AVVERTENZA

Il Comitato parlamentare per la sicurezza della Repubblica ha svolto un'indagine approfondita su una delle questioni che più condizionerà lo scenario di sicurezza internazionale e nazionale nel prossimo futuro. La diffusione esponenziale dei sistemi e degli strumenti informatici e tecnologici porta con sé anche una maggiore vulnerabilità delle infrastrutture critiche nazionali, oltre che mettere a rischio le tutele della riservatezza e delle libertà dei cittadini, accrescere lo spazio di manovra delle organizzazioni criminali, creare un'area porosa nell'attività di salvaguardia della proprietà intellettuale, dei segreti industriali e delle informazioni che attengono la sicurezza nazionale.

La presente Relazione riferisce sugli esiti di tale indagine. Si articola in una premessa di sintesi delle nuove problematiche strategiche riferite ai compiti del Comitato; nella descrizione dell'attività svolta; nell'illustrazione delle caratteristiche del fenomeno a livello globale; nell'analisi delle ricadute per il nostro Paese; nella presentazione delle principali risultanze delle attività di intelligence*; nella proposta di interventi per rafforzare la capacità di analisi dei nostri apparati di sicurezza e per potenziare le attività di prevenzione e contrasto alle minacce.*

PAGINA BIANCA

1. Premessa.

Nelle relazioni internazionali e strategiche, la cifra di questo inizio di XXI secolo è l'interdipendenza. Sotto il termine generico di « globalizzazione » ricade una vasta serie di declinazioni che coinvolgono attori statuali e non, privati cittadini, imprese e istituzioni. Il compito di proteggere la sicurezza nazionale si fa, per questo, sempre più complesso, mentre si afferma il principio che vede la sicurezza emergere come un « bene » sempre più indivisibile, nella sua dimensione orizzontale e verticale.

La tutela collettiva della sicurezza ha come primo obiettivo la galassia delle minacce non-statuali, o asimmetriche, la cui pericolosità cresce proporzionalmente alla moltiplicazione dei possibili strumenti di offesa. È il caso del terrorismo di matrice integralista, il cui messaggio è meglio veicolato oggi anche grazie alla diffusione di internet e degli strumenti di comunicazione virtuale; o della minaccia posta dalla proliferazione di armi di distruzione di massa, stimolata dalla capacità di sofisticazione delle reti criminali transnazionali o del terrorismo nel garantirsi l'accesso a tecnologie sensibili e segreti industriali.

Se nella lunga parentesi della Guerra Fredda la tecnologia è stata un fattore di superiorità strategica nella competizione tra le due superpotenze, impegnate anche a militarizzare lo spazio e a sviluppare reti informatiche che potessero servire le rispettive strategie militari, oggi sempre più l'accento si sposta sulla virtualizzazione delle relazioni internazionali e quindi, potenzialmente, dei conflitti.

Lo spazio cibernetico è un nuovo fondamentale campo di battaglia e di competizione geopolitica nel XXI secolo. Lo Stato nazionale, la cui sovranità viene erosa proprio dal processo di globalizzazione, può proiettare i propri interessi e dispiegare le proprie strategie difensive sulla grande « autostrada virtuale » costituita dal *web*, dalle reti di comunicazione, dai circuiti telematici, dai sistemi e dalle reti computerizzate. Non sono poche le analisi strategiche che evidenziano come le prossime guerre tra Stati non verranno più iniziate dalle Forze Armate, ma saranno concentrate su un massiccio utilizzo di attacchi informatici per sabotare preventivamente la capacità di risposta o di offesa degli avversari e per arrecare pesanti danni, non virtuali ma materiali. Al tempo stesso, nello spazio cibernetico si concentrano attori asimmetrici che, da soli, costituiscono una seria minaccia alla sicurezza delle Nazioni. Il grande spazio telematico globale, di dimensioni virtualmente infinite, è solcato anche da reti criminali organizzate, il cui obiettivo è di sottrarre denaro, truffare o raggirare a scopo di lucro cittadini ed organizzazioni; da movimenti del terrorismo fondamentalista, impegnati a cementare consenso, attrarre nuovi adepti o diffondere messaggi attraverso la rete; agenzie di spionaggio non governative, in grado di sottrarre informazioni rilevanti alla *business community*, falsando in questo modo la leale concorrenza.

