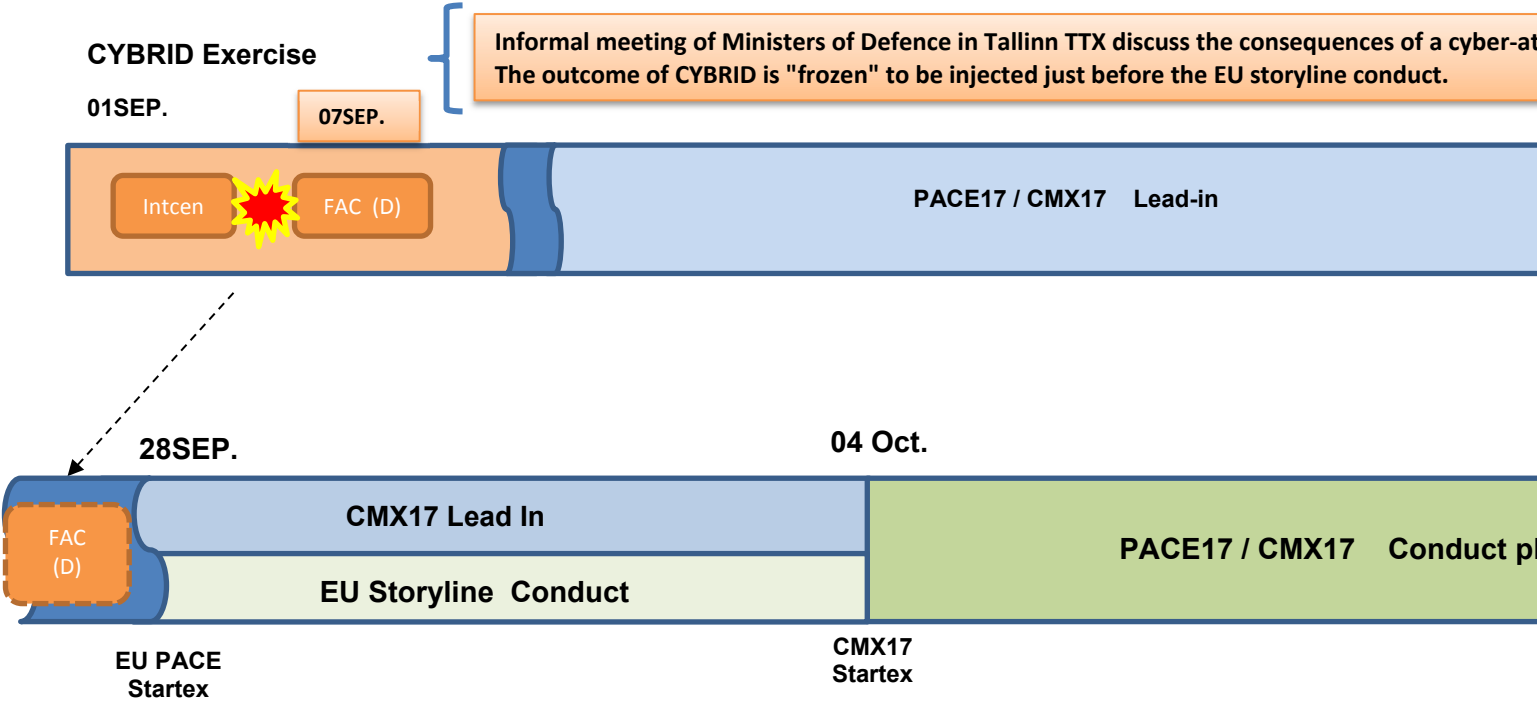
B.   TIMELINES OF THE EXERCISES

14.   There are 3 interlinked exercises: The Estonian CYBRID exercise, the EU PACE17 and NATO's CMX17.

15.   **CYBRID** is a table top exercise conducted under the Estonian EU Presidency aiming at raising awareness at the political/ministerial level of cyber threats during an informal meeting of EU defence ministers in Tallinn on the 7 September. The exercise will also demonstrate how coordinated and targeted cyber-campaigns can disrupt military operations and the wider consequences for the EU.

16.   The EU PACE17 storylines will build on the CYBRID exercise scenario and will use the political guidance of the informal meeting of EU defence ministers (modified, if needed) to kick-off EU PACE17. This will be done by way of a time jump that "freezes" the outcome of meeting and then injects it (via DISTAFF) just before the start of EU PACE17.

17.   **EU PACE 17** has been designed to be coordinated and conducted in parallel with NATO CMX17. As NATO's scenario is classified up to the level of secret (including open media sources), the planning of the EU PACE17 has required the design of two distinct but linked conduct phases (phase I and II), in order to fulfil the overarching objectives as set out in the EXSPEC.

18. **NATO CMX 17 LEAD-IN (01Sep-04Oct):** During this phase NATO will inject a daily number of classified events for the NATO and EU TA but there will be no interaction with NATO during this phase. The purpose is only to fictitiously build up the escalation of the crisis.

19. **EU PACE17 LEAD IN (23Sep-28Sep):** During this phase the EU will inject its own events of the EU storyline to both TAs in the EU as well as in NATO. There is <u>no interaction</u> with NATO TA during this phase, as NATO is still in their lead-in phase and only start their conduct phase on the 4 Oct. This EU parallel storyline is set in the same geopolitical environment as the CMX 17.

20. **EU PACE17 CONDUCT PHASE I (28Sep-04Oct):** This phase starts with the outcome of the CYBRID carried out on the 7 September. It also overlaps with the CMX 17 lead-in. There will be no interaction with NATO other than the EU injecting its events into NATO's lead-in scenario. The EU staff TA will only play the EU storyline, while it will continue to receive information on the wider crisis presented by CMX17, in order to get prepared for the common conduct phase (Phase II). Phase I has two overlapped storylines:

    - **EU Storyline A "Cyber-attack":** Designed to continue with the events played in CYBRID, to challenge the EEAS crisis response mechanism (CRM) and allow the participation of MS through Council Committees (e.g. PSC, EUMC, PMG).
    - **EU Storyline B "Oil shipping companies"**: Designed to activate the crisis response mechanisms in the Council (IPCR) and the Commission (ARGUS) in order to trigger interaction with the EEAS CRM, which will be the first one activated and under which the bulk of the sense-making activities will take place. It will also prepare the EU institutions to enter Phase II to interact with the rest of NATO's storylines.

21. The outcome of the TA play during EU PACE17 Phase I will be then injected by the DISTAFF to CMX 17 at its STARTEX, as a set of new events for NATO's TA. During Phase II, both the EU's and NATO's TA will receive the same classified events. The EU and NATO will interact at staff-to-staff level in this phase.

