INFORMATICA

Internet e information warfare

• **ACCESSI, gestione.** Gestione degli *accessi* →**I09141 -**

• **AGENTI CIBERNETICI, Duqu, Flame, Gauss.** Agenti cibernetici: Duqu, Flame, Gauss; duqu, malware *tool* per l'accesso remoto →**I09142 -**

• **ALGORITMI, algoritmi "deep learning".** Algoritmi di *deep learning*: immagini ad alta risoluzione →**I09143 -**

• **ALGORITMO RSA.** Crittografia, algoritmo RSA (attualmente dominante) →**I09144 -**

• **AMAZON, Jeff Bezos: acquisizione del Washington Post.** Jeff Bezos, proprietario del sito web "Amazon": acquisto del quotidiano "Washington Post" →**I09145 -**

• **AMBIENTE TELEMATICO, Evernet: reti costanti.** Ambiente telematico, *Evernet* (era di reti costanti): interdipendenza ed effetti a catena →**I09146 -**

• **AMBIENTE TELEMATICO, reti: criticità.** Reti informatiche, elementi di maggiore debolezza dei sistemi sociali ed economici moderni →**I09147 -**

• **AMBIENTE TELEMATICO, spazi cibernetici e spazi reali.** Spazi cibernetici e spazi reali →**I09148 -**

• **AMBIENTE TELEMATICO, spazi cibernetici: aspetti "non virtuali" (fisici).** Ambiente cibernetico, aspetti "non virtuali" (quindi *fisici*): cavi sottomarini utilizzati dalle reti informatiche per la trasmissione dei messaggi (informazioni) tra due punti →**I09149 -**

• **AMBIENTE TELEMATICO, spazi cibernetici: opacità.** Opacità dell'ambiente cibernetico →**I09150 -**

• **ANALISI, Easy Recovery Professional.** Informatica, intelligence: Easy Recovery Professional, programma che consente l'analisi dei dischi rigidi dei computer danneggiati oltreché il rinvenimento di files danneggiati o cancellati per errore →**I09151 -**

• **ANALISI, filtri informatici e analizzatori semantici.** Intelligence, analisi: filtri informatici e analizzatori semantici →**I09152 -**

• **ANALISI, gruppo di analisi: minima consistenza necessaria.** Informatica, intelligence: gruppo di analisi, minima consistenza necessaria in termini di elementi →**I09153 -**

• **ANALISI.** ***L'intelligence nel XXI secolo: il rapporto fra analisi e politiche.*** Intelligence, scopo principale: soddisfazione delle esigenze di informazione (307); LO STRUMENTO, IL MESSAGGIO E L'UTILIZZATORE POLITICO (308): Marshal McLuhan, sociologo canadese: grande teorico e profeta delle moderne comunicazioni (309); *villaggio globale* (309); UNO SGUARDO AL SETTORE PRIVATO DELL'INFORMAZIONE E DELLA CONOSCENZA (310): comunicazioni, informazione, conoscenza: i mutamenti radicali intervenuti (311); attività B2B (*business to business*) (311); attività B2C (*business to consumer*) (311); FATTORI DEL CAMBIAMENTO: UN ORDINE NUOVO DI INRORMAZIONE E CONOSCENZA? Mutamento radicale nell'intelligence, dalla *raccolta* (XX secolo) all'*analisi* (XXI secolo): i quattro fattori principali del cambiamento (312); "intermestica" (*intermestic reality*) (312, 314); rivoluzione digitale: effetti-chiave prodotti sull'analisi di intelligence (313); nuovo disordine mondiale post-guerra fredda: sovraccarico informativo per l'intelligence (313 e s.); tre tipi di intelligence: estera, sicurezza interna, polizia (315); manipolazione dell'informazione e disinformazione (315 e s.); IL RAPPORTO ANALISI-POLITICHE, IL VERSANTE DELLE POLITICHE: Albert Einstein: tempi necessari alla soluzione dei problemi (318); errori dell'intelligence: due accuse più aspre di fallimento (318); politica, primo ministro (o presidente della repubblica): radicale mutamento di ruolo (319 e s.); analisi trasversale (319 e s.); intelligence, tre concetti: dati, informazione, conoscenza (321); Urss, Stalin: errore previsionale riguardo l'attacco militare tedesco del 1941 (321); disinformazione, elevata vulnerabilità del livello politico alle operazioni di *disinformazione* o *intossicazione*: utilizzo scientifico del metodo *spin* (322); intelligence, allocazione delle risorse: costi dell'attività di raccolta e costi di quella di analisi (322 e s.); VERSANTE DELL'ANALISI E DELLA VALUTAZIONE NEL RAPPORTO ANALISI/POLITICHE: intelligence, funzione analitica: attività e sottofunzioni (323); gerarchia, azzeramento della: organizzazioni "piatte" e non gerarchiche (324); analista, figura del: analista di valutazione e analista di intelligence nazionale (325 e ss.); analisi di intelligence: schema 24/7 (327 e s.) →**I09154 -**

• **ANONYMOUS, Guy Fawkes.** *Anonymous*, Guy Fawkes →**I09154/1 -**

• **ANONYMOUS, "hactivismo" (o "cyber-resistenza).** *Anonymous*, "hactivismo" (o "cyber-resistenza) →**I09154/2 -**

• **ANONYMOUS, sequestro di un'attivista dai narcos messicani.** Messico, *narcos* (narcotrafficanti): operazione "#OpCartel", sequestro di un'attivista di Anonymous →**I09154/3 -**

• **ANTIVIRUS, firewall: obsolescenza.** Antivirus, firewall: sistemi ormai superati dalla realtà (2012) →**I09154/4 -**

• **ANTIVIRUS, F-Secure.** Finlandia, Mikko Hipponen e la società di sicurezza produttrice di antivirus F-Secure →**I09155 -**

• **APPLE, paradisi fiscali: società off-shore a Jersey.** *Paradise Papers* (paradisi fiscali), Apple: costituzione di società off-shore sul territorio dell'isola di Jersey (Apple Operations International e Apple Sales International) →**I09156 -**

• **ARABIA SAUDITA, siti web: attacchi a Hizbullah.** I siti web sauditi fanno eco all'odio anti-Hizbullah →**I09157 -**

• **ARENA DIGITALE GLOBALE.** ***Arena digitale e politica internazionale: una chiave interpretativa.*** Arena digitale globale (ADG); Explorations in Cyber International Relations (ECIR); Usa, ADG: mantenimento di una posizione egemonica nei primi venti anni di esistenza; *anarchia strutturale* e *interdipendenza complessa*, concetti solitamente contrapposti. I PILASTRI DELL'ADG: IL PRIMO "STRATO" DEL CYBERSPAZIO: backbones ed exchange points: cavi ottici, antenne e satelliti; mappatura del primo strato del cyberspazio (fonte CNN, 16 luglio 2012) **(immagine)**; ADG, pilastri fondanti del sistema (i tre elementi che rendono possibili le interconnessioni globali): cavi ottici (sottomarini e terrestri), antenne della telefonia cellulare, satelliti orbitanti nello spazio; AT&T, upstream internet provider; internet service provider (ISPs), definizione di; collegamenti: sistemi sottomarini oceanici intercontinentali; geography submerine cable map; telegeography's free interactive submarine cable map; geography submarine cable map **(immagine)**; telegeography's free interactive submarine cable map **(immagine)**; informazioni, sistema di trasmissione di informazioni; asimmetrie di potere all'interno dell'arena digitale, concetto di; cyberspazio, fondamenti logici: dalla *low* alla *high* politics; CONFIGURAZIONE ANARCHICA DELL'ADG: IL PREDOMINIO AMERICANO: i modelli ICANN e Verisign, la *primacy* Usa nella gestione nella gestione di tutti gli indirizzi IP e del web; ICANN, società di gestione di tutti gli indirizzi IP (Internet Assigned Numbers Authority); DARPA (Defense Advanced Research Projects Agency), iniziale gestione per conto del Governo Usa delle funzioni anagrafiche di internet (indirizzi IP); Russia, Valdimir Putin: polemica sul monopolio Usa (ICANN) nel *domaine name system*; Internet, opposizione Usa al controllo internazionale sulla rete; ITR (International Telecommunications Regulations), Trattato: conferenza di Dubai del 3

dicembre 2012; web, spazio pubblico di internet: la parte *emersa* dell'universo digitale; Verisign, azienda americane gestrice del *domain name service-registry* per oltre la metà dei siti internet di tutto il mondo e, inoltre, di quelli riconducibili all'amministrazione Usa (.gov); W3C (consorzio); Tim Lee Berners, fondatore del web; ERCIM (European Research Consortium for Informatics and Mathematics), organismo con sede ad Antopolis (Francia); W3C members around the world **(immagine)**; top 20 web hosting countries **(immagine)**; ADG, assenza di governance globale; Joseph Nye, definizione di «cyberspazio»; controllo di internet: la struttura anarchica dell'arena digitale globale non ha prodotto una diffusione del potere, ma una solida gerarchia di fatto; l'ADG non è il paradiso dell'eguaglianza: la posizione "conservativa" degli attori egemoni; imprinting, teoria dell'organizzazione e influenza del modello originario: il condizionamento dello sviluppo. EVOLUZIONE DELLA STRUTTURA DELL'ADG: I FATTORI DEL MUTAMENTO: fattori esogeni ed endogeni all'ADG; multipolarità, tendenza verso di essa ed effetti prodotti sugli equilibri nell'arena digitale; finanza, crisi finanziaria: la "bolla" dot.com esplosa nel 2001 negli Usa; digitale, grandi infrastrutture: blocco degli investimenti; André Blum, giornalista della testata "Wired"; comunicazioni, collegamenti sottomarini: la relazione transpacifica, il Pacific Crossing-I Cable; comunicazioni, collegamenti sottomarini transpacifici: 7+4 sistemi di cavi in fibre ottiche; sistemi di cavi sottomarini che attraversano l'oceano **(immagine)**; progetto per nuovi sistemi di cavi sottomarini **(immagine)**; Submarine Telecoms Industry Report, rapporto frutto dell'analisi in profondità del complesso degli aspetti dell'industria e del mercato dei "cable" sottomarini; NTT Group, colosso pubblico-privato giapponese del settore delle comunicazioni; Artico, reti e stazioni tlc (telecomunicazioni): la dura competizione tra gli Usa, Canada e Russia; canale di Suez, "collo di bottiglia" più pericoloso e incerto dei sistemi di interconnessione globale; Usa, interessi strategici nazionali nel settore delle telecomunicazioni: *sovraesposizione* e approccio "liberal" all'interconnettività digitale; Cina Popolare, Huawei Technologies Co. Ltd, secondo produttore mondiale di componentistica per telecomunicazioni: minacce portate alla sicurezza nazionale degli Usa; Usa, *Cybersecurity Act of 2012:* progetto di legge relativo alla sicurezza digitale; Chuck Hagel, Segretario alla Difesa Usa; Martin E. Dempsey, generale statunitense; John D. Rockefeller IV, senatore statunitense; i *multiple linkage* di Nye e Kehoane e la tendenza "anarchica" di Waltz; interconnessioni: interdipendenze settoriali e interdipendenze in materia di sicurezza; dinamiche future del cyberspazio: mutua deterrenza e sistema di relazioni tra *megafortezze* digitali; Cina Popolare, cybersecurity: riforma della legge per la salvaguardia del segreto di stato (2010); "balcanizzazione" di internet e declino degli Usa nella veste di potenza egemone all'interno

dell'arena digitale globale (ADG); Usa, fine della *primacy* internazionale nel settore delle telecomunicazioni digitali; Usa, criticità: l'eccesso di interdipendenza; il primo ventennio di esistenza dell'arena digitale globale (ADG); cyberspazio: primo *strato* (o *livello*), gruppi ristretti di imprese del settore delle telecomunicazioni e di governi nazionali; Cina Popolare, egemonia nel cyberspazio: la politica del presidente della Repubblica Hu Jintao; Hillary Clinton, Segretario di Stato Usa: egemonia nel cyberspazio, furti cinesi di tecnologie e incursioni digitali; Cina Popolare, rapporti con gli Usa: la For Us-China Economica and Security Review Commission; lettera del generale Dempsey al senatore John D. Rockefeller IV →**I09157/1 -**