La comunità internazionale oggi accetta il fatto che la protezione dell'atmosfera, dell'idrosfera, della litosfera e della biosfera – considerati « beni universali » – sia responsabilità di tutti i Paesi. La stessa

considerazione deve applicarsi alla « *cyber*-sfera », che è fondamentale per la nostra vita quotidiana, il nostro benessere materiale e la nostra sicurezza. In un'era in cui gli attacchi informatici stanno crescendo in tutto il mondo, il segretario di Stato Usa Hillary Clinton ha avuto ragione nell'affermare che un attacco ad una rete di computer di una nazione « può essere un attacco a tutte quante ». Queste aggressioni non fanno che ricordarci che il *cyber*-spazio, nuovo elemento costitutivo dei beni comuni, è già minacciato. Esso deve essere considerato come proprietà comune per il bene di tutti, proprio come lo spazio esterno, le acque internazionali e gli spazi aerei internazionali. E come succede per la pirateria oceanica e il dirottamento di aerei, il crimine informatico non dovrebbe restare impunito se vogliamo salvaguardare i nostri interessi condivisi e collettivi.

Prima del latino *gubernare*, i greci usavano la parola *kybernan* per indicare il comando; e *kybernos* corrispondeva al nostro « capitano ». Una definizione di questa minaccia, i cui attori, mezzi, fini e bersagli mutano più velocemente delle loro contromisure, può estrapolarsi dal « *Cyberspace Policy Review* », pubblicato dalla Casa Bianca nel giugno 2009, che rappresenta lo stato dell'arte della dottrina della sicurezza cibernetica degli Stati Uniti, ovvero delle politiche dell'Amministrazione tese alla « sicurezza e stabilità dell'infrastruttura globale delle informazioni e comunicazioni » (1).

Pur non avendo pretese di completezza, questa descrizione sembrerebbe tradirne una minore concretezza; testimonianza del fatto che, anche per le maggiori potenze, la formulazione di una dottrina coerente e unificata per contrastare le nuove minacce rimane un compito estremamente complesso, oltre che per le esigenze di riservatezza, a causa delle sue mille variabili, accresciute dalla mancanza di una « dottrina » codificata e accettata dalle parti in causa.

La molteplicità dei possibili autori di un attacco informatico e dei loro fini fa sfumare il valore dei parametri necessari per tarare e impostare una strategia di difesa. L'assenza di barriere all'ingresso, l'anonimato, l'asimmetria nella vulnerabilità dei bersagli implica una capacità diffusa di esercitare il potere e determina il superamento del tradizionale confronto tra Stati-Nazione come attori centrali delle relazioni internazionali, tre secoli e mezzo dopo il Trattato di Westphalia, che ne sancì la primazia.

Il passaggio da una potenza dominante all'altra nell'arena politica internazionale è un evento storicamente comune e conosciuto. La vera novità di questo XXI secolo è, invece, la frammentazione del potere. La tecnologia, per molto tempo, è stata propensa a favorire il consolidamento delle gerarchie politiche. La moderna tecnologia, prevalentemente a causa dei suoi bassi costi, sembra favorire il decentramento politico attraverso l'universalizzazione virtuale dell'uso del potere. Nel 1993 esistevano circa 50 siti internet; alla fine di quel decennio ne esistevano oltre 5 milioni. Nel 2010 solo in Cina si sono registrati 400 milioni di utenti. Nel 1980 le telefonate trasmesse dai fili di rame potevano « trasportare » appena una pagina di informa-

---

(1) « *Cyberspace Policy Review* », su www.whitehouse.gov, 6/2009.

zioni al secondo; oggi la fibra ottica può trasmettere 90.000 volumi in un secondo. Nel 1980 un gigabyte di massa di archiviazione occupava lo spazio fisico di una stanza; oggi, 200 gigabyte di informazioni sono trasportabili in una tasca, attraverso una *pendrive*.

Le strategie e le modalità della competizione sul *web* sono difficilmente conoscibili, in virtù di un mutamento costante determinato dal salto tecnologico.

Se la Guerra Fredda è finita dal punto di vista geopolitico e militare, non si può affermare altrettanto per il dominio informatico. La politica di distensione avviata dal presidente americano Barack Obama riguarda anche il *web*, con l'obiettivo dichiarato di scongiurare il pericolo di una *cyber*-guerra tra grandi potenze.

