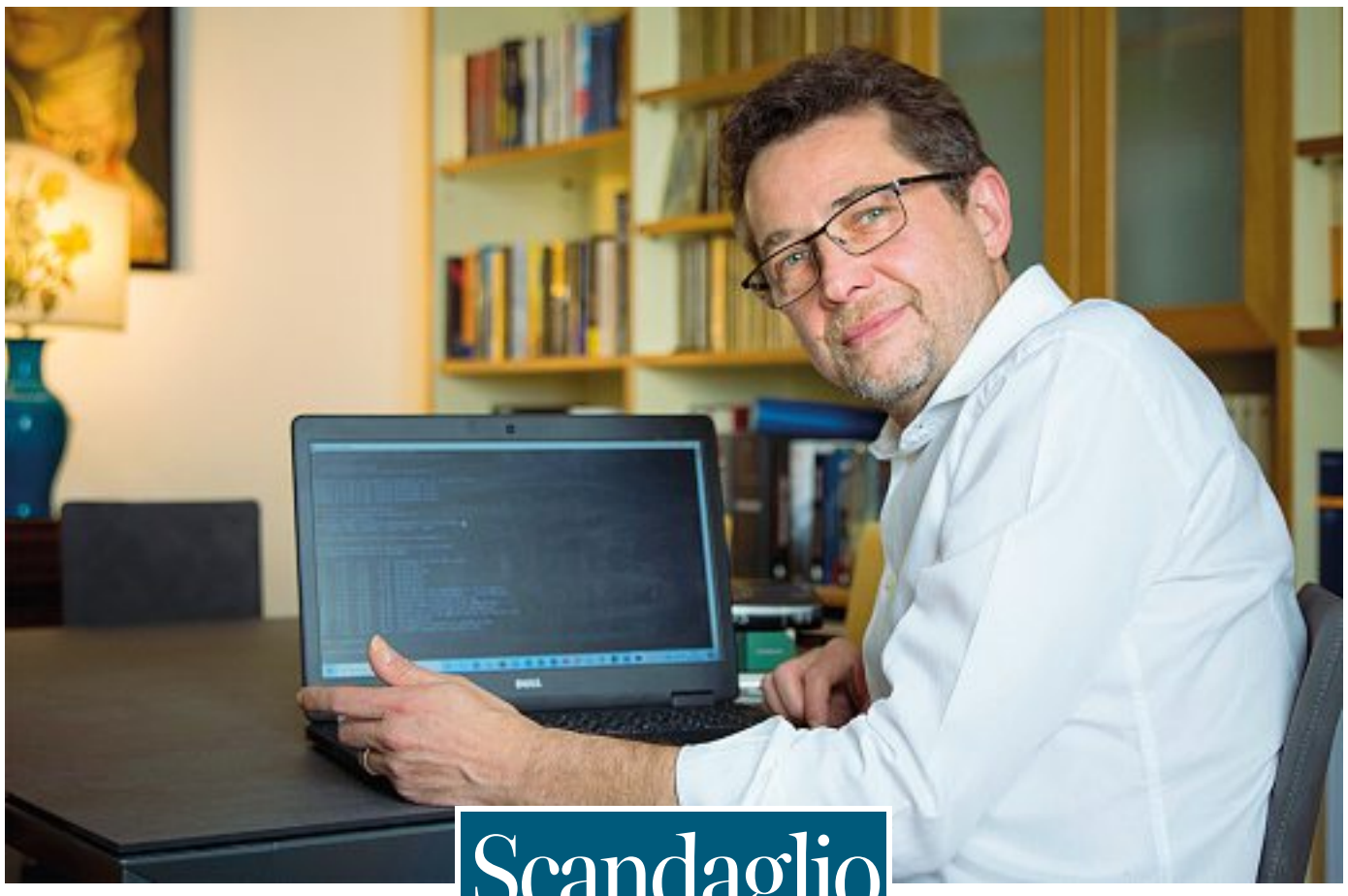
CONFESSIONI

Alessandro Curioni L'esperto di cybersecurity diventato romanziere «Per come è fatta la Rete non si può escludere una discreta Apocalisse»

di **Stefano Lorenzetto**



Censura Alessandro Curioni, 54 anni, esperto di sicurezza informatica. Sotto, nel tondo, Edward Snowden, l'ex tecnico della Cia che usava il dark web per sfuggire alla censura

