INSTITUTE OF STRATEGIC STUDIES

web: www.issi.org.pk
phone: +92-920-4423, 24
fax: +92-920-4658

Issue Brief

(Views expressed in the brief are those of the author, and do not represent those of ISSI)

1st EU CYBRID 2017

September 29, 2017

Written by: Aamna Rafiq, Research Associate *Edited by: Najam Rafique*

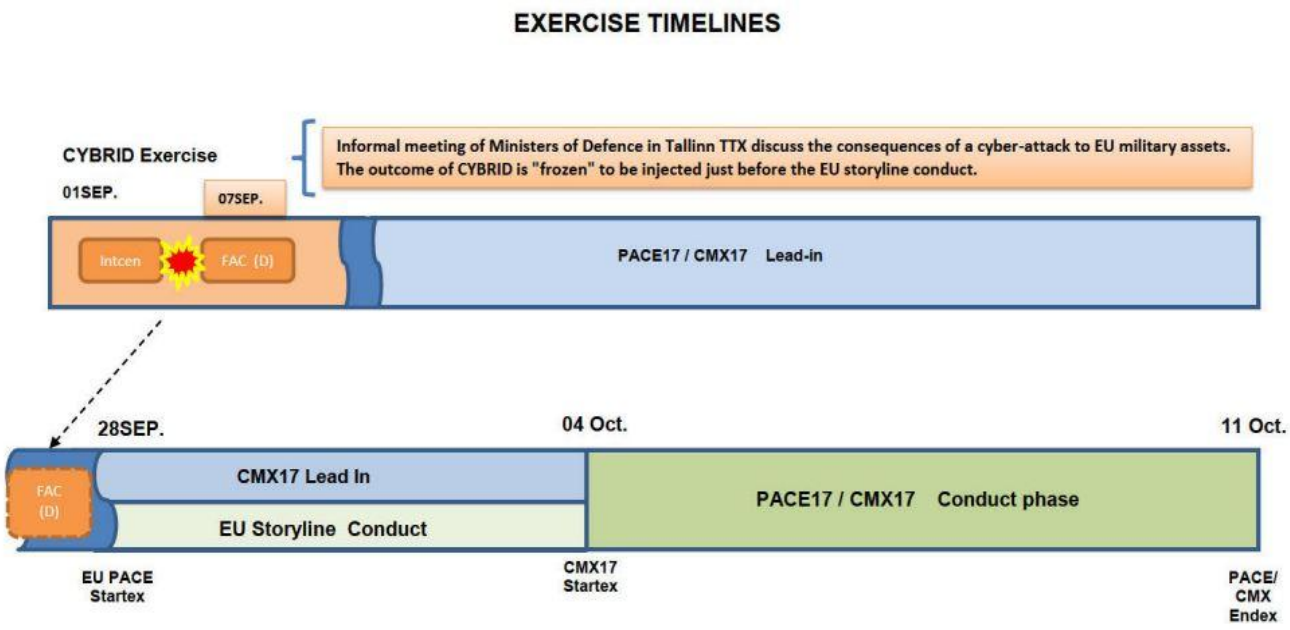
EU Defence Ministers assembled in Tallinn, Estonia on September 7-8, 2017 for first ever strategic table-top cyber defence exercise "EU CYBRID 2017" – a blend of cyber and hybrid warfare techniques. The primary aim of the exercise was to improve the situational awareness, crisis response and strategic communication at political level for effective utilisation of cyber defence techniques in the wake of future crisis. This exceptionally significant exercise was a joint initiative of the Estonian Presidency of the Council of Europe, the European Defence Agency (EDA) and the Estonian Ministry of Defence. The exercise demonstrated that how coordinated and targeted cyber-campaigns can disrupt military operations and generate wider consequences for the EU.[1]

