Difesa

L'ascesa della sicurezza cibernetica

Carlo Trezza
18/01/2012

Le prospettive di un uso militare dello strumento informatico (*cyber warfare*) sono oggetto di crescente attenzione. L'"arma" cibernetica sfugge alla classica distinzione tra armi convenzionali e di distruzione di massa e rientra nella nuova realtà della guerra condotta "in poltrona", di cui i velivoli senza pilota (Uav) sono l'espressione più corrente.

Il mondo è sempre più dipendente dalla rete informatica divenuta ormai parte delle "infrastrutture critiche", al pari delle centrali elettriche, satelliti, strutture aeroportuali e ferroviarie, che sono essenziali per la sopravvivenza di una nazione. Il confronto informatico è già in atto in campo civile: l'interferenza a scopi criminosi occupa sempre più le forze dell'ordine di molti paesi, lo spionaggio industriale con mezzi informatici è divenuto una pratica diffusa.

Quinto scenario

Era inevitabile che emergesse una dimensione militare per proteggersi da possibili azioni di spionaggio e sabotaggio, ma anche per prepararsi ad azioni di natura offensiva. Gli strateghi americani parlano dello spazio cibernetico come quinto scenario bellico che si aggiunge a quello terrestre, marittimo, aereo e spaziale. Nel maggio del 2009 l'infrastruttura digitale venne definita dal presidente Obama "un assetto strategico nazionale". L'anno successivo venne stabilito nel Maryland un Comando cibernetico (*US Cyber Command*). Una struttura operativa analoga risulta esser stata creata nel Regno Unito.

Nel giugno dello scorso anno i ministri della difesa Nato inserirono la *cyber defense* nella pianificazione militare dell'Alleanza. L'Unione europea ha concentrato la propria attenzione sugli aspetti civili attraverso la costituzione di Enisa (*European network and information security agency*) che dal 2004 opera dall'isola di Creta quale piattaforma per lo scambio di informazioni e di migliori pratiche nel campo della sicurezza informatica. Le misure adottate dai rimanenti principali attori internazionali sono meno note: il grado di trasparenza in questo, come in altri settori della sicurezza, è di norma più elevato nel mondo occidentale.

I mezzi di informazione rilevano le capacità di paesi come Cina, India, Israele, Iran e Russia. Quest'ultima è stata indicata quale presunto punto di partenza di attacchi cibernetici contro l'Estonia nel 2007 e la Georgia nel 2008. Finora l'esempio più eclatante è stato l'uso del "verme" informatico denominato *Stutnex* che infiltrò nel 2010 il contestato impianto iraniano di arricchimento dell'uranio di Natanz, danneggiandone le centrifughe e rallentandone la produzione.

Forte sviluppo

Una delle peculiarità dell'arma cibernetica è l'anonimato: è arduo individuare gli autori degli attacchi. Non provoca vittime: distrugge o danneggia apparecchiature, impianti, centri di comunicazioni, ma non colpisce direttamente gli esseri umani. Potrebbe rientrare nella fattispecie delle armi *non letali*, che renderebbero meno cruento l'uso della forza ai fini del mantenimento della pace e l'attuazione del Capitolo VII della Carta dell'Onu. Sono numerose, e ancora da approfondire, le implicazioni etiche, umanitarie e giuridiche (*jus in bello et ad bellum*).

Al vertiginoso sviluppo civile e militare dello strumento informatico non ha corrisposto un'analoga evoluzione sul piano normativo. Poco si è fatto soprattutto per prevenire una corsa agli armamenti. Lo sforzo maggiore è venuto dalle Nazioni Unite. Due seminari dell'Istituto di Ricerche sul disarmo (Unidir) hanno aperto la strada ad una serie di risoluzioni dell'Assemblea generale e ad alcune raccomandazioni del Consiglio consultivo per gli affari del disarmo del segretario generale dell'Onu.

