Guerra cibernetica

Da Wikipedia, l'enciclopedia libera.

Il termine **guerra cibernetica**[1] (noto nell'ambito operativo militare del mondo anglofono come *cyberwarfare*) è l'insieme delle attività di preparazione e conduzione di operazioni di contrasto nello spazio cibernetico. Si può tradurre nell'intercettazione, nell'alterazione e nella distruzione dell'informazione e dei sistemi di comunicazione nemici, procedendo a far sì che sul proprio fronte si mantenga un relativo equilibrio dell'informazione. La guerra cibernetica si caratterizza per l'uso di tecnologie elettroniche, informatiche e dei sistemi di telecomunicazione.

Indice

Dominio cibernetico

A livello strategico lo spazio cibernetico è considerato il più recente ambiente di guerra ovvero il quinto dominio dopo terra, mare, cielo e spazio.

A livello geopolitico gli Stati Uniti detengono il primato su questo ambiente dato dal possesso delle principali aziende tecnologiche di portata planetaria, unito al relativo potenziale di intercettazione e attacco e alla disponibilità di gran parte delle infrastrutture della connessione (server, cavi, centri di stoccaggio dati, eccetera).

Anche possedendo questi vantaggi logistici lo spazio cibernetico per sua conformazione offre l'occasione di sfruttare le enormi ignote vastità per sfidare avversari di forze impari, in modi altrimenti inimmaginabili negli altri domini. Per sua natura le battaglie in questo dominio sono svolte principalmente da agenzie di servizi segreti e raramente si riesce a individuare gli attori responsabili ed ancora più difficilmente poterli giudicare in base a una giurisdizione univoca. La pervasività odierna della Rete nella vita dei singoli cittadini come nelle infrastrutture dove ormai è diventata indispensabile al loro funzionamento, se da un lato comporta un esteso controllo centralizzato di contro presenta una fragilità intrinseca del sistema che può essere infiltrato in qualsiasi momento e danneggiato anche nei punti più vitali nonostante tutte le precauzioni[2].

Tipi di attacchi

Esistono molte metodologie di attacco nella guerra cibernetica.

- **Attacco a infrastrutture critiche**: i servizi energetici, idrici, di combustibili, di comunicazioni, commerciali, dei trasporti e militari sono tutti potenziali obiettivi di questo genere di attacchi.
- **Vandalismo web**: attacchi volti a modificare indebitamente pagine web, chiamati in gergo *deface*, o a rendere temporaneamente inagibili i server (attacchi denial-of-service). Normalmente queste aggressioni sono veloci e non provocano grandi danni se l'attaccante non riesce ad avere un accesso con privilegi abbastanza elevati da permettergli di intercettare, rubare o eliminare i dati presenti sul sistema colpito.
- **Intralcio alle apparecchiature** (*equipment disruption*): le attività militari che utilizzano computer e satelliti per coordinarsi sono potenziali vittime di questi attacchi. Ordini e comunicazioni possono essere intercettati o sostituiti, mettendo a rischio le operazioni.
- **Raccolta dati**: informazioni riservate ma non adeguatamente protette possono essere intercettate e modificate, rendendo possibile lo spionaggio.
- **Propaganda**: messaggi politici che possono essere spediti o resi disponibili in rete a scopo di coordinamento o per la guerra psicologica, fake news.

Attacchi conosciuti

- Gli Stati Uniti d'America hanno ammesso di essere stati sotto attacco da parte di diversi Stati, ad esempio Cina e Russia. I due attacchi più famosi sono passati alla storia con i nomi di Titan Rain e Moonlight Maze.[3]
- Attacco alla centrale atomica dell'Iran da parte degli Stati Uniti d'America: operazione Stuxnet.

Regole base

Le regole base della cyberwarfare sono:

- minimizzare la spesa di capitali e di energie produttive e operative;
- sfruttare appieno tecnologie che agevolino le attività investigative e di acquisizione di dati, l'elaborazione di questi ultimi e la successiva distribuzione dei risultati ai comandanti delle unità operative;
- ottimizzare al massimo le comunicazioni tattiche, i sistemi di posizionamento e l'identificazione amico-nemico (IFF - "*Identification Friend or Foe*").