• **ARMI A ENERGIA DIRETTA. *Le armi cibernetiche.*** Cyberweapons (armi cibernetiche), non univocità e condivisibilità del significato del termine; arma, definizione di; Armi a energia diretta: attacchi elettromagnetici nello spazio cibernetico; Difesa, ambiente cibernetico e argomenti associati: computer network operation, cyber-defense, cyberweapons, eccetera →**I09158 -**

• **ARMI A ENERGIA DIRETTA, interferenze sistemi avversari: progetto "Champ".** Armi a energia diretta (EMP), interferenza, danneggiamento e distruzione dei sistemi elettronici dell'avversario: il progetto CHAMP sviluppato dall'USAF Research Laboratory →**I09159 -**

• **ARPANET.** Arpanet (1968) e World Wide Web (www) →**I09160 -**

• **ASIMMETRIC WARFARE, tecnologie informatiche: attacco alla rete.** *Asimmetric Warfare* (guerra asimmetrica), impiego di tecnologie informatiche ai fini di un attacco alla rete che consenta il conseguimento dell'obiettivo di colpire le infrastrutture critiche dell'avversario →**I09161 -**

• **AUTOAPPRENDENTI (macchine).** Macchine *autoapprendenti* →**I09162 -**

• **AUTOSTRADA DELL'INFORMAZIONE.** Autostrada dell'informazione →**I09163 -**

• **BANCHE DATI, indici.** Banche dati: indici →**I09164 -**

• **BIAGINI FOLCO. *Information Warfare 2012.*** *Information Warfare 2012: armi cibernetiche e processo decisionale*, indirizzo di saluto di Folco Biagini →**I09165 -**

• **BIG DATA, definizione di.** Big data, analisi di grandi quantità di dati: definizione del termine →**I09166 -**

• **BIG DATA, Francia: investimenti settore militare (2019-25).** Difesa francese, legge di programmazione militare per il quinquennio 2019-2025: il ministro

Florence Parly annuncia ingenti stanziamenti per finanziare il piano per l'innovazione che vede al cento la ricerca sull'intelligenza artificiale (IA) e i big data →**I09166/1 -**

• **BLOGSPHERA, informazioni in rete: trattamento.** Intelligence economica, trattamento delle informazioni ricavate dalla rete (blogsphera) →**I09167 -**

• **BLOGSPHERA, social networking analysis.** Social networking analysis (SNA), branca di studio delle relazioni sociali che prende in esame il particolare genere di network noto come *blogsphera* →**I09168 -**

• **BOLOGNA KDD CENTER.** Bologna KDD Center (BKC95) e società Temis SA (TE00), analisi di intelligence: estrazione di informazioni da grandi raccolte di documenti e funzioni di ricerca →**I09169 -**

• **BONIFICA →(RINVIO) al riguardo vedere la medesima voce nella scheda "COMUNICAZIONI/INTERCETTAZIONI";**

• **BOTNET.** PC (personal computer), *flash mob* e collegamento a una *botnet* →**I09170 -**

• **BOTNET,** *Botnet*, reti di computer infettati da virus e resi schiavi →**I09171 -**

• **BRUTE FORCE.** *Bruteforce* e *buffer overflow*, concetti pionieristici di distribuzione dei *malware* nella rete Internet →**I09172 -**

• **BUFFER OVERFLOW.** *Bruteforce* e *buffer overflow*, concetti pionieristici di distribuzione dei *malware* nella rete Internet →**I09173 -**

• **C4I (e Internet).** Internet come alternativa al sistema C4I (Comando, Controllo, Comunicazioni, Computers e Intelligence) →**I09174 -**

• **CAIN (programma).** Intelligence informatica, CAIN: programma che consente di rilevare e tracciare utenze e password utilizzate in rete senza protezione →**I09175 -**

• **CARNIVORE, programma FBI.** Federal Bureau of Investigation (FBI), programma *Carnivore* →**I09176 -**

• **CERF VINTON G..** Vinton G. Cerf, vero "padre" di Internet →**I09177 -**

• **CERT.** CERT (Computer Emergency Response Team), gestione delle problematiche della sicurezza: funzioni svolte →**I09178 -**

• **CIBERNETICO (spazio) →(RINVIO) al riguardo vedere le schede "AMBIENTE TELEMATICO" e "CYBERSPAZIO" in questa stessa cartella;**

• **CIRCE, intercettazioni telefoniche rete mobile: gestione.** Sistema *Radar*, piattaforma informatica dedicata al supporto anti-frode; infrastruttura *Circe*, strumento per la gestione delle intercettazioni telefoniche effettuate su rete mobile →**I09179 -**

• **CNO.** Computer Network Operation (CNO) →**I09180 -** 76/69 e s..

• **COLLABORATIVE FILTERING.** *Collaborative filtering*: selettori *Amazon* e *Copernic* →**I09181 -**

• **CONTROLLO DELLA RETE, Narus: realizzazione apparati.** Narus, realizzazione di apparati di controllo della rete →**I09182 -**

• **CONTROSPIONAGGIO INDUSTRIALE, settore informatico privato.** Sicurezza del mantenimento e della trasmissione delle informazioni sensibili, collaborazione servizi segreti con il settore informatico privato: il controspionaggio industriale effettuato a favore di imprese private che assumono una valenza pubblica →**I09183 -**

• **CRACKABILITÀ, sistemi informatici.** *Crackabilità* degli odierni sistemi informatici →**I09183/1 -**

• **CRACKER, definizione.** Definizione di *cracker* →**I09184 -**

• **CRIMINI INFORMATICI, computer crime.** Computer crime, insieme di crimini informatici connessi mediante l'ausilio di sistemi informatici: accesso abusivo a sistemi informatici; illecita intercettazione di comunicazioni telematiche; predisposizione di apparecchiature idonee all'intercettazione →**I09185 -**

• **CRIMINI INFORMATICI, FBI: Cybercrime Division.** FBI, Crimini informatici: Cybercrime Division →**I09186 -**

• **CRIMINI INFORMATICI.** *Cybercrime* →**I09187 -**

• **CRYPTOVIROLOGY.** Crittografia, *Criptovirology*: tecniche avanzate di crittografia utilizzate per evitare la "detection" oppure per fornire una *Data Theft Deniability* →**I09188 -**

• **CRITICITÀ →(RINVIO), al riguardo vedere anche le voci "INFRASTRUTTURE CRITICHE" e "SICUREZZA INFORMATICA" in questa stessa scheda;**

• **CRITTOGRAFIA, cifratura →(RINVIO), al riguardo vedere anche la scheda: "INTELLIGENCE/Comunicazioni e intercettazioni" alla voce medesima;**

• **CYBERCIVILTÀ.** Cyberciviltà →**I09189 -**

• **<u>CYBERSPAZIO</u>, asimmetrie.** Era del *Cyberspazio*: relazioni asimmetriche diffuse; asimmetria e anonimato, elementi strutturali della realtà politico-strategica dello spazio cibernetico: vantaggio dell'attaccante rispetto al difensore →**I09190 -**

• **<u>CYBERSPAZIO</u>, definizione.** Definizione di *cyberspazio* →**I09191 -**

• **<u>CYBERSPAZIO</u>, cyberwar: nuovo dominio delle operazioni militari.** *Cyberwarfare*: *cyberspace* (spazio cibernetico) come nuovo dominio delle operazioni militari: dalla protezione delle reti alla pianificazione e alla esecuzione delle operazioni →**I09192 -**

• **<u>CYBERSPAZIO</u>, spazio politico virtuale e formazione del consenso.** Spazio (cibernetico) politico *virtuale*, effetti generati dalle sue dinamiche: formazione e gestione (a livello globale e/o locale) del consenso delle opinioni pubbliche nella rete →**I09193 -**

• **<u>CYBERSPAZIO</u>, trasformazioni strutturali causate dalla fine della società westfaliana.** Fine della società westfaliana: evidenti trasformazioni strutturali della realtà politico-strategica dello spazio cibernetico e mutamento dei "soggetti d'interesse" →**I09194 -**

• **<u>CYBERSPAZIO</u>.** Cybersecurity →**I09195 -**

• **<u>CYBERTERRORISMO</u> (e Information Warfare), difesa delle infrastrutture critiche.** ***Difesa delle "infrastrutture critiche" dell'economia nazionale e tutela della privacy: il problema del controllo governativo sulle tecnologie crittografiche.*** INTERNET E SICUREZZA: *Arpanet* e ridondanza dei nodi paritetici; 1995, diffusione delle tecnologie di Internet nel mercato civile (settori B2C - *Business to consumer* e B2B - *Business to Business*); CYBERSPAZIO E CRIMINALITÀ ORGANIZZATA: crimini contro la riservatezza, l'integrità e la disponibilità di sistemi e dati; crimini legati alla contraffazione di dati; crimini relativi al contenuto dei sistemi; violazioni del copyright; IL MITO DEGLI HACKERS: ridotto numero di comunicazioni di avvenute violazioni da parte di hacker comunicate alle Autorità da parte di società private; pericolosa amplificazione del fenomeno; CYBERTERRORISMO: Usama bin Laden e al-Qa'eda in generale; Usa, ipotesi di attacco strategico di guerra informatica; strumenti di cyberattack (bombe logiche, trojan horses, worms, virus, sniffers, denial of service, eccetera); Usa, Presidential Decision Directive 63 (classificazione in diverse categorie delle minacce provenienti dalla cyberdimensione); STRUMENTI DI DIFESA E TECNOLOGIE ANTI-INTRUSIONE: password e certificati digitali; algoritmi della crittografia a chiave pubblica; firewall e *Intrusion Detection*; analisi semantica; cracking (delle password), test

di; antivirus; hoaxes (virus mai esistiti e con potenzialità distruttive irrealizzabili) ed effetto spamming nella rete; VPN (Virtual Private Network); CRITTOGRAFIA: definizione, scopi e applicazione; crittanalisi; cifratura *one-time* pad (sicura); crittogafia, tecniche crittografiche e concetti alla loro base che le definiscono: *confusione* e *diffusione*; crittografia, principio base (principio di Kerkhoff); cifratura, due tipologie esistenti: cifratura a chiave simmetrica e cifratura a chiave asimmetrica; CRITTANALISI, TECNICHE CRITTANALITICHE: lunghezza della chiave di cifratura e robustezza di un sistema; INFRASTRUTTURE CRITICHE: Usa, NIPC (National Infrastructure Protection Center); Usa, CERT (Computer Emergency Response Team); CRITTOGRAFIA E PRIVACY: algoritmi crittografici; sistemi tipo Key Recovery; ECHELON: filtraggio delle comunicazioni mediante l'impiego di tecniche di tipo semantico o basate su parole chiave; CARNIVORE (FBI): network analyzer o *sniffer* installato in ambiente Microsoft Windows →**I09196 -**

• **<u>CYBERTERRORISMO</u> (e Information Warfare), difesa delle infrastrutture critiche.** ***La protezione dei sistemi tecnologici d'intelligence e le nuove minacce transnazionali: il ruolo dell'industria strategica nazionale ed europea.*** Elsag, gruppo Finmeccanica: azienda operante nel settore dell'Information Communication Technology (ICT) (289); ICT e intelligence: dipendenza crescente (289); informazioni, integrazione e connettività totale: il concetto di *All to All* (290 e s.); business intelligence (290); *data driven management* (291); informazione: transizione da un sistema compartimentato a uno in rete (291); informazione in rete, principali minacce ala sicurezza: direzioni di provenienza (291 e s.); Richard Feynmann, ex hacker divenuto in seguito premio Nobel per la fisica (292); hackers: livello di pericolosità (292); *the human factor* (292, 293, 295); criminalità organizzata e spionaggio in rete: gli obiettivi (292); terrorismo internazionale (292); altri soggetti (292); principali difese (292); firewalls e loro punti deboli (293); crittografia e sue vulnerabilità (294); *attacco distribuito* (alla crittografia) (294); Trojan (294); Active Network Monitoring (294); analisi dei *logfiles* (295); industria strategica (295); miniaturizzazione dei circuiti integrati: legge di Moore (296); calcolatore quantistico (296 e s.); crittografia: algoritmo RSA (attualmente dominante) (297); *bit* di informazione (297) →**I09197 -**

• **<u>CYBERTERRORISMO</u>, definizione.** *Cyberterrorismo*, atti di terrorismo cibernetico: definizione di →**I09198 -**

• **<u>CYBERTERRORISMO</u>, prevenzione: Usa, National Infrastructure Protection.** National Infrastructure Protection, prevenzione del *cyberterrorismo* →**I09199 -**

