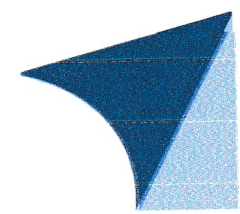
Cento e una voce di informatica giuridica

a cura di

Agata C. Amato Mangiameli

Guido Saraceni

Giappichelli



VIA PO, 21 - TEL. 011-81.53.111 - FAX 011-81.25.100
http://www.giappichelli.it

ISBN/EAN 978-88-921-4350-0

G. Giappichelli Editore

Questo libro è stato stampato su carta certificata, riciclabile al 100%

Stampa: Stampatre s.r.l. - Torino

[24] Cyberterrorismo/Cyberwar | *S.B.*

La guerra informatica (cyberwar) consiste solitamente nelle azioni di uno Stato nazionale, il quale, penetrando nei computer o nelle reti digitali di un altro Paese, causa danni o interruzioni del funzionamento. Il cyberspace [v. voce] rappresenta il quinto dominio della guerra, essendo divenuto cruciale per le operazioni militari quanto lo sono la terra, il mare, l'aria e lo spazio. Il cyberspace rappresenta oramai l'ultima frontiera dei conflitti, basti pensare a quanti Paesi abbiano addirittura creato dei veri e propri eserciti specializzati nelle cyberwars. Attraverso il cyberspace, il nemico può prendere di mira le industrie, il mondo accademico, il governo, le basi militari aeree, terrestri, marittime e spaziali. Allo stesso modo in cui l'aviazione ha trasformato il campo di battaglia durante la seconda guerra mondiale, il cyberspazio ha modificato le barriere che proteggono una Nazione da un attacco contro il suo commercio e le sue comunicazioni. Sfruttando la rete informatica e le sue relative tecnologie, è possibile pianificare e compiere veri e propri atti di guerra, paragonabili ad uno scontro a fuoco, causando conseguenze economiche anche peggiori per il Paese offeso.

I soggetti nemici nel cyberspazio sono principalmente Stati, ma a volte anche semplici persone fisiche che vanno dai dilettanti agli hacker [v. voce] professionisti altamente qualificati. Tuttavia, si discute sulla correttezza del termine cyberwar quando ci si riferisce a soggetti non statali, quali, appunto, i gruppi terroristici. In tal caso, il termine cyberterrorismo può sembrare più calzante rispetto a quello di cyberwar perché gli attacchi nel cyberspazio vengono effettuati in modo imprevisto ed ovviamente anonimo. Eppure, può non essere agevole elaborare una concreta definizione di cyberterrorismo, a causa dei problemi connessi allo stesso termine terrorismo. Se considerassimo la guerra come la continuazione della politica con altri mezzi (come il cyberterrorismo), la cyberwar potrebbe essere definita come un'estensione della politica mediante azioni aggressive intraprese nel cyberspazio da soggetti statali (o

strutturalmente non statali, ma coadiuvati da uno Stato) che rappresentano una grave minaccia per la sicurezza di un altro Stato.

Tale atto viene inoltre condotto con strumenti e finalità la cui pericolosità può variare a seconda delle circostanze. Quel che è certo è che, in un mondo interconnesso, le armi informatiche su larga scala hanno il potenziale di essere altrettanto distruttive quanto quelle biologiche. Gli attacchi informatici rappresentano ormai il primo step delle operazioni belliche, come avvenuto in Ucraina durante l'invasione russa del 2022, quando diversi appartenenti a banche e dipartimenti governativi ucraini sono diventati inaccessibili.

Un noto esempio di attacco informatico è il Denial of Service (DoS), attuato al fine di impedire il corretto funzionamento di una macchina o di una risorsa di rete. Gli attacchi informatici possono causare diffusi black out o bloccare strutture industriali, come dimostra il malware [v. voce] Stuxnet. Sebbene estremamente efficace nel ritardare il programma nucleare iraniano, quest'ultimo ha dimostrato che le armi informatiche possono essere non solo difensive, ma anche offensive. Gli aspetti *sui generis* e non tradizionali della cyberwar sin qui descritti ci consentono di ipotizzare, per il futuro, una 'cyber Pearl Harbor' – o un 'cyber 11 settembre'. Inoltre, il decentramento strutturale e le dimensioni del cyberspazio lo rendono estremamente difficile da governare da un punto di vista politico. Gli attori non statali possono svolgere un ruolo importante nelle cyberwar. Piccoli gruppi di programmatori altamente qualificati sono in grado di avere un forte impatto sulla politica mondiale, condividendo le loro gesta sul web e divulgando le proprie tecniche di attacco. Peraltro, esiste un fiorente e pericoloso mercato nero delle armi informatiche. Il web è così diventato uno spazio in cui prosperano pirati e mercenari digitali.

Nella sua versione 'soft', la cyberwar può essere condotta con atti di propaganda informatica al fine di influenzare l'opinione pubblica. Si tratta di una forma di guerra psicologica che sfrutta soprattutto i social media [v. voce] e il deep web. Allo stesso modo, lo spionaggio informatico implica che i dati degli utenti vengano registrati ed analizzati. Ciò detto, la cooperazione internazionale è essenziale per costruire condizioni favorevoli per una 'pace digitale', o, quantomeno, per lottare per essa. Qualsiasi operazione militare, sia cinetica che cibernetica [v. vo-

ce], dovrebbe rispettare alcune regole e principi, in particolare i principi di umanità, necessità militare, distinzione, proporzionalità e precauzione. Possiamo augurarci che queste regole vengano rispettate nelle cyberwar, ma possiamo stare certi non lo saranno mai nel cyberterrorismo.

Bibliografia minima essenziale

Campagnoli M.N., *I nuovi volti del terrore dal terrorismo islamico al cyber terrorismo,* Key, Milano, 2017.

Lucas G., *The Ethics of Cyber Warfare*, Oxford University Press, Oxford, 2017.