doi: 10.14664/rcvs/240

Criminalità e cyberspazio, alcune riflessioni in materia di cybercriminalità

Criminalité et cyberespace : quelques réflexions sur la cybercriminalité

Criminality and cyberspace: some reflections on cybercrime

*Maurizio Tonellotto**

Riassunto
Lo sviluppo tecnologico avvenuto negli ultimi anni ha trasformato la società in uno "spazio iperconnesso" determinando terreno fertile per la proliferazione di nuove forme di criminalità. In questo articolo si vogliono delineare gli aspetti salienti della criminalità nel cyberspazio attraverso un approccio socio-criminologico con un'analisi del quadro teorico di riferimento ed uno sguardo alla normativa nazionale ed europea. Saranno poi presentate alcune riflessioni in merito agli attori coinvolti in questi nuovi scenari, evidenziando la necessità di dover elevare gli standard di sicurezza e di scambio informativo ma anche di consapevolezza e conoscenza degli strumenti e delle tecnologie da parte di chi quotidianamente ne fa largo utilizzo.

Résumé
L'évolution technologique de ces dernières années a transformé la société en un "espace hyper-connecté", tout en créant un terrain fertile pour l'émergence de nouvelles formes de criminalité. À partir d'une perspective socio-criminologique, cet article vise dans un premier temps à décrire les principaux aspects de la criminalité dans le cyberespace en proposant une analyse des approches théoriques en la matière et quelques réflexions sur législation nationale et européenne. Ensuite, l'attention sera focalisée sur les acteurs impliqués dans ces nouveaux scénarios, en soulignant notamment la nécessité de renforcer les standards de sécurité, l'échange d'informations mais aussi la sensibilisation et la connaissance des technologies par ceux qui en font un usage quotidien.

Abstract
The development of information technologies in recent years has transformed our society into a "hyper-connected space" in which the pitfalls, the risks as well as the damages to the victims have grown exponentially, developing new forms of crime. This article aims to outline the aspects of crime in cyberspace through a socio-criminological approach with an analysis of the theoretical framework and a look at national and European legislation. Some reflections on security will then be presented on the actors involved in new scenarios, highlighting the need to raise the security standards and data and information exchange but also of awareness and knowledge of tools and technologies by those who daily use them extensively.

Key words: criminalità informatica, cyber-criminologia, sicurezza informatica, NIS, hacking

* Dottore di Ricerca in Sociologia, professore a contratto presso l'Università di Bologna.

1. Introduzione

Lo sviluppo tecnologico avvenuto negli ultimi anni ha trasformato la nostra società in uno spazio iperconnesso dove progressivamente buona parte delle attività si sono spostate verso scenari virtuali. In questo senso parafrasando Hobsbawm[1], gli ultimi trent'anni potrebbero essere definiti come "il secolo brevissimo": sistemi di comunicazione mobili, dispositivi *smart* sempre connessi, gps, sistemi domotici, IoT e assistenti vocali, hanno radicalmente cambiato il nostro quotidiano, riducendo le distanze, velocizzando le interazioni, sviluppando nuove opportunità di *business* e definendo altrettante nuove dinamiche sociali[2]. Il cyberspazio, lo *spazio-non-spazio*, astrattamente può essere immaginato come sviluppato su tre livelli distinti. Alla base, lo strato tecnologico che ne garantisce i confini ed il funzionamento: è in costante divenire e risponde alle necessità del mercato, dei governi, delle multinazionali e degli attori che fruiscono dei servizi proposti. Al vertice vi è lo strato di *governance*, un livello strategico dove attori istituzionali e privati ne definiscono le regole ed i limiti, sviluppando nuovi mercati, programmi economici o politici. È il livello di appannaggio dei governi e delle società *high tech*. In questo livello coesistono ed interagiscono soggetti pubblici e privati, attori che cooperano e competono sul mercato, definendo l'offerta ma anche attivando meccanismi di desiderio sul consumatore finale, sviluppando modalità di risposta innovative per generare nuove domande e, in taluni casi, anche limitandone l'accesso attraverso politiche censorie che incidono sulla fruibilità dei servizi e sulle libertà individuali. Lo strato intermedio, quello sociale, è lo spazio non fisico dei fruitori (consumatori?) dei servizi offerti: vengono svolte le molteplici attività, siano esse produttive, di comunicazione, condivisione e scambio informativo ma anche ludiche; a questo livello avvengono tutte quelle continue interazioni necessarie ed ormai indispensabili per il quotidiano (Tonellotto, 2020).

