CEMA – ett koncept för cyber- och elektromagnetiska aktiviteter

Projektet Omvärldsanalys av koncept och teknik för cyberförsvar kartlägger kunskap som kan ha relevans för cyberförsvaret. Här görs en preliminär analys av konceptet cyber- och elektromagnetiska aktiviteter (CEMA).

Vad är CEMA?

CEMA som koncept introducerades av amerikanska försvarsmakten i början av 2010-talet. Det utgör integreringen av cyberdomänens och elektromagnetiska spektrumets militära aktiviteter (cyberkrig och telekrig). Konceptet är tillämpbart på alla datorsystem, men främst på de med trådlösa gränssnitt. I CEMA kombineras cyberaktiviteter mot datorer med elektromagnetisk spaning och störning mot lägre lagers signaler. I skärningen mellan telekrig och cyber berörs också trafikanalys, positionering, identifiering samt injicering av vilseledande information.

Varför är CEMA relevant för cyberförsvaret?

Med CEMA kan resultat uppnås som kompetenserna inom cyber respektive telekrig inte kan uppnå var för sig. Ett exempel är att införa skadlig kod på en digital enhet som får denna att senare utföra något som avsiktligt orsakar röjande signaler, vilka kan snappas upp elektromagnetiskt.

Hur kan CEMA användas?

Det teoretiska exemplet ovan skulle kunna omsättas i att med cyberangrepp stänga av flygläget på en mobiltelefon, följt av att med telekrig spåra var mobiltelefonens användare befinner sig. Det finns även indikationer på att CEMA har använts skarpt. Dessa indikationer är dock svåra att värdera eller belägga eftersom tekniska detaljer saknas i öppna källor. Det kan också vara svårt att avgöra om det är integrerat som CEMA eller separata cyberangrepp och telekrig. Två exempel som nämnts som skarp användning av CEMA är cyberangrepp via satelliter som stört ut internetleverantörer i Ukraina samt påstådd israelisk användning av särskilt utformade elektromagnetiska pulser för att införa skadlig kod i syriska ledningssystem.

En (upphävd) brittisk doktrin (JDN 1/18) beskrev att CEMA kunde möjliggöra tre typer av samordnat agerande:

1. *Alternativt agerande*, där CEMA ersätter kinetiska angrepp, t.ex. för att begränsa potentiell skada på civila.
2. *Sekventiellt agerande* där t.ex. cyberangrepp tvingar (vallar) motståndaren att använda ett alternativt kommunikationssystem som sedan kan påverkas elektromagnetiskt.
3. *Kombinerat agerande*, där CEMA t.ex. slår ut felsökningsmjukvara medan kinetiska angrepp förstör utrustning som då kräver felsökning.

Organisatoriskt kan CEMA-personal placeras i renodlade enheter, ingående som celler i andra organisationsdelar, eller som operatörer i specialförband; samt både på taktisk nivå och längre upp. CEMA är också relevant vid underrättelsearbete samt i kombination med icke-kinetiska förmågor inom informationsoperationer och psykologiska operationer.

FOI-forskning på området

FOI har sedan tidigare forskat om CEMA ur ett tekniskt, snarare än konceptuellt, fokus. Ibland har forskning gjorts från telekrigsperspektiv och ibland som cybersäkerhets-analyser av exempelvis ledningssystem som baseras på mjukvarudefinierad radio. FOI har även undersökt detta integrerat som CEMA, men det arbetet är ännu i sin linda.

Rekommendation till Försvarsmakten

- Analysera när CEMA är relevant, beroende på uppgift, kompetens, fjärråtkomst och tid.
- Öva på användning av CEMA. Detta kräver en övningsmiljö för CEMA, gärna med egna telekomnät och kinetiska effekter i likhet med amerikanska Muscatatuck-anläggningen.
- Genomför försök att återskapa påstådda CEMA.
- Utred organisatoriska former för CEMA, där olika kompetenser kan samverka.

Författare: Henrik Karlzén.

FOI Memo: 9268
Forskningsområde: Cyberförsvar och cybersäkerhet
Godkänd av: Pauline Ärlebäck

2026-04-08