Il confronto tra le diplomazie di USA e Russia riguarda anche un'ipotesi di versione digitale del recente Trattato Start-2, firmato nell'aprile 2010 a Praga e che prevede il taglio del 30% nel numero delle testate atomiche disponibili per i due Paesi.

Già durante l'Amministrazione di George W. Bush, la Russia aveva avanzato la proposta di un accordo, in ambito ONU, per il controllo e la limitazione della proliferazione di agenti virtuali di distruzione, dai virus malevoli ai *software* per le incursioni e il sabotaggio di reti strategiche su vasta scala. Gli USA, in quella circostanza, accettarono solo di circoscrivere il negoziato alle cosiddette minacce asimmetriche, ovvero all'utilizzo della rete da parte delle organizzazioni criminali transnazionali. Oggi le prospettive di un accordo più largo sembrano più concrete, soprattutto se rapportate all'urgenza di mettere in atto un sistema difensivo non spurio, alla luce delle ambizioni crescenti esercitate dalle potenze informatiche emergenti, a cominciare dalla Repubblica Popolare cinese, l'India o l'Iran.

In particolare, le implicazioni della militarizzazione dello spazio cibernetico condotta dalla Cina sono state analizzate da numerosi studi e rapporti internazionali (2). In un rapporto presentato al Congresso dal Dipartimento della Difesa americano si evidenzia come la Cina sia in procinto di espandere la capacità di offesa militare dai tradizionali domini di terra, mare, cielo allo spazio cibernetico, con lo scopo di rendere vulnerabili le infrastrutture critiche dei principali concorrenti strategici e ridurre così il *gap* militare e tecnologico.

Sotto il profilo prettamente dottrinale, la proiezione cibernetica di Pechino è persino antecedente a quella delle più rilevanti e note rivoluzioni negli affari militari, a cominciare da quella americana. In un noto testo del 1999, gli alti vertici dell'Esercito cinese (PLA – *People's Liberation Army)* teorizzavano una forma di conflitto in grado di trascendere le frontiere e le distanze fisiche, attraverso l'utilizzo della rete telematica (3).

---

(2) Tra gli altri, si veda Brian Mazanec, « *The art of (cyber)war* », The Journal of International Security Affairs, dicembre 2009.

(3) Qiao Liang, Wang Xiangsui, « *Unrestricted Warfare* », Pan American Publishing Company, 2002.

Secondo uno studio dell'*Institute for Security Technolgy Studies* (4) del 2008, la Cina è la sola potenza emergente che abbia già sviluppato capacità operative nei cinque domini relativi alla superiorità cibernetica: elaborazione di una dottrina operativa, capacità addestrative, capacità di simulazione, creazione di unità addestrate alla guerra cibernetica, sperimentazione di attacchi *hacker* su larga scala. Rispetto a quest'ultimo punto, significativa è stata la campagna conosciuta con il nome in codice « *Titan Rain* »: tra il 2003 ed il 2005, centinaia di computer di uffici dell'Amministrazione americana e di governi dell'Europa occidentale furono sistematicamente attaccati da *hacker* i cui *server* di accesso alla rete, venne poi verificato, si trovavano nella provincia cinese del Guandong.

Alla base della capacità di Pechino rispetto allo spazio cibernetico c'è l'opzione strategica della deterrenza: lo scopo dei vertici militari asiatici è di dissuadere altre potenze dall'assumere una politica troppo aggressiva nei confronti di Pechino. Si tratta di una autentica rivoluzione negli affari strategici, poiché, fino ad oggi, il concetto di deterrenza era stato utilizzato esclusivamente con riferimento all'arma atomica e alla mutua dissuasione che ha congelato le possibili prove di forza militare tra le due superpotenze della Guerra Fredda.

L'estensione di tale dottrina allo spazio cibernetico rappresenta un vantaggio ed un limite allo stesso tempo. Essa è un vantaggio nella misura in cui non presenta lo stesso potenziale distruttivo di un attacco atomico (benché una combinazione tra le due cose non si possa escludere): appare piuttosto improbabile, a titolo di esempio, che la Cina possa rispondere ad una eventuale *escalation* militare con gli USA nello Stretto di Taiwan con la minaccia nucleare; ma potrebbe benissimo attivare un esercito di *cyber*-combattenti per infliggere danni notevoli al sistema di sicurezza americano. Il limite di tale estensione del perimetro strategico della deterrenza risiede nella difficoltà di renderla una dottrina simmetrica, che risponda cioè a criteri di logica estrema. Un attacco attraverso la rete potrebbe risultare difficilmente identificabile, non facilmente arrestabile e dalle conseguenze non completamente prevedibili.