Tre strati paralleli in continua interazione tra loro. Qualsiasi modifica all'interno di un determinato livello ingenera un *feedback* immediato ed un adattamento ancora più rapido nei restanti. Il crimine, in questo dominio, può essere considerato un elemento di rottura, un *breakdown*; un collasso delle interazioni, che si riflette su ogni singolo strato. La mancanza di una delimitazione spaziale e la speditezza delle interazioni produce, in tal senso, minacce globali e troppo spesso indifferenti dai confini nazionali. Il crimine informatico può determinare processi di vittimizzazione con effetti a lungo termine, può essere diretto indifferentemente verso persone, infrastrutture, istituzioni, imprese o governi, provocando effetti devastanti anche sulle economie nazionali. L'interconnessione dei sistemi di informazione e comunicazione e la natura globale ed a-territoriale del cyberspazio richiedono un costante impegno ed una continua ed incessante cooperazione internazionale per affrontare in maniera concertata le sfide, calmierare i rischi e contrastare gli effetti della criminalità.

Il cyberspazio presenta elementi innovativi e unici che producono terreno fertile allo sviluppo di nuove forme di criminalità. Innanzitutto le reti

[1] Lo storico britannico Eric Hobsbawm nel suo *Il secolo breve. 1914-1991: l'era dei grandi cataclismi*, ed Ita. Rizzoli 2014, espone la tesi che il periodo compreso fra la prima guerra mondiale ed il crollo dell'Unione Sovietica presenti un carattere coerente che, pur non coincidendo con il ventesimo secolo, ne rappresenti la parte fondamentale.

[2] Sono passati poco più di 30 anni dal primo collegamento italiano a quella che verrà chiamata rete Internet. Il 30 Aprile del 1986 dai laboratori di Pisa del CNUCE-CNR (Centro universitario per il calcolo elettronico), viene inviato il primo pacchetto ICMP (Ping) dall'Italia con destinazione Roaring Creek, in Pennsylvania (USA), pochi instanti dopo dagli Stati Uniti arrivò la risposta "Ok", dando così formalmente vita al primo nodo della rete Internet in Italia.

informatiche, Internet tra tutte, riducono anche se in maniera virtuale, le distanze tra una enorme molteplicità di utenti con estrema rapidità d'azione, semplicità ed economicità. Si stima che ad oggi siano circa 5,2 miliardi gli utenti connessi alla rete Internet, ciò significa che il 65,6% della popolazione mondiale è *online* e, con un tasso di crescita annuo pari a 1,35%, oltre 1 milione di nuovi utenti si uniscono alla rete ogni singolo giorno (Internet WorldStats, 2021). Sono invece oltre 10 miliardi i dispositivi mobili collegati alla rete in tutto il mondo, numero che supera abbondantemente l'attuale popolazione mondiale stimata in 7,9 miliardi (GSMA Intelligence, 2021). Lo studio di Datareportal (2019) ha evidenziato come tre quarti degli utenti di Internet effettuano almeno un acquisto *online* ogni mese e il numero di utenti che acquista esclusivamente attraverso dispositivi mobili è in rapidissimo aumento. Solo nel 2018, oltre 2,8 miliardi di persone hanno acquistato beni di consumo, generi alimentari o elettrodomestici *online*, con un incremento di crescita del 3% rispetto all'anno precedente. Si stima poi che la quantità di denaro destinata al mercato dei beni di consumo online superi 1,75 trilioni di dollari all'anno (Datareportal, 2019).

È ormai assodato come solo pochissime aziende attualmente non facciano uso di tecnologie cablate per la produzione di beni o servizi e sicuramente nessun ente governativo al mondo è isolato dalla rete o è avulso dai servizi IT. Le nuove tecnologie sono diventate accessibili a tutti, anche a persone che non hanno particolari competenze tecniche.

2. Criminologia e cybercriminologia: un approccio teorico allo studio della criminalità nel cyberspazio

Prima di analizzare gli aspetti fenomenologici del *cybercrime*, appare necessario definire a livello teorico la criminogenesi del comportamento deviante all'interno della società dell'informazione. É stato evidenziato come il modello proposto da Cohen e Felson (1979) nella teoria delle attività abituali possa essere applicabile, con i necessari adattamenti, anche al contesto adimensionale del cyber spazio (Eck, Clark, 2003; Junger *et al.*, 2017). Il modello nella sua elaborazione originaria prende spunto dagli approcci culturali proposti nella tradizione della Scuola di Chicago, che postulano una convergenza tra crimine, momento dell'azione e spazio. Individuando dunque un elemento di contatto o un legame diretto tra aggressore, vittima e azione deviante (Shaw, McKay 1942; Eck, Weisburd, 1995). Alcuni autori forniscono una critica all'applicazione del modello proposto da Cohen e Felson nell'ambito del crimine informatico, rilevando come il momento dell'azione sia caratterizzato dall'assenza di contatto diretto tra criminale e vittima e secondariamente, evidenziando una asincronia temporale tra azione deviante e le sue conseguenze (vittimizzazione) (Reyns, *et al.* 2011).

Eck e Clarke (2003) sono stati tra i primi a rilevare tale eccezione nell'applicazione del modello di Cohen e Felson in uno spazio fluido quale può essere definita la rete internet: luogo dove il tempo e lo spazio sono relativi. La lacuna, sostenevano, si evidenzia a meno di definire le reti come spazi integrati e dunque concepiti come luoghi compositi: uno spