A. Cyberespionage

Crittografia

- Crittografia simmetrica/asimmetrica, Steganografia, C. centralizzata/decentralizzata, uso di reti neurali e deeplearning nella crittografia
- Crittografia quantistica [Darpa Quantum Network] [protocollo BB84, prot. Di Ekert] [Cifrario perfetto; C. di Vernam, limiti: 1)problema del numero perfettamente casuale, 2)sicurezza nella generazione e nello scambio di una chiave monouso, 3)problema della custodia, poi eliminazione e non riutilizzo della chiave]>>>Project Venona (GCHQ, NSA)

Crittoanalisi >>>metodi di raccolta dati: SIGINT, ELINT, COMINT, OSINT ecce cc

- OSINT (open source intelligence):
    - a. Importanza del settore privato (information brokering, demodossalogia)
    - social media intelligence (problema delle fake news, v. sotto)
    - termini chiave: engagement, mirroring, data leak, search by image, search by code, data scraping, content analytics, metadata extraction, triangolazione di utenti/dati,darkweb monitoring, ideological indicators

B. Cyberwar, Cybercrime

1-Cyberattacco

- tecniche di attacco (o indagine)[sottocategoria: attacchi distribuiti, in part. Tramite "Zombie pc"]: phishing, attacco DOS, Man In The Middle, vulnerability test
- attacchi important: Stuxnet, Titan Rain, Wannacry, Project Raven, Uncle Maker Attack, attacco all'Estonia(2007) [Nato>Manuale di Tallin]

2-Cyberpropaganda<—>IA<—>Fake News<—>Guerra informativa

!!importanza della tutela e della difesa di media, cultura e lingua nazionale[v. punto C, in tema di LLM]!!

3-Cyber+IA+Hardware

- suite hardware e software [nb: costo economico basso. Ad es. v. "Arduino"]
- rapporto tra tecnologie strategiche (golden power) e capacità deterrente
- esempio: sciami di droni killer connessi in rete

C. Cybersecurity, Contromisure

- Red Team<—> CSIRT [importanza delle collaborazioni internazionali: Enisa, Europol, Nato, Interpol]
- Cultura della Sicurezza> coinvolgimento attori privati strategici> Intelligence economica
- Governo di IA e LLM, trasparenza/conoscibilità degli algoritmi

D. Spunti di Approfondimento

- Governo (e law enforcement) della dimensione cyber (cybersovranità) ha ricadute positive per la sicurezza
- Nuovi scenari per la segretezza delle operazioni di intelligence: l'importanza della resilienza ai Data Leak
- Cyberworld, Internet, e la cultura organizzativa: 1. Peculiarità dei modelli gestionali (FAQ, RFC, Teaming); 2. Rapporto tra cultura amministrativa (pubblica) e ingegneristica (privata)
- L'agente cyber e le collaborazioni istituzionali (F. dell'ordine, F. Armate, Governo, Università, Aziende, Organizzazioni Internazionali)