• **CYBERTERRORISMO, vulnerabilità società post-moderne.** *Cyberterrorismo* e vulnerabilità delle società post-moderne: scarsa privacy nella società digitale; delinquenti elettronici, più pronti a usare il sistema che a distruggerlo →**I09200 -**

• **CYBERTERRORISMO.** *Cyberterrorismo* →**I09201 -**

• **CYBERTERRORISMO.** *Cyberterrorismo*: Internet e reti di computer →**I09202 -**

• **CYBERTERRORISMO.** ***Nuove forme di guerra.*** Nuove forme di guerra, *information warfare* e nuove minacce: *cyberterrorismo* e *cyber-crimes* →**I09203 -**

• **CYBERWAR, cyber-attack e cyber-security, infowar.** *Cyberwar*, *cyberattack* e *cybersecurity*; lo spionaggio elettronico: i casi Echelon e Google; l'*infowar* e le "nuove" dimensioni della potenza; l'*infowar* come *political economic warfare* →**I09204 -**

• **CYBERWAR, cyber-security: Selex ES.** *Cyberwar*, *cybersecurity*: Finmeccanica, Selex ES, attività svolte nel settore della sicurezza informatica (cybersecurity) →**I09205 -**

• **CYBERWAR, cyber-attack e ritorsioni: "linea rossa".** *Cyberwar*, *cyberattack* ed eventuali ritorsioni a essi: la ricerca di regole internazionali che definiscano un "linea rossa" oltrepassata la quale vengono previste sanzioni in quanto l'attacco informatico viene considerato alla stregua di un atto di violenza internazionale →**I09206 -**

• **CYBERWAR, cyber-attack: denial-of-service-attack.** *Cyberwar*, *cyber-attack*: il *denial-of-service-attack* →**I09207 -**

• **CYBERWAR, cyber-attack: Usa, piani anti-Iraq.** *Cyberwar*, Usa: piani elaborati al Pentagono relativi ad azioni di attacco informatico nei settori economico e finanziario volti a bloccare i fondi depositati all'estero da emissari dell'Iraq di Saddam →**I09208 -**

• **CYBERWAR, cyber-space e cyber-warfare.** *Cyberspace* e *cyberwarfare* (spazio cibernetico) →**I09209 -**

• **CYBERWAR, cyber-space: nuovo dominio delle operazioni militari.** *Cyberwarfare*: *cyberspace* (spazio cibernetico) come nuovo dominio delle operazioni militari: dalla protezione delle reti alla pianificazione e alla esecuzione delle operazioni →**I09210 -**

• **CYBERWAR, definizione.** *Cyberwar*, definizione →**I09211 -**

• **CYBERWAR, deterrenza.** *Cyberwar*: può esistere una deterrenza cibernetica? sicurezza di tipo *reattivo*: concetti di "deterrenza" e di "ritorsione" →**I09212 -**

• **CYBERWAR, deterrenza: cumulative deterrence (Almog).** *Cumulative deterrence and war on terrorism* (D. Almog) →**I09213 -**

• **CYBERWAR, difese.** *Cyberwar*, difese dai *cyber-attack* →**I09214 -**

• **CYBERWAR, difese: Cina popolare, VII Dipartimento PLA.** *Cyberwar*, difese dai *cyber-attack*: Cina popolare, competenze attribuite al VII Dipartimento dello stato maggiore dell'Armata popolare di liberazione (PLA) →**I09215 -**

• **CYBERWAR, guerra illimitata.** *Cyberwar*, "era della guerra": il conflitto diviene *perenne* (concetto di "guerra illimitata") →**I09216 -**

• **CYBERWAR, hard (aspetti).** *Cyberwar*, aspetti "hard" e controllo cibernetico del trattamento numerico della realtà →**I09217 -**

• **CYBERWAR, hot cyberwar.** *Hot cyberwar* e *cyber guerra fredda* →**I09218 -**

• **CYBERWAR, penetration tester.** *Cyberwar*, *penetration tester* acquisito dall'esterno →**I09219 -**

• **CYBERWAR, potenza: diffusione e concentrazione.** Cyberwar: fenomeni della diffusione della Potenza e della concentrazione della potenza →**I09220 -**

• **CYBERWAR, spionaggio: Cina popolare, Huawei e ZTE.** Cina popolare, Huawei e ZTE, colossi cinesi del settore delle telecomunicazioni: accuse formulate dagli Usa relative ad attività di spionaggio e di vendita in America di apparati di rete viziati da *backdoors* →**I09221 -**

• **CYBERWAR, spionaggio: Cina popolare, infezione di hardware esportati negli Usa.** Hardware, infezioni dei microchips assemblati negli stabilimenti industriali della Cina Popolare e successivamente inseriti nei computer prodotti da Intel, Motorola e Texas Instruments, e in uso presso il Pentagono per la gestione di sofisticati sistemi d'arma →**I09221/1 -**

• **CYBERWAR.** ***La guerra cibernetica.*** Guerra cibernetica: *Cyberwar* e armi cibernetiche; riflessioni sulla dottrina di impiego della *cyberwar* e mutamenti nelle teorie della guerra; mutamenti nella dottrina di impiego della *cyberwar*: teorie e codifiche della guerra, dubbi al riguardo; deterrenza: *cyber-deterrenza* →**I09222 -**

• **CYBERWEAPONS, beacon.** Armi cibernetiche, *beacon* (faro): virus impiegato dagli americani allo scopo di raccogliere informazioni sul programma nucleare iraniano →**I09223 -**

• **CYBERWEAPONS, caratteristiche e aumento della precisione.** *Cyberweapons* (armi cibernetiche), caratteristiche e aumento della loro precisione →**I09224 -**

• **CYBERWEAPONS, caratteristiche e aumento della precisione. (tabella)** Aumento della precisione dei danni procurati dalle armi cibernetiche →**I09225 -**

• **CYBERWEAPONS, caratteristiche e possessori: ambiguo concetto.** *Cyberweapons* (armi cibernetiche), caratteristiche peculiari e soggetti che se ne stanno dotando sia nel campo del lecito che dell'illecito; l'ambiguo concetto di *cyberweapons*; *malware*, digital profiling, caratteristiche delle armi cibernetiche, vita operativa estremamente breve delle armi cibernetiche, C4 ISTAR (Command, Control, Communications, Computers, Intelligence, Surveillance, Target Acquisition, Reconnaissance) →**I09226 -**

• **CYBERWEAPONS, contrasto della minaccia.** *Cyberweapons* (armi cibernetiche), contrasto e contenimento a livello globale: una sfida strategica; minacce multidimensionali e interdipendenti, filosofie di contrasto: maggiore integrazione tra i vari apparati governativi interessati e rafforzamento del coordinamento interministeriale →**I09227 -**

• **CYBERWEAPONS, definizione di.** Cyber weapon (arma cibernetica), definizione e concetto →**I09227/1 -**

• **CYBERWEAPONS, Doku e Stuxnet.** Cyberweapons (armi cibernetiche), Doku e Stuxnet (malware) →**I09228 -**

• **CYBERWEAPONS, Stuxnet.** Cyberweapons (armi cibernetiche), virus (*worm*) "the bug" (Stuxnet): sviluppo a opera dell'Unità 8200 dell'intelligence israeliana in collaborazione con la NSA statunitense in vista di un attacco cibernetico alla centrale nucleare iraniana di Natanz; effetti distruttivi arrecati dal virus *stuxnet* →**I09229 -**

• **CYBERWEAPONS, "Zeus".** Cyberweapons (armi cibernetiche), *Zeus*: prima arma cibernetica a prevedere una diffusione selettiva e l'utilizzo di un sistema C2 (comando e controllo) per l'attivazione dell'arma e la ricezione di ordini sui compiti da eseguire →**I09230 -**

• **CYBERWEAPONS, analisi tecnologica.** ***L'analisi tecnologica delle cyberweapons per lo sviluppo della cyber-resilience.*** L'analisi tecnologica delle *cyberweapons* per lo sviluppo della *cyber-resilience* →**I09231 -**

• **CYBERWEAPONS, relazioni internazionali e sicurezza globale.** ***Le ripercussioni delle armi cibernetiche sulle relazioni internazionali e sulla sicurezza globale.*** Era cibernetica: linee di tendenza che caratterizzano le relazioni internazionali: *cyberweapons* (armi cibernetiche), fattori potenzialmente destabilizzanti dei rapporti strategici fra stati →**I09232 -**

• **CYBERWEAPONS, sviluppo: approcci tecnologici.** ***Lo sviluppo delle armi cibernetiche: un approccio organico agli aspetti tecnologici.*** Armi cibernetiche (*cyberweapons*), sviluppo: un approccio organico agli aspetti tecnologici →**I09233 -**

• **CYBERWEAPONS.** ***Le armi cibernetiche.*** *Cyberweapons* (armi cibernetiche), non univocità e condivisibilità del significato del termine; arma, definizione di; Armi a energia diretta: attacchi elettromagnetici nello spazio cibernetico; Difesa, ambiente cibernetico e argomenti associati: *computer network operation*, *cyber-defense*, *cyberweapons*, eccetera →**I09234 -**

• **CYBERWEAPONS.** ***Riflessione da parte del costruttore di sistemi militari complessi.*** *Cyberweapons* (armi cibernetiche), riflessioni da parte del costruttore di sistemi militari complessi →**I09235 -**

• **DARPA, Amber: ricognitore senza pilota.** DARPA (Defense Advanced Research Projects Agency), agenzia dipendente dal Dipartimento della Difesa Usa (DoD): Amber, prototipo di ricognitore senza pilota a grande autonomia →**I09236 -**

• **DARPA, cyber-attack: difese automatizzate.** DARPA (Defence Advanced Research Project Agency), cyber-attack "unmanned": sistemi difensivi automatizzati →**I09237 -**

• **DARPA, prodotti.** DARPA (Defense Advanced research Project Agency), prodotti: tecniche *filtering & routing*, "Topic", "taiga", "Noemic", "Madicia" →**I09238 -**

• **DARPA.** DARPA (Defense Advanced Research Project Agency), gli inventori di Internet →**I09239 -**

• **DATAGATE →(RINVIO) al riguardo vedere la specifica scheda;**

• **DDOS.** DDOS (Distributed Denial of Service), tipologia di attacco informatico: interruzione del servizio mediante meccanismi di saturazione →**I09240 -**

• **DECRETO PISANU.** Giuseppe (“Beppe”) Pisanu, decreto Pisanu →**I09241 -**

• **DEFCON.** *Defcon*, importante evento underground informatico →**I09242 -**

• **DEFEACEMENT, vandalismo informatico.** Defeacement (*defacement*, “defacciamento”), attività di vandalismo informatico avente quale obiettivo la deturpazione o la sostituzione della pagine iniziale di un sito web mediante l’inserimento in essa di messaggi propagandistici o derisori; illecita sostituzione della home page di un sito web →**I09243 -**

• **DISCLAIMER.** Disclaimer →**I09244 -**

• **DOMINI, standard dei domini.** *Domìni*, standard: terra, mare, aria, spazio →**I09245 -**

• **ECHELON →(RINVIO) al riguardo vedere anche la scheda “NSA”;**

• **ECHELON, monitoraggio comunicazioni WiFi.** CIA e NSA, ECHELON e mappatura delle comunicazioni WiFi effettuata da Google →**I09246 -**

• **ECHELON, US Navy Intelligence: SIGINT, NAVSECGRU (Naval security Group Command).** US Navy, ECHELON: Naval security Group Command →**I09247 -**

• **ECHELON, US Navy Intelligence: SIGINT.** US Navy Intelligence, ECHELON: ruolo svolto dalla Marina degli USA →**I09248 -**

• **ECHELON, US Navy Intelligence: SIGINT: NAVSECGRU (Naval security Group Command).** US Navy, ECHELON: Naval security Group Command, attività svolte in Italia nella base di Napoli →**I09249 -**

• **ECHELON.** Il sistema ECHELON →**I09250 -**

• **E-COMMERCE, crescita fatturato (2014).** E-Commerce, crescita del fatturato e sottrazione di notevoli quote di mercato alle vendite nei format tradizionali →**I09251 -**

• **EDGE.** Informatica, EDGE: tecnologia di collegamento iperveloce a Internet →**I09252 -**

• **EFF.** Electronic Frontier Foundation (EFF), organizzazione che sostiene e promuove la libertà sul web →**I09253 -**

