

Si intitola "Cyber Espionage & Cyber Counterintelligence. Spionaggio e controspionaggio cibernetico" ed è un saggio divulgativo sulle modalità e le tecniche di ricerca e assimilazione di informazioni in Rete.

Lo ha scritto Antonio Teti, 53 anni di Lanciano, docente al master di Intelligence dell'università della Calabria, al Master digital heritage cultural communication through digital technologies della Sapienza di Roma e di Cyber Security alla Scuola di perfezionamento per le forze di polizia di Roma. Il libro, edkto da Rubettino, è in uscita in questi giorni.

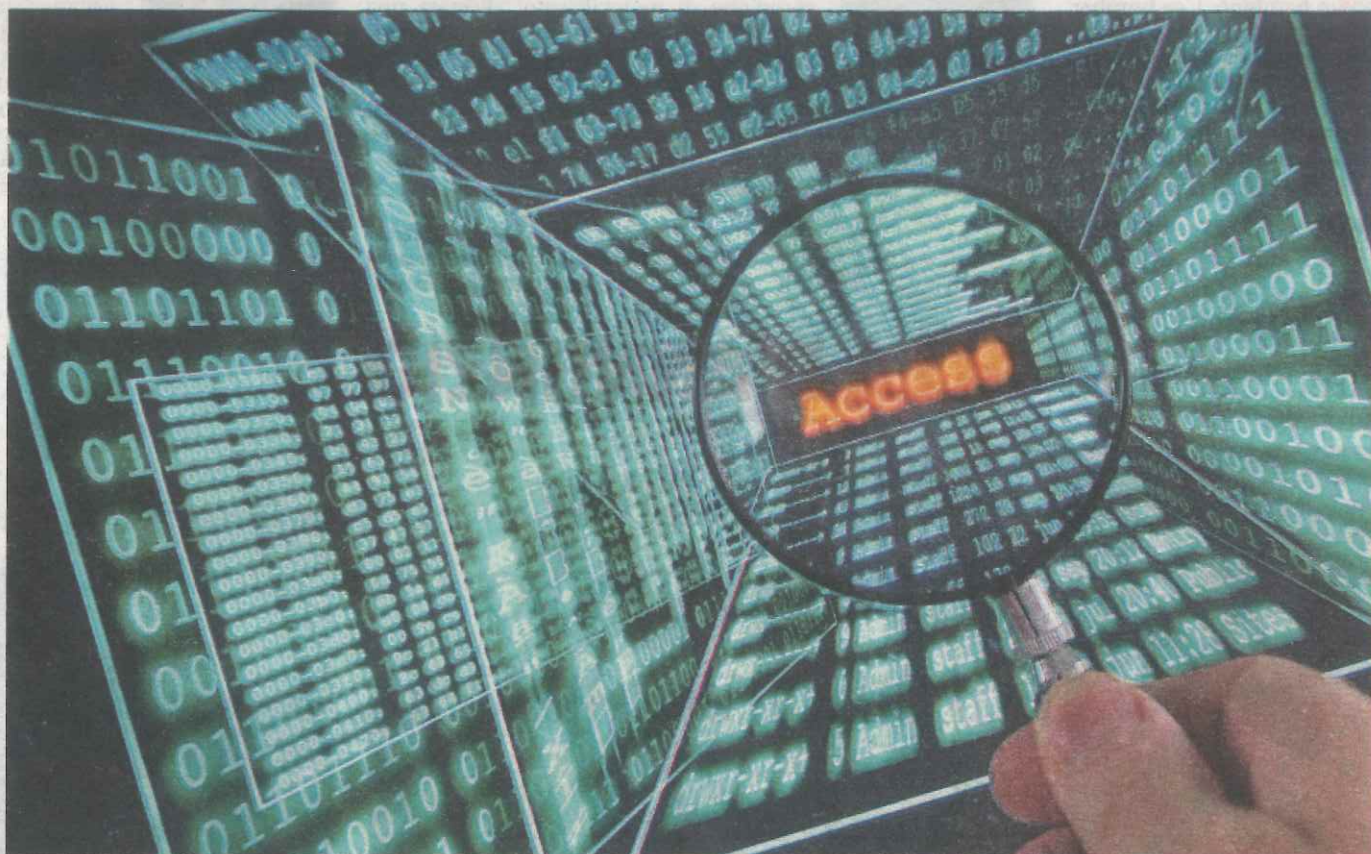
Teti ne parla in questa intervista al *Centro*.