22. During this phase, the TA is expected to play from 09h00 to 17h30.

23. **EU PACE CONDUCT PHASE II (04 Oct-11Oct):** This phase coincides with CMX17 conduct phase. It is a "free play" and the EU training audience will interact with NATO at staff-to-staff level and respond to all events injected by NATO. In this phase:

- All documentation, including correspondence etc. becomes EU-NATO classified (releasable to institutions) as it will merge with the rest of storylines in CMX17. This means that all EU security rules must be complied with (EU staff must be security cleared, meetings must take place in secured meeting rooms, etc).

- The participation of EU Member States (MS), other EU entities, international organisations etc. is simulated by DISTAFF.

- During the EU PACE17 conduct phase II, the TA is expected to play from 07h00 to 21h00. The TA should be aware that this also includes the weekend 7-8 October.

- As this part of the exercise is classified, each EU institution/service involved will ensure the availability of a secured working space.

_____

EXERCISE TIMELINES

CYBRID Exercise

01SEP.

07SEP.

Informal meeting of Ministers of Defence in Tallinn TTX discuss the consequences of a cyber-at
The outcome of CYBRID is "frozen" to be injected just before the EU storyline conduct.

Intcen   FAC (D)

PACE17 / CMX17   Lead-in

28SEP.

04 Oct.

FAC (D)

CMX17 Lead In

EU Storyline Conduct

PACE17 / CMX17   Conduct pl

EU PACE Startex

CMX17 Startex

PACE 17 – CONDUCT PHASES

PHASE 1 (NON EU CLASSIFIED/EU CLASSIFIED)

PHASE 2 (EU-NATO CLA

28SEP.   (CMX17 Lead In)   **04 Oct.**   PACE17 / CMX17   Conduct ph

FAC (D)

**EU PACE
Startex**

EU Storylines Conduct

**CMX17
Startex**

- CONNECT TO CYBRID
- MEMBER STATES PLAY:
  - EUMC
  - PSC

- ACTIVATE EU CR MECHANISMS
- PREPARE FOR CMX-17
- CONNECT TO CMX-17

PHASE 2:

- RESPOND TO CR
- **ONLY STAFF TO**
- REAL TRAINING

CYBER ATTACK   **OIL SHIPPING COMPANIES CRISIS**   **EU+NATO STORYLINES**

C.   **ROLE OF PARTICIPANTS**

24.   The TA from EU institutions in both phases of EU PACE17 is composed by those identified by their respective hierarchies, to play in a realistic manner the role as responders to the crisis as portrayed in the exercise. It is highly recommended that the TA is different from the staff that has been involved in the planning of the exercise. The composition and expertise of the staff that will play as TA is to be decided by each Division/Service according to the scenario of the exercise and the emphasis put on the four strands in the EXSPEC (Stratcom, Crisis Response, Cyber, and Situational Awareness). The TA will play its role as it would do in a real crisis situation using its communications channels and the locations assigned to it.

25.   Member States are involved as TA only during phase 1 (Capitals, EU Council Committees). As this is an event driven exercise Capitals will be invited to react swiftly and timely.

26.   Member States which participate in CMX17 are reminded not to use or refer to any information of the CMX17 scenario during the conduct of EU PACE17.

27.   The DISTAFF is a joint (EEAS/COMMISSION/COUNCIL) team in charge of the conduct, monitoring and steering of the exercise.

D.   **OBSERVATION**

28.   This exercise is a pilot project with NATO under the PACE concept. EU partners, third countries and International Organisations will not be invited to observe the exercise.

E.   **ASSUMPTIONS**

29.   The exercise will focus on the procedures relating to EU Crisis Management. However, a number of aspects that would normally exist will not be put into play for this exercise. The following general assumptions apply to this exercise:

- Procedures and processes, not individuals, will be evaluated.

- The exercise scenario will be as realistic and plausible as possible. It will contain sufficient details for the players to act. However, due to the limited time, players should focus more on the activation of the Crisis Response Mechanisms and processes and the interaction with other institutions, than in the solution of the fictitious crisis.

F. ARTIFICIALITIES AND CONSTRAINTS[1]

30. It is recognized that certain artificialities and constraints will detract from exercise realism. However, exercise players are to accept these artificialities as a means of facilitating the accomplishment of the exercise objectives.

31. The main artificialities and constraints are:

- Due to the classification of the Phase II documentation (open sources information are also classified), TA will need to work in secured environments.

- During Phase II the DISTAFF will cover part of the role of the Strategic level and will simulate the levels above (Council and MS).

- Participants may need to balance exercise play with real-world emergencies. Real-world emergencies[2] will take priority.

G. PRE-EXERCISE ACTIVITIES

32. An information / educational session for the TA is foreseen on the 4 of September to raise awareness on the exercise and the implementation of these Exercise Instructions. A calling message will be issued in due time.

33. The TA is expected to be already familiar with the EU Protocol on Countering Hybrid Threats (EU Playbook) in view of this session.

---

[1] Artificialities are designed to enhance or improve exercise realism. Constraints are exercise limitations that may detract from exercise realism.

[2] Real world emergencies: These emergencies must be duly explained in the First Impression Report.

H.   INTELLIGENCE

General Background

34.   Within the EEAS, the EUMS Intelligence Directorate (EUMS INT) and the EU Intelligence and Situation Centre (INTCEN) work together under the umbrella of the Single Intelligence Analysis Capacity (SIAC) arrangement. Whenever possible the SIAC brings together the available intelligence analytical capability of both communities to provide the intelligence support to the EU decision-making process.

35.   Within the INTCEN an EU Situation Room has been put in place to ensure global, comprehensive and timely situational awareness to underpin the EU's external action. The EU Situation Room is a permanent stand-by body that provides worldwide monitoring and current situation awareness 24 hours a day, 7 days a week, all year round. It acts as a situation information hub for all relevant stakeholders from the EU institutions. It acts as the EEAS switchboard and embeds within situation reports or flash reports all crisis related information provided, among others, by EU Delegations, EU MS, EU CSDP Operations and Missions, EUSR teams, and International Organisations. The EU Situation Room is the first point of contact for all information on crisis situations in close contact with the Watch Keeping Capability of the EUMS Military Staff.

36.   Within the framework of SIAC, finished Intelligence products from MS (External, Domestic and Defence Intelligence Organisations – IO) are fused with information from the EEAS and EU Commission into all-source Intelligence products which are distributed to all MS (to the PSC and the EUMC), MS IO, appropriate EEAS and the EU Council General Secretariat bodies. In order to improve the efficiency of the SIAC, the analysts of both organizations are organised within their geographical or thematic area of specialisation. This allows both EUMS INT and INTCEN to maintain their full analytical capability and, makes it easy for the analysts to co-ordinate and work jointly with their counterparts.

