Autore: Enrico Novari - *Luglio 1999*

Alla ricerca dei perchè della rete

D) ***Il dott. Lorenzo Valeri è ricercatore presso l'Information Warfare Programme of ICSA. In cosa consiste la sua attività? Per conto di chi viene svolta? Quali scopi si prefigge?***

R) La mia attività di ricerca consiste nell'analizzare l'impatto di Internet e delle sue tecnologie dal punto di vista strategico e militare. In particolare, il mio interesse si sta concretizzando in una tesi di dottorato sponsorizzata dalla Marie Curie Research Fellowship della Commissione Europea, che vuole analizzare se le organizzazioni statali e le multinazionali collaborino o meno nello sviluppare strumenti e regolamenti nel campo della sicurezza informatica.
L'International Centre for Security Analsys fa parte del Dipartimento di Studi di Guerra del King's College di Londra. Il centro, che svolge principalmente funzioni di consulenza per certi dipartimenti del governo inglese ed alcune societ, Ë stato fondato nell'ottobre 1996, assumendo una precisa fisionomia solo nell'aprile 1997. I nostri progetti sono essenzialmente volti a seguire sviluppi commerciali, tecnologici e legislativi nel campo della sicurezza informatica, di cui vengono analizzati i diversi impatti. Un particolare interesse è diretto a studiare come i terroristi e altri gruppi utilizzano Internet nelle loro attivit. Il nostro obiettivo è riscontrabile nel fornire risposte accademiche, spesso anche contrarie alle normali correnti di pensiero sull'argomento, alle organizzazioni che devono affrontare problematiche di sicurezza informatica quando s'imbattono nella rete.Maggiori informazioni sulle nostre attività sono disponibili sul nostro sito http://www.kcl.ac.uk/orgs/icsa/

D) ***Per Information Warfare s'intende, comunemente, l'insieme di azioni volte a compromettere sistemi informatici e di comunicazione civili e militari del nemico, e la simultanea protezione da simili attacchi portati da esterni. Un estraneo a tale tematica potrebbe pensare alla trama di un film di fantascienza o ad una copertura per studi di altro genere. Si è mai trovato a dover convincere qualcuno sull'effettiva importanza ed attualità di tale tematica? Quali strumenti dialettici ha utilizzato?***

R) Come detto precedentemente, i miei colleghi ed io cerchiamo di dare risposte accademiche ad un argomento dove le speculazioni e gli approcci tipo "teorie della cospirazione" abbondano enormemente. L'Information Warfare ha attirato molta attenzione da parte di vari giornalisti e scrittori. In fondo è comprensibile, visto che combina una certa paura per lo strumento "Internet" con un innato interesse di molte persone per terrorismo e crimine organizzato. Il mio approccio, che devo dire si basa esclusivamente su dati di origine non classificata,è quello di pormi sempre la domanda "perchè"? Perchè un gruppo terrorista vuole usare Internet con scopi diversi rispetto ai più comuni (es. propaganda, comunicazione)? Lo stesso per il crimine organizzato: perchè un gruppo mafioso vuole entrare dentro banche dati, quali sono i suoi obbiettivi, quali azioni rientrano nella sua strategia? Cerco di sviluppare simili argomentazioni per analizzare il rischio di operazioni di Information Warfare relative a possibili attacchi informatici, se così vogliamo definirli, organizzati anche da multinazionali ed organizzazioni di Intelligence. Partendo dalle mie risposte a simili "perchè", sono riuscito a presentare delle risposte abbastanza logiche che alcuni addetti ai lavori hanno valutato positivamente. In conclusione, il mio principio per studiare l'Information Warfare è: dietro ogni attività umana c'è sempre una ragione, una motivazione, uno scopo, soprattutto quando tale attività si sviluppa in un campo come quello informatico, che richiede molto lavoro, studio e dedizione.