Scandaglio il dark web e scovo chi ricatta le aziende e gli Stati

Era piuttosto improbabile che Alessandro Curioni, docente di sicurezza dell'informazione alla Cattolica di Milano, potesse manifestare attitudini diverse da quelle che lo hanno reso famoso nel settore della cybersecurity. Dopo che la madre Stefania Maroni, all'epoca redattrice in Rcs Periodici, si separò dal marito, il giovanotto crebbe con due padri adottivi, entrambi cronisti, prima Giorgio Caiati e poi Luciano Lanza, quest'ultimo caporedattore del settimanale economico *Il Mondo*, uno dei fondatori, mezzo secolo fa, di *A Rivista Anarchica*, la prima testata a indagare sulle trame della strage di piazza Fontana. L'imprinting lo spinse a diventare a sua volta giornalista. Ma da 23 anni Curioni applica solo all'informatica le buone pratiche della professione apprese in casa. Oggi è uno dei più quotati esperti nel campo del cybercrime. A lui ricorrono enti e aziende che incappano nei pirati del web. E sempre a lui si rivolgono per la formazione dei dipendenti colossi quali Eni, Edison, A2A, Pepsi.

È così che malware, spyware, phishing, rootkit, trojan, worm sono diventati i coprotagonisti di un romanzo, *Il giorno del Bianconiglio* (Chiarelettere), definito da Curioni «cyberthriller», che vede in azione un suo alter ego, Leonardo Artico. «Mi sono ispirato a fatti realmente accaduti negli ultimi cinque anni. Ho cominciato a scriverlo dopo che 80.000 abitazioni di Kiev rimasero prive della luce a opera di pirati informatici sponsorizzati da Mosca per destabilizzare l'Ucraina. Un tipico attacco di Stato».

Invece gli hacker penetrati nel sistema della Regione Lazio agivano per lucro.

«Da tempo mi chiedevo non se sarebbero arrivati, ma quando. Non è stata certo un'azione più grave e sofisticata di quella che a maggio ha bloccato il Colonial pipeline, l'oleodotto della costa orientale degli Stati Uniti che porta il carburante dal Texas a New York. Dopo aver razionato la benzina per cinque giorni, la compagnia si è rassegnata a pagare il riscatto: quasi 5 milioni di dollari».

Ha fatto bene o male?

«Malissimo. L'80 per cento delle volte i delinquenti ci riprovano proprio perché hai ceduto. Nel caso specifico, sul conto in bitcoin dell'organizzazione criminale è transitato il corrispettivo di 90 milioni in dollari, segno che molte vittime non hanno denunciato i banditi».

Perché s'è cimentato in questo ramo?

«Dopo tanti anni passati da giornalista davanti al monitor del pc, ho voluto capire che cosa ci stesse dietro. All'epoca eravamo solo 20, forse 10, a farlo in Italia. Nel mondo dei ciechi l'orbo diventa re».

Quali strumenti di lavoro utilizza?

«Due computer portatili. Non ci vuole molto per scendere nella selva oscura».

Si riferisce al dark web, immagino.

«Già. Un tempo ci passavo tre ore al mese, oggi me ne basta una. Lo scandaglio se rubano dati a un mio cliente».

Ignoro come si faccia a entrarvi.

«È sufficiente scaricare un browser dal sito *www.torproject.org*, che ovviamente riveste di rispettabilità la propria missione con un proclama altisonante: "Promuoviamo i diritti umani e difendiamo la privacy online attraverso software libero e reti aperte". Attenzione: lì non c'è l'equivalente di Google».

Niente motori di ricerca.

