SOCIETÀ GEOGRAFICA ITALIANA ONLUS

ISTITUTO GINO GERMANI
DI SCIENZE SOCIALI
E STUDI STRATEGICI

Corso di Alta Formazione

SPIONAGGIO ECONOMICO, INDUSTRIALE E SCIENTIFICO

LA SICUREZZA ECONOMICA NAZIONALE SOTTO ATTACCO

Roma, 2-3-4 aprile 2020

Società Geografica Italiana - Palazzetto Mattei in Villa Celimontana

Via della Navicella, 12 – Roma

Per informazioni e richieste di partecipazione si prega di contattare:

fondazionegermani@gmail.com

L'Istituto Gino Germani di Scienze Sociali e Studi Strategici e la Società Geografica Italiana (SGI) organizzano il corso di alta formazione sul tema "**Spionaggio economico, industriale e scientifico: la sicurezza economica nazionale sotto attacco**", che si svolgerà il 2-3-4 aprile 2020 presso la sede della SGI, Palazzetto Mattei in Villa Celimontana, Via della Navicella, 12 (Roma). Le attività del corso si svolgeranno dalle ore 9 alle ore 18:30.

Introduzione

Lo spionaggio economico-industriale e scientifico, praticato sia da Stati che da attori non-statali, rappresenta uno strumento sempre più diffuso di guerra economica. I servizi d'intelligence di molti Stati mirano ad acquisire segreti industriali e scientifici di altre nazioni da conferire alle proprie imprese e centri di ricerca nazionali, al fine di potenziarne la competitività e risparmiare ingenti costi di ricerca e sviluppo (e/o per modernizzare i propri apparati militari).

Obiettivo privilegiato di tali attacchi spionistici, condotti con tecniche cibernetiche e/o tradizionali, sono le imprese che investono consistenti risorse in ricerca e sviluppo - e soprattutto quelle operanti in settori strategici e high-tech - ma nessun tipo di azienda o settore economico é escluso. I danni inflitti dallo spionaggio economico-industriale alle imprese e alle economie nazionali sono molto consistenti: i paesi colpiti subiscono un calo di competitività internazionale e spesso la perdita di un grande numero di posti di lavoro, con possibili ripercussioni negative per la loro stabilità sociale e politica.

Le aziende e i centri di ricerca scientifica italiani, anche quelli operanti in settori sensibili per la sicurezza e la difesa nazionale, subiscono danni crescenti a causa della sottrazione - ad opera di servizi segreti esteri, imprese straniere e/o concorrenti, e strutture private d'intelligence - di *know-how* pregiato, proprietà intellettuale, dati aziendali sensibili e altre informazioni di carattere strategico. Ciò costituisce una grave minaccia allo sviluppo economico e alla competitività del sistema-Italia.

La sicurezza economica nazionale, inoltre, è insidiata da azioni di ingerenza economico-finanziaria poste in essere da attori stranieri, statali e non-statali, che mirano all'acquisizione di posizioni dominanti in settori d'interesse strategico del sistema-paese

Obiettivi didattici

Il corso approfondirà, anche con la discussione di casi-studio e testimonianze di operatori dell'intelligence, la minaccia crescente dello spionaggio economico-industriale e scientifico attuato da servizi segreti stranieri e da strutture private d'intelligence: un'attività condotta sempre più di frequente nello spazio cibernetico.

I partecipanti, inoltre, acquisiranno una conoscenza panoramica delle metodologie e tecniche offensive, sia tradizionali che cibernetiche, utilizzate nelle operazioni di ricerca e acquisizione illecita di segreti economici e scientifico-tecnologici. Infine, il corso fornirà essenziali contromisure pratiche e tecniche di controspionaggio a tutela delle informazioni strategiche e il capitale intellettuale di imprese e centri di ricerca.

Al termine del corso i corsisti riceveranno un Attestato di Partecipazione.

Contenuti del corso

1) **Lo spionaggio economico, industriale e scientifico (EIS) nell'era della guerra economica.**
   a) Definizione del fenomeno e profili normativi.
   b) Evoluzione dello spionaggio come strumento di guerra economica nel XXI secolo.
   c) Azioni di ingerenza economico-finanziaria miranti ad acquisire il controllo di industrie di interesse strategico.
   d) La crescente rilevanza dello spazio cibernetico nelle operazioni spionistiche in campo economico-industriale.
   e) Danni provocati dagli attacchi spionistici alle economie nazionali e alle imprese.
   f) I confini, spesso sfumati, tra spionaggio industriale e spionaggio militare.
   g) Attività di acquisizione illecita di tecnologie destinate alla proliferazione di armi di distruzione di massa.

2) **Gli attori dello spionaggio EIS : servizi d'intelligence stranieri avversari e alleati.**
   a) I servizi d'intelligence cinesi.
   b) I servizi d'intelligence russi.
   c) I servizi d'intelligence iraniani e di altre potenze emergenti del mondo non-occidentale.
   d) Servizi d'intelligence di Paesi occidentali e alleati (Francia, Israele) .
   e) Società estere di alta tecnologia collegate a servizi segreti stranieri.

3) **Gli attori dello spionaggio EIS: attori non-statali leciti e illeciti.**
   a) Imprese che prendono di mira i propri *competitors* o agiscono per conto di attori statali.
   b) Strutture private d'intelligence dedite al commercio di informazioni segrete.
   c) Organizzazioni criminali attive nel business della contraffazione.

d) Criminali informatici e *hackers* indipendenti che agiscono autonomamente o al servizio di attori statali o non-statali.

