US EUROPEAN COMMAND AFTER ACTION REPORT

Action Officer (Rank/Name/DSN)	Directorate/Branch:	Date of Event (DD MMM YY):
(b)(6), (b)(3) (130b)	ECJ67 – ICE	25-27 Jun 2019

Event Name: Baltic Ghost TTX & US/POL KLE

Overview: The 2019 Baltic Ghost TTX was held in Legionowo, Poland from 25-27 June with participation from Enhanced Forward Presence (eFP) contributing nations and organizations. Poland, Germany, Lithuania, Latvia, Estonia, Netherlands, and the United Kingdom, as well as the Multinational Coordination Element, North East (MNCE-NE) were present. The ECJ6, BG Biank, and Polish National Cyber Security Center (NCSC) Director, (b) (6), visited with participants as they worked through an eFP focused cyberspace defense scenario. Following the visit to Baltic Ghost, the US and POL leaders participated in an official ceremony to sign the Cyberspace Cooperation Agreement and answer questions posed by the media. This key leader engagement served as the final approval to begin cooperation in cyberspace.

Participants: official participant list is attached

- Nations: Poland, Estonia, Latvia, Lithuania, Germany, the Netherlands, United Kingdom and United States
- US Organizations: National Guard State Partnership Program: Maryland, Illinois, Michigan, and Pennsylvania, AFCYBER, DISA, and USEUCOM.

Baltic Ghost Discussion Points:

- Baltic Ghost focused on three primary objectives:
  - Understand the operational and strategic-level impacts of a cyber-attack and the appropriate cyber defense to support military operations.
  - Inform perspectives on the roles and responsibilities and decision rights and authorities of key stakeholders (U.S. and NATO) during a coalition and allied response.
  - Share best practices for collective cyber defense processes, procedures, and structures.
- The Cyber Defense Management Board (CDMB), established following Baltic Ghost 2018 briefed their newly established lines of effort aimed at moving from a unity of standards to a unified force:
  - LOE1: Establishment of a federated force structure.
  - LOE2: Establishment of a cyber Common Operational Picture (COP)
  - LOE3: Establishment of a cyber defense framework.
- Common challenges expressed by all personnel included continued information sharing challenges, understanding what is relevant for the operational commander, and users' disregard of integrity and confidentiality of communications when availability is a challenge.
- The Netherlands briefed on current European Union (EU) Permanent Structured Cooperation (PESCO) projected aimed at creating a volunteer Quick Reaction Force – Cyber, to assist with National cyber defense issues on a case by case basis. There have been four EU PESCO Cyber missions since its instantiation last year. Countries hosting are responsible for logistics of teams and signing hold harmless waivers.

KLE Discussion Points:

- (b)(3) (130e)
  - (b)(3) (130e) (b) (6) (b)(3) (130e) ."
  - (b)(3) (130e)