37.   The authorities and relations with MS of both the EUMS INT Directorate and EU INTCEN are explained below:

1. The EUMS INT Directorate maintains direct links to the MS Defence Intelligence Organisations (DIOs). Under the authority of DGEUMS within its Terms of Reference (TORs), it is responsible for providing the HR / VP and EUMC with analytical products from a military perspective as necessary.

2. The INTCEN maintains direct links to the MS Civilian National Intelligence and Security Organisations. Under the authority of its director within its TORs, it is responsible for providing the HR / VP, the PSC, the OpCdr and the appropriate instances of the EEAS and the Council with strategic assessments. It obtains diplomatic reports from EU delegations and the MS and answers from Civilian National Intelligence Services to Requests for Information (RFI) and, via the EU Situation Room, it exchanges information with a wide network of stakeholders with the EU (EEAS HQ, EU Delegations, the European Commission, the Council and the situation centres of the Member States and other International Organisations such as the UN and the OSCE.

38. Regarding geospatial Intelligence products, the CMPD has, on behalf of the HR / VP, the tasking authority for the EU SatCen via the CMPD POC. EU INTCEN and EUMS INT can provide additional tasking.

39. INTCEN and in particular its Hybrid Fushion Cell will issue RFIs and deliver intelligence products as part of their contribution to Situational Awareness. These products may be EU classified.

Assumptions

40. For EU PACE17 purposes, DISTAFF will inject additional supporting information or incidents and simulated response, including replies to RFIs received from the EU PACE17 TA / participants.

I.   **STRATCOM / SPP**

41.   EEAS STRATCOM is, in close cooperation with HRVP's Spoke Person Service responsible for the real life strategic communication STRATCOM regarding PACE 17 and within the scenario play.

42.   STRATCOM will determine, in close coordination with the Council media team, the relevant master messages, the channels to be used and audiences to be targeted. It is intended to issue one press release at the outset of EU PACE17 Phase I and one at the end of Phase II. In addition, webpages or social media will be used to promote messages relating to the exercises and interaction with NATO.

43.   STRATCOM will endeavour to produce a video (Breaking News) explaining the crisis as portrayed in EU PACE17 to be shown to the TA as an introduction to the exercise.

44.   During the conduct phase STRATCOM will assist the DISTAFF with the injecting of events.

J.   **INFORMATION MANAGEMENT**

Introduction

45.   This chapter outlines the information needs of EU PACE17 and specifies the information infrastructure required to support these needs. It also specifies the appropriate working practices to ensure that information is reliable and secure. Finally, the basis for information exploitation is provided by specifying the organisation of information in files and setting standards for registration in log files and logbooks.

46.   The purpose of Information Management (IM) is to ensure that appropriate information is available where and when needed to support business or organisational objectives. Furthermore this information should be of known reliability and presented in a form which is easily assimilated by decision-makers.

47. This IM chapter does not include information flows out of the framework of the exercise.

48. A detailed set of operating procedures regarding the exchange of classified information between EU and NATO staff will be issued ahead of the envisaged information session on 4 Sep.

Context and Execution

49. EU PACE 17 involves the exercising of different levels (Technical, Operational, Strategic) of the EU Playbook on with NATO. There is no overarching IM ruling policy which covers all participating entities. However, the respective Security Rules are coordinated.

Scope of Chapter / Plan

50. This IM chapter is valid for EU PACE 17 and focuses on the TA. The purpose of the IM chapter is to increase the awareness of expected IM principles to be used during EU PACE17.

51. This IM-chapter is written from the perspective that all participants of the exercise whether DISTAFF, TA or participants in general have the required IT-skills needed to fulfil his / her role and responsibility.

Roles and Responsibilities

52. During the exercise the roles related to IM and CIS are divided between DISTAFF (including the Information Manager), EEAS/BA.IBS.6 (unclassified and restricted communications) and EEAS/BA.IBS.7 (confidential and above communications and classified information registries).

53. As stated above there is no overarching Information Policy which includes all participating entities. The equivalent responsibility of the Senior Information Officer (SIO) is exerted by the lead OPR.

54. The Information Support Officer (ISO) will man the iHub (registry), and manage the preferred single-information-point-entry to the DISTAFF, sending and receiving information, perform IMPEX and manage the registry.

55. Exchange of highly classified documents between EEAS, Commission and the Secretariat General of the Council will take place via the respective central registries.

Information Communities

56. The "internal information community" consist of the TA and the DISTAFF. The TA has generic or particular Training Objectives (TO) in the exercise. Those with particular training objectives are the focal points of IM:

- In EEAS, they are the COMCEN, the Central Registry, the DISTAFF, the Watch keepers and the NOC (Network Operating Centre) of the Secure Communications Division.

- In the European Commission, they are the Central Registry – CENTER – and the Local Registry of the DG HOME.

- In the General Secretariat of the Council, it is the central registry Bureau des Informations Classifiées, the BIC.

57. Point-of-Contact for the Internal Information Community with particular training objectives is the IMgr.

58. The "external information community" consist of those participants in the exercise that do not have any training objectives as they are considered to be mainly consumers of information.

Standard Document Formatting Rules

59. If a document is expected to be sent and approved by an Institution the usual document rules apply.

60. A document which is to be approved by the COUNCIL shall be 1 (one) document (no separate annex), and there can be no embedded documents.

61. If the document is classified as CONFIDENTIEL UE / EU CONFIDENTIAL, and it is supposed to be distributed as the COUNCIL document, it can be up to 20 Mb, since it will only be distributed in hard copy or on DVDs. Lower classifications (RESTREINT UE / EU RESTRICTED, LIMITE / LIMITED, UNCLASSIFIED, PUBLIC) which must be put into Council Workflow system, cannot exceed **4 Mb** in size, otherwise they will be rejected by the Council and cannot be distributed.

Electronic Ways-of-Working (eWoW) - General

62. In order to avoid archiving problems and difficulties in the management of files, duplication of documents should be avoided.

63. Key points are:
- subject matches uniquely and unequivocally the information inside,
- emails, used to send files, get the same subject name as the only one file attached,
- the same file gets the same name, even if it's sent on different means,
- the parallel use of different systems must be mentioned.

64. **In view of facilitating the appropriate monitoring of the exercise by DISTAFF, any official message or documentation circulated electronically among participants has to include the following addressees as cc: E-mail SOLAN or other system (classified information or not): PACE 17_DISTAFF.**

Functional Mailboxes (fmb)

65. To ensure that the information reaches the right entity, in right time the usage of functional mail boxes (fmb) is strongly recommended. The fmb gives the possibility to have several users.