Nel 2010 esperti di quindici paesi (tra cui l'Italia) raccomandarono a Ban Ki moon misure per rafforzare la fiducia e ridurre i rischi nel campo delle tecnologie dell'informazione e della comunicazione. Gli esperti torneranno a riunirsi quest'anno. Nel settembre dello scorso anno Cina, Russia, Tajikistan e Uzbekistan presentarono all'Onu un progetto di Codice di condotta volto a prevenire l'impiego delle tecnologie informatiche a fini ostili.

Opportunità

Sono di rilievo anche gli sviluppi sul piano concettuale e della formazione con il contributo

Vedi anche

La sfida digitale dell'Italia, *di Felice Simonelli*

Futuro digitale per le forze armate, *di Michele Nones, Alessandro Marrone*

Le sfide dell'intelligence nel sistema globale, *di Massimo D'Alema*

Temi

Difesa | Mercato della difesa

Archivio Articoli

Politica estera italiana	Unione europea
Sicurezza, difesa terrorismo	Mediterraneo e Medio Oriente
Economia internazionale	Est Europa e Balcani
Usa e rapporti transatlantici	Africa
Istituzioni internazionali	Asia
Energia e ambiente	America Latina

Gli articoli più letti

delle organizzazioni non governative. La *cyber security* è stata il punto focale di un recente convegno tenutosi ad Andalo (Trento) nel quadro delle attività di Isodarco, la Scuola internazionale sul disarmo e la ricerca sui conflitti, che opera in Italia ed all'estero dal 1966.

Circa quindici docenti e cinquanta studenti provenienti dalle principali università e centri di studio internazionali (numerosi i partecipanti americani, cinesi e russi), hanno affrontato la nuova realtà cibernetica nelle sue molteplici articolazioni. Il corso, animato in gran parte da docenti italiani, ha permesso di fare passi in avanti nella comprensione di un problema sinora visto come materia per pochi iniziati e di portarlo all'attenzione anche dei giovani.

L'impegno dell'Italia non si limita dunque agli interventi nelle sedi multilaterali; il convegno ha posto in luce una nostra nicchia di eccellenza che merita di essere conosciuta e sostenuta.

Il percorso avviato dall'Onu e dalla società civile può apparire lungo e macchinoso. Esso ha permesso tuttavia di portare la questione sotto i riflettori internazionali promuovendo una maggiore trasparenza e prevedibilità. Molto rimane ancora da fare, ma il terreno è oggi più fertile per evitare che la rete web si trasformi da strumento di collaborazione e dialogo in uno strumento di confronto.

Carlo Trezza è Ambasciatore e membro del Consiglio consultivo del segretario generale dell'Onu per le questioni del disarmo.

English summary: Cyber military capabilities to protect states from international espionage and sabotage and to engage in possible offensive actions, are gaining ground. Although the degree of transparency is not uniform, it is believed that all major international players are involved in these activities. Cyber weapons do not fit into the traditional distinction between WMDs and conventional weapons and like the UAVs belong to the category of "armchair" weapons . Because they damage or destroy equipment, critical infrastructure, and communication centers rather than directly harming human beings, they may be considered *non lethal,* suitable for UN Chapter VII operations. US strategists speak of cyber warfare as the fifth scenario for military confrontation along with ground, sea, air and space.

The fast growth of civilian and military cyber activities has not been matched by a similar pace in the normative field. The most conspicuous effort to address this issue was developed within the United Nations and has gone through the various echelons of the UN process: UNIDIR, Advisory Board of the UN Secretary General, UN General Assembly culminating in a report from an ad hoc Group of Governmental Experts. A draft Code of Conduct was submitted by China, Russia, Tajikistan and Uzbekistan at last year's General Assembly. Civil society is also active: cyber security was the focus of a recent course organized by the International School on Disarmament and Research on Conflict (ISODARCO) in Andalo (Italy) in January of this year. The active participation of students in the debate was one of the added values.

Although the path the UN has undertaken may appear long and cumbersome, it has the merit of having placed cyber weapons in the international spotlight and has fostered greater transparency and predictability. Much remains yet to be done to prevent the Internet, originally aimed at promoting international dialogue and cooperation, from becoming, instead, aan additional instrument for international confrontation.