I social media rappresentano una porzione virtuale della nostra vita: quali sono le nostre "armi di difesa" per evitare che il web diventi ostaggio di cyber criminali o di fake news?

I social media hanno assunto una funzione predominante nelle nostre esistenze. Sulle "armi di difesa" ho una precisazione da fare: la vera arma in grado di difenderci dai pericoli e dalle insidie che si celano all'interno del mondo virtuale è rappresentata da noi stessi. Possiamo certamente dotarci di applicazioni software e piattaforme hardware in grado di proteggere i nostri dispositivi tecnologici, come antivirus o sistemi di cifratura dati, ma se non si svilupperà una solida cultura della sicurezza dei dati personali finalizzata ad uso responsabile e consapevole degli strumenti digitali, saremo sempre oggetto di attacchi informatici di ogni genere. Se continueremo ad inserire in rete le immagini dei luoghi in cui ci troviamo, le foto dei nostri familiari, le informazioni personali e dei nostri amici, i dati di geo-localizzazione, saremo sempre delle facili prede per gli hacker.

Nel libro si parla anche di controspionaggio cibernetico. Si tratta di contrasto alle azioni di spionaggio?

Esattamente, il controspionaggio cibernetico è l'attività d'intelligence finalizzata al contrasto allo spionaggio condotto all'interno del Cyberspazio. Tuttavia, in ambito digitale, sussistono non poche differenze con le attività



Il saggio di Antonio Teti (a destra la copertina) si intitola "Cyber Espionage & Cyber Counterintelligence. Spionaggio e controspionaggio cibernetico"

Antonio Teti

CYBER ESPIONAGE E CYBER COUNTERINTELLIGENCE

SPIONAGGIO E CONTROSPIONAGGIO CIBERNETICO



RUBETTINO

» «Spetta innanzitutto a ognuno di noi osservare la massima attenzione su cosa immettiamo in Rete ben sapendo che nulla potrà essere cancellato»

«Vi spiego come difenderci dagli spioni su Internet»

Il docente abruzzese Antonio Teti spiega in un saggio i pericoli della Rete
«Non inserite nei social foto di familiari e le vostre informazioni personali»



Antonio Teti

di controspionaggio tradizionale. La prima è data dall'assoluto anonimato che governa queste attività: l'identità di chi genera le azioni di disinformazione, inganno, infiltrazione e attacco non sono mai certe. Le ipotesi possono essere molteplici, ma non vi è mai certezza. Accusare la Cina, la Russia o la Corea del Nord di azioni di cyber espionage è diventato un luogo comune. La verità è che tutti spiano tutti. D'altronde le agenzie di intelligence servono a questo.

Privacy e cyber intelligence. Fino a che punto può

spingersi l'analisi delle informazioni sulla Rete?

Una tecnica diffusamente utilizzata da decenni nel campo dell'intelligence è l'Open Source Intelligence (OSINT), che si basa sulla raccolta di informazioni attraverso la consultazione di fonti di pubblico accesso. Per fonti pubbliche intendiamo i mezzi di comunicazione tradizionali e più diffusi, come i giornali, le riviste, i canali televisivi, la radio. Ad essi si affiancano i new media o per meglio intendere, il web, i social network, le applicazioni di in-

stant messaging. Nel mio precedente libro, "Open Source Intelligence & Cyberspace. La nuova frontiera della conoscenza", ho ampiamente descritto le tecniche di OSINT all'interno del Cyberspazio, cercando di spiegare, citando non pochi case study, come sia straordinariamente facile acquisire legalmente informazioni che possono essere di grande utilità. Pertanto il problema della violazione della privacy interessa anche la volontà e i desideri della stessa vittima, nel caso in cui egli stesso si renda responsabile della diffusione dei suoi dati sensibili o riservati. In tal caso, la disponibilità online di informazioni private ne consente l'acquisizione e l'utilizzo da parte di chi ne volesse fare uso. In altri termini, spetta in primis ad ognuno di noi osservare la massima attenzione su cosa immettiamo in Rete, ben sapendo che nulla potrà essere mai cancellato dal quel gigantesco repository informativo rappresentato dal Cyberspazio.