File Naming-Convention

66. The file naming-convention is the following:

   – Space are replaced by a "_".YYYYMMDD-C-ORIGINATOR-Subject-Version

   Where:

   YYYYMMDD is the date of the year, month and day, e.g. 20170905,

   C is the abbreviated level of classification:

   S for SECRET UE / EU SECRET,

   C for CONFIDENTIEL UE / EU CONFIDENTIAL,

   R for RESTREINT UE / EU RESTRICTED,

   L, as marking for LIMITÉ / LIMITED,

   U for unclassified.

   ORIGINATOR is the LAST NAME_First name of the originator, e.g. DOE_John,

   Subject is the abbreviated and security neutralised title of the content, e.g.

   Missing_resources,

   Version is the status and number of the version, e.g. draft_0.9,

   E.g. 20170905-S-DOE_John-Missing_resources-draft_0.9.

67. The maximum amount of signs for the filename and the file-path in the folder structure is 254 signs, therefore it is recommended to keep the name as short as possible.

Documents

68. Any document created should have "**EXERCISE - EXERCISE - EXERCISE**" placed in the Header of each page below the classification level.

Messages

69. All messages should include, after the subject, and in end of the last page the string: "**EXERCISE - EXERCISE – EXERCISE**".

70. When appropriate, the drafter of the message should include the expiry time of the message.

71. After that string, an Exercise Qualifier (EQ) can be used to provide information on authority and distribution. The following EQs messages can be used:

- "DISTAFF EVENT", from DISTAFF to players containing exercise related fictitious events,

- "DISTAFF EYES ONLY from DISTAFF to DISTAFF,

- "DISTAFF CONTROL", for controlling messages from DISTAFF to TA

- "NO PLAY", from the OSEs or OCEs to "ALL EXERCISE PARTICIPANTS".

72. The following "NO PLAY" messages can be issued by:

- OSE: TERMINATION OF THE EXERCISE, incl. an EMERGENCY,

- OSE or OCE: TEMPORARY SUSPENSION OF THE EXERCISE.

EU Classified Information (EUCI)

73. In accordance with current EU Security Rules, EU PACE17 participants must use accredited information tools to send or receive EU Classified Information (EUCI).

74. In cases where EUCI needs to be sent through more than one accredited communication system the sender should state:
"THIS INFORMATION HAS ALSO BEEN SENT OVER XXX".
Where XXX indicates the transmission means used. Each participant receiving a EUCI must apply for precautions or add a filter to identify the eventual arrival of identical messages coming in through various means.

Classification of Documents

75. It is up to the originator to decide the classification in accordance to the content.

76. If the documents are to be approved by the EEAS then they need to be written in line with classifications of the EEAS. The creation of EUCI shall follow the latest EEAS decision regarding security rules for protecting EUCI.

77.	The most used classifications are:

- 	SECRET UE / EU SECRET (S-UE / EU-S). Revealing the context might cause severe damage to the EU or one or several MS.

- 	CONFIDENTIEL UE / EU CONFIDENTIAL (C-UE / EU-C). Revealing the context might cause great harm to the EU or one or several MS.

- 	RESTREINT UE / EU RESTRICTED (R-UE / EU-R). Revealing the context is inappropriate and might cause harm if revealed too early.

78.	The classification should be in 18pt bold, Centre, in footer and header on each page.

79.	**Note! LIMITE or LIMITED is not a classification but a distribution marking.** It means a restricting circulation of the document concerned solely to the EU institutions. Relevant exercise planning documents and information related to EU PACE17 and marked as LIMITE may be released to NATO under the authority of the OCEs, in line with doc. 11336/11.

80.	In principle, it is expected that the majority of messages during the conduct of EU PACE17 will be up to RESTREINT UE/ EU RESTRICTED classification level.

DISTAFF Messages and Distribution of Events

81.	DISTAFF will be responsible for injecting fictitious exercise-related events. All such messages will have the following format:

EXERCISE – EXERCISE – EXERCISE

    SIMULATED ORIGINATOR: AAAAA (only if applicable)

    EVENT NUMBER: NNNN

    DATE OF RELEASE: (Date Time Group)

    EVENT TEXT

EXERCISE – EXERCISE – EXERCISE

82.	DISTAFF will use IT systems as the situation demands (the same net that will normally carry the information).

Request for Information

83.   During the conduct phase of EU PACE17, all requests from the TA for additional information (RFI) must be addressed to the appropriate <u>participating</u> institution / agency / body as defined in the Exercise Specifications.

84.   In case of a request for information can only be provided by a non-participating entity, DISTAFF will simulate represents all EU institutions / agencies / bodies that are not defined as TA as well as representing all other non EU institutions and International Organisation.

Information Infrastructure

85.   This section outlines the information needed for the community to cover the Information Management chapter and as derived from the exercise overall purpose or Training Objectives. It also gives a specification of the information infrastructure required for these needs to be met.

Factors Affecting Information Exchange

86.   Due to risk of instability within the software it is **not allowed to EMBEDD** documents within other documents.

87.   **Note!** Documents with annex / appendix could either be kept separate or compiled together using the function of "Section Breaks" in Microsoft Word.

Specification of Information Infrastructure

88.   All classified information exchanges between institutions must go through the respective central registries except for the Commission which will use the Local Registry of the DG HOME.

