Il racconto di scenari apocalittici alimenta negli Usa il mercato della sicurezza: un giro d'affari di 14 miliardi di euro l'anno. Anche la Nato voleva occuparsene, ma l'Europa non ci è cascata.

L'Unità, *12 dic. 2010*

di **Pino Arlacchi**

«Nell'arco di un quarto d'ora, 157 grandi aree metropolitane sono state messe in ginocchio da un blackout elettrico che le ha colpite durante l'ora di punta. Nuvole di gas velenosi si estendono sopra Wilmington e Houston. Le riserve di petrolio di molte città stanno bruciando nelle raffinerie in fiamme. I convogli delle metropolitane di New York, Oakland, Washington e Los Angeles si sono scontrati l'un l'altro. Gli aeroplani precipitano uno dopo l'altro a causa delle collisioni nelle aerovie fuori controllo. Le vittime sono già migliaia».

Questo è lo scenario evocato dal più noto esperto americano di cybersecurity, Richard Clarke, ex-esperto di criminalità sotto Clinton, ed ex-amico mio.

La causa dell'Apocalisse? Un attacco terroristico ai sistemi di gestione dell'energia elettrica e dei trasporti, ormai largamente informatizzati. Le probabilità dell'Apocalisse? Vicine allo zero. Molto inferiori a quelle di uno scontro tra la terra e un asteroide vagante. Non sto esagerando. Studiosi del calcolo delle probabilità ed astronomi hanno misurato proprio questo tipo di rischi. Perché è da queste misurazioni che dipendono le politiche di protezione. O meglio, dovrebbero dipendere, dato che in questo campo il terrore, la disinformazione e la truffa regnano incontrastati.

Fino a questo momento, il virus della paura indotta da una minaccia super-gonfiata come quella del terrorismo informatico ha contagiato un solo paese, gli Stati Uniti. Ma lì la produzione di panico è uno dei business più fiorenti, tanto che qualcuno già parla di un "complesso militare-informatico" che fattura oltre 14 miliardi dollari all'anno.

Il business che ha fatto ricco il mio ex-amico Clarke, titolare della Good Harbor consulting, azienda di cybersecurity ed altro. I suoi consigli sono quasi infallibili, data le probabilità che le minacce da cui vuole proteggere i suoi clienti hanno di materializzarsi.

Nella vecchia Europa e nel resto del mondo c'è poca voglia di tremare di paura al pensiero

degli hacker che mettono a ferro e a fuoco un paese per ordine di un gruppo terroristico o di una potenza ostile. Un mese fa, il segretario generale della NATO è stato severamente criticato, durante un'audizione al Parlamento europeo, da alcuni deputati che gli hanno chiesto di portare uno straccio di prova a sostegno della necessità che anche l'Alleanza atlantica si occupi della delinquenza informatica. La sua risposta semplicemente non c'è stata. E non per dovere di riservatezza, ma per imbarazzo dovuto a debolezza di argomenti.

Le fantasie a pagamento dei profeti di sventura si sono sposate, però, con gli interessi dell' l'industria mediatica globale. Essa sta tentando di forzare la mano diffondendo le più inverosimili fesserie, come quella del quindicenne con i brufoli che riesce a forzare i codici di accesso del Pentagono e raggiungere la stanza dei bottoni dei missili nucleari.

In realtà, quasi tutti gli esperti sia di terrorismo che di informatica che non campano del panico altrui sono concordi nel ridimensionare drasticamente la scala dei danni che la criminalità e la guerra informatica hanno inflitto finora, o che possono infliggere, a un sistema paese o a una rete logistica e comunicativa. Gli argomenti-chiave sono tre:

La debolezza dei moventi. In un mondo nel quale le strategie di competizione e di dominio tra gli stati si basano sempre più sul "soft power" (vedi il successo di Cina, Unione europea, Brasile, India, Russia, Turchia e simili), diminuisce anche l'incentivo a iniziare una guerra o un'azione di destabilizzazione grave per via informatica. «Perché mandare in tilt Wall Street? – ha risposto un hacker cinese ben informato – quando ne siamo i proprietari? ».

La superiorità delle armi tradizionali. Ciò vale soprattutto per i gruppi terroristici i quali hanno valutato più volte l' uso di tecnologie informatiche o di armi non convenzionali, optando invariabilmente per strumenti semplici ed affidabili come esplosivi, armi leggere, coltelli. L' 11 settembre è stato fatto usando dei tagliacarte e non delle tastiere. Il numero dei morti per terrorismo informatico finora è zero. E anche il terrorismo va decrescendo.

La forza dei sistemi di protezione. I profeti della sventura informatica descrivono sequenze di atti catastrofici come se dall'altro lato non ci sia nessuno a reagire. Ed omettendo dolosamente di informare il pubblico su alcuni fatti che ridurrebbero del 98% il volume del pallone che stanno gonfiando. Il più importante è che i sistemi davvero sensibili non sono fisicamente connessi ad Internet e sono quindi inaccessibili ad hacker e terroristi. Le agenzie di intelligence e di polizia, le forze armate, il controllo del traffico aereo e della distribuzione dell' energia elettrica, le centrali nucleari, non comunicano con alcuna rete esterna, e neppure tra di loro. Sono sistemi chiusi, e non da oggi, ma dall' inizio dell' era informatica. Non usano software commerciali, ma se li fanno confezionare su misura.

Ciò provoca un altro tipo di problemi, quello della non-condivisione delle informazioni tra agenzie di sicurezza, che è molto più serio di quello del terrorismo informatico, e che avrebbe potuto far evitare l'11 settembre. Ma nessuno ne parla perché non è sexy, non si presta a produrre paura e non fa fare soldi.