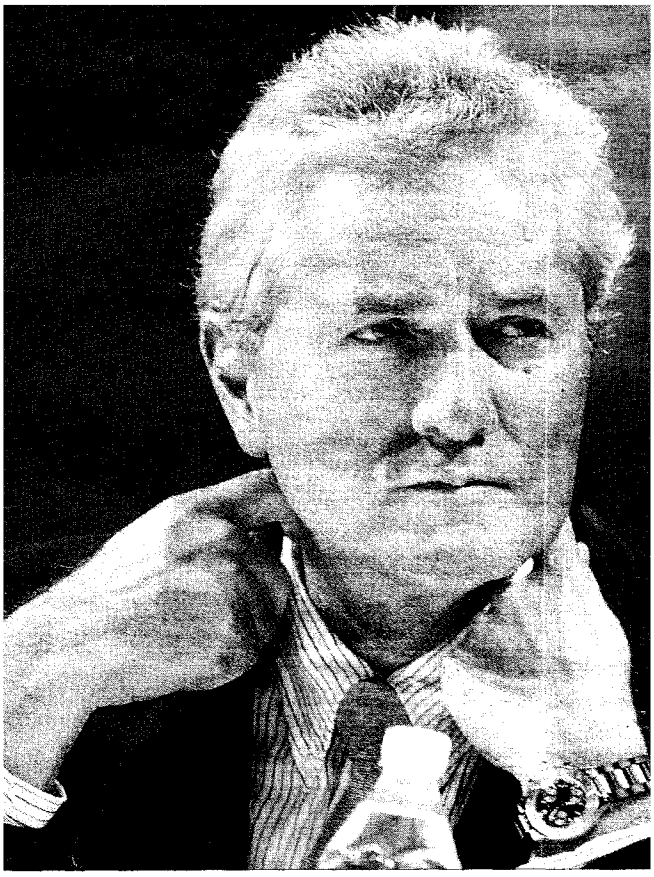
GUERRE INFORMATICHE. LA RELAZIONE DI RUTELLI AL COMITATO PARLAMENTARE PRESIEDUTO DA D'ALEMA

L'Italia senza difese dal cyber-spazio L'appello del Copasir



LE MINACCE PER IL PAESE. In ottanta pagine i pericoli che provengono da un vero e proprio «continente nuovo». La richiesta a Palazzo Chigi di istituire una task-force per elaborare una nuova «strategia per la sicurezza della Repubblica».

DI FABRIZIO D'ESPOSITO

Ottanta pagine per tracciare i pericoli che arrivano da «un continente nuovo» vero e proprio e che potrebbero portare a una «guerra informatica tra grandi potenze» dagli effetti «più devastanti di uno tsunami». Il continente nuovo è il cyber-spazio, tout court. E le ottanta pagine sono quelle della relazione approvata il 7 luglio scorso dal Copasir, il Comitato parlamentare per la sicurezza della Repubblica presieduto da Massimo D'Alema. Titolo: «Possibili implicazioni e minacce per la sicurezza nazionale derivanti dall'utilizzo dello spazio cibernetico». Un lavoro avviato dal predecessore di D'Alema, Francesco Rutelli, che è anche relatore del corposo documento. Dopo la Guerra Fredda, dunque, la competizione tecnologica tra Stati è approdata a una dimensione più virtuale e meno militare. Con una variabile enorme favorita dalla globalizzazione: l'asimmetria degli attori (le reti criminali che truffano a scopo di lucro, i terroristi fondamentalisti, le agenzie di spionaggio non governative) cui spesso è impossibile risalire. Questo il perimetro dell'analisi: «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».

Di qui, la frammentazione del potere, «vera novità di questo XXI secolo». Così mentre una volta la competizione tecnologica segnava una gerarchia tra paesi, adesso succede il contrario. Ecco i dati che riassumono la questione: «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 informazioni 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». Sul fronte della sicurezza virtuale, gli Stati Uniti sono il paese più attivo, con l'istituzione di un Cyber com-

mand presso il Pentagono, «forte di quasi 90mila uomini». In pratica, un esercito schierato su un confine invisibile. Ma la vera sorpresa, secondo la relazione del Copasir, è la Cina comunista, che già nel 1999 aveva fornito un contenuto dottrinale alla militarizzazione dello spazio cibernetico: «Secondo uno studio dell'*Institute for Security Technology Studies* 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 e il 2005, centinaia di computer 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».

Nella preparazione del documento, il Copasir ha svolto un lungo elenco di audizioni nonché acquisito note sulla sicurezza fornite da società e associazioni: Terna spa, Finmeccanica, Sogei, Rfi, Eni, Abi, Poste italiane. Un lavoro di elaborazione che ha portato a suddividere le minacce provenienti dal cyber-spazio in quattro tipologie: cyber-crime (organizzazioni specializzate in truffa, furto d'identità, sottrazione indebita di informazion o di creazioni e proprietà intellettuali); cyber terrorism (utilizzo della rete a fini di propaganda, denigrazione o affiliazione da parte di gruppi terroristici); cyber espionage (furto di segreti industriali sia civili sia militari); cyber war (scenari relativi a guerre informatiche tra nazioni).

In questo contesto, l'Italia si ritrova come «organo primario nella lotta contro il cyber-crime» la Polizia Postale. Ma il punto nevralgico è «la dimensione globale della minaccia cibernetica». E in questo caso c'è ancora parecchio da fare. La raccomandazione finale è al premier e al governo, con l'istituzione di una task-force coordinata da Palazzo Chigi: «Il limite principale si riscontra nella dimensione della prevenzione della minaccia e nell'assenza di una pianificazione coordinata ed unitaria al livello del vertice politico per mettere al sicuro il più possibile i sistemi strategici nazionali connessi alla rete informatica. Per ovviare a tali carenze, si ritiene di dover raccomandare al governo di dotarsi di un impianto strategico-organizzativo che assicuri una leadership adeguata e predisponga chiare linee politiche per il contrasto alle minacce e il coordinamento tra gli attori interessati. Tale obiettivo potrebbe essere raggiunto assegnando questi compiti ad una struttura di coordinamento presso il presidente del Consiglio dei ministri, o presso l'Autorità delegata, organizzata ridefinendo l'attività delle strutture esistenti, con una rimodulazione delle attuali competenze e responsabilità». Una struttura cui dovrebbe essere assegnati vari compiti per formulare una «Strategia per la Sicurezza della Repubblica». Tre in particolare: «Definire compiutamente la minaccia e predisporre un documento di sicurezza nazionale dedicato alla protezione delle infrastrutture critiche materiali e immateriali; predisporre un piano d'intervento che definisca il perimetro della sicurezza cibernetica italiana, definendo i ruoli e le responsabilità di tutti i soggetti responsabili della sicurezza informatica nazionale; redigere, in stretto coordinamento con gli interlocutori istituzionali e privati, a cominciare dai nostri apparati di intelligence, le politiche strategiche di protezione, resilienza e sicurezza cibernetica».

(ha collaborato Angela Gennaro)

DALLA RELAZIONE

«Lo spazio cibernetico è un nuovo fondamentale campo di battaglia e di competizione geopolitica nel XXI secolo. 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»


Italia

L'Italia senza difese dal cyber-spazio L'appello del Copasir