Organizzazione

Con il cyberwarfare si conosce un radicale riassetto delle concezioni organizzative militari. Le tradizionali strutture gerarchiche si vedono progressivamente soppiantate da sistemi a rete, con nuovi ruoli di complementarità e integrazione. Si fanno così spazio entità operative caratterizzate da:

- ridotta consistenza numerica;
- elevato livello di supporto tecnologico;
- efficacia assoluta.

Controspionaggio cyberspaziale

Il controspionaggio cyberspaziale è l'insieme delle misure atte a identificare, penetrare o neutralizzare operazioni straniere che usano i mezzi cyber come metodologie di attacco primario, così come gli sforzi dei servizi stranieri di intelligence che, attraverso l'uso di metodi tradizionali, cercano di portare avanti attacchi di cyberwarfare[4].

Note

1. **^** Cfr. in Riccardo Busetto, *Il dizionario militare: dizionario enciclopedico del lessico militare*, Bologna, 2004, Zanichelli, ISBN 9788808089373
2. **^** Limes,*La rete a stelle e strisce. Cyberwarfare, dove nessuno domina*, GEDI, n 10, 2018, ISSN 2465-1494

3. ^ (EN) Reuters: L'U.S. Air Force si prepara a combattere nel cyberspazio (http://www.propagandamatrix.com/articles/november2006/031106_b_cyberspace.htm) Archiviato (https://web.archive.org/web/20070221032158/http://www.propagandamatrix.com/articles/november2006/031106_b_cyberspace.htm) il 21 febbraio 2007 in Internet Archive.
4. ^ (EN) Controspionaggio cibernetico degli Stati Uniti (http://ncix.gov/issues/cyber/index.php) Archiviato (https://web.archive.org/web/20150402154318/http://ncix.gov/issues/cyber/index.php) il 2 aprile 2015 in Internet Archive.

Bibliografia

- Maddalena Oliva, *Fuori Fuoco. L'arte della guerra e il suo racconto*, Bologna, Odoya 2008. ISBN 978-88-6288-003-9.
- Daniel Ventre, *La guerre de l'information*, Hermès-Lavoisier, Sept.2007.
- Daniel Ventre, *Information Warfare*, Wiley-ISTE, Nov. 2009.
- Daniel Ventre, *Cyberguerre et guerre de l'information. Stratégies, règles, enjeux*, Hermès-Lavoisier, Sept.2010.
- Daniel Ventre, *Cyberespace et acteurs du cyberconflit*, Hermès-Lavoisier, April 2011.
- Daniel Ventre, *Cyberwar and Information Warfare*, Wiley-ISTE, July 2011.
- Daniel Ventre, *Cyberattaque et Cyberdéfense*, Hermès Lavoisier, August 2011.

Voci correlate

- Sicurezza informatica
- Armi a impulso elettromagnetico
- Guerra elettronica
- ELINT
- Intelligence
- High Energy Radio Frequency weapons (HERF)
- SIGINT
- PRISM (programma di sorveglianza)
- Operazione Aurora
- Hacker
- Stuxnet
- Attacco informatico
- Network-centric warfare

Altri progetti

- Wikimedia Commons (https://commons.wikimedia.org/wiki/?uselang=it) contiene immagini o altri file su **guerra cibernetica (https://commons.wikimedia.org/wiki/Category:Cyberwarfare?uselang=it)**

Collegamenti esterni

- *Sistema di informazione per la sicurezza della Repubblica*, su *sicurezzanazionale.gov.it*.
- *DPCM 27 gennaio 2014 – Strategia nazionale per la sicurezza cibernetica*, su *sicurezzanazionale.gov.it*.
- *CyberDifesa.it - notizie sulla guerra cibernetica*, su *cyberdifesa.it*.
- *Esercitazioni di "Cyber Defence" per la Difesa*, su *difesa.it*.
