

# NAVIGAZIONE

(inerziale, satellitare, cartografia, mappe 3D)

- **DSMAC, navigazione non GPS: missile TOMAHAWK.** Navigazione, sistemi non GPS che equipaggiano, tra gli altri, i missili TOMAHAWK: DSMAC (Digital Scene MAPPING Correlation) e TERCOM (TERrain CONtour Matching)  
→MA39698/A01 -
- **GPS, criticità: vulnerabilità agli attacchi cibernetici.** GPS (Global Positioning System), debolezza del sistema Usa nei confronti degli attacchi cibernetici nemici; vulnerabilità ad azioni di *spoofing* →MA39698 -
- **GPS, Navstar: jamming, esperienze operative.** Jamming (disturbi) al Navstar GPS (Global Positioning System) di una brigata corazzata in offensiva su un fronte di ampiezza e profondità media →MA39698/1 -
- **GALILEO, tecnologia satellitare: supremazia globale.** Galileo, rete europea di telecomunicazioni satellitari concepita come alternativa alla rete GPS (Global Positioning System): i fallimenti dei tentativi europei di affrancamento dalla dipendenza tecnologica dagli Usa →MA39698/2 -
- **INR, apparati installati sull'UAV RQ-170.** Inertial Navigation System (INR), apparati installati a bordo dell'UAV RQ-170 SENTINEL prodotto dalla Lockheed Martin →MA39698/3 -
- **INFORMATION WARFARE, “drone warfare”: UAV e controllo del cyberspazio.** *All'attacco dei droni: minaccia cyber e guerra aerea robotizzata.* *Drone warfare*, UAV/UCAV (SAPR, sistemi a pilotaggio remoto) e controllo dello spazio cibernetico: la guerra aerea robotizzata. RIVOLUZIONI SPAZIALI E CONQUISTA DEL CYBERSPAZIO. IL MONDO COME UNA “DINAMO”: Alfred von Schlieffen, teorico del blitzkrieg (guerra lampo); cyberspazio e tempo: cyberspazio, dimensione all'interno della quale la categoria di tempo viene compressa e annullata; cyberspazio: definizione compiuta e popolarizzazione del termine; era cibernetica e processo di mondializzazione: definizione datane dall'urbanista francese Paul Virilio; Usa, National Security Strategy 2005: il cyberspazio quale nuovo teatro operativo. SMART POWER: DALLA DISSUAZIONE NUCLEARE ALLA DISSUAZIONE TECNOLOGICA: moderni sistemi d'arma, crescenti dipendenze dal processo di trasmissione dei dati tramite computer, reti wireless e GPS: elevati livelli di interconnessione nei sistemi militari e conseguente aumento sia delle capacità di combattimento che delle fonti di possibile vulnerabilità; GPS (Global Positioning System), attacco ai