EU PACE 17 – Classified Information Flows – NATO RELEASABLE TO EU – EUCI RELEASABLE TO NATO
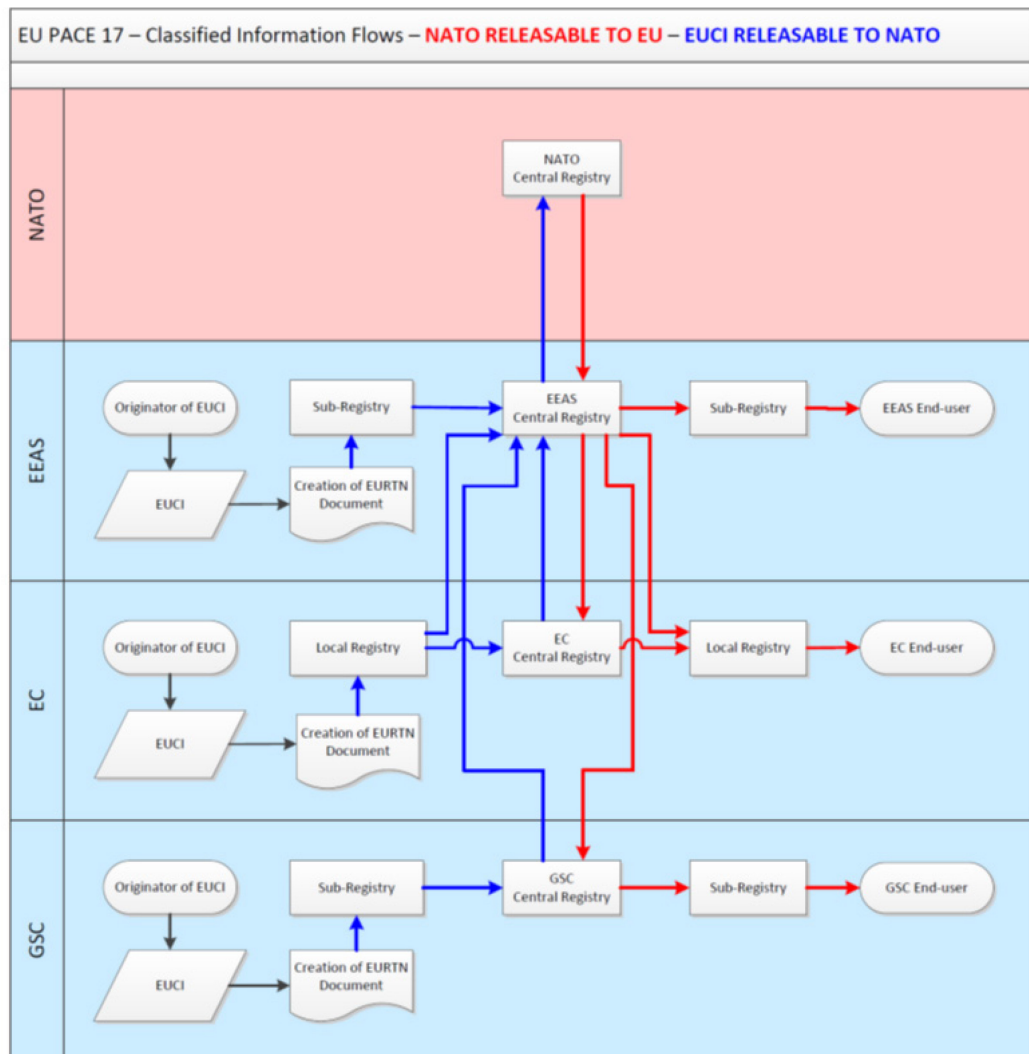
Information Assurance

89. This section covers the general procedures to follow to ensure that information is always available and not compromised.

90. The Information Assurance during the exercise is based on:

- The Security Rules, policies and security notices of the respective organisations.
- The SecOPs of each communication or information system.
- The file-naming convention of the exercise.
- The DISTAFF shall be in copy of all exchanges.

Organisation of Information

91. The information during the exercise will be managed in 6 (six) locations:

   - the folder structure on unclassified IT X-drive (X:\EEAS Exercises\004 PACE 17),

   - the unclassified functional mail box (PACE 17_DISTAFF@eeas.europa.eu),

   - the functional in tray in RUE (PACE17_DISTAFF),

   - the folder structure on SOLAN,

   - the MARS space on SOLAN,

   - the mail box on SOLAN (PACE17_DISTAFF).

92. DISTAFF will manage a logbook for unclassified information on the X-drive and for the classified information on SOLAN; there the email messages will be gathered for later analysis or reuse.

DTG	INFORMATION	From	TO (only TO)	Remarks
15FEB2016	 Imbedded email	DISTAFF	All training audience and participants	Message STARTEX

Illustration of LOGBOOK concept

Implementation

93. As part of the implementation, the exercises IM policies will be briefed to the DISTAFF, other briefs will be performed upon request.

94. Reiterating; this IM-chapter is written from the perspective that the participants of the exercise, whether DISTAFF, TA or participants in general has the required IT, EUCI management and security skills necessary to full fill his/her role and responsibility.

K. COMMUNICATION INFORMATION SYSTEMS (CIS) ARRANGEMENTS

General Situation

95. The EU PACE17 CIS will be based on existing EU owned systems.

96. In all cases, real world operations will retain precedence over exercise needs.

Security

97. In accordance with the Security Rules in force, EU PACE17 participants must use accredited information systems or tools to send or receive classified information.

98. Transfer of information between CIS of different security domains will go through an "Air Gap" interface. Transfer of Classified Information between two security domains is only possible if the recipient system is bearing a security accreditation at least at the same classification level as the classification level of the document to be transferred.

99. In principle, it is expected that most of information during the conduct of PACE17 will be classified at the RESTREINT UE / EU RESTRICTED level.

For Classified Information up to SECRET UE/EU SECRET

BICES

100. BICES provided by NATO is the system used for exchange of classified **intelligence information** between NATO, Missions SOPHIA and ALTHEA, EEAS.EUMS, EEAS.INTCEN, EEAS.BA.IBS.7 and CERT.EU.

NSWAN – SHAPE Link

101. This is the main link to connect NATO to the EEAS via the workstations in EUMS' Watch keepers and NPLT. The classified information has to be transferred via an air-gap to another system like SOLAN.

SOLAN

102. SOLAN is the system for exchange of EUCI inside EEAS and with the Central Registry of the Council. Information can be exchanged via e-mail with attachments and via the IM Application MARS.

CIMS

103. CIMS is the system for exchange of EUCI between EEAS HQ and EU Delegations around the world. It's used equally to exchange EUCI with the European Commission on five specific sites, like the SG or the DG HOME.

For Classified Information up to CONFIDENTIEL UE / EU CONFIDENTIAL

CORTESY CDM

104. CORTESY CDM is the system that could be used for the exchange of EUCI between the EEAS, the GSC, the 28 Ministries of Foreign Affairs, the majority of EU Permanent Representations in BRUSSELS and the European Commission.

105. Entities without direct access to CORTESY could exchange information via the EEAS COMCEN. The information has to be sent to the COMCEN functional mailbox clearly indicating the recipient and having "PACE 17" as starting part of the email subject.

For Classified Information up to RESTREINT UE / EU RESTRICTED

ACID

106. This tool provides off-line encryption for transmission of files over the Internet.

107. All the players have to determine one central post for the reception and internal distribution as well as the external dissemination of the ACID encrypted files.

108. All the players have to ensure the compatibility of their ACID certificate or to request it if needed.

109. In order to avoid any loss of time due to outdated ACID keys, all the players are requested to update their ACID directory prior to the CIS COMCHECK.

110. All the players have to communicate their functional email address to the PACE 17_DISTAFF@eeas.europa.eu at least two weeks before the COMCHECK.

RUE

111. RUE is to be used within the Commission and all entities of EEAS, EU Delegations included. The missions, EUSR and agencies are not connected to the system and therefore must use ACID.

For Unclassified Information including LIMITÉ / LIMITED

112. A standard unclassified workstation connected on the intranet can be used for the exchange of unclassified data including LIMITÉ / LIMITED.