Photography Credit: *European Defence Agency (EDA)*

EU and NATO signed a Joint Declaration in Warsaw on July 8, 2016 to step up their coordination on such exercises for 2017 and 2018. As a first step towards the implementation of this declaration, three interlinked exercises were designed: EU CYBRID 2017; EU PACE17 (Parallel and Coordinated Exercise); and NATO CMX17 (Crisis Management Exercise). These exercises are taking place from September 1 to October 11, 2017. NATO is taking the lead in 2017, whereas the EU will lead in 2018. [2]

[1] "First cyber exercise at EU ministerial level focuses on strategic decision-making," European Defence Agency, https://www.eda.europa.eu/info-hub/press-centre/latest-news/2017/09/07/first-cyber-exercise-at-eu-ministerial-level-focuses-on-strategic-decision-making., last modified September 7, 2017.

[2] Politico-Military Group, "Exercise Instructions (EXINST) for the EU PACE17 Parallel and Coordinated Exercise with NATO CMX17," *Council of the European Union* (Brussels, July 14, 2017): 4-5,



Source: *Council of the European Union*, 2017

The core objectives of EU CYBRID 2017[3] are to:

i. Exercise strategic communication to enhance EU-NATO media coordination in crisis situation.

ii. Test the interoperatability of EU crisis management systems at operational level.

iii. Use the "EU Hybrid Fusion Cell" for better situational awareness and rapid response at tactical level.

iv. Highlight the cyberconstraints after analysing the coordination for cybersecurity incidents.

v. Exchange classified information between EU institutions and between EU and NATO.

vi. Initiate discussion within Council of Europe with the aim to adopt the responsive measures.

In EU CYBRID 2017, a closed-door exercise scenario was created in which fictional rouge elements launched multiple catastrophic cyber-attacks on EU-led military operations at EU Headquarter (Rome)

http://www.statewatch.org/news/2017/jul/eu-council-pace-crisis-management-exercise-plan-11256-17.pdf., accessed September 27, 2017.

[3] Ibid., 6 -7.

and its subordinate maritime assets in the Mediterranean Sea in conjunction with a social media campaign to discredit the operations and trigger massive protests. Each of the EU`s defense ministers was assigned the job to control the simulated crisis over the course of 90 minutes, both individually and collectively. The performance of ministers was not very impressive, but they called the exercise an exciting and eye opening experience. According to Ms. Ursula von der Leyen, German Defence Minister, *"The adversary is very, very difficult to identify, the attack is silent, invisible. The adversary does not need an army, but only a computer with internet connection."*[4] Chief Executive of the European Defence Agency, Mr. Jorge Domecq highlighted the importance of the exercise in following words:

> *"Cyber; the fifth domain of warfare, must be given as much attention as land, air, sea and space. There is no 100% protection in cyber. It is imperative that EU Defence Ministers test their cyber defence mechanisms. The buy-in of Member States is key for the EU to have the necessary skills, technology and capabilities."*[5]

NATO has recognized cyberspace as a new warfare domain and firmly believes that cyber threats have the potential to activate the collective defence clause. This ground-breaking cyber defence initiative has been taken at a time when NATO networks are fighting with 60% increase in cyber attacks during the last one year.[6] This exercise is central for the expansion of EU military potential in cyberspace. The political consensus achieved from EU CYBRID 2017 will support the member states in the construction of advance cyberdefence infrastructure and trained cyber military taskforce equipped with reactive and proactive cyber technology along with advance information sharing network. It opened a whole new avenue of opportunities for Europe to increase its contribution to NATO and vice versa. It is a symbol of mutual political, financial and military support of NATO and EU to ensure the collective defence of Europe.

---

4 Robin Emmott, "Cyber alert: EU ministers test responses in first computer war game," *Reuters*, September 07, 2017, https://www.reuters.com/article/us-eu-defence-cyber/cyber-alert-eu-ministers-test-responses-in-first-computer-war-game-idUSKCN1BI0HR

5 "First cyber exercise at EU," European Defence Agency.

6 Robin Emmott, "Cyber alert," *Reuters*.