«Solo un mare magnum di attività illegali: spaccio di droga, vendita di armi, prostituzione, file piratati, frodi informatiche, pedopornografia. E snuff movie, i video di torture e omicidi realmente commessi. Va detto però che gli oppositori dei regimi, come quelli cinese e nordcoreano, hanno solo il dark web per aggirare la censura. Anche Edward Snowden, l'ex tecnico della Cia che svelò i programmi segreti di sorveglianza di massa dei governi statunitense e britannico, dovette servirsi di questo canale».

Quali insidie cela il 5G dei cellulari?

«Lo standard di trasmissione della telefonia mobile è la mano sulla culla, la leva che governa il mondo. Se diventa l'unica rete e i due operatori principali, Huawei e Zte, sono tutt'e due cinesi e già stanno lavorando al 6G, americani ed europei fanno bene a non stare tranquilli».

Che cos'è la cyberwar?

«Il nuovo modo di combattere le guerre fra Stati. Oggi non c'è più James Bond con la Walther Ppk: al posto della pistola le spie usano la tastiera del pc. Idem il cybercrime, in assoluto il crimine con il più alto margine di guadagno e il più basso tasso di punibilità. Prendere questa gentaglia è veramente difficile».

Ne fanno le spese molte aziende?

«È capitato a Unicredit, Enel, Luxottica, Campari, Miroglio. Tantissimi altri casi non finiscono sui giornali. Quando mi chiamano a occuparmene, firmo accordi di riservatezza blindatissimi».

Un imprenditore come fa a difendersi?

«Oggi mette tanta tecnologia fra sé e il mondo esterno. Ma l'anello debole è l'essere umano, un dipendente o un fornitore. Mandare una mail fasulla e chiedere di cliccare sul link malevolo è assai più facile che architettare un attacco informatico, per il quale servono mesi di lavoro. Otto volte su 10 la trappola scatta così. Negli altri due casi vengono sfruttate le vulnerabilità dei sistemi tecnologici».

La reazione di chi finisce in ostaggio?

«Il responsabile della sicurezza: "Lo sapevo che prima o poi sarebbe capitato". Il titolare: "In che modo posso contenere i danni?". Purtroppo spesso fatica a uscirne senza pagare i malviventi. Un fabbricante di pentole può continuare a produrre e a raccogliere gli ordini per telefono. Ma una compagnia assicurativa come fa a gestire le polizze dei clienti?».

Il ricatto più diffuso qual è?

«"Ti abbiamo copiato e crittografato l'intero sistema. Se vuoi tornare a utilizzare i file, paga. Altrimenti li vendiamo". A Electronic Arts, la più famosa società di videogiochi, a giugno hanno sottratto 780 gigabyte di progetti, tra cui il codice sorgente del popolarissimo Fifa 21».

Ci sarà pure chi non scuce i bitcoin.

«Solo coloro che dispongono di un backup, cioè la copia di sicurezza dell'archivio eseguita ogni sera su un server, dalla quale si possono ripristinare i dati dopo aver formattato l'intero sistema che è stato violato. Il guaio è che questi salvataggi per comodità vengono lasciati online e i criminali sanno dove cercarli».

Devo dedurne che Dropbox, One Drive, iCloud e altre nuvole sono insicure?

«Sono più sicure dei nostri pc. Ma talmente grandi da diventare un obiettivo».

Lei ha mai investito in criptovalute?

«Offerte ne ho ricevute una valanga. Però non ho mai posseduto un bitcoin. Per formazione mentale non mi avventuro in ciò che non posso controllare. È il motivo per cui non ho titoli di Borsa. Investo solo sui miei 20 dipendenti».

Che insidie si annidano in TikTok?

«Le stesse presenti in Facebook e in tutti i social. Anzitutto adescamenti e truffe. Ho assistito una ragazza che aveva condiviso con il moroso la password del proprio account. Appena si sono lasciati, lui l'ha cambiata, s'è impadronito del profilo e ha iniziato a postare infamità».

È vero che i cellulari ci ascoltano?