D) ***In un articolo dello scorso anno lei suggeriva una classificazione degli attori dell'Information Warfare composta di hackers, mercenari delle tecnologie (compresi terroristi e mafie) ed organizzazioni statali. Ad un anno di distanza gli attori sociali di tale scenario sono rimasti gli stessi o denota delle differenze? Nello stesso articolo, la sua conclusione citava la necessit di un maggiore potenziamento delle difese informatiche, dovuto alla notevole velocità con cui s'implementavano e miglioravano le tecnologie d'attacco. Ad un anno di distanza come giudica tale sviluppo delle difese informatiche rispetto ai reali rischi che esse corrono?***

R) Assumo che lei si riferisca all'articolo apparso su "Limes", la rivista italiana di Geopolitica. In linea generale confermo quanto scritto in quella occasione. Devo anche aggiungere che tale classificazione non è certo nuova, soprattutto se si analizzano alcuni studi compiuti, tra la fine degli anni 70 ed i primi anni 80, ;da parte della US Department of Defence, oppure dalla Rand Corporation sotto l'egida di William Ware.
Giova inoltre ricordare che tali studi sono disponibili su CD facendone richiesta al Department of Computer Science della University of California, Davis, dove si sta svolgendo un progetto di ricerca sulla storia della sicurezza informatica. Le novità da me introdotte riguardano la sottoclassificazione di ognuno di questi agenti. Per quanto concerne gli hackers/crackers, è necessario fare importanti differenziazioni in base all'età, alle motivazioni ed ai rischi. Inoltre, con il crescente successo di LINUX e di altri open source software,è importante differenziare tra hackers (termine di connotazione positiva sviluppato da Richard Stallman del GNU project) e crackers. Riguardo ai terroristi, sto attualmente lavorando su una specifica classificazione. Non mi pare di scorgere alcun movimento in questa direzione da parte di gruppi terroristici mediorientali, forse a causa di motivi politici, tecnici e di propaganda. Vedo invece un trend in questa direzione nei gruppi terroristici come White Supremaciss, Patriots e Militia. Questi gruppi, agendo in un ambiente come gli USA dove Internet è particolarmente sviluppato, hanno

una migliore percezione delle capacità offensive di questo strumento. Inoltre, molti governi occidentali puntano su Internet come strumento di successo economico. Un gruppo ideologicamente contrario a questi governi può usare la rete per provare ad incidere su queste politiche. E' importante sottolineare che l'utente medio ha paura di Internet e, se non rassicurato, non fornisce il proprio numero di carta di credito on-line facilmente. Se poi vede che siti governativi vengono penetrati costantemente si può chiedere: ma se la CIA non e' sicura, come può esserlo una certa http://www...com di cui non so niente? Il terrorista può giocare su questa paura. Devo ammette che per quanto concerne il crimine organizzato, ritengo le mie assunzioni iniziali ancora valide, tuttavia non dimentico quanta ricerca deve essere ancora effettuata per capire meglio il fenomeno.

D) ***Uno degli scenari che vengono citati, addentrandosi nel suo campo, èla possibilità che un domani si arrivi a combattere una guerra senza alzarsi dal monitor del proprio computer, un conflitto iper-tecnologico rapido ed incisivo come, la Serbia insegna, raramente lo sono le guerre attuali. Ritiene possibile tale scenario? A che punto siamo lungo lo sviluppo che porterebbe a tale modalità di conflitto?***

R) La guerra è morte, è sangue, ed Internet non cambierà certo questo modo di essere, non arriverà mai a sostituire, purtroppo, l'utilizzo della violenza fisica. Quello che Internet e le altre tecnologie fanno è rendere gli strumenti più efficienti, sebbene l'errore umano sia sempre in agguato come dimostrato dagli errori nei bombardamenti della NATO. La mia risposta è: nel mondo dei sogni, forse, una guerra potrebbe svolgersi solo con il computer; la realtà è molto differente come dimostrato dalla guerra in Serbia.

