Zeitschrift: Rivista militare della Svizzera italiana
Herausgeber: Lugano : Amministrazione RMSI
Band: 73 (2001)
Heft: 6

Artikel: La guerra dell'informazione come strategia militare e civile
Autor: Sibilia, Riccardo
DOI: https://doi.org/10.5169/seals-247517

La guerra dell'informazione come strategia militare e civile

Cap Riccardo Sibilia

Resoconto del simposio "Information Warfare" (21-23 novembre) dell'Associazione degli Ufficiali delle Forze Aeree (AVIA) ed alcune considerazioni personali.

Dire che l'informazione è la risorsa fondamentale che per quantità e qualità influenza direttamente la presa di decisione e quindi il successo di qualsiasi impresa, è un'asserzione tanto banale quanto vera. Già nel 500 a.C. lo stratega e generale cinese "Sun Tzu" teorizzava (e metteva in pratica) delle metodologie di guerra contro la condotta e considerava sia l'aspetto della superiorità dell'informazione (avere più e migliori informazioni sul nemico rispetto ad esso) che l'aspetto della presa di decisione avversaria (confondere l'avversario, guerra psicologica).

L'avvento delle moderne tecnologie dell'informazione facilitano e ottimizzano da un lato i processi decisionali a tutti i livelli (p.e. la guida radar di un missile, i sistemi di comando e controllo a livello tattico, operativo o strategico ma anche gli utensili di decisione per il settore civile in ambito industriale o bancario), ma nel contempo espongono tali processi a nuove forme di minacce che per i diretti interessati sono spesso difficili da concepire e evitare e ancora più difficili da riconoscere una volta attive.

La guerra dell'informazione è nata concettualmente all'inizio degli anni 90. I principali attori in questo campo erano e sono gli Stati Uniti. Se essi dispongono da un lato della necessaria dominanza tecnologica per al meglio poter sfruttare questa forma di conflitto in maniera offensiva, è altresì vero che la fortissima dipendenza da tecnologie dell'informazione in ambito militare ma soprattutto civile li rende estremamente vulnerabili ad un uso asimmetrico di questa strategia.

Nel corso di questo decennio, sia la dottrina che i mezzi d'impiego in questo campo sono stati sviluppati ed affinati enormemente. Specialmente i settori della guerra psicologica e del "Computer Network Defense and Attack" hanno approfittato di fondi di ricerca piuttosto grossi negli USA ed in altri paesi quali Francia, Inghilterra, Israele, Cina, Svezia e altri.

Se gli stati giocano un ruolo importante, gli attori non statali guadagnano la possibilità di sfruttare le debolezze dei processi decisionali odierni con dei mezzi del tutto simili a quelli sviluppati nel settore militare. In molti casi è addirittura il settore militare e governamentale ad approfittare degli sviluppi e delle scoperte civili. Per esempio, nell'ambito del "Computer Network Attack", si sa che organizzazioni come la "National Security Agency" (NSA) sviluppano e usano tecniche di hacking e viri informatici per acquisire ed eventualmente manipolare e cancellare informazioni su sistemi informatici. Il "Federal Bureau of Investigation" (FBI) ha recentemente iniziato un programma di sviluppo per un cavallo di troia per facilitare le indagini e l'ascolto legale su sistemi informatici. Queste tecniche, prima prerogativa di studenti sedicenni dotati di PC e di modem, sono ora diventate delle "armi" o dei mezzi di intelligence.

Al simposio dell'AVIA ci siamo prefissi lo scopo di dare una vista d'insieme sul soggetto coprendo aspetti militari e civili, da strategici a tattici. Distribuiti su tre giorni sono stati trattati rispettivamente la guerra dell'informazione in una prospettiva militare, la protezione dell'infrastruttura critica civile e gli aspetti strategici civile e per terminare gli aspetti tecnici e le soluzioni per proteggersi dalle minacce informatiche.

In fine di serata del secondo giorno si è anche svolto un corso d'introduzione che è stato anche seguito dai partecipanti al corso di stato maggiore generale.

Il referente principale del primo giorno, Prof. Dan Kuehl della prestigiosa "National Defence University" di Washington ha presentato la vista d'insieme di questo settore negli Stati Uniti, piazzandolo nel contesto strategico e ha elucidato i possibili sviluppi futuri. I referenti elvetici hanno presentato lo stato dei lavori all'interno del dipartimento della difesa, in particolare il sig. Vernez del gruppo operazioni dello stato maggiore generale ha presentato lo stato dei lavori di un gruppo di specialisti del settore per gettare le basi di una dottrina della guerra dell'informazione. Il ten col SMG Lingg ha presentato nel suo ruolo di istruttore parte del programma d'insegnamento che viene impartito ai corsi di condotta e stato maggiore di Lucerna.

In qualità di insegnate e ricercatore presso la "Freie Universität" di Berlino e cittadino della Repubblica popolare Cinese, il Dr. Zhang ha presentato in ma-

Per concludere si può dire che il simposio ha permesso di avere una visione d'insieme sulla guerra dell'informazione e ha mostrato come il fatto che si usi la parola "guerra" non significa che il problema sia da relegare ai militari o che la preponderanza delle questioni tecnologiche ne faccia un tema per pochi specialisti di informatica. Al contrario è un problema che riguarda tutti (lo stato, le aziende, il militare ma anche il singolo cittadino) e che le soluzioni si possono solo trovare se chi ha il privilegio e dovere di decidere (direttore aziendale, personalità politica o quadro dell'esercito che sia) si ritrova con una sufficiente cognizione di causa e capisce la necessità di agire.

niera molto impressionante gli sviluppi e le tendenze in questo settore nel suo paese d'origine. In particolare ha enfatizzato il fatto che nei prossimi anni ci si potrà attendere una comunità attiva di hackers in Cina per quantità senza confronto nel mondo occidentale.

Gli aspetti psicologici della guerra dell'informazione sono stati trattati nella presentazione del generale di brigata (a riposo) Loup Francart (forze armate francesi). Egli ha aperto la sua conferenza con la frase "se non si dice il perché, il cosa e il come delle proprie azioni, altri se ne occuperanno, perseguendo però i propri interessi". Nella sua presentazione ha poi descritto gli aspetti che caratterizzano l'ambiente psicologico (in particolare in una situazione di conflitto) e i fattori che possono influenzarlo o essere usati per plasmarlo.

Un tuffo nella tecnica dell'informazione si è avuto con la presentazione di Dennis McCallam della ditta Logicon, Inc. (oggi di proprietà della Northrop Grumman, Inc.). Egli ha dimostrato in maniera chiara e lampante che con le nostre misure di protezione delle reti basate su uno o più "firewall" standard e un sistema anti-virus (così com'è uso comune in Europa e in Svizzera) ci troviamo alla preistoria della tecnica di sicurezza informatica. Le forze aeree americane impiegano sistemi in grado non solo di rispondere dinamicamente ad un attacco su rete e di allarmare in tempo reale un'apposita unità di sorveglianza, ma anche di ripristinare il servizio prodotto da un certo sistema e di verificare continuamente la consistenza dei dati trattati. Con questo sistema, una manipolazione dei dati anche molto perfezionata ha poche possibilità di passare inosservata.

L'ultima presentazione della giornata è stata offerta dal sig. Olaf Lukas della ditta "Rohde und Schwarz". Questa ditta è da anni uno dei leader dei sistemi di esplorazione e sorveglianza elettronica e di sicurezza ed è quindi stato estremamente interessante ascoltare a cosa ci si può attendere nella dimensione elettromagnetica del moderno campo di battaglia (p.es. l'ascolto e il disturbo di comunicazioni satellitari o l'importanza ed il ruolo dei sistemi di telecomunicazione civili per le moderne operazioni militari).

La prima giornata si è conclusa con una discussione con tutti gli autori e il pubblico, condotta magistralmente dal "chairman" della conferenza, Div Peter Regli. La seconda e terza giornata sono state concepite per raggiungere un pubblico di manager nel settore privato e pubblico. Temi di ordine strategico sono stati trattati nel secondo giorno. Al centro soprattutto era la questione della protezione dell'infrastruttura critica di uno stato e del ruolo dello stato nell'assicurare la sicurezza della società dell'informazione. Le attività intraprese in questa direzione in Germania sono state presentate da niente di meno che la direttrice responsabile di questo settore presso l'ufficio federale per la sicurezza delle tecniche dell'informazione di Bonn (Bundesamt für die Sicherheit in der Informationstechnologien), sig.ra Marit Blattner. In questo settore anche in Svizzera ci sono numerose attività che sono state presentate dal sig. Kurt Haering, direttore della fondazione InfoSurance e da Hansperter Lingg, direttore del SICTA (Swiss Information and Communication Technologies Association). Da noi molte attività hanno origine dai diversi gruppi di lavoro formatisi dopo l'esercizio di condotta strategica 97 (SFU 97). In particolare InfoSurance è una fondazione a finanziamento misto pubblico/privato che si prefigge lo scopo di far prendere coscienza del problema e di trovare soluzioni concrete ad un livello strategico di condotta delle imprese e di governo. Anche un rappresentante del centro di ricerca olandese TNO (centro fondato dal ministero della difesa) ha riferito su di uno studio delle vulnerabilità di Internet nei paesi bassi e sulle conseguenze per l'economia privata.