«Ho fatto un esperimento. In un corso aziendale ho ripetuto 30 volte la frase "Avengers endgame". Più tardi, tra i risultati di Google mi è apparsa la data di uscita del film *Avengers: Endgame*».

Il Face Id dell'iPhone è sicuro?

«Al 95 per cento. Ma è stato provato che il riconoscimento del viso o delle impronte digitali si può aggirare. In ogni caso teniamo presente che i delinquenti valutano l'economia dello sforzo».

Che significa?

«Il mare è pieno di pesci. Se pigliarne uno diventa faticoso, il cyberpirata non ci perde tempo: si butta su un altro. Dobbiamo imparare a renderci invisibili».

Perché Signal attira più di WhatsApp?

«È una moda. Si dice che un software senza fini di lucro garantisca maggiore segretezza. Ma una prospettiva di guadagno deve pur esserci. Tutti ci spiano allegramente. Su Internet nulla è gratis. Paghiamo in natura. Siamo merce. O davvero qualcuno crede che Google abbia creato Android, il sistema operativo per smartphone, in un empito di generosità? E perché dovrebbe regalarci Gmail, la casella di posta elettronica? Adesso persino l'Ue ci spierà per legge».

Parla del regolamento Chatcontrol approvato dal Parlamento europeo?

«Sì, una pericolosa deroga alla direttiva in materia di privacy. Con il pretesto di contrastare la diffusione del materiale pedopornografico, tutta la nostra messaggistica, dagli sms alle mail, sarà vagliata dall'Ai, l'intelligenza artificiale».

Suggerisce di tollerare i pedofili?

«Dico solo, perché li studio, che gli algoritmi intelligenti a volte sbagliano. Ha presente i falsi positivi? Ciononostante eventuali comunicazioni sospette saranno vagliate da uomini in carne e ossa di Google, Facebook, WhatsApp, che potranno inviarle alla polizia. In pratica gente che compra e vende informazioni avrà accesso ai messaggi degli utenti».

E se arriva un virus informatico che si rivela imbattibile quanto il Covid-19?

«Chi lo escogitasse ne rimarrebbe a sua volta vittima, quindi la speranza è che si astenga dall'inventarlo. In caso contrario, il 95 per cento delle attività collasserebbe. Resteremmo senza acqua, elettricità, gas, trasporti. Le aziende si fermerebbero. Una discreta Apocalisse. Per com'è fatta la Rete, non la escludo».

Ma è fatta così male?

«È multistrato. Internet si appoggia ad altre due tecnologie: le telecomunicazioni e l'energia elettrica. Ciò crea più interdipendenze, quindi maggiori rischi».

Totò si chiedeva: «Siamo uomini o caporali?». Non pensa che dovremmo domandarci: siamo uomini o terminali?

«Siamo uomini che la pandemia ha trasformato in terminali. Prima non stavo 12 ore al pc. Ero in aula a largo Gemelli o nelle aziende. Vedevo persone vere».

Ci salvano i backup, a patto che... «Nuvole» più sicure dei pc ma così grandi da diventare bersagli I cellulari ci ascoltano: ho la prova

Chi è

- Alessandro Curioni nasce a Milano il 16 marzo 1967. Sposato con una manager del settore pubblicitario, due figli di 21 e 14 anni
- Docente di sicurezza informatica nella facoltà di giurisprudenza dell'Università Cattolica e giornalista. Nel 2003 pubblica *Hacker@tack* (Jackson Libri), cui seguono per Mimesis *Come pesci nella rete, La privacy vi salverà la vita, Questa casa non è un hashtag!, La protezione dei dati* e *Cyber war* (con Aldo Giannuli)
- Nel 2008 fonda Di.Gi. Academy, azienda specializzata in formazione e consulenza nella cybersecurity, della quale è tuttora presidente e azionista
- Da poco ha pubblicato con Chiarelettere *Il giorno del Bianconiglio*, primo romanzo di una serie con protagonista Leonardo Artico, cacciatore di pirati informatici sul web. Passa 10 ore al giorno al pc e altre 2 con in mano lo smartphone, «tutte per lavoro»