4) **Metodologie e tecniche tradizionali utilizzate nello spionaggio EIS.**
   a) Human Intelligence (HUMINT) e il ruolo dell'*insider* infedele.
   b) Ricerca tramite strumenti tecnologici: Signals Intelligence (SIGINT), Imagery Intelligence (IMINT), Measurement and Signatures Intelligence (MASINT).
   c) Open Source Intelligence (OSINT)
   d) Inganno e *pretext tradecraft*.
   e) Trash Intelligence (TRASHINT).

5) **Metoodologie e tecniche cyber utilizzate nello spionaggio EIS.**
   a) Come evolvono le tecniche offensive: *social engineering* e attacchi *spear phishing*, *back doors, malware*, *adminware, supply-chain operations*.
   b) Il ruolo dell'*insider* infedele nelle operazioni di cyber-spionaggio
   c) Le tecnologie di nuova generazione (Intelligenza Artificiale e *Internet of Things*) e il loro impatto sulla sicurezza cibernetica.

6) **Settori industriali e scientifico-tecnologici di interesse prioritario per gli attori dello spionaggo EIS.**
   a) Tecnologie dell'informazione e della comunicazione.
   b) Industria della difesa, tecnologie militari, armi convenzionali e di distruzione di massa (nucleari, chimiche e biologiche).
   c) Settore energetico, incluse le energie alternative e rinnovabili.
   d) Nuovi materiali e tecnologie manifatturiere avanzate.
   e) Biotecnologie, tecnologie biomediche e farmaceutiche.
   f) Tecnologie avanzate di produzione agricola.
   g) Tecnologie di protezione ambientale.

7) **Contromisure: strumenti e strategie di controspionaggio e controingerenza economico-industriale.**
   a) Il ruolo dei servizi d'intelligence e sicurezza nel contrasto allo spionaggio EIS e all'ingerenza economico-finanziaria.
   b) Principali metodologie e tecniche di controspionaggio economico-industriale.
   c) Linee-guida di una strategia di protezione del patrimonio scientifico, tecnologico e industriale nazionale.

Docenti

Parteciperanno come docenti autorevoli esperti italiani e stranieri, tra cui:

Giulio Terzi di Sant'Agata, Presidente del Comitato Globale per lo Stato di Diritto "Marco Pannella", è stato Ministro degli Esteri.

Paolo Salvatori già Direttore della Divisione Controproliferazione e della Divisione Controterrorismo dell'AISE, è scrittore e docente in materia di intelligence, sicurezza nazionale e internazionale.

Adriano Soi, già responsabile delle relazioni istituzionali del Dipartimento Informazioni per la Sicurezza (DIS), è docente di intelligence e sicurezza nazionale presso la Scuola di Scienze Politiche "Cesare Alfieri" dell'Università degli Studi di Firenze.

Julian Richards, direttore del Centre for Security and Intelligence Studies dell'Università di Buckingham [Regno Unito]; ha lavorato per circa 20 anni nel comparto intelligence e sicurezza del Governo britannico.

Tommaso Profeta è *Chief Security Officer* di Leonardo. Ha prestato servizio come funzionario nella Polizia di Stato presso le sedi di Roma, Palermo, Napoli e Washington, DC (USA).

Michele Colajanni è professore ordinario presso il Dipartimento di Ingegneria dell'Informazione dell'Università degli Studi di Modena e Reggio Emilia.

Paolo Costantini, generale della riserva della Guardia di Finanza, già funzionario dei Servizi di intelligence e sicurezza italiani, é amministratore delegato di Rotas Consulting – A Legal Intelligence Firm.

Giuliano Tavaroli, già responsabile della sicurezza di Pirelli e Telecom, é *Senior Advisor* di Strategic Risk Consulting.

Gregorio D'Agostino, fisico teorico, è *Knowledge Exchange Officer*, ENEA, e docente di sicurezza informatica presso l'Università degli Studi di Roma "Tor Vergata".

Luca Mainoldi, studioso di sistemi d'intelligence e di geopolitica, è consigliere scientifico di *Limes. Rivista Italiana di Geopolitica*.

Luigi Sergio Germani, coordinatore scientifico del Corso, è Direttore dell'Istituto Gino Germani di Scienze Sociali e Studi Strategici.

Parteciperanno, inoltre, altri esperti italiani e stranieri.

Destinatari:

- Funzionari delle Istituzioni di difesa e sicurezza.
- Funzionari di tutte le amministrazioni dello Stato.
- Security managers di imprese, esperti di *corporate security, risk-management, business intelligence* e intelligence privata.
- Personale di imprese, con particolare riferimento alle infrastrutture critiche e all'industria strategica nazionale.
- Esperti delle università, dei think tank, e del settore privato specializzati in temi attinenti la sicurezza nazionale e internazionale.
- Decisori politici e loro collaboratori.
- Operatori dei mass media specializzati in sicurezza e intelligence.

- Giovani laureati, studenti e professionisti interessati ad approfondire la propria conoscenza del mondo dell'intelligence e di temi attinenti la sicurezza nazionale ed internazionale.

Il costo del corso è 350 Euro + IVA. È previsto uno sconto del 10% per appartenenti agli organismi di Sicurezza Nazionale, alle Forze di Polizia e alle Forze Armate, e per studenti universitari.

Per informazioni e richieste di partecipazione si prega di contattare: fondazionegermani@gmail.com.

Telefono: 06-6948 0308 Telefono mobile: 389-2843352

www.fondazionegermani.org