Secure Voice

113. Secure VoIP up to the SECRET UE / EU SECRET level will be available.

114.   The NATO secure VTC facilities are located in Kortenberg 150 and available for NATO-EU communication. The POC is the NATO Permanent Liaison Team (Lt Col Robert Hart) at 02 584 2807 or 02 584 5539. Approval and technical support is normally provided in a day.

CIS Responsibilities

115.   EEAS.BA.IBS.6 will have the overall responsibility for all EU unclassified and restricted communications used during EU PACE17.

116.   EEAS. BA.IBS.7 will have the overall responsibility for all EU classified systems used during EU PACE17 from CONFIDENTIEL UE / EU CONFIDENTIAL level and above, as well as all cryptography of all level.

117.   EUMS CIS DIR will coordinate with the EEAS BA.IBS 6 / BA.IBS.7 in order to provide CIS support to the DISTAFF.

Operational and Technical Support on all CIS and secure phones

118.   The EEAS IT HELPDESK will provide first line support for all CIS and secure phone related issues during the working hours (08.00 – 18.00, BRUSSELS time). The concerned specific technical team will manage the problem from the second level.
   - Phone number: +32.2.584 33 33.
   - Email: EEAS-IT-HELPDESK@eeas.europa.eu

Operational and Technical Support on CORTESY

119.   The EEAS COMCEN will provide the first line support. COMCEN staff is present from (07.30 – 20.00 hrs, BRUSSELS time) from Monday to Friday and from (10.00 – 13.00, BRUSSELS time) on Saturday. Outside the working hours the COMCEN Permanence can be contacted (e.g. for a message with priority URGENT DESKBY) and a COMCEN officer can be on site within 2 hours.

- E-Mail: comcen@eeas.europa.eu

- Phone numbers:

- During working hours: +32 2584 6286

- Outside Working Hours: +32 475 24 7560

CIS Testing

120. Prior to STARTEX, a communication test will be conducted in order to check the CIS connectivity between the different entities and to confirm the identity of the distant end users.

121. The test will be divided in two phases:
     - The first one scheduled for the first week of Sep focusing on the DISTAFF capacities and communication testing within BRUSSELS in particular exchange of information between different EU buildings in BRUSSELS.
     - The second one will take place one week before STARTEX and will focus on the connectivity between BRUSSELS and other entities / players and will confirm the identity of the distant end users.

     Following the testing, a routine schedule of message transmission will be maintained until STARTEX.

CIS Monitoring

122. From STARTEX, the EEAS COMCEN will keep track of EUCI exchange statistics.

123. The EEAS COMCEN will ensure that DISTAFF EYES ONLY messages will be distributed only to DISTAFF.

124. After the exercise, EEAS COMCEN will produce traffic statistics (analysis of traffic flow and volume) and report concerning the systems under their responsibility.

125. In particular, a lesson learnt section will be developed on problems encountered / resolved and with eventual workaround or new solution proposals.

L. SECURITY

Storage of Classified Information

126. EUCI which is classified RESTREINT UE/EU RESTRICTED shall be stored in suitable locked office furniture in an Administrative Area (or its national equivalent) or a Secured Area (or its national equivalent). It may temporarily be stored outside a Secured Area (or its national equivalent) or an Administrative Area (or its national equivalent) provided the holder has undertaken to comply with compensatory measures laid down in security instructions issued by the respective security authority (EEAS SA or NSA).

127. EUCI which is classified CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET may be handled:
    - in a Secured Area (or its national equivalent);
    - in an Administrative Area (or its national equivalent) provided the EUCI is protected from access by unauthorised individuals.

128. EUCI which is classified CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET shall be stored within a Secured Area (or its national equivalent), in a security container or strong room.

Access to Classified Information

129. Access to information classified RESTREINT UE/EU RESTRICTED does not require a security clearance and is granted after:

- the individual's statutory or contractual status has been established,

- the individual's need-to-know has been determined,

- They have been briefed on the security rules and procedures for protecting EUCI and acknowledged in writing their responsibilities to protect EUCI in accordance with this.

130. An individual shall only be authorised to access information classified CONFIDENTIEL UE/EU CONFIDENTIAL or above after:

- their need-to-know has been determined;

- they have been granted a Personal Security Clearance (PSC) to the relevant level or is otherwise duly authorised by virtue of his functions in accordance with national laws and regulations; and

- they have been briefed on the security rules and procedures for protecting.

Registering of Classified Documents

131. All material classified CONFIDENTIEL UE/EU CONFIDENTIAL and above shall be registered when it arrives at or leaves an organisational entity.

132. EU Classified Information handled in CIS and bearing a classification marking CONFIDENTIEL UE/EU CONFIDENTIAL and above; must be registered when it has left the CIS.

Destruction or Declassification

133. At the time of its creation, the originator shall indicate, where possible, and in particular for information classified RESTREINT UE/EU RESTRICTED, whether EUCI can be downgraded or declassified on a given date or following a specific event (ENDEX).

134. Documents subject to registration (CONFIDENTIEL UE/EU CONFIDENTIAL or above) shall be destroyed by the responsible registry on instruction from the holder or from a competent authority. The logbooks and other registration information shall be updated accordingly.

IT Security

135. Security breaches and compromise of classified information must be immediately reported to the respective security officer and to the PACE 17 Information Manager. If there is a suspicion that Classified Information is compromised or leaked the originator must be immediately informed.

136. Security Investigators may take appropriate actions to safeguard the trail of evidence in a manner that is proportionate to the seriousness of the matter under investigation.

J   POST EXERCISE REPORTING PROCEDURES

Exercise Reports

137. All TA, either individually and/or as entity, is obliged to send a First Impression Report (FIRs) in accordance with the format provided in ANNEX C to the Lead-OPR to the following e-mail address
Tom.Robbert@eeas.europa.eu **with a copy to** PACE 17@eeas.europa.eu

138. Member States and all other participants to EU PACE17 may also provide FIRs to the Lead-OPR.

139. The FIRs will provide the basis for the OPRs initial draft Final Exercise Report (FER) which will be discussed in a Post-Exercise Discussion (PXD) to be held in the format of a PMG meeting.

140. Once the FER has been agreed by PMG it will be sent to PSC for notation.

141. The OCEs may decide to send the FER to COREPER for notation.

Evaluation (Strategic Level Lessons Collection)

Lessons at OPR and TA level

142. Each stakeholder is responsible for the collection of lessons and the conduct of the analysis at its level:

    - DISTAFF Lessons (under the authority of the lead OPR) for lessons related to the **planning and conduct of the exercise**;
    - TA lessons collected by the different OPR,s (EEAS, COUNCIL, COMMISSION).