D) ***L'inglese Duncan Campbell, nel suo recente rapporto per conto dello Scientific and Technical Option Assesment office del Parlamento Europeo, ha descritto il sistema Echelon come in grossa difficoltà, in via di trasformazione. Non sarebbe più capace di distinguere ogni parola basandosi su codici-chiave, incapace di rispondere alle complicazioni tecnologiche che arrivano dal fronte dei nuovi sistemi di comunicazione. Nella sua veste di esperto del settore, come giudica tale rapporto? Il tentativo di ridimensionare un reale pericolo per la nostra privacy o la reale descrizione di un sistema d'intercettazione realmente indietro coi tempi? In generale, qualè la sua opinione in merito a tale strumento ed al suo reale utilizzo dal 1947 ad oggi?***

R) Come tutti i rapporti, per un ricercatore come me essi sono essenziali per studiare un fenomeno complicato come quello dell'Intelligence, soprattutto la così detta COMINT, COMmunication INTelligence. E' difficile esprimere un giudizio sulla validità della affermazioni di Campbell su tali tecnologie. Personalmente, considero forse le sue affermazioni esagerate, visto che una delle regole dell'Intelligence sta nel non dire come le cose vengono effettivamente fatte. Considero interessante che questo aspetto sia stato confermato da Withfield Diffie, colui che viene sovente indicato come l'inventore del sistema di crittografia a chiave asimmetrico, anche se un simile studio era stato sviluppato alcuni anni prima dal GCHQ di Cheltenham. Visto che di parla di tecnologie segrete da utilizzare per attività particolari, non vedo proprio come Campbell, attualmente corrispondente del "Guardian" a San Francisco, possa avere una conoscenza di tali strumenti. Non sono personalmente in grado di dare un giudizio sull'attuale efficacia di Echelon, come nel passato e nel futuro. Tuttavia, vorrei dire che questi strumenti e organizzazioni funzionano perchè non lasciano mai trapelare come fanno le cose. Come detto prima, per chiunque abbia degli interessi in questo campo meno si viene a sapere al riguardo e meglio è. Questo comprende anche il parlare in pubblico. Di conseguenza, sono sempre attuali accuse di efficienza o scenari da "grande fratello orwelliano" da parte di giornalisti. In conclusione, il mio giudizio sui rapporti relativi allo STOA non è granchè positivo , in quanto non hanno indicato niente di nuovo visto che le informazioni proposte erano già liberamente disponibili, e non in posti secreti ma in normali biblioteche di scienze informatiche, senza andare tanto lontano. Rimango molto interdetto dal fatto che questi rapporti siano stati sponsorizzati dal Parlamento Europeo, quindi da una istituzione, ed ho forti dubbi sulla loro indipendenza da una specifica via politica. Nel futuro sarebbe interessante che si facessero degli studi differenti da questi.

D) ***Il mese scorso, negli USA, si è svolto il processo a Kevin Mitnick, per alcuni simbolo di libertà e contro-utilizzo dei mezzi informatici rispetto a quelli generalmente consigliati, per altri esempio di criminalità informatica e destabilizzazione del sistema. Lei come si pone nel difficile giudizio su tale individuo e sul significato del suo operato? Esiste il rischio che diventi il capro espiatorio di un sistema che sta sfuggendo di mano a chi intendeva usare la rete come strumento di controllo generalizzato? Che il suo caso diventi uno strumento in mano a chi si occupa di difese informatiche per richiedere un budget più alto, più attenzione dai media e pene più severe per i prossimi Mitnick?***

R) Sul processo di Mitnick ci sarebbe molto da scrivere. Personalmente ritengo giusto che questo personaggio sia finito in galera per il bene dello sviluppo di Internet e del commercio elettronico. Si possono esprimere delle riserve su come sia stato trattato Mitnick in carcere, sul suo reale pericolo. Tuttavia, non lo considero assolutamente un capro espiatorio. Certamente il suo caso ha aperto la porta ad enormi problemi ad esso collegati, tuttora insoluti, che devono essere risolti al più presto.