• **ELECTRONIC WARFARE, info-spam: conflitto NATO-Jugoslavia 1999.** Jugoslavia, guerra del 1999*: Electronic warfare*, azioni di *Info-spam* dell’intelligence di Belgrado contro la rete informatica Usa →**I09254 -**

• **ELECTRONIC WARFARE, cyberwar.** ***La guerra elettronica nella quinta dimensione.*** La guerra elettronica nella quinta dimensione →**I09255 -**

• **ELETTRONICA, vita utile di una innovazione.** Elettronica, tempi medio di obsolescenza nella produzione di servizi (in rapporto a quelli della produzione industriale – settore primario) e durata della vita utile di una innovazione introdotta in questo specifico settore →**I09256 -**

• **ENCASE.** Informatica, intelligence: ENCASE, programma utilizzato nell'informatica forense per l'analisi del contenuto di dischi rigidi di computer e l'eventuale recupero di file rimossi o parzialmente danneggiati →**I09257 -**

• **ERCIM.** European Research Consortium for Informatics and Mathematics (ERCIM), organismo avente sede ad Antopolis (Francia) →**I09257/1 -**

• **ESTONIA, cyber attacchi (2007-08).** Cyber attacchi subiti dall'Estonia nell'aprile del 2007 e nel 2008; differenti tipologie di attacchi informatici subiti da Estonia e Iran →**I09258 -**

• **ETNO.** European Telecommunication National Operator (ETNO) →**I09259 -**

• **FINX, sistema operativo.** Informatica, sistema operativo FINX realizzato da Selex ES (Finmeccanica Sistemi integrati) →**I09260 -**

• **FLASH MOB.** PC, *flash mob* e collegamento a una *botnet* →**I09261 -**

• **FORMATTAZIONE, formattazione del disco rigido.** Informatica, formattazione del disco rigido di un computer →**I09262 -**

• **FTP, sistema di trasferimento file.** Informatica, Internet: FTP (File Transfert Protocol), sistema di trasferimento dei file →**I09263 -**

• GCHQ (Government Communication Headquarters) →(RINVIO) al riguardo vedere la scheda "GRAN BRETAGNA/INTELLIGENCE";

• **GEORGIA, cyber attacchi (2008).** Cyber attacchi subiti dalla Georgia nel 2008 →**I09264 -**

• GHIONI FABIO →(RINVIO) al riguardo vedere anche la specifica scheda;

• **GHIONI FABIO.** Fabio Ghioni →**I09265 -**

• **GIUSTIZIA, indagini: informatica e telefonia.** Informatica e telefonia, nuovi terreni di indagine fino al 2002 "snobbati" dagli investigatori nel corso delle inchieste: la decretazione in materia di collaborazione con gli inquirenti da

parte dei gestori telefonici, decreti legislativi nnº 70/2003 e 196/2003 (revisione della *legge sulla privacy*) →**I09266 -**

• **GLOBALIS, sito internet.** *Globalis*, sito internet di analisi dei trend mondiali nell'era della globalizzazione (Stephan Richter, Washington) →**I09267 -**

• **GOOGLE, mappatura mondiale comunicazioni.** Google, mappatura mondiale di tutte le comunicazione mobili →**I09268 -**

• **GOOGLE, motore di ricerca: principale strumento OSINT.** OSINT, Google: motore di ricerca, principale strumento per la ricerca di informazioni su fonti aperte →**I09269 -**

• **GOOGLE, oscuramento: Cina popolare.** Cina popolare, oscuramento del motore di ricerca *Google* e conseguente crisi diplomatica con gli Usa →**I09270 -**

• **GOOGLE, tecniche di scelta.** Google, intelligence economica: tecniche di scelta →**I09271 -**

• **HACKER, attacchi informatici: "Hands on hacking", corso specialistico.** *Hands on hacking*, corso specialistico organizzato da *Zone-H* nell'ambito del quale vennero utilizzate le tecniche di attacco informatico, messe in pratica contro obiettivi simulati →**I09272 -**

• **HACKER, Black hats: definizione.** *Black hats*, hacker dotato di grandi capacità in campo tecnico ma animato da intenti non eccessivamente limpidi →**I09273 -**

• **HACKER, definizione.** Definizione di *hacker*, *cracker* e di *lamer* →**I09274 -**

• **HACKER, ethical hacking: definizione.** Definizione del termine *ethical hacking* nella sua accezione primigenia →**I09275 -**

• **HACKER, Jargon File.** "Jargon File", *bibbia* hacker opera di Raphael Finkel ed Eric Steven Raymond →**I09276 -**

• **HACKER, psicologia individuale.** Psicologia di un hacker: casi ricorrenti di soggetti di giovane età manifestanti difficoltà nella socializzazione con le altre persone →**I09277 -**

• **HACKER, Shimomura e Mitnik.** "Hackers" e "crackers": Tsutomu Shimomura e Kevin Mitnik →**I09278 -**

• **HACKER, Telecom Italia: security, incursione nella rete informatica Vodafone.** Telecom Italia, *security*: incursione nella rete informatica di Vodafone, gestore di telefonia concorrente →**I09279 -**

• **HACKER, terminologia.** Hacker, significato originario dei termini: “black hats”, “white hats”, “grey hats” e “cracker” →**I09280 -**

• **HDSL.** Telefonia, HDSL: termine di una linea in un punto →**I09281 -**

• **HFT.** High Frequency Trading (HFT), intermediazione finanziaria ad alta frequenza: negoziazioni velocissime e intense effettuate nel corso di una giornata borsistica →**I09282 -**

• **IBM, criticità: DGSE francese, spionaggio industriale a danno dell’azienda.** DGSE (Direction Générale de la Securité Extérieure), effettuazione di operazioni di intelligence (spionaggio industriale/Intelligence Competitiva) ai danni di importanti società americane (IBM, Texas Instruments) per conto di società francesi concorrenti →**I09283 -** 83/387.

• **IBM, intelligence economica: valutazioni di mercato.** IBM, valutazioni relative al mercato potenziale nel settore dell’intelligence economica (BIS) per gli anni 2000 →**I09284 -**

• **ICT, Psyops: decisori politici e opinioni pubbliche.** Condizionamento dei responsabili politici di uno stato e delle opinioni pubbliche interne, nuove frontiere scientifiche e tecnologiche: i progressi registrati nei settori dell’information technology (ICT), delle neuroscienze e nella semiotica →**I09285 -**

• **IKON, sonda per intercettazioni (progetto).** Fabio Ghioni, *Ikon*: progetto di sonda per intercettazioni destinata all’utilizzo da parte dell’Autorità giudiziaria sviluppato nei primi anni Duemila; Roberto Preatoni, uomo di fiducia di Fabio Ghioni nell’ambito del progetto →**I09286 -**

• **INFORMATICA, automazione: sviluppi anni ‘70 e ‘80.** Informatica e automazione dei vari settori produttivi avvenuta negli anni Settanta e Ottanta →**I09287 -**

• **INFORMATICA, computer: capacità dei dischi rigidi (memoria).** Informatica, computer: *terabyte* e *gigabyte*, volume di capienza dei dischi rigidi delle macchine →**I09288 -**

• **INFORMATICA, computer: personal computer, Commodore 64.** Personal computer: il *Commodore 64* →**I09289 -**

• **INFORMATICA, computer: potenze di calcolo e rete cooperativa di macchine.** Informatica, computer: potenze elevate di calcolo gestibili soltanto mediante una rete cooperativa di macchine →**I09290 -**

• **INFORMATICA, personale tecnico: ricorrenti atteggiamenti caratteriali.** Informatica, personale tecnico e addetti, atteggiamenti caratteriali frequentemente riscontrati: comportamento improntato alla presunzione e al distacco →**I09291 -**

• **INFORMATICA, programmazione: linguaggi, VB Script.** Informatica, linguaggi di programmazione: VB *Script* (Visual basic scripting edition) →**I09292 -**

• **INFORMATICA, rivoluzione informatica: tendenza all'intangibilità.** *Rivoluzione informatica*: totale alterazione della natura del tempo, dello spazio e della distanza nelle interazioni moderne; la tendenza all'*intangibilità* →**I09293 -**

• **INFORMATION OVERLOAD, superamento del problema.** Information warfare, *data mining* e *text mining*: superamento del problema costituito dall'*information overload* →**I09294 -**

• **INFORMATION SHARING.** Information Sharing →**I09295 -** 76/53.

• **INFORMATION STRYKE, difficoltà.** *Information warfare*, *Information strike*: difficoltà alla base →**I09296 -**

• **INFORMATION TECHNOLOGY, sviluppi.** Information Technology (IT), sviluppi →**I09297 -**

• **INFORMATION TECHNOLOGY, Usa: delocalizzazione Usa in India.** Information Technology (IT), Usa: delocalizzazione delle imprese in India e crescita del settore (2008-15) →**I09298 -**

• **INFORMATION WARFARE (e WMD), nuove minacce terroristiche.** Terrorismo, nuove minacce: armi di distruzione di massa (WMD) e Information Warfare →**I09299 -**

• **INFORMATION WARFARE e terrorismo.** Terrorismo e Information Warfare →**I09300 -**

• **INFORMATION WARFARE, "Total Warfare" e "Digital Warfare".** *Total Warfare* (guerra totale) e *Digital Warfare* (guerra digitale) →**I09301 -**

• **INFORMATION WARFARE, attacchi "casuali".** *Information warfare*, attacchi sulla Rete: attacchi cosiddetti "casuali" (non collegati) e collegamenti tra *agenti* →**I09302 -**

• **INFORMATION WARFARE, attacchi informatici →(RINVIO) al riguardo vedere la voce "CYBERWAR" all'interno di questa stessa scheda;**

• **<u>INFORMATION WARFARE</u>, attacchi informatici.** *Information warfare*, attacchi informatici: attacco cibernetico oppure *cyberwar*? →**I09303 -**

• **<u>INFORMATION WARFARE</u>, attacchi informatici a sistemi bancari.** Attacchi informatici ai sistemi bancari: attacchi alle infrastrutture di un paese, il caso di Gauss; malware Gauss, virus limitato a una ben determinata struttura (le banche) e a selettive aree geografiche ((Israele, Palestina, Libano); Kaspersky Lab; HTTPS, comunicazioni dai computer in maniera cifrata; attacchi effettuati da cybercriminali; esempi di malware: Zeus e Spyeye (Spy Eye); "banking malware" →**I09304 -**

• **<u>INFORMATION WARFARE</u>, attacchi informatici a infrastrutture finanziarie: impatti economico e organizzativo.** Attacchi alle infrastrutture finanziarie, banche e aziende attraverso l'impiego di armi cibernetiche (Cyberweapons): impatti di natura economica e organizzativa; cyber risk aziendale: danni reputazionali; CSO (Chief Security Officier); evoluzione dell'information security manager; Next Value, società indipendente del settore intelligence IT e new media; information security, % di spesa destinata alla specifica voce dalle imprese commerciali; CISO (Chief Information Security Officier); IBM, studio sulla sicurezza cibernetica aziendale (anno 2012); impatto degli attacchi informatici sul valore economico delle aziende; media, principali quotidiani Usa: fonti di notizie relative ad attacchi informatici; *information security branches*; attacchi DOS; *information security* e rischio reputazionale; *corporate reputation*; perdita reputazionale, effetti nel campo finanziario; definizione di "reputational risk"; Banca d'Italia, Circolare nº263 del 27 dicembre 2006 in materia di nuove disposizioni di vigilanza prudenziale per le banche →**I09305 -**

• **<u>INFORMATION WARFARE</u>, attacchi informatici a infrastrutture finanziarie.** ***Attacchi alle infrastrutture finanziarie attraverso armi cibernetiche.*** Attacchi alle infrastrutture finanziarie attraverso l'impiego di armi cibernetiche (Cyberweapons) →**I09306 -**

• **<u>INFORMATION WARFARE</u>, attacchi informatici: cyberweapons.** ***Cyberweapons: genesi di un attacco e impatto sui sistemi decisionali.*** *Information warfare*, attacchi informatici: *cyberweapons*, genesi di un attacco e impatto sui sistemi decisionali: *digital profiling* (profilo digitale); definizione di infrastruttura critica; teorie sui modelli decisionali applicate alle organizzazioni complesse e scopi degli attacchi informatici →**I09307 -**

• **<u>INFORMATION WARFARE</u>, attacchi informatici: APT.** Advanced Persistent Threat (APT), tipologia di attacco informatico →**I09307/1 -**