La decisione in caso di crisi a livello strategico in ambito politico / militare erano tema della seconda presentazione del generale Francart. Anche in questo caso un ottimo fondamento teorico e una chiara visione per l'aspetto pratico hanno caratterizzato la presentazione. La buona gestione di una crisi dipende in gran parte dalla preparazione delle persone incaricate e dalla capacità di riconoscere precocemente i segni premonitori della crisi. Egli propone anche una metodologia generale per seguire una crisi nelle sue fasi, sempre tenendo conto dei fattori importanti in ognuna di esse.

Il terzo giorno era in gran parte dedicato alle soluzioni delle vulnerabilità legate alle tecniche dell'informazione. Gli speakers erano per la maggior parte rappresentanti di industria e servizi dell'informazione e informatica e non si sono limitati a presentare o promuovere i loro prodotti, ma hanno portato un vero valore aggiunto in termini di "know-how". Particolarmente interessante erano le presentazioni riguardanti gli approcci di standardizzazione delle pratiche di sicurezza e l'enunciato che la sicurezza è un fattore primario e di qualità di un prodotto informatico e non una funzionalità accessoria. Si sono trattati anche i temi del futuro dei metodi criptografici in software o hardware e quelli di una gestione e analisi per intelligenza artificiale dei protocolli generati da "firewalls" e "intrusion detection systems".

La vulnerabilità delle reti senza fili molto in voga in questi tempi sono pure state oggetto di discussione. Infatti queste reti, senza misure addizionali, sono prone ad attacchi informatici molto semplici da realizzare e con conseguenze spaventose.

Il corso d'introduzione ha visto quattro presentazioni di referenti estremamente competenti. Il divisionario Peter Regli ha presentato i rischi e pericoli che caratterizzano l'era dell'informazione. In particolare si è anche soffermato sulla minaccia asimmetrica e sul ruolo preponderante che la stampa ha nell'ambito della guerra dell'informazione.

Stefan Vogt, direttore della sicurezza per il gruppo UBS ha parlato della gestione del rischio, soprattutto

informatico, a livello di una grande banca in un ambito multinazionale. Inutile dire che i problemi che si pongono possono essere confrontabili a quelli che si presentano ad un'entità come uno stato. Le soluzioni e metodologie presentate permettono di valutare e gestire efficacemente il rischio. Per dirlo con le sue parole "to fail to prepare is to prepare to fail" ossia: mancando di preparasi ci si prepara a fallire.

Per concludere si può dire che il simposio ha permesso di avere una visione d'insieme sulla guerra dell'informazione e ha mostrato come il fatto che si usi la parola "guerra" non significa che il problema sia da relegare ai militari o che la preponderanza delle questioni tecnologiche ne faccia un tema per pochi specialisti di informatica. Al contrario è un problema che riguarda tutti (lo stato, le aziende, il militare ma anche il singolo cittadino) e che le soluzioni si possono solo trovare se chi ha il privilegio e dovere di decidere (direttore aziendale, personalità politica o quadro dell'esercito che sia) si ritrova con una sufficiente cognizione di causa e capisce la necessità di agire.

Un'altro aspetto primario del simposio era favorire il dialogo e la discussione tra i partecipanti e permettere il "networking". L'eccellente direzione dei lavori da parte di Peter Regli, caratterizzata da competenza in materia, simpatia e umore, ha permesso di raggiungere questo scopo.

Anche la buona ristorazione, con dei "lunch buffet" offerti dopo le sessioni, ha influenzato positivamente l'ambiente.

Sia in ambito civile che militare c'è in Svizzera ancora molto da fare per rispondere alla sfida della guerra dell'informazione e – come ha detto il direttore del simposio – in molti casi dormiamo ancora il sonno degli innocenti. Come comitato d'organizzazione crediamo di aver dato un piccolo contributo nella buona direzione. ■

Sia in ambito civile che militare c'è in Svizzera ancora molto da fare per rispondere alla sfida della guerra dell'informazione e in molti casi dormiamo ancora il sonno degli innocenti.

Riccardo Sibilia, dipl. Phys. ETH

Ticinese, domiciliato in canton Argovia, dirige un gruppo di "system engineering" nel campo della sicurezza informatica e criptologia presso la ditta Ascom Systec. Fino alla metà del 2001 era attivo quale collaboratore scientifico al politecnico federale di Zurigo (presso l'istituto di tecnica di sicurezza militare – IMS) dove dal 1995 ha svolto della ricerca nell'ambito della guerra dell'informazione e della rivoluzione negli affari militari (RMA).

Nel comitato d'organizzazione del simposio si è occupato del programma tecnico e della acquisizione dei referenti.

Come miliziano svolge la funzione di ufficiale di condotta di guerra elettronica nella "LW Radar Abt 15", con il grado di capitano.