Lessons Relevant for the Political-Strategic Level

143. The elaboration of the lesson should be done in accordance with the template provided in ANNEX B. The level of classification of those lessons must be considered carefully.

Observation Form

144. The Observation Form should be send to: PACE 17@eeas.europa.eu

    Subject of the message: EU PACE17 Observation – Training Audience XXXXX

Date	Event	Action
by 21 Oct	First Impression Reports (FIR)	All Participants
	Compilation of lessons observed	OPRs
TBD	Initial draft Final Exercise Report (FER) to be drafted and distributed	CPT/OPRs
TBD	**Post Exercise Discussion (PXD)**	**CPT and MS exercise experts**
TBD	Exchange of lessons with NATO	
not later than 5 weeks after PXD	Notation of FER exercise reporting process completed	PSC

————————

M.   EU PACE17 STORYLINE

Geopolitical settings

145.   Real geography and real assets are being played.

Operation AIFOS

146.   The EU Operation "AIFOS" has been operating in the Mediterranean since 2015 with a core mandate to "undertake systematic efforts to identify, capture and dispose of vessels and enabling assets used or suspected of being used by migrant smugglers or traffickers, in order to contribute to wider EU efforts to disrupt the business model of human smuggling and trafficking networks in the Southern Central Mediterranean and prevent the further loss of life at sea." Operation "AIFOS" is led by an EU Operation Headquarter in Rome (OHQ).

FROTERRE

147.   FROTERRE is a quasi-democratic country increasingly assertive about its potential economic world power and military strength. FROTERRE is therefore searching for an increased geopolitical role but both its economic interests and values are opposite to those of the EU and the rest of the western world.

148.   The FROTERRE government has very advanced offensive cyber capabilities and controls hackers, hacktivists, and the national media. These groups disseminate propaganda develop tools for intelligence agencies, and hack into networks and databases in support of FROTERRE security objectives. FROTERRE's use of such proxies complicates attribution making it harder to determine who is behind the attack, constraining potential cyber deterrence against government entities.

149. FROTERRE is frequently accused of being behind hybrid/cyber attacks to harass western countries to weaken their economic and geopolitical influence. Attribution in many of the cases cannot be confirmed as most of these attacks are well below the threshold of a hybrid/cyber war.

150. In an attempt to increase its legitimacy vis a vis the international community, the current president of FROTERRE has declared that elections will be held in 2018, but there is only a limited opposition which to a large extent is controlled by the government. No international observation will be allowed to follow the electoral process.

NEWBORN EXTREMIST STATE (NEXSTA)

151. NEXSTA is a global terrorist group belonging to a religious sect, whose main political objective is to establish its caliphate worldwide. Their ideology clashes with the western culture and lifestyle as they see western countries as being decadent and a threat to their religious values.

152. Their primitive modus operandi is to impose their rule, religion and culture notably on European countries by means of persuasion, force or terror extortion.

153. NEXSTA has demonstrated only rudimentary cyber knowledge and is currently focused on propaganda. They have shown interest in improving their cyber capabilities, including through the use of hackers for hire.

AGG "Anti-globalisation Group"

154. AAG is an international movement that is opposed to political globalization. AGG is frequently using social media to pass propaganda messages, organizing riots disguised as demonstrations, all combined with email spamming. AGG, who is sponsoring NGOs in several EU countries, has been accusing EU Member States of having an increased military presence in the Mediterranean. According to some intelligence sources, AGG receives financial support from several countries rather hostile to the EU, including in particular FROTERRE, as well as Cryptocurrency payments from anonymous private sponsors worldwide.

APT MANTICORE WOLF

155. APT MANTICORE WOLF is a cyber threat actor that recently has shown a sharp increase in their cyber capacities and capabilities to target military structures.

APT CHIMERA WOLF

156. APT CHIMERA WOLF is a cyber threat actor that is specialized in industrial espionage particularly in the oil sector.

157. Some western private industry cyber companies have suggested that the interest of these cyber groups acting against the EU seem to align with other hostile actors such as FROTERRE.

SUMMARY OF THE GLOBAL CONTEXT

158. Since August 2017, a substantial number of EU MS have been subject to widespread cyber-attacks of different nature and intensity directed towards their critical infrastructures. At the same time, fake news posted mostly on social media claims that the EU and its MS are unwilling and unable to cope with the effects of the attacks. The EU (and NATO) has not been able to determine with certainty whether these attacks are due to criminal activities or orchestrated by a specific state actor or a non-state actor (a terrorist organization) or both. However, intelligence reports suggest that many of these cyber-attacks are possibly attributable to FROTERRE and/or its allies and proxies. Intelligence reports also suggest that the cyber-attacks are supported by fake news on social media with a view to create distrust and chaos.

LEAD IN EVENTS

159. DISTAFF will inject a number of events between 23 to 28 Sept.

––––––––––––––––

EU PACE17

Request for Information (RFI)

Form

REQUEST FOR INFORMATION
*1 CONTROL NUMBER: DATE/TIME: /
*2. PRIORITY: (HIGH/MEDIUM/LOW)
*3. INFORMATION REQUIRED: (Free text)
*4. JUSTIFICATION:
*5. BACKGROUND:
6. COMMENTS:
07. LEVEL OF CLASSIFICATION OF REPLY:

EU PACE17

Lessons Observation Form

EU PACE17 Lessons Observation Form

Lesson Observation	*The Lesson Observation should be SMART:* *Specific* *Measurable* *Attainable* *Relevant* *Time bounded*
Activity	**EU PACE17**
Title	*The title should reflect the domain covered and provide the main features of the Lesson.*
Detailed description of the facts	*This paragraph should answer the five questions:* *Who? (Stakeholders involved)* *What? (Action performed)* *Where? (Information on space, environment or location)* *When? (Information on time)* *What for? (Rationale of the action performed)*
Description of the operational impact	*This paragraph should depict the overall effect on the operational output:* *In which extent?* *In which manner?*

———————

EU PACE17

First Impression Report (FIR)