• **<u>INFORMATION WARFARE</u>, attacchi informatici: difesa, criticità, mancata percezione del rischio.** *Cyberwar*, criticità delle difese da un attacco informatico: la mancata percezione del rischio da parte della vittima (human factor) →**I09308 -**

• **<u>INFORMATION WARFARE</u>, attacchi informatici: difesa, tempi medi risoluzione del problema.** *Cyberwar*, attacchi informatici: tempi medi di risoluzione del problema da parte dell'attaccato →**I09309 -**

• **<u>INFORMATION WARFARE</u>, attacchi informatici: effetti.** *Information warfare*, attacchi informatici: alcuni effetti sul sistema "obiettivo" →**I09310 -**

• **<u>INFORMATION WARFARE</u>, attacchi informatici: evoluzione.** *Cyberwar*, evoluzione degli attacchi informatici: attacchi ai dispositivi mobili, Facebook mobile, *phishing*, C2 (comando e controllo) →**I09311 -**

• **<u>INFORMATION WARFARE</u>, attacchi informatici: fasi.** *Cyberwar*, fasi dell'attacco informatico: acquisizione di informazioni sull'obiettivo, realizzazione di un codice, fase dei test, attacco, verifica del risultato →**I09312 -**

• **<u>INFORMATION WARFARE</u>, attacchi informatici: fasi, timeline.** *Cyberwar*, *timeline* di un attacco informatico: 1-progettazione, obiettivo: cosa, dove, chi, danno digitale o fisico; 2-acquisizione informazioni sull'obiettivo designato: raccolta negli ambiti d'intelligence e in quello tecnico; 3-effettuazione, armi cibernetiche (*cyberweapons*): micidialità, infallibilità, durata, codici "malevoli" delle armi cibernetiche, intrusioni di tipo diretto, semidiretto, indiretto; 4-fase dei test; 5-attacco; 6-valutazione dei risultati →**I09313 -**

• **<u>INFORMATION WARFARE</u>, attacchi informatici: rappresaglia, proporzionalità della risposta.** *Cyberwar*, rappresaglia a un attacco cibernetico nemico: proporzionalità della risposta; sicurezza di tipo *reattivo*: concetti di "deterrenza" e di "ritorsione"; reazione a un attacco: proporzionalità (non sproporzione) della risposta anche in considerazione dei rapporti e delle relazioni internazionali →**I09314 -**

• **<u>INFORMATION WARFARE</u>, attacchi informatici: USAF, base di Creech (2011).** USAF, attacco cibernetico subito nell'ottobre 2011 dalla base di Creech (Nevada): infezione delle war room (stanze di comando) degli UCAV PREDATOR e REAPER a quel tempo operativi nei cieli dell'Afghanistan causata da un virus informatico (keylogger) →**I09314/1 -**

• **<u>INFORMATION WARFARE</u>, definizione di.** Information warfare, definizione di →**I09314/2 -**

• **<u>INFORMATION WARFARE</u>, "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; èra 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 DISSUASIONE NUCLEARE ALLA DISSUASIONE 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 ROBOTTIZZATA: 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 subìto 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 protesa 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 **→I09314/3 -**

• **<u>INFORMATION WARFARE</u>, E-jihad.** *E-jihad*, conflitto cibernetico combattuto tra israeliani e palestinesi **→I09315 -**

• **<u>INFORMATION WARFARE</u>, electronic warfare e cyber warfare.** Information warfare: categorie di *electronic warfare* e di *cyber warfare* →**I09315/1 -**

• **<u>INFORMATION WARFARE</u>, infrastrutture critiche e guerra asimmetrica.** Guerra asimmetrica e infrastrutture critiche esposte a potenziali attacchi: stime per il 2015 elaborate prima dell'undici settembre 2001 →**I09316 -**

• **<u>INFORMATION WARFARE</u>, infrastrutture critiche: difesa.** ***Difesa delle "infrastrutture critiche" dell'economia nazionale e tutela della privacy: il problema del controllo governativo sulle tecnologie crittografiche.*** INTERNET E SICUREZZA: *Arpanet* e ridondanza dei nodi paritetici; 1995, diffusione delle tecnologie di Internet nel mercato civile (settori B2C - *Business to consumer* e B2B - *Business to Business*); CYBERSPAZIO E CRIMINALITÀ ORGANIZZATA: crimini contro la riservatezza, l'integrità e la disponibilità di sistemi e dati; crimini legati alla contraffazione di dati; crimini relativi al contenuto dei sistemi; violazioni del copyright; IL MITO DEGLI HACKERS: ridotto numero di comunicazioni di avvenute violazioni da parte di hacker comunicate alle Autorità da parte di società private; pericolosa amplificazione del fenomeno; CYBERTERRORISMO: Usama bin Laden e al-Qa'eda in generale; Usa, ipotesi di attacco strategico di guerra informatica; strumenti di cyberattack (bombe logiche, trojan horses, worms, virus, sniffers, denial of service, eccetera); Usa, Presidential Decision Directive 63 (classificazione in diverse categorie delle minacce provenienti dalla cyberdimensione); STRUMENTI DI DIFESA E TECNOLOGIE ANTI-INTRUSIONE: password e certificati digitali; algoritmi della crittografia a chiave pubblica; firewall e Intrusion Detection; analisi semantica; cracking (delle password), test di; antivirus; hoaxes (virus mai esistiti e con potenzialità distruttive irrealizzabili) ed effetto spamming nella rete; VPN (Virtual Private Network); CRITTOGRAFIA: definizione, scopi e applicazione; crittanalisi; cifratura one-time pad (sicura); crittogafia, tecniche crittografiche e concetti alla loro base che le definiscono: *confusione* e *diffusione*; crittografia, principio base (principio di Kerkhoff); cifratura, due tipologie esistenti: cifratura a chiave simmetrica e cifratura a chiave asimmetrica; CRITTANALISI, TECNICHE CRITTANALITICHE: lunghezza della chiave di cifratura e robustezza di un sistema; INFRASTRUTTURE CRITICHE: Usa, NIPC (National Infrastructure Protection Center); Usa, CERT (Computer Emergency Response Team); CRITTOGRAFIA E PRIVACY: algoritmi crittografici; sistemi tipo Key Recovery; ECHELON: filtraggio delle comunicazioni mediante l'impiego di tecniche di tipo semantico o basate su parole chiave; CARNIVORE (FBI): network analyzer o *sniffer* installato in ambiente Microsoft Windows →**I09317 -**

• **<u>INFORMATION WARFARE</u>, IWC 2012 Roma.** Information Warfare Conference Rome 2012 (IWC 2012) →**I09318 -**

• **INFORMATION WARFARE, pirateria informatica e intelligence economica: turbative e contrasto dell'economia italiana.** (Intelligence economica) ingerenza economica dei servizi di intelligence dei Paesi occidentali e loro tentativi di contrasto posti in essere a danno dell'industria italiana all'estero attraverso operazioni di turbativa di mercati valutari e finanziari, oltreché atti di pirateria informatica: i contenuti delle relazioni semestrali presentate al Parlamento della Repubblica dai servizi di informazione per la sicurezza italiani →**I09319 -**

• **INFORMATION WARFARE, pirateria informatica: RFT, programma "Rahab".** Germania, servizi di intelligence federali, specializzazione nei settori delle intercettazioni telefoniche e della pirateria informatica: il programma *Rahab* sviluppato negli anni Ottanta →**I09320 -**

• **INFORMATION WARFARE, sottocategorie.** *Information warfare* (guerra dell'informazione), suddivisione in 7 sottocategorie: C2W; IBW; EW; PSYOPS; HW; E1W; CW →**I09321 -**

• **INFORMATION WARFARE, C2: Elt/950 "Loki".** C2 (Comando e Controllo), Elettronica s.p.a.: sistema Loki (Elt/950); armi cibernetiche moderne: utilizzo di server di comando e controllo →**I09322 -**

• **INFORMATION WARFARE, Usa.** Usa, controllo dello spazio e dell'*infosfera*: l'intervento Americano sulla Rete →**I09323 -**

• **INFORMATION WARFARE.** ***Nuove forme di guerra.*** Nuove forme di guerra, *information warfare* e nuove minacce: *cyberterrorismo* e *cyber-crimes* →**I09324 -**

• **INFORMATION WARFARE.** ***Nuove minacce transnazionali con mezzi non convenzionali.*** Nuove minacce transnazionali con mezzi non convenzionali: mezzi di offesa non convenzionali o *mezzi tecnici asimmetrici*; sicurezza nazionale e sovranità nazionale: mutamento costante all'interno di un processo dinamico; minacce: diffusione delle competenze tecniche ed elevata disponibilità di materiali; minacce: microvelivoli comandati a distanza con sistemi GPS e di controllo di volo automatico; sostanze che producono modifiche strutturali e aggressivi contro i materiali; minacce alle reti di fornitura; mezzi non letali e antipersona; information warfare; information warfare, Serbia: gruppo hackers *Crna Ruka*; minacce: microonde di elevata potenza impiegabili contro sistemi elettronici; minacce all'ambiente; minacce: sostanze radioattive; conflitto asimmetrico: capacità degli attori più deboli; "hardening" (irrobustimento) →**I09325 -**

• **INFORMATIZZAZIONE (e terziarizzazione).** Terziarizzazione e rivoluzione informatica nell'economia della Russia post-sovietica →**I09326 -**

• **INFOVALORIZZAZIONE.** Infovalorizzazione, effetto della diffusione delle informazioni che conduce a sinergie in grado di incrementare le capacità dei singoli: *azione collaborativa* mediante la fusione dei dati disponibili →**I09326/1 -**

• **INFOWAR, Psyops: comunicazione, manipolazione delle percezioni e dei comportamenti.** *Infowar* e comunicazione, applicazione delle nuove Information Communication Technologies (ICT): tecniche di diffusione di media audiovisivi in tempo reale a copertura globale; sviluppi di semantica, semiotica e neuroscienze; manipolazione delle percezioni dell'opinione pubblica e conseguente induzione a comportamenti voluti; manipolazione attraverso media interattivi e media tradizionali: diversi livelli di efficacia; le *dissonanze cognitive* →**I09327 -**

• **INFRASTRUTTURE CRITICHE, definizione.** Analisi *cyber-difesa*, azioni preventive: 7 quesiti alla loro base e definizione di infrastruttura critica →**I09328 -**

• **INFRASTRUTTURE CRITICHE, apparati informatici: SCADA.** SCADA (Supervisory Control and Data Acquisition), apparati informatici delle infrastrutture critiche: controllo di supervisione e acquisizione dati, la gestione e il controllo delle infrastrutture critiche →**I09329 -**

• **INFRASTRUTTURE CRITICHE, rischi: incidenti informatici.** Criticità: incidenti informatici →**I09330 -**

• **INFRASTRUTTURE CRITICHE, rischi: interruzione alimentazione elettrica.** Infrastrutture critiche collegate a complesse reti di computer, esposizione a gravi conseguenze derivanti dall'interruzione dell'erogazione di energia elettrica destinata all'alimentazione delle apparecchiature: il caso della crisi energetica in California →**I09331 -**

• **INTELLIGENCE, computer: lettura testi cancellati.** Computer, lettura di un testo precedentemente cancellato (*delete*) →**I09332 -**

• **INTELLIGENCE, era delle informazioni: maggiori volumi e velocità.** Intelligence nell'era delle informazioni, attuale situazione: disponibilità di maggiori volumi di informazioni e superiore velocità nella trasmissione dei dati →**I09333 -**

• **INTELLIGENCE, informatica e Internet.** Intelligence, rari casi di ricerca e sviluppo (culturale e tecnologico): l'informatica e Internet al servizio delle agenzie di difesa e sicurezza →**I09334 -**

• **INTELLIGENCE, informatica: terrorismo informatico.** Terrorismo informatico, "Ombre asimmetriche": libro sull'intelligence informatica scritto da Fabio Ghioni e Roberto Preatoni →**I09335 -**

• **INTELLIGENCE, intelligence tecnico-militare.** ***L'intelligence tecnico-militare.*** L'intelligence tecnico-militare →**I09336 -**

• **INTELLIGENCE, trasmissioni celate da telefax a PC (unifile).** Informatica, intelligence: impiego del telefax per l'invio di documenti a un personal computer portatile allo scopo di celare l'origine del dato (unifile) →**I09337 -**

• **INTELLIGENCE.** L'Intelligence nell'era dell'informazione →**I09338 -**..

