Editoriale

di *Ernesto Ugo Savona*[*]

Il recente Rapporto Europol su *Serious Organized Crime Threat Assesment* (SOCTA, 2017) classifica, in modo felice, il *cybercrime* nella categoria del *Crime as service (CaaS)* indicando la pluralità delle configurazioni di questa forma di criminalità della quale si sa meno di quanto se ne parla. Benvenuto quindi un numero di questa Rivista su questo tema.

Il *cybercrime*, come criminalità di servizio vuol dire che le attività in rete sono strumentali al compimento di reati, spesso di tipo tradizionale, commessi da singoli o organizzazioni. Una prima tipologia è indicata dalla stessa Europol e consiste nelle seguenti modalità (non esaustive): *malware* e furti di identità, *Cryptoware*, *Network Attacks*, frodi nei pagamenti, frodi nei pagamenti con le carte di credito, materiale pornografico per lo sfruttamento sessuale di minori. I reati diciamo "tradizionali" che sono implicati sono i furti e le estorsioni, insieme a reati tipici relativi allo sfruttamento sessuale di minori. L'uso della rete a scopi di reclutamento da parte dei terroristi dell'ISIS ha esteso questa forma di criminalità di servizio anche al terrorismo.

Se si comprende la natura di queste tipologie è molto più difficile risalire al modello di *business* che c'è dietro. Si tratta di organizzazioni criminali estese o piccole? Si tratta di individui capaci nel produrre gli strumenti criminali e venderli a chi li vuole utilizzare? Lo strumento del *cybercrime* è di per se anonimo e garantisce l'anonimato e nei casi accertati ci sono tutte le possibili combinazioni organizzative. Da organizzazioni criminali, come nel caso dell'operazione *Avalanche* che ha coinvolto un'indagine di quattro anni in 30 paesi su una piattaforma capace di lanciare dei *malware* a livello globale, a singoli individui capaci di "sequestrare" criptando i dati di una azienda, per chiedere un riscatto per liberarli. Una estorsione che non pre-

[*] Direttore di Transcrime (Joint Research Centre on Transnational Crime) dell'Università Cattolica del Sacro Cuore di Milano in cooperazione con l'Università di Bologna e Perugia.
ernesto.savona@unicatt.it

Sicurezza e scienze sociali V, 3/2017, ISSN 2283-8740, ISSNe 2283-7523
DOI: 10.3280/SISS2017-003001

senta le tracce di esplosioni o ha le caratteristiche di minacce dirette facilmente identificabili.

Questa fluidità del *cybercrime* rende molto complessa la comprensione del "chi" e quindi la sua identificazione a fini di giustizia ma rende altresì difficile la sua prevenzione per una strutturale assenza di dati sul problema. È un problema che resta anche se le polizie di tutto il mondo a livello internazionale e nazionale vanno creando piattaforme di collaborazione sempre più numerose nelle quali sono anche coinvolti i privati. Si sa abbastanza del "come" (*modus operandi*) ma poco del "chi" ma anche poco del "quanto" cioè l'impatto.

L'ostacolo maggiore alla diffusione dei dati sul *cybercrime* o meglio su alcune sue tipologie dipende dalle stesse vittime. Alcune società di gestione delle carte di credito rilasciano i dati delle frodi come messaggio per accrescere la prudenza dei lori clienti. Le banche non rilasciano i dati sugli attacchi informatici di cui sono vittime per evitare il panico nella clientela. Se c'è un caso di estorsione pagano il riscatto e risolvono il caso internamente. Il bilancio dei dati è complessivamente povero.

Mancando i dati anche la ricerca criminologica sul *cybercrime* stenta a decollare. Il *cybercrime* può essere un ottimo incrocio tra criminologia e tecnologia ma occorre sempre ragionare sui rapporti di causa ed effetto tra le diverse variabili in gioco. Senza questo ragionamento c'è il rischio, ormai molto diffuso, di diffondere come ricerca sociale di tipo criminologico alcune soluzioni tecnologiche che seguono percorsi di ricerca diversi.

Come ovviare a questa carenza di dati necessari ad una comprensione dei problemi e al loro monitoraggio? La collaborazione tra pubblico e privato è essenziale e va necessariamente accresciuta. I dati giudiziari che arrivano dopo molto tempo e ad operazione conclusa sono episodici e non rappresentativi. Occorrerebbe specificare ulteriormente i dati rilevati attraverso le denunce di reato del sistema SDI ampliando le tipologie e rendendole uniformi a quelle rilevate da altri paesi. Eurostat e UNODC stanno lavorando in questa direzione. Un sistema unico di catalogazione dei dati sulla criminalità già *in progress* agevolerebbe e di molto la conoscenza dei problemi in Italia e altrove. Molto di più occorrerebbe fare sul versante delle vittime e sulla loro propensione alla denuncia. Sia che si tratti di banche o di individui che sono vittime di frodi o di estorsioni. Su questo terreno le campagne di informazione sono sicuramente promettenti ma non bastano. Occorre far crescere la consapevolezza della necessità di forme di cooperazione stretta sui temi nuovi della sicurezza tra cittadini ed istituzioni che guardano al futuro ed alla complessità criminale dei prossimi anni.