sistemi della specie: alterazione delle coordinate e riorientamento della posizione degli assetti militare sul teatro di conflitto, i casi verificatisi nel corso delle operazioni in Afghanistan e Iraq; Gorgon Star, sistema di sorveglianza equipaggiante gli UCAV Predator; Usa, Strategic Defense Guidance 2012 (Amministrazione Obama), linee di difesa previste per il futuro: UAV, operazioni condotte da forze speciali (SF) e azioni di cyberwar; abbandono del concetto relativo alla Two-Land-War Capabilities; Counter-Insurgency, dottrina: "The accidental guerriglia fighting small wars in the Midst of a Big One" (D. Kilcullen); USAF, cyber warfare operations: basi militari "dedicate" di Lakeland (Georgia) e Houston (Texas); Usa, "Olympic Games": programma utilizzato per l'aggressione cibernetica a un altro stato nel corso dell'Amministrazione Obama; Usa, cyberwar: vulnerabilità del sistema americano agli atti di guerra cibernetica (Richard Clarke); NATO, iniziativa *Smart Defense*: vertice alleato di Chicago del 2012; Anonymous, Guy Fawkes; Stratfor, agenzia privata di intelligence; Messico, *narcos*: operazione "#OpCartel", sequestro di un'attivista di Anonymous; GUERRA ROBOTIZZATA: VANTAGGI POLITICI E MINACCE CYBER: UCAV Predator, Central Intelligence Agency (CIA) e US Joint Operation Command: campagne di sorveglianza e bombardamento in tutto il mondo; war, robotica: sistemi d'arma interamente dipendenti da canali di comunicazione remoti; guerra e politica, radicale e completo ripensamento nelle società occidentali moderne: *l'età post-eroica* (Luttwak, Sheehan); Call of Duty 4, simulatore computerizzato per l'addestramento al combattimento aereo; Federal Bureau of Investigations (FBI), Shawn Henry: ex ufficiale dell'agenzia esperto in materia cyber; "dromologia" (Paul Virilio); USAF, UCAV, Unmanned Aircraft System: Flight Plan 2009-2047; UCAV, Northrop Grumman X-47B: primo aereo da guerra completamente autonomo; US Navy, UCAS (Unmanned Combat Air System): sistema X-47B; Usa, nucleare: Department of Energy, National Security Site (ex depositi di stoccaggio di materiali nucleari situati nel Nevada); cyberwar, sabotaggi cibernetici ai centri di controllo di sistemi strategici civili; «autonomia» e «automazione», differenze; DARPA (Defense Advanced Research Projects Agency), sistema X-47B. CYBER-DIROTTAMENTI, COME L'IRAN HA CATTURATO "LA BESTIA": LA TECNICA SPOOFING: Central Intelligence Agency (CIA), programma nucleare iraniano: drone RQ-170 SENTINEL («bestia di Kandahar»), cyber-dirottamento iraniano dell'UAV spia statunitense (4 dicembre 2011); Pasdaran, generale Ali Amir Ajzadeh (comandante del Corpo dei Guardiani della Rivoluzione iraniana): *affaire* RQ-170 SENTINEL; (media) CNN, Chris Lawrence: corrispondente dal Pentagono; jamming: capacità iraniane nel settore del disturbo elettronico (2012); Us Cyber Consequences Unit, *think tank* americano: John Baumgartner; Iran, rete di sorveglianza dello spazio aereo: sistema AVTOBAZA di produzione russa;

*spoofing*; Global Positioning System (GPS), debolezza del sistema di navigazione Usa nei confronti degli attacchi cibernetici nemici; National Security Agency (NSA), sistema di comunicazione criptato per UCAV; Deloitte Center for Cyber Innovation; Los Alamos National Laboratory; aviationintel.com; RQ-4 GLOBAL HAWK, UCAV; UAV e UCAV, segnature: emissioni “silenti” difficilmente identificabili dai radar nemici; Iran, difesa aerea: possibile abbattimento del drone Usa RQ-170 SENTINEL nel dicembre 2011; Inertial Navigation System (INS), apparati installati sul drone RQ-170 SENTINEL realizzato dalla Lockheed Martin; Russia e Iran, cyber warfare: esperti inviati da Mosca implicati nel dicembre 2017 nel sabotaggio del drone Usa RQ-170 SENTINEL; PAY-PERVIEW: SORVEGLIANZA AEREA E PROTEZIONE DELLE INFORMAZIONI: Iraq, 2009, milizia sciita: interruzione del flusso di informazioni e cattura di immagini militarmente sensibili da un UCAV PREDATOR in volo; laptop, impiego da parte dei guerriglieri in Iraq, Afghanistan e Pakistan; PREDATOR, UCAV: costi delle operazioni di manomissioni cibernetiche; Austin University (Texas), conduzione di studi sulla manomettibilità dei droni; Usa, dipartimento della Homeland Security; DENTRO LA STANZA DEI DRONI: IL RISCHIO DEL CONTAGIO INFORMATICO: trasmissioni, sicurezza dei canali di informazione in ambiente militare: ripensamenti e revisioni; USAF, criticità, attacco cibernetico subito nell’ottobre 2011: base militare di Creech (Nevada), infezione delle stanze di comando dei droni PREDATOR e REAPER operativi in Afghanistan causata da un virus informatico (keylogger); Usa, cyber defense: Host Based Security System; Leon Panetta, direttore della Central Intelligence Agency (CIA): sicurezza cibernetica; Usa, 6 comandi militari regionali (Geographic Combattant Command): il Joint Cyber Center; Ground Control Station (GCS); velivoli, mappe di navigazione; Kaspersky Lab; DALLA LINEA MAGINOT AL PROGETTO CRASH: LA NECESSITÀ DI UN FIREWALL “ELASTICO”: DARPA, cyber security: studio di un protocollo di sicurezza da applicare (anche) nell’uso di sistemi di volo a pilotaggio remoto (SAPR); Kathleen Fischer (DARPA), esperto di cyber security; Windows, piattaforma: veicolo di diffusione di *malware*; “crackabilità” degli odierni sistemi informatici; *firewall*, antivirus: sistemi ormai superati dalla realtà (2012); virus *keylogger*; infezioni degli hardware: microchips assemblati in Cina e successivamente inseriti nei computer (Intel, Motorola, Texas Instruments) in uso al Pentagono per la gestione di sofisticati sistemi d’arma; Usa, numero di droni operativi (anno 2012) nella CIA e nell’USAF; Regina Dugan, ex direttore del DARPA; Usa, cyber-dominio: marcate capacità offensive, ma contemporanea vulnerabilità dei sistemi di difesa; Howard Shrobe; Clean-Slate Design of Resilient, Adaptive Security Host (CRASH), sistema di sicurezza nei confronti della minaccia cyber mutuato dal sistema immunitario umano e dalla capacità adattiva degli organismi biologici avanzati;