• **INTERNET, indirizzi Internet: assegnazione.** Internet, registri per l'assegnazione degli indirizzi: *Ripe*, *Arin*, *Lacnic*, *Apnic*, *Afrinc* →**I09339 -**

• **INTRUSIONI TELEMATICHE, intercettazioni telematiche.** Informatica, intercettazione telematica: definizione della fattispecie →**I09340 -**

• **INTRUSIONI TELEMATICHE, progressi nel settore.** Nuove frontiere dell'intelligence: sviluppi nei settori delle intercettazioni telefoniche, delle decrittazioni delle comunicazioni cifrate e delle intrusioni nelle banche dati →**I09341 -**

• **INTRUSIONI TELEMATICHE, sabotaggio: riattivazioni utenze avversario.** Intrusioni telematiche, azioni di sabotaggio: riattivazioni di utenze precedentemente cessate per frode →**I09342 -**

• **INTRUSIONI TELEMATICHE, SCAN.** SCAN (scansione delle porte), attività in grado di consentire la comprensione delle vulnerabilità di una macchina remota al fine di sfruttarle per il compimento di attività di intrusione telematica →**I09343 -**

• **INTRUSIONI TELEMATICHE, spionaggio informatico: spyware/software maligni.** Spionaggio telematico, *spyware* (o "software maligni"): programmi per la raccolta occulta di informazioni →**I09344 -**

• **INTRUSIONI TELEMATICHE, spionaggio informatico: trasferimento massivo dati.** Spionaggio telematico, trasferimento massivo di dati verso località esterne all'azienda attaccata (caso Rizzoli Corriere della Sera) →**I09345 -**

• **INTRUSIONI TELEMATICHE, spionaggio: abbagliamento computer "bersaglio", Arp Spoofing.** Spionaggio telematico, programmi informatici in grado di "abbagliare" i computer oggetto dell'attività intrusiva: il caso *Arp Spoofing* di Telecom Italia →**I09346 -**

• **INTRUSIONI TELEMATICHE, Telecom Italia: indagine ROS Carabinieri.** Arma dei Carabinieri, Reparto Operativo Speciale (ROS): indagine su intrusioni telematiche all'interno di Telecom Italia →**I09347 -**

• **INTRUSIONI TELEMATICHE, tracciamento: "stampaggio" dati.** Informatica, intelligence; tracciamenti, tracce lasciate dai CD anonimi: lo "stampaggio" dei dati ivi contenuti mediante l'utilizzazione della propria casella di posta elettronica comporta un'impronta della traccia linguistica del sistema impiegato (es.: italiano, portoghese, eccetera) →**I09348 -**

• **ITR (trattato), conferenza di Dubai (2012).** Trattato ITR (International Telecommunications Regulations), conferenza di Dubai del 3 dicembre 2012 →**I09348/1 -**

• **IP (Internet Protocol).** Informatica, indirizzo "IP" (Internet Protocol) →**I09349 -**

• **IRAN, cyber attacchi (2008).** Cyber attacchi subiti dall'Estonia nel 2008; differenti tipologie di attacchi informatici subiti da Estonia e Iran →**I09350 -**

• **IRAN, cyber attacchi: stuxnet (2010).** Iran, programma nucleare, Siemens: attacco nucleare al software di controllo dei Programmable Logic Controller (PLC) mediante il "worm" *stuxnet* (2010) →**I09351 -**

• **IRAN, Internet: Gooya.** Iran, siti Internet: *Gooya* →**I09352 -**

• **IRAN, secolarizzazione e weblog religiosi.** ***I giovani alla ricerca dello spazio perduto.*** Le nuove generazioni iraniane stanno riconquistando i luoghi reali e virtuali del dibattito pubblico, grazie anche a Internet: i weblog religiosi. Molti sognano di emigrare →**I09353 -**

• **ISDN.** Integrated Services Digital Network (ISDN), linea telefonica complessa in grado di fornire servizi aggiuntivi superiori alla classica conversazione →**I09354 -**

• **ISTAR.** ISTAR (Intelligence, Surveillance, Target Acquisition and Reconnaissance); ISTAR, schiacciante superiorità Usa nel settore →**I09355 -**

• **LAMER, definizione.** Definizione di *hacker* e di *lamer* →**I09356 -**

• **LAN ETHERNET, rete (network): sistema missioni navali Seaguardian Mk-4.** LAN *Ethernet*, rete (network), sistema di missione impiegato dalle unità navali SEAGUARDIAN Mk-4 realizzato da Astim; GUI (Graphic User Interface); TMS (Tactical Mission System), configurazioni; Linux OX (ambiente); CMS (Combat Management System) →**I09357 -**

• **LAPTOP.** Computer laptop; dati sul programma nucleare iraniano contenuti →**I09359 -**

• **LAPTOP, impiego da parte dei guerriglieri.** Laptop, impiego da parte dei guerriglieri in Iraq, Afghanistan e Pakistan →**I09359/1 -**

• **LEARNING CURVE, formazione del personale e introduzione tecnologie.** Intelligence, *learning curve*: applicazione nella preparazione del personale e nell'inserimento di nuove tecnologie e di processi associati →**I09360 -**

• **MAGLAN CYBER WARLABS.** Maglan Cyber Warlabs →**I09360/1 -**

• **MALWARE, diffusione: Windows.** Malware, diffusione attraverso la piattaforma Windows →**I09360/2 -**

• **MALWARE, Gauss.** Attacchi informatici ai sistemi bancari: attacchi alle infrastrutture di un paese, il caso di Gauss; *malware* Gauss, virus limitato a una ben determinata struttura (le banche) e a selettive aree geografiche ((Israele, Palestina, Libano); Kaspersky Lab; HTTPS, comunicazioni dai computer in maniera cifrata; attacchi effettuati da cybercriminali; esempi di *malware*: Zeus e *Spyeye* (Spy Eye); "banking malware" →**I09361 -**

• **MALWARE, Trojan.** Information warfare, *malware*: famiglia dei *Trojan* →**I09362 -**

• **MALWARE, varie tipologie di virus.** *Cyberweapons* (armi cibernetiche), *malware*: varie tipologie di virus (bombe logiche, *worm*, *trojan*, eccetera) →**I09363 -**

• **MALWARE.** *Cyberweapons* (armi cibernetiche), caratteristiche peculiari e soggetti che se ne stanno dotando sia nel campo del lecito che dell'illecito; l'ambiguo concetto di *cyberweapons*; *malware*, *digital profiling*, caratteristiche delle armi cibernetiche, vita operativa estremamente brevi delle armi cibernetiche →**I09364 -**

• **McAFFE, sicurezza informatica.** McAffe, impresa industriale attiva nel settore della sicurezza informatica →**I09365 -**

• **MEDIA ELETTRONICI, innovazioni informatiche e crisi testate giornalistiche.** Innovazioni in campo informatico, siti web e crisi delle testate giornalistiche: i casi del “Washington Post”, del “New York Times”, del “Boston Globe” e di “Le Monde” →**I09366 -**

• **MEDIA ELETTRONICI.** Mass media elettronici: stimolo della curiosità intellettuale e della creatività di individui e sistemi sociali in un’era di istruzione di massa →**I09367 -**

• **MEDIO ORIENTE, difficile controllo della Rete.** Internet, difficoltà incontrate dai governi arabi nell’azione di controllo della Rete →**I09368 -**

• **MELISSA WORM.** *Melissa worm*, diffuso per mezzo della posta elettronica (e-mail) →**I09370 -**

• **METADATI, controllo dei: NSA.** Metadati di conversazioni telefoniche: NSA (National Security Agency), controllo di milioni di cittadini statunitensi →**I09371 -**

• **METADATI, MAC.** National Security Agency (NSA), MAC (Metadata Analysis Center): analisi veloce dei dati raccolti in rete →**I09372 -**

• **METADATI, telefonia cellulare: indagini, risalita a luogo chiamata.** Telefonia cellulare, metadati e indagini: risalita ai luoghi di effettuazione delle chiamate →**I09373 -**

• **METADATI, Xkeyscore.** *Xkeyscore*, sistema di utilizzazione dei metadati →**I09374 -**

• **MICROPROCESSORI, aumento efficienza.** Progressi ottenuti nei settori delle biotecnologie e delle nanotecnologie e correlato incremento dell’efficienza dei microprocessori →**I09375 -**

• **MICROSOFT, attacchi subiti.** Microsoft, attacchi informatici subiti nell’ottobre 2000 →**I09376 -**

• **MICROSOFT, cyberspazio: NSA (grande fratello).** NSA e Micrososft, coordinamento tra il maggiore produttore mondiale di *software* e l’agenzia di intelligence statunitensi: partecipando alla programmazione del Browser, la NSA si trova nelle condizioni di poter leggere posta e pagine web aperte dagli utenti →**I09377 -**

• **MICROSOFT, cyberspazio: NSA.** La NSA e Micrososft →**I09378 -**

• **MICROSOFT, Francia: "demicrosoftizzazione".** Francia, "demicrosftizzazione" degli apparati informatici della pubblica amministrazione →**I09379 -**

• **MICROSOFT, Germania: sospetti.** Germania, sospetti sulla Microsoft in relazione al sistema Windows →**I09380 -**

• **MINACCE INFORMATICHE, difese: esperienze operative.** ***Minaccia cibernetica-strategia di difesa, esperienze operative.*** Minaccia cibernetica-strategia di difesa, esperienze operative: minaccia relativa ad attacchi cibernetici ed effetti sul piano psicologico, diffusione di una sensazione di insicurezza generalizzata in grado di indurre reazioni nelle forme della sfiducia irrazionale nei confronti delle nuove tecnologie; rischi, incremento quale conseguenza della diffusione sempre più estesa delle applicazioni tecnologiche; informatica, caratteristiche del moderno contesto digitale; vulnerabilità del sistema: utenti finali (persone e aziende) e congegni digitali in loro uso; definizione di "armi cibernetiche"; definizione di *botnet*; le grandi banche dati; servizi di *cloud computing*; nozione di "dato" →**I09380/1 -**

• **MINACCE INFORMATICHE, analisi specifica della vittima.** Minacce cibernetiche: analisi specifica della vittima finalizzata al raggiungimento dei risultati →**I09381 -**

• **MINACCE INFORMATICHE, 4 categorie: vulnerabilità software "aperti".** Minacce cibernetiche: esistenza di quattro diverse categorie e vulnerabilità in Internet insita nei *software aperti* a causa della esposizione delle porte di accesso alle intrusioni pirata →**I09382 -**

• **MINACCE INFORMATICHE, contrasto: CRASH.** Clean-Slate Design of Resilient, Adaptive Security Host (CRASH), sistema di sicurezza nei confronti della minaccia cibernetica mutuato dal sistema immunitario dell'essere umano e dalla capacità adattiva degli organismi biologici avanzati →**I09382/1 -**

• **MINACCE INFORMATICHE, cyberweapons: contrasto, mitigazione e localizzazione.** Cyber weapons (armi cibernetiche), contromisure opposte agli attacchi: mitigazione e localizzazione; *Snapshot*; Usa, FSISAC (Financial Services Information Sharing and Analysis Center) →**I09383 -**

• **MINACCE INFORMATICHE, cyberweapons: contrasto, Polizia di Stato, CNAIPIC.** Strategie di contrasto delle minacce cibernetiche, pilastri basilari: Ruolo della Polizia delle Telecomunicazioni (tlc) e linee guida alla base dell'espletamento delle attività di tutela da essa poste in essere; il Centro nazionale anticrimine informatico e di protezione delle infrastrutture critiche (CNAIPIC); magistratura italiana, repressione dei reati informatici: gli uffici

giudiziari specializzati nelle investigazioni in tale specifico settore attivi presso le Procure Distrettuali della Repubblica →**I09383/1 -**

• **MINACCE INFORMATICHE, minaccia "liquida".** Minacce informatiche: la *minaccia liquida*, di non facile categorizzazione →**I09384 -**

• **MINACCE INFORMATICHE, propagazione.** Minacce cibernetiche, propagazione: facilitazione e incremento del livello di vulnerabilità complessiva; la graduale moltiplicazione dei punti di accesso e la contestuale standardizzazione ai fini dell'interoperabilità delle soluzioni tecnologiche →**I09385 -**

• **MINACCE INFORMATICHE, sicurezza economica nazionale.** Le minacce informatiche alla sicurezza economica nazionale: implicazioni per la comunità d'intelligence →**I09386 -**

