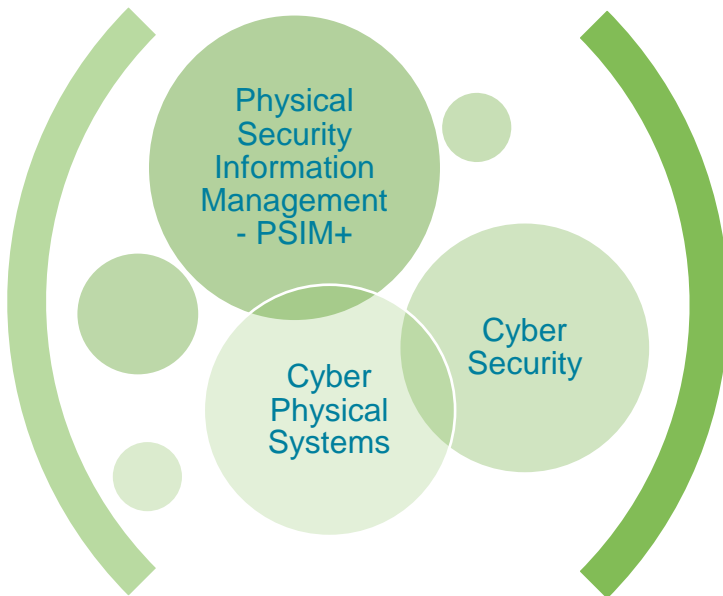


All-Hazards Infrastructure Protection

All-Hazards Infrastructure Protection to Kinetic-Cyber Threats



•Detection

- ☐ Informazioni sullo stato dell'asset
- ☐ IoT, Diagnostica, Sensori
- ☐ Cyber Security systems

•Assessment

- ☐ Situational Awareness
- ☐ Early Warning, pattern
- ☐ Analytics, Interoperabilità

•Response

- ☐ Common Operating Picture
- ☐ Dispacciamento
- ☐ Informazioni alle parti (aziendali e istituzionali)
- ☐ Creazione di scenari

•Remediation – Recovery

- ☐ Pianificazione ed esecuzione di procedure

Cyberattacks are no longer how to steal information, these are attacks that are meant to shut down a country.

Priorità per la sicurezza delle infrastrutture critiche

•Persone: quantità ed organizzazione delle personale preposto alla sicurezza (proprio o terzi)

- Definizione delle organigrammi, team e responsabilità
- Catene di comando e livelli di escalation
- Coordinamento con risorse interne, esterne ed pubbliche

•Processi: garantire l'esecuzione di procedure standardizzate

- Definire Standard Operating Procedures
- Definire scenari e valutare impatti
- Stabilire piani di recovery e remediation
- Definire risorse e modalità di intervento di Computer Security Incident Response Team (CSIRT) e Emergency Response Team (ERT)

•Sistemi: supportare la gestione di scenari complessi che richiedano il trattamento enormi moli di informazioni

- Strumenti flessibili e scalabili
- Interoperabilità dei sistemi ed organizzativa (mezzi e personale) interna e verso l'esterno
- Gestione diversi livelli di comando
- Implementazione workflows e business rules a livello tattico e strategico
- Supporto all'esecuzione delle procedure, circolazione informazione
- Dispiegamento e gestione coordinata di risorse fisiche e/o virtuali, interne e/o esterne

*Security is always
excessive until it's
not enough.*