Di fronte a questi rapidi sviluppi, i principali attori della scena mondiale sono impegnati ad assumere iniziative di difesa il più possibile efficaci. Con un provvedimento senza precedenti, il Senato americano ha approvato una legge che autorizza la Casa Bianca ad assumere pieni poteri di emergenza in caso di *cyber*-attacco alle infrastrutture strategiche del Paese (5). Il Parlamento ha redatto, con il supporto degli uffici governativi, una lista di *provider* internet, siti, autostrade telematiche e telefoniche considerate strategiche per la sicurezza nazionale. A tali operatori privati, il Presidente degli Stati Uniti potrà imporre lo spegnimento in caso di minaccia impellente alla sicurezza nazionale o di possibile perdita di vite umane. Tale

---

(4) http://www.ists.dartmouth.edu.

(5) « *Protecting cyberspace as a national asset Act* », S. 3480, giugno 2010, http://www.opencongress.org/bill/111-s3480/show.

provvedimento fa seguito alla revisione della strategia nazionale di protezione dello spazio cibernetico richiesta dal Presidente americano, che ha evidenziato le principali vulnerabilità del sistema nazionale, suggerendo possibili rimedi (6).

Gli attori che possono avvalersi dello strumento informatico per azioni ostili vanno dall'*hacker* individuale che agisce a scopo di lucro, fino all'apparato governativo che persegue obiettivi geopolitici o propagandistici, come nel caso degli attacchi informatici verso l'Estonia nel 2007, passando per la criminalità organizzata e i gruppi terroristici (7). Questi ultimi, ad esempio, usano il *cyber*-spazio per tutto lo spettro delle loro attività, dal reclutamento al finanziamento, alla propaganda e, in misura sempre maggiore, anche all'attacco informatico vero e proprio (8) teso a procurare un danno all'avversario. In definitiva, un attacco informatico può provenire pressoché da chiunque, per qualunque fine.

Lo stesso discorso vale per il ventaglio dei possibili bersagli. Dai conti correnti dei singoli cittadini alla sicurezza delle strutture più sensibili dello Stato, la crescente dipendenza dalle infrastrutture telematiche che pervade tutte le sfere della società rende virtualmente infiniti i potenziali obiettivi della minaccia cibernetica, e quindi le strutture da difendere.

A titolo di esempio, va notato come, nel loro rapporto annuale, reso pubblico il 21 giugno 2010, i servizi di *intelligence* tedeschi abbiano avvertito che due sono i principali rischi per la democrazia della Germania e la sua stabilità: l'estremismo politico e lo spionaggio industriale. L'*intelligence* federale punta il dito in particolare contro Cina e Russia, due Paesi descritti alla frenetica ricerca di *know-how* tecnologico e industriale e che vedono nel composito panorama industriale tedesco un terreno fertile per possibili incursioni informatiche e per la sottrazione di creazioni, segreti e brevetti. Dalla Cina, l'interesse riguarda soprattutto i processi produttivi, le scoperte scientifiche e i nuovi prodotti. Dalla Russia, invece, l'interesse è rivolto al grande settore energetico tradizionale o alternativo.

Secondo l'associazione tedesca delle imprese, il danno provocato dal *cyber*-spionaggio in Germania è in crescita esponenziale (9).

2. L'attività del Comitato parlamentare per la sicurezza della Repubblica.

Il Comitato parlamentare per la sicurezza della Repubblica, nel mese di settembre 2009, ha deliberato su proposta del presidente *pro-tempore* e relatore del presente documento, senatore Francesco Rutelli, l'inizio di un'attività di indagine sulle possibili implicazioni e

---

(6) « *Cyberspace policy review* », su www.whitehouse.gov.

(7) Per un elenco delle diverse possibili fonti di minacce informatiche prese in considerazione dallo *United States Computer Emergency Security Program* (US-CERT) si veda www.us-cert.gov.

(8) Vds. ad esempio: Directorate General External Policies of the EU, « *Cyber Security and Politically, Socially and Religiously Motivated Cyber Attacks* », 2/2009.

