Die Relevanz von CEMA (Cyber-Electromagnetic Activities) für die Überlebensfähigkeit und Robustheit zukünftiger militärischer Plattformen“

Ziel und Ablauf

Der Workshop hatte das Ziel einen Dialog über das CEMA (Cyber-Electromagnetic Activities) Konzept zu ermöglichen. Dazu sollten sowohl ausgewählte Komponenten von CEMA anhand von konkreten Beispielen eingeführt werden, als auch die Terminologie vor dem Hintergrund unterschiedlicher Verwendung auf nationaler und übernationaler (NATO) Ebene geklärt werden.

Dazu wurden im Workshop mehrere Impulsvorträge mit unterschiedlichen Schwerpunkten präsentiert. Als öffentlich bekanntes Beispiel für die Möglichkeiten und Herausforderungen im Bereich CEMA, wurde dabei exemplarisch auf Sicherheitsrisiken bei der Nutzung von kommerziellen Drohen eingegangen, die daraus entstehenden Gefährdungslage einerseits sowie die Möglichkeiten zur Drohnenabwehr andererseits. Erwähnenswert sind hierbei insbesondere Angriffsvektoren die auf die Steuerlinks und damit die Navigation der Drohnen abzielen. Hier zeigt sich auch eine gewisse Ambiguität da einerseits durch zusätzliche Absicherung verhindert werden soll, dass Dritte ohne Autorisierung eine Drohne kapern und zweckentfremden können und auf der anderen Seite Behörden und an andere autorisierte Nutzer Drohnen idealerweise mindestens temporär übernehmen können sollten z.B. um eine direkte Gefährdung von Personen auszuschließen.

Eine zunehmende Verknüpfung der Datenräume über unterschiedlichste Kommunikationswege wurde aufgezeigt. Dabei wurde erläutert, welche Informationen aus einem System bei einer ganzheitlichen Analyse abgegriffen werden können. Als Herausforderungen wurden dabei die hohe Marktdynamik sowie die wachsende Flut an Daten herausgestellt.

Es wurde auch die Möglichkeit vorgestellt CEMA unter dem Aspekt der „Threat Informed Defense“ zu beleuchten. Dabei wurde herausgearbeitet, dass eine Kombination der Fähigkeiten und Informationen aus den Bereichen Elektronischer Kampf und Cybersecurity neue Analyse- und Reaktionsmöglichkeiten schaffen, welche den Verlust einer militärischen Drohne an feindliche Kräfte verhindern könnten.

Abschießend wurde herausgestellt, dass jeder Teil der Kommunikationskette potentiell kombinierbaren Angriffen ausgesetzt ist und diese während Entwicklung und Nutzung permanent neu bewertet werden müssen, da aus naheliegenden Gründen auf einen Informationsaustausch in Zukunft nicht verzichtet werden kann.

Im Anschluss wurden in mehreren Kleingruppen anhand von leitenden Fragen und unter dem Eindruck der Impulsvorträge CEMA Herausforderungen und Lösungsansätze diskutiert. Anschließend wurden die von den Teilgruppen gesammelten Impressionen vor dem Plenum zusammengefasst.

Erarbeitete Kernaussagen

Im Workshop wurden die folgenden Kernaussagen erarbeitet:

Herausforderungen und/oder Chancen

- Komplexität (neue Angriffsvektoren und erweiterte Risikoanalysen) durch zusätzliche Dimension (Durchdigitalisierung der Informations- und Prozessflüsse) sowohl als Problem als auch als Chance → Dualität der Cybersecurity im militärischen Bereich lässt sich auf CEMA

erweitern: Schutz eigener Plattformen ist genauso zu betrachten wie die Angriffsmöglichkeiten auf gegnerischer Systeme

- Personelle & Strukturelle Herausforderungen im Bereich CEMA: Expertenwissen in beiden Bereichen (Cyber & Elektronischer Kampf) notwendig & mögliche Harmonisierung der Führungsstrukturen in unterschiedlichen Domänen notwendig
- Auf Grund der Gefährdungslage ist eine Absicherung auf allen Ebenen der IT notwendig, insbesondere deshalb, weil viel nicht-standardisierte IT genutzt wird
- Eine aktive Ausnutzung von entdeckten Schwachstellen (z.B. Einschränkung von Systemfunktionen) ist nicht in allen Fällen sinnvoll, da ein aktiver Angriff die Chancen auf Entdeckung erhöht und somit potenziell eine langfristige Ausnutzung verhindert
- Informationsvorsprung durch ein kombiniertes Lagebild von Cyber und EW („CEMA-Lagebild“) welches durch aufdecken von Informationsflüssen & deren Interpretation (ggf. auch Entschlüsselung von Informationen) Informationsüberlegenheit erzeugt

Vorgeschlagene Maßnahmen

- Allgemeine Sensibilisierung für aus CEMA hervorgehende sicherheitsrelevante Effekte sowohl beim Militär als auch in der Industrie
- Ganzheitliche Betrachtung und Härtung des Eigensystems im gesamten Lebenszyklus:
  - Pre-screening/Adaptierung von COTS Systemen und Komponenten in der Supply Chain durch Trusted Parties und Behörden
  - Aktives Monitoring der Systeme im Einsatz, z.B. hinsichtlich ihrer Kommunikation
- Standardisierung von Security-Testprozeduren (bzw. das Vorgehen bei deren Erstellung)
- Aktive Verwendung existierenden Safety- & Security-Standards und Vorgaben auch wenn nicht durch Regularien explizit vorgeschrieben

Zusätzliche Anmerkungen/Anekdoten

Erfahrung zeigt, dass Störungen im CEMA Bereich nicht nur beabsichtigt, sondern auch unbeabsichtigt stattfinden können. Zum Beispiel durch unbeabsichtigte Strahlung von COTS Komponenten → Abstrahlhygiene der eigenen Systeme (insbesondere bei COTS-Evaluierung) wird immer wichtiger