Name of TA

EU PACE17 First Impression Report – *Name of TA*

A.   General Comments

B.   Dates and Participation to the Exercise

C.   Achievement of the Exercise Aim

D.   Achievement of the Exercise Objectives

E.   Exercise Planning Issues

    1.   Planning Organisation and Meetings

    2.   Planning Documents

    3.   Financing of the Exercise

    4.   Scenario

    5.   Pre Exercise Activities

F.   Exercise Documentation Issues

G.   Exercise Conduct Phase

    1.   Military / Civilian Planning Process

    2.   Coordination:

        a.   of EEAS and Commission planning

        b.   of EU and Member States activities

    3.   DISTAFF activities

H.   Communications Issues

    1.   Information Flow

    2.   Work with the Different IT Systems

I.   EU Exercise Participation

    1.   Planning Phase

    2.   Conduct Phase

    3.   Evaluation Phase

J.   Comments on EU Crisis Management Procedures Evaluation

K.   Recommendations and other Aspects (as appropriate)

———————————

Abbreviations and Acronyms

A	
AFFGEN	General Affairs
AGG	Antiglobalisation Group
ARGUS	General European Rapid Alert System
B	
BIC	Bureau des Informations Classifiées
C	
CERT-EU	Computer Emergency Response Team for the EU Institutions, Bodies and Agencies
CFSP	Common Foreign and Security Policy
CIS	Computer and Information Systems
CMPD	Crisis Management and Planning Directorate
CMX	Crisis Management Exercise
COM	Commission
COMCHECK	Communications Check
CPCC	Crisis Planning and Conduct Capability
CPT	Core Planning Team
CPX	Command Post Exercise
CRM	Crisis Response Measures
CSDP	Common Security and Defense Policy

D	
DGBA	Directorate General Budget and Administration
DG CNECT	Directorate General for Communications Networks, Content and Technology
DG COMM/SPP	
DG ECHO	Directorate General Communications/Spokespersons Service
	Directorate General European Civil Protection and
DG ENER	Humanitarian Aid Operations
DG GROW	Directorate General for Energy
DG HOME	Directorate General Internal Market, Industry, Entrepreneurship
DG SANTE	and SMEs
DIINST	Directorate General for migration and home affairs
DIO	Directorate-General Health and Food Safety
DISTAFF	DISTAFF Instructions
DSG	Defence Intelligence Organisation
	Directing Staff
	Deputy Secretary General
E	
EC	European Commission
EEAS	European External Action Service
ENDEX	End of the exercise
EQ	Exercise Qualifier
EU	European Union
EUCI	European Union Classified Information
EU OPSWAN	European Union Operation Wide Area Network
EUMC	European Union Military Committee
EUMS	European Union Military Staff
EUJMS INT	Euroepean Union Military Staff Intelligence Directorate
EU SatCen	European Union Satellite Centre
eWoW	electronic Ways-of-Working
EXINST	Exercise Instructions
EXSPEC	Exercise Specifications

F	
FAC	Foreign Affairs Council
FER	Final Exercise Report
FIR	First impression Report
fmb	Functional Mailbox

G	
GSC	General Secretariat of the Council

H	
HR/VP	High Representative of the Union for Foreign Affairs and Security Policy / Vice-President of the Commission

I	
IBS	Security, Infrastructure, Budget and Information Technology Registry
iHub	Information Management
IM	Information Manager
IMgr	Intelligence Centre
INTCEN	Intelligence Organisation(s)
IO	Integrated Political Crisis Response
IPCR	Information Support Officer
ISO	Information Technology
IT	

J	
JRC	Joint Research Centre

K	

L	
LO	Liaison Officer

M	
MEL/MIL	Main Efvent List / Main Inject List
MS	Member State(s)

N	
NATO	North Atlantic Treaty Organization
NEXSTA	Newborn Extremist State
NGO	Non Governmental Organisation
NIC	National Intelligence Cell
NILO	National Intelligence Liaison Officer
NPLT	NATO Permanet Liaison Team
NSWAN	NATO Secure Wide Area Network
O	
OCE	Official Conducting the Exercise
OHQ	Operations Headquarters
OSCE	Organization for Security and Co-operation in Europe
OSE	Official Scheduling the Exercise
OpCdr	Operations Commander
OPR	Official with primary Responsibility
P	
PACE	Parallel and Coordinated Exercise
PMG	Politico-Military Group
POC	Point of Contact
PRISM	Prevention of conflicts, Rule of law/. SSR, Integrated approach,. Stabilisation and Mediation
PSC	Political and Security Committee
PT	Planning Team
PXD	Post Exercise Discussion
Q	
R	
RFI	Request for Information
RLS	Real Life Support

S	
SDA	Shared Data Area
SECPOL	Security policy
SG	Secretary General
SHAPE	Supreme Headquarters Allied Powers Europe
SIAC	Single Intelligence Analysis Capacity
SIO	Senior Information Officer
SITCEN	Situation Centre
SOP	Standing Operations Precedure
SPP	Spokespersons Service
STARTEX	Start of the exercise
STRATCOM	Strategic Communications
SVTC	Secure Video Teleconference
T	
TA	Training Audience
TO	Training Objective
TOR	Terms of Reference
TTX	Table-Top Exercise
U	
UN	United Nations
V	
VoIP	Voice over Internet Protocol
VTC	Video Teleconference
W	
X	
Y	
Z	

REFERENCES

(A) Council Conclusions on the Implementation of the Joint Declaration by the President of the European Council, the President of the European Commission and the Secretary General of the North Atlantic Treaty Organization (Doc. 15283/16 of 06/12/2016).

(B) Joint Communication to the European Parliament and the Council - Joint Framework on countering hybrid threats - A European Union response (JOIN(2016) 18 final on 06/04/2016).

(C) Joint Staff Working Document - EU Operational Protocol For Countering Hybrid Threats – 'EU Playbook' (SWD(2016) 227 final on 05/07/2016).

(D) Parallel And Coordinated Exercises concept between NATO and the EU (PACE) noted by PSC on 9 February (doc. 5916/17).

(E) Exercise Policy of the European Union under the Common Foreign and Security Policy (Doc. 18047/1/13) including its Guidelines for the Scheduling and Implementation of EU Exercises (doc. 18048/1/13).

(F) Draft European Union Programme of Exercises and Exercise-Related Activities under CFSP 2017-2021 (doc. 6137/17).

(G) Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Commission provisions on "ARGUS" general rapid alert system (COM(2005) 662 final).

(H) Finalisation of the CCA review process: the EU Integrated Political Crisis Response (IPCR) arrangements (doc. 10708/13).

(I) Council Decision 2014/415/EU of 24 June 2014 on the arrangements for the implementation by the Union of the solidarity clause.

(J) IPCR preparedness policy (doc. 15138/13).

(K)   IPCR Standard Operating Procedures (doc. 12607/15).

(L)   Integrated Situational Awareness and Analysis (ISAA) Standard Operating Procedures
        (DS 1570/15).

(M)   Exchange of EU classified information (EUCI) with third States and international
        organisations (doc. 10833/16, 30 June 2016).
        http://data.consilium.europa.eu/doc/document/ST-10833-2016-INIT/en/pdf

(N)   Council Decision 2013/488/EU on the security rules for protecting EU classified information
        and Council Decision 2014/333/EU amending Council Decision 2013/488 on the security
        rules for protecting EU classified information.

(O)   Handling of documents internal to the Council (doc. 11336/11, 9 June 2017).

_____