(9) Si veda: B. Romano, « *La Germania attacca le spie industriali* », Il Sole 24 Ore, 23 giugno 2010.

minacce per la sicurezza nazionale derivanti dall'utilizzo dello spazio cibernetico. È stato altresì stabilito di acquisire la consulenza di esperti per supportare utilmente il Comitato nella redazione di una completa Relazione al Parlamento sul tema.

Sono stati quindi affidati incarichi di consulenza alla società *Rand Europe Corporation*, per inquadrare il tema dal punto di vista strategico, tecnologico e normativo; al dottor Andrea Margelletti, presidente del Centro studi internazionale (CESI) con il compito di analizzare i rischi per la sicurezza nazionale del *cyber-crime* negli ambiti governativi e militari, e al dottor Alessandro Politi, analista OSINT, per l'analisi delle eventuali ricadute del *cyber-crime* sui settori civili ed economici, tra cui energia e servizi, telecomunicazioni, finanza e trasporti. Ha partecipato, inoltre, alla fase di elaborazione dei testi il dottor Gianluca Ansalone.

Il Comitato ha svolto le audizioni:

– il 2 dicembre 2009 del colonnello Umberto RAPETTO, comandante del Nucleo speciale frodi telematiche della Guardia di Finanza;

– il 16 marzo 2010 del prefetto Giovanni DE GENNARO, direttore generale del DIS;

– il 14 aprile 2010 del dottor Domenico VULPIANI, Consigliere per la sicurezza informatica e la protezione delle infrastrutture critiche della Polizia di Stato;

– il 28 aprile 2010 dei rappresentanti delle società Telecom (dottor Damiano TOSELLI), Vodafone (dottor Gaetano COSCIA), Wind (dottor Vincenzo FOLINO) e H3G (dottor Roberto COSA);

– il 18 maggio 2010 del dottor Raoul CHIESA, consulente dell'UNICRI;

– il 20 maggio 2010 dell'ambasciatore Giancarlo ARAGONA, nella sua qualità di membro del Gruppo di Riflessione Strategica della NATO, impegnato nella definizione del nuovo concetto strategico dell'Alleanza;

– il 1° luglio 2010 di un alto rappresentante del sistema di sicurezza di un governo europeo, con l'obiettivo di valutare le politiche di contrasto alla minaccia adottate in quel Paese.

Inoltre, in data 6 maggio 2010, il presidente del Comitato, onorevole Massimo D'Alema, d'intesa con il relatore, senatore Francesco Rutelli, ha inviato a soggetti istituzionali e società, individuati per la loro particolare e specifica competenza nel settore, una richiesta volta a conoscere le loro valutazioni « *sull'evoluzione della minaccia e le tendenze prevedibili; sulle strategie di prevenzione adottate sotto il profilo aziendale, sul contributo alla tutela delle infrastrutture critiche nazionali, nonché sulla qualità della collaborazione con le istituzioni preposte* ».

Tutti coloro che sono stati interpellati hanno fornito il loro contributo trasmettendo al Comitato un documento che è stato acquisito agli atti dell'indagine. In particolare:

• la Terna SpA ha trasmesso un elaborato dal titolo « Nota sui rischi alla sicurezza nazionale derivanti dal *cyber-crime* »;

• la Sogei ha trasmesso una « Nota riguardante il *cyber-crime*: strategie di prevenzione della minaccia »;

• la Finmeccanica ha inviato un elaborato dal titolo « *Cyber-security – Cyber warfare*. Definizioni, descrizione »;

• la RFI – Rete Ferroviaria Italiana ha inviato una relazione su « Strategie di Rete Ferroviaria Italiana per il contrasto al *cyber-crime* »;

• l'ENI ha trasmesso una « Nota di approfondimento sui rischi per la sicurezza nazionale derivanti dal *cyber-crime* »;

• l'ABI – Associazione bancaria italiana – ha inviato un elaborato dal titolo « Valutazioni in merito al fenomeno del *cyber-crime* nel settore bancario italiano »;

• Poste italiane ha inviato una relazione dal titolo « *Cybercrime* e *cybersecurity* »;

• il Garante per la protezione dei dati personali, professor Francesco Pizzetti, ha trasmesso il documento « Rischi derivanti dal *cyber-crime*: quadro nazionale e ruolo dell'Autorità ».