• **MIT, TMRC.** TMRC (Teach Model Railroads Club), organizzazione studentesca del Massachusetts Institut of Technology (MIT) →**I09387 -**

• **MORRIS ROBERT, "Morris worm".** Robert Morris, "Morris worm": primo *malware* in grado di autoreplicarsi e diffondersi in modo autonomo attraverso la rete Internet →**I09388 -**

• **NATO, cyber-defense policy: nuovo concetto strategico (2011).** Nato, nuovo concetto strategico in materia di *information warfare*: la *Cyber Defense Policy* approvata nel 2011 e la sicurezza dello spazio cibernetico →**I09390 -**

• **NATO, sicurezza informatica: NCIRC.** Nato, NCIRC (Nato Computer Incident response Capability): sicurezza informatica, difesa e contrasto delle minacce poste alle reti delle telecomunicazioni (tlc) →**I09391 -**

• **NETCENTRIC WARFARE.** Netcentric warfare →**I09392 -**

• **NETWORK INTELLIGENCE (NI).** 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 →**I09392/1 -**

• **OPEN DATA.** Open data →**I09392/2 -**

• **PHISHING, pirateria informatica.** *Phishing*, sottrazione fraudolenta delle credenziali bancarie mediante e-mail e siti Internet costruiti ad arte; pirateria informatica, *phishing*: metodologia in base alla quale mediante l'invio di e-mail false (ad esempio quelle apparentemente provenienti da banche, istituti finanziari o servizi postali) conducono gli utenti della rete su pagine web

altrettanto false che richiedono l'inserimento di username e password di account personali; secondo questa modalità i male intenzionati cercano di carpire, attraverso una tecnica di ingegneria sociale, accessi a conti correnti o a servizi strettamente personali →**I09393 -**

• **POLIS D'ISTINTO, agenzia investigativa di Emanuele Cipriani →(RINVIO) al riguardo vedere le schede "ITALIA/SERVIZI SEGRETI/SISMI-SISDE";**

• **PRISM, programma intelligence Usa. (immagine)** Programma Prism, spiegazione del funzionamento effettuata mediante la proiezione di una slide il 1º aprile 2013 →**I09394 -**

• **PRISM, programma intelligence Usa.** Prism, programma supersegreto di raccolta di informazioni in rete (Internet) mediante l'analisi di dati ricavati da server →**I09395 -**

• **PROCESSO DECISIONALE, condizionamento.** Cyberwar, condizionamento dei processi decisionali dell'avversario: effetti di natura psicologica ingenerati nella popolazione (quali, ad esempio, i timori relativi alla sottrazione di dati relativi alle carte di credito); minaccia: punti di transito fra *domini* e sistemi informatici che divengono anelli deboli delle catene di processo →**I09396 -**

• **PROCESSO DECISIONALE, condizionamento: attacchi informatici.** *Cyberwar*, condizionamento dei processi decisionali dell'avversario: sistemi decisionali e teorie sui modelli decisionali applicate alle decisioni complesse; scopi degli attacchi informatici →**I09397 -**

• **PROF, E-mail: Casa bianca.** USA, Casa Bianca: PROF, sistema interno di posta elettronica →**I09398 -**

• **PROFILING, business intelligence: Fabio Ghioni.** Spionaggio informatico, intervento di Fabio Ghioni all'HITB in Malesia: *Corporation vs corporation, profiling modern espionage* →**I09399 -**

• **PROFILING, digital profiling.** Armi cibernetiche (*Cyberweapons*), profilo digitale di un "obiettivo" (*digital profiling*) →**I09400 -**

• **RACCOLTA, text mining.** ***Nuove forme di guerra, nuove forme di intelligence: text mining.*** Nuove forme di guerra, nuove forme di intelligence: text mining. Nuove forme di guerra: *Information warfare* e nuove minacce; nuove tecnologie per la guerra; guerra multidimensionale; guerre senza soldati; nuove forme di terrorismo: i nuovi terroristi e il *cyber-terrorismo*. Nuove forme d'intelligence: le intenzioni politiche e la loro identificazione; *text mining*: una prospettiva militare; informazione elaborata. Uno sguardo tecnico al *text*

mining: fase di *reprocessing* linguistico; fase di scoperta di regole; le fonti dei dati; le tecniche. Applicazioni ed esempi: applicazioni militari; applicazioni civili: *Competitive Intelligence* in IBM; *Competitive intelligence* in IBM: esempio di utilizzo →**I09401 -**

• **RADAR, piattaforma informatica.** Sistema *Radar*, piattaforma informatica dedicata al supporto anti-frode; infrastruttura *Circe*, strumento per la gestione delle intercettazioni telefoniche effettuate su rete mobile →**I09402 -**

• **REATI INFORMATICI, articolo 615 quinquies C.P..** Articolo 615 *quinquies* del Codice penale, reati informatici: diffusione di programmi diretti a danneggiare o interrompere un sistema informatico →**I09403 -**

• **REATI INFORMATICI, articolo 617 quater C.P..** Reati informatici, articolo 617 quater del Codice penale: intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche →**I09404 -**

• **REATI INFORMATICI, criticità indagini (Italia).** Inchieste giudiziarie aventi a oggetto reati informatici: difficoltà incontrate dagli inquirenti nel dimostrare la relazione macchina-uomo →**I09405 -**

• **REATI INFORMATICI, intercettazioni illegali: d.lg. nº259/2006.** Reati informatici, intercettazioni telefoniche e telematiche: decreto legislativo nº259 del 22 settembre 2006 recante norme in materia di distruzione delle intercettazioni illegali →**I09406 -**

• **REPLY, società di consulenza.** Informatica, Reply: società di consulenza del settore →**I09407 -**

• **RICICLAGGIO DI DENARO, transazioni telematiche: meccanismo.** Riciclaggio di denaro attraverso le transazioni telematiche: meccanismo di funzionamento →**I09408 -**

• **SCIF.** Sensitive Comparmented Information Facility (SCIF), installazione per la ricezione di informazioni sensorie multiple →**I09409 -**

• **SCRIPT KIDDIE.** *Script kiddie*, significato del termine →**I09410 -**

• **SEAGUARDIAN Mk-4, sistema missioni navali.** LAN *Ethernet*, rete (network), sistema di missione impiegato dalle unità navali SEAGUARDIAN Mk-4 realizzato da Astim (Ravenna, Italia); GUI (Graphic User Interface); TMS (Tactical Mission System), configurazioni; Linux OX (ambiente); CMS (Combat Management System); SEAGUARDIAN Mk-4, sistema di missione per unità navali di nuova generazione prodotto da Astim: gestione di un superiore numero di sensori di scoperta (di superficie e subacquei), di attuatori (sistemi d'arma) e di

contromisure in un *range* di missioni militari più ampio rispetto al passato, sia a bordo di unità navali che a terra →**I09411 -**

• **SERVER, DVS: domini, estensioni e suffissi.** Internet, server DNS (Domain Name Service): mattone basilare sul quale è costruito l'intero modello della rete; *domini*, *estensioni*, *suffissi* →**I09412 -**

• **SERVER.** Server →**I09413 -**

• **SICUREZZA INFORMATICA, attività svolte dalle security aziendali.** Fabio Ghioni, idee innovative e orientamenti riguardo la realizzazione di una security aziendale efficace; attività poste in essere dalla security aziendale sotto la sua supervisione: sonde di intercettazione, sistemi di tracciamento, consulenze, sviluppo e forniture di nuovi sistemi informatici →**I09414 -**

• **SICUREZZA INFORMATICA, CLUSIT.** CLUSIT, Associazione italiana per la sicurezza informatica →**I09415 -**

• **SICUREZZA INFORMATICA, comunicazioni: rete di sotto superfice.** Informatica, ricerca della sicurezza nelle comunicazioni nella rete: ricorso a reti di sotto superfice che utilizzano siti web di copertura →**I09416 -**

• **SICUREZZA INFORMATICA, criticità: assenza garanzie su impermeabilità dei sistemi.** Sicurezza informatica, impermeabilità dei sistemi: assenza di garanzie in merito a causa della complessità dei processi interni alle aziende e della dinamicità dell'evoluzione informatica →**I09417 -**

• **SICUREZZA INFORMATICA, difesa: tecnica "Trusted Computing".** Difesa dagli attacchi informatici, la tecnica *Trusted Computing* e la TPM (Trusted Platform Module) →**I09418 -**

• **SICUREZZA INFORMATICA, difesa: industria.** ***Il punto di vista della grande industria nazionale sulla Cyber Defence.*** Il punto di vista della grande industria nazionale sulla Cyber Defence →**I09419 -**

• **SICUREZZA INFORMATICA, Guardia di Finanza: Nucleo frodi telematiche.** Sicurezza informatica, Guardia di Finanza: Nucleo speciale frodi telematiche, operazione "hi-tech hate" →**I09420 -**

• **SICUREZZA INFORMATICA, Italia: cibernetica e information warfare, livello di sicurezza.** Sicurezza cibernetica nazionale in Italia: 2012, *Information Warfare Conference Rome*; l'Italia di fronte alle sfide di sicurezza dello spazio cibernetico →**I09421 -**

• **SICUREZZA INFORMATICA, Italia: impreparazione security aziendali (2001).** Sicurezza informatica, Italia: 2001, impreparazione delle security aziendali ad affrontare lo specifico problema in quanto strutture fino a quel momento basate su principi e modelli organizzativi tipici dei contesti militari →**I09422 -**

• **SICUREZZA INFORMATICA, Italia: normativa vigente.** Sicurezza cibernetica nazionale in Italia, normativa vigente in materia: leggi 124/2007 e 133/2012 →**I09423 -**

• **SICUREZZA INFORMATICA, Italia: strategie nazionali, Copasir (Relazione 2010).** Comitato parlamentare per la sicurezza della Repubblica (COPASIR), terrorismo cibernetico e *cyberwar*: Relazione del 7 luglio 2010, possibili implicazioni e minacce per la sicurezza nazionale derivanti dallo spazio cibernetico →**I09424 -**

• **SICUREZZA INFORMATICA, Italia: strategie nazionali.** Strategie nazionali di sicurezza cibernetica: costituzione di strutture centrali di direzione e pianificazione in materia di sicurezza →**I09425 -**

• **SICUREZZA INFORMATICA, Onu: Impact e Itu.** Onu, International Multilateral Partnership Against Cyber Threats (IMPACT) e International Communication Union (ITU) →**I09426 -**

• **SICUREZZA INFORMATICA, operatori: psicologia, propensioni caratteriali.** Sicurezza informatica, operatori del settore: aspetti psicologici della personalità, propensioni caratteriali evidenziate dalla tendenza a forme di chiusura (nei confronti degli altri) a fronte della circolazione di informazioni (nel proprio microcosmo) che prefigurano la formazione di un "pensiero comune" →**I09427 -**

• **SICUREZZA INFORMATICA, prevenzione: cerchi concentrici e ridondanza.** Sicurezza informatica, misure di prevenzione: logica dei *cerchi concentrici* e ridondanza delle strutture →**I09428 -**

• **SICUREZZA INFORMATICA, prevenzione: cyber-difesa, analisi.** Analisi *cyber-difesa*, azioni preventive: 7 quesiti alla loro base e definizione di infrastruttura critica →**I09429 -**

• **SICUREZZA INFORMATICA, prevenzione: misure da assumere ai meeting aziendali.** Sicurezza informatica, misure di prevenzione da assumere prima che inizi un importante meeting aziendale →**I09430 -**

• **SICUREZZA INFORMATICA, ricerca della.** La ricerca della sicurezza informatica →**I09431 -**

• **SICUREZZA INFORMATICA, simulazione intrusioni.** Internet, sicurezza informatica: simulazioni di intrusioni nei sistemi →**I09432 -**

• **SICUREZZA INFORMATICA, siti internet: indagine analitica Online.** Internet, sicurezza informatica: operazioni di indagine analitica di un sito Online →**I09433 -**

• **SICUREZZA INFORMATICA, Telecom Italia: Security Technology and Innovation Summit (2006).** Telecom Italia, *Security Technology and Innovation Summit*: 2006, l'azienda guidata da Tronchetti Provera si interessa al mercato della sicurezza →**I09434 -**

• **SICUREZZA INFORMATICA, UE: EECTF.** Unione europea, sicurezza cibernetica e agenda digitale europea: EECTF (European Electronic Crime Task Force) partecipazione della Squadra Telecomunicazioni (TLC) della Polizia di Stato italiana →**I09435 -**

• **SICUREZZA INFORMATICA, UE: Direttiva 114/2008, istituzione ENISA.** Unione europea, sicurezza cibernetica e protezione da *cyber-attack* delle infrastrutture critiche (energia e trasporti): la Direttiva 114/2008 e l'istituzione di ENISA (European Network and Information Security Agency) →**I09436 -**

• **SICUREZZA INFORMATICA, UE: EISAS ed E3PR.** Unione europea, sicurezza cibernetica e agenda digitale europea: EISAS (European Information Sharing and Alerting System) e il gruppo di lavoro E3PR (European Public Private Partnership for Resilience) →**I09437 -**

• **SICUREZZA INFORMATICA, UE: sicurezza cibernetica, EUGS.** EUGS (Global Strategy for the the EU's Foreign and Security Policy), adottata dall'EU Council/Generla Affairs nel giugno 2016: delinea la strategia per la protezione dell'Unione europea dalla minacce esterne considerate nella loro dimensione *non militare* relativa a terrorismo, minacce ibride, sicurezza cibernetica ed energetica, criminalità organizzata →**I09438 -**

• **SICUREZZA INFORMATICA.** Sicurezza informatica, attività condotta all'interno di un sistema finalizzata alla verifica di sue eventuali debolezze nell'utilizzazione di informazioni sensibili →**I09439 -**

• **SICUREZZA, modifica dei termini.** Sicurezza, equazione della modifica dei termini: lo sganciamento dai livelli quantitativi e qualitativi (arsenali) →**I09440 -** 76/32.