COMBOTS (combat robots), categoria elaborata da Matthew Hipple; “paleo-wireless”, tecnologie; GPS, vulnerabilità nei confronti di azioni *spoofing*; navigazione, metodi non satellitari (GPS) che equipaggiano – tra gli altri – i missili TOMAHAWK: TERCOM (Terrain Contour Matching) e DSMAC (Digital Scene Mapping Correlation). MODERN WARFARE. “Nuove guerre”, coinvolgimento di attori alternativi agli stati e presenza di minacce *di terzo tipo* (non interstatuali, di lunga durata e dal carattere irregolare): invalidità del modello trinitario clausewitziano; information warfare: categorie dell’*electronic warfare* e della *cyber warfare*; Usa, droni: accuse di un ricorso indiscriminato a questo strumento; rete *anonymous*, “hactivismo” o “cyber resistenza”; Russi, Vladimir Putin: minacce portate da blogger appartenenti al variegato universo di protesta dell’opposizione; network intelligence (NI), capacità di estrarre e porre in correlazione le informazioni e i dati che si muovono sulla rete allo scopo di fornire una piena *situational awareness* per la sicurezza cyber delle forze armate e dello stato; USAF, Air Force Electronics Systems Center’s Cyber Integration Division: Vince Ross, program manager; ISTAR (intelligence, surveillance, target acquisition and recoinnassance), schiacciante superiorità Usa nel settore; Tacticization of Strategy (Michael Handel), superamento del canale di trasmissione tra il *warfare* e la *strategia*: errata convinzione che la superiorità tecnologica sia da sola sufficiente a rendere superfluo il livello tattico e operativo della guerra; *drone warfare*: ampliamento geografico  
→MA39698/4 -

• **INTELLIGENT AWARENESS, sistema di navigazione e Situation Awareness.**

Situation Awareness (consapevolezza della situazione), INTELLIGENT AWARENESS: sistema per la navigazione basato sulla fusione delle informazioni raccolte da vari sensori presentate nella forma della mappa 3D mediante l’applicazione di tecnologie LIDAR (Light Detection and Ranging); presentazione nel corso del Seatrade Cruise Global di Fort Lauderdale (Usa); progetto AAWA (Advanced Autonomous Waterborne Applications), studi e sperimentazioni tecnologiche finalizzati alla realizzazione di una “nave autonoma”; imprese industriali impegnate nel progetto: Rolls-Royce Remote & Autonomous Operations, Liro Lindborgh, General Manager →MA39699 -

• **SIGMA 40, sistema di navigazione inerziale: installazione su sottomarini.**

Sigma 40, sistema di navigazione inerziale prodotto dall’industria francese Safran Electronics & Defense: fornitura alla marina olandese, installazione sui quattro sottomarini classe WALRUS; L3 KEO, periscopio di concezione tradizionale; siluri Mk-48 Mod. 4 e siluri Mod. 7 →MA39700 -

• **SENSORI MAGNETO INERZIALI.** Navigazione, sensori magneto-inerziali impiegabili in assenza di segnale GPS: SYSNAV →MA39700/1 -

- **TERCOM, navigazione non GPS: missile TOMAHAWK.** Navigazione, sistemi non GPS che equipaggiano , tra gli altri, i missili TOMAHAWK: DSMAC (Digital Scene MApping Correlation) e TERCOM (TERrain COntour Matching)

→MA39700/2 -