3. Sicurezza globale ed utilizzo dello spazio cibernetico: definire il fenomeno.

Il *cyber*-spazio non è più solo lo spazio di diffusione per i mezzi di comunicazione di massa, da quelli tradizionali a quelli a più elevate vocazioni innovative. Esso è piuttosto un nuovo continente, ricco di risorse ma anche di insidie. Di fronte alla crescente militarizzazione di questo spazio, i governi del pianeta – ed in particolare le grandi potenze – sono impegnati in una accelerata competizione. La Russia ha ereditato dall'URSS un sistema, noto con l'acronimo di Sorm-2, in grado di copiare in *backup* ed in tempo reale qualsiasi singolo *bit* (10) che transita nello spazio sovrano russo. La Cina ha attrezzato una rete difensiva nazionale, una sorta di enorme filtro in grado di scremare le informazioni di navigazione su internet considerate dannose, sgradite al governo centrale.

Negli anni '60 dello scorso secolo il primato strategico tra USA e URSS si affermava con le missioni spaziali e i satelliti spia; oggi la competizione per la sicurezza si sta spostando rapidamente sulle reti tecnologiche. Non a caso, la relazione annuale presentata nel 2010 al Comitato parlamentare per i servizi di informazione da Dennis Blair,

---

(10) *Binary digit* (cifra binaria): Unità di misura elementare di informazioni dei calcolatori.

allora direttore della *National Intelligence* americana pone la minaccia cibernetica al primo posto, per la crescita esponenziale della capacità di « rubare, corrompere, danneggiare o distruggere gli *asset* pubblici e privati essenziali per la nazione americana ».

Tocca a ciascun Paese, e anche all'Italia, occuparsi di queste minacce che incidono in maniera profonda su qualsiasi attività economica, sociale e istituzionale delle nostre comunità.

Chi ha una responsabilità pubblica nei sistemi democratici occidentali dovrà cercare di conciliare in maniera efficace la prevenzione delle minacce con il pieno godimento dei diritti di ciascun cittadino, tra cui rientrano quelli alla riservatezza delle comunicazioni e alla libertà di espressione e di pensiero.

I tre elementi costitutivi dello Stato nazionale sono direttamente coinvolti dal potenziale utilizzo per fini criminali delle reti informatiche: l'individuo, il sistema economico e le istituzioni.

Nel primo caso, possiamo considerare il criminale virtuale come una versione contemporanea del truffatore *d'antan* e la frode telematica come una diversificazione di portafoglio per i *network* criminali transnazionali, la cui capacità finanziaria è alimentata anche da questi circuiti.

Gli internauti e gli operatori economici sono i bersagli privilegiati di una congerie di criminali dal profilo molto diverso: dai variopinti *hacker*, eroi o anti-eroi della pubblicistica, fino a strutture ben organizzate e aggressive, che originano dalle mafie transnazionali, dalle reti di criminalità finanziaria e anche dalle reti terroristiche.

Ma è sul terreno della competizione strategica tra Stati che si gioca la posta più alta, che influirà sui nuovi equilibri internazionali.

Concettualmente, occorre acquisire un elemento importante: quei Paesi che definiscono pubblicamente strategie e meccanismi difensivi rispetto alle minacce cibernetiche sono in grado di organizzare in parallelo capacità offensive. Si stanno formando, cioè, dottrine di impiego che sono basate sulla capacità di attaccare un potenziale nemico, di azzerarne le difese e colpirne obiettivi strategici, anche come parte di pianificazioni di attacchi militari, senza che esistano definizioni condivise di questo nuovo spazio di competizione e potenziale contrapposizione strategica.

A sua volta, la sicurezza delle infrastrutture informatiche che assicurano il funzionamento delle linee critiche è divenuta una priorità nella ridefinizione della sicurezza nazionale: infrastrutture logistiche e di viabilità, reti elettriche e telefoniche, *pipeline* per il trasporto di idrocarburi, circuiti finanziari sono reti di sensibilità strategica per la vita di un Paese. Non meno sensibili dei comandi satellitari e dei sistemi di controllo del traffico aereo sono le reti e i dialoghi tra macchine che muovono generatori, dighe, ascensori, pompe, treni, piattaforme petrolifere. I *network* informatici e telematici ne rappresentano una metastruttura, una « rete delle reti », il cui danneggiamento può provocare il *black-out* delle operazioni, dalle più elementari a quelle vitali. Un attacco ai nodi sensibili di connessione tra questi *network* può « accecare » parti importanti dei sistemi esistenti. La novità delle minacce legate al *cyber*-spazio è che