• **SID (Signal Intelligence Directorate), metadati: analisi contenuti.** NSA (National Security Agency), Signal Intelligence Directorate (SID): controllo

esercitato sul MAC (Metadata Analysis Center) e sulla AAD (Advanced Analysis Division), organismo preposto all'analisi di contenuti e metadati generati in rete oppure di natura telefonica →**I09441 -**

• **SITUATIONAL AWARENESS.** Guerra, *situational awareness* condivisa e operazioni basate su una "simultaneità multidimensionale" →**I09442 -**

• **SNIFFER, "sniffaggio" di una rete telematica.** *Sniffer*, *sniffing*, «*sniffare* una rete telematica»: significato del termine →**I09443 -**

• **SOC.** Security Operation Center (SOC) →**I09443/1 -**

• **SONY, Play Station 3.** Sony, Play Station 3 →**I09444 -**

• **SORVEGLIANZA ELETTRONICA, "Tempesta": trasmettitore di impulso.** Tempesta, trasmettitore di impulso elettromagnetico per la sorveglianza elettronica e gli attacchi tattici prodotto dalla Elettronica s.p.a. →**I09445 -**

• **SORVEGLIANZA GLOBALE, filosofia della.** La filosofia della sorveglianza globale →**I09446 -**

• **SPETTRO ELETTROMAGNETICO, fabbisogno di banda e limiti: Italia.** Italia, spettro elettromagnetico: limiti derivanti dal fabbisogno di banda; il piano di assegnazione delle frequenze →**I09447 -**

• **SPIONAGGIO TELEMATICO, abbagliamento computer bersaglio: Arp Spoofing.** Spionaggio telematico, programmi informatici in grado di "abbagliare" i computer oggetto dell'attività intrusiva: il caso *Arp Spoofing* di Telecom Italia →**I09448 -**

• **SPIONAGGIO TELEMATICO, business intelligence: Fabio Ghioni.** Spionaggio informatico, intervento di Fabio Ghioni all'HITB in Malesia: *Corporation vs corporation, profiling modern espionage* →**I09449 -**

• **SPIONAGGIO TELEMATICO, tecniche di intrusione nei computer bersaglio.** Spionaggio telematico, intrusione nei computer "obiettivo" mediante l'impiego di un programma camuffato all'interno di una *e-mail* (messaggio di posta elettronica) inviata agli indirizzi prestabiliti (cosiddetti messaggi spia) →**I09450 -**

• **SPOOFING, dirottamento UAV stealth RQ-170 SENTINEL.** ***Cyber-dirottamenti: come l'Iran ha catturato "la bestia"; la tecnica spoofing.*** UAV spia americano RQ-170 SENTINEL (noto anche come «la bestia di Kandahar» impiegato dalla CIA nel monitoraggio del programma nucleare iraniano:

dirottamento e cattura da parte delle forze di sicurezza di Teheran avvalendosi della tecnica *spoofing* il 4 dicembre 2011 →**I09450/1 -**

• **SVANITY FAIR, sito internet di gossip.** *Svanity Fair*, sito internet di gossip che nel marzo 2003 pubblicò alcune foto compromettenti di Afef Jnifen, moglie del presidente di Telecom Italia Marco Tronchetti Provera →**I09451 -**

• **TASSONOMIA, tassonomie comuni.** Tassonomie comuni per la classificazione e la descrizione di diverse tipologie di problemi (esempio: frodi e incidenti informatici) →**I09452 -**

• **TECNOTRONICO, sviluppo e attacchi.** Sviluppo tecnotronico e attacchi tecnotronici →**I09453 -**

• **TELECOM ITALIA, security aziendale: Fabio Ghioni →(RINVIO) al riguardo vedere la scheda "TELECOM ITALIA/SECURITY" presente in questa stessa cartella oppure la scheda "GHIONI FABIO";**

• **TELEFONIA, UMTS →(RINVIO) al riguardo vedere anche la scheda "COMUNICAZIONI/TELECOMUNICAZIONI imprese del settore";**

• **TEMPO, fattore tempo.** Spionaggio telematico, fattore tempo →**I09454 -**

• **TERRORISMO, ricorso a strumenti telematici: rivendicazione assassinio Biagi.** Brigate rosse-Partito comunista combattente (BR-PCC o *nuove Brigate rosse*), omicidio del giuslavorista Marco Biagi avvenuto il 19 marzo 2002: rivendicazione dell'azione a mezzo Internet; per la prima volta uno strumento potente e diretto come la rete viene utilizzato in un contesto terroristico; notevole padronanza degli strumenti telematici da parte dei militanti dell'organizzazione armata: evitate la tracciatura e le limitazioni alla navigazione in rete; Fabio Ghioni, consulente informatico della Procura della Repubblica nel corso dell'inchiesta giudiziaria sul caso dell'omicidio del giuslavorista Marco Biagi assassinato dai terroristi delle BR-PCC nel 2002; errori sui dati telefonici commessi nel corso dell'indagine →**I09455 -**

• **TERRORISMO, ricorso alla steganografia linguistica applicata al web.** Terrorismo islamista, cellule operative dormienti sparse nel mondo: addestramento dei militanti effettuato mediante tecniche virtuali, la steganografia linguistica applicata al web →**I09455/1 -**

• **TRASHING.** Informatica, *trashing*: pratica di recupero dell'hardware dismesso da un computer che, altrimenti, verrebbe destinato alla rottamazione come rifiuto e non re-impiegato da un'altra macchina →**I09456 -**

• **UNIONE EUROPEA, agenda digitale: Strategia 2020.** Unione europea, *Strategia 2020*: agenda digitale →**I09457 -**

• **UPDATED ISCMMS, Australia: sottomarini classe COLLINS.** Royal Australian Navy, sottomarini classe Collins (HMAS *Collins*, HMAS *Waller* e alter due unità): *updated* ISCMMS (Integrated Ship Control Management and Monitoring System) realizzato dalla Saab e destinato all'integrazione sulle unità sottomarine a opera dell'Australia's Collins Class (ASC), *prime contractor* →**I09458 -**

• **URMET.** Urmet, azienda produttrice di registratori e apparecchiature elettroniche per le intercettazioni vocali e telematiche →**I09459 -**

• **USA, sicurezza informatica: Bush e Obama.** USA, *cyber security* durante le amministrazioni di Bush e di Obama →**I09460 -**

• **USA, intercettazioni comunicazioni membri del Congresso.** Eric Holder, procuratore generale americano che autorizzò le intercettazioni delle comunicazioni dei cittadini statunitensi e dei deputati membri del *Commitee on Intelligence* del Congresso e del Senato →**I09461 -**

• **USA, NSA: information warfare, contrasto attacchi.** USA, NSA (National Security Agency): assunzione in massa di personale per il contrasto degli attacchi in ambito Information warfare →**I09462 -**

• **USB, drive rimovibile.** Informatica, periferica USB: *drive* rimovibile →**I09463 -**

• **US CYBER COMMAND.** US Cyber Command →**I09463/1 -**

• **US CYBER CONSEQUENCES.** John Bumgartner, analista del *think tank* americano Us Cyber Consequences →**I09463/1 -**

• **VATILEAKS, IOR: codici cifrati in rete e fuga di notizie riservate.** *Vatileaks*, IOR: codici cifrati in rete e fuga di notizie riservate →**I09464 -**

• **VATILEAKS, Segreteria di Stato: lotte di successione.** *Vatileaks*, lotte di successione per il vertice della Segreteria di Stato →**I09465 -**

• **VATILEAKS.** *Vatileaks* →**I09466 -**

• **VIRTUALIZZAZIONE DELLA SICUREZZA.** Concetto di *virtualizzazione* della sicurezza →**I09466/1 -**

• **VIRUS INFORMATICI, "I'love you".** *I'love you*, virus informatico →**I09467 -**

• **VIRUS INFORMATICI, "worm animaletto".** *Information warfare*, gruppo Rizzoli Corriere della Sera: procedura impiegata nel corso dell'incursione nei computer attuata mediante virus informatico *worm* "animaletto" →**I09468 -**

• **VIRUS INFORMATICI, "worm" di nuova generazione: codici di attacco.** Virus informatici: *worm* di nuova generazione: codici di attacco in grado di colpire obiettivi dalla vulnerabilità facilmente riscontrabile sulla rete, tendenti a bloccare ogni attività informatica fino a condurre alla paralisi di singoli servizi o di intere aziende →**I09469 -**

• **VIRUS INFORMATICI.** Virus informatici: I'love you e Mafia Boy →**I09470 -**

• **VIRUS, Conficker.** Virus, Conficker →**I09471 -**

• **VIRUS, SQL Hammer.** Virus, SQL Hammer →**I09472 -**

• **WAR DRIVING.** War driving →**I09473 -**

• **WEB, parte "emersa" dell'universo digitale.** Web, spazio pubblico di internet: parte emersa dell'universo digitale →**I09473/1 -**

• **WEB, Tim Lee Berners.** Tim Lee Berners, fondatore del web →**I09473/2 -**

• **WHOIS.** Whois →**I09474 -**

• **WI-FI, intrusioni informatiche e information warfare.** Information warfare, utilizzazione della tecnologia WiFi per un attacco o un'intrusione informatica: impossibile risalita al personal computer responsabile dell'azione →**I09475 -**

• **WI-FI, monitoraggio comunicazioni: Echelon.** CIA e NSA, Echelon: mappatura delle comunicazioni WiFi effettuata da Google →**I09476 -**

• **WIKI, applicazioni.** *Wiki*, applicazioni: contenuto o servizio fruibile in rete realizzato con il contributo apportato dagli stessi utenti →**I09477 -**

• **WIKILEAKS →(RINVIO) al riguardo vedere la scheda "INTELLIGENCE/WIKILEAKS";**

• **WIKIPEDIA, assenza di verifiche di qualità.** *Wikipedia*, assenza di verifiche di qualità →**I09478 -**

• **WIND, security aziendale: "tiger team".** Wind, security aziendale: 2001, formazione del primo *tiger team* di informatici/hacker →**I09479 -**

• **WIPING, cancellazione complessa di dati.** *Wiping* di una postazione informatica: cancellazione complessa dei dati che non consente alcuna successiva possibilità di recupero →**I09480 -**

• **<u>WIRELESS</u>, paleo-wireless.** Tecnologie *paleo-wireless* →**I09480/1 -**

• **<u>WIRELESS</u>, reti wireless: intrusioni e anti-intrusioni.** Reti *wireless*: intrusioni e anti-intrusioni →**I09481 -**

• **<u>ZONE-H</u>, "Hands on hacking": corso specialistico attacchi informatici.** *Hands on hacking*, corso specialistico organizzato da *Zone-H* nell'ambito del quale vennero utilizzate le tecniche di attacco informatico, messe in pratica contro obiettivi simulati →**I09482 -**

• **<u>ZONE-H</u>.** Zone-H, osservatorio indipendente per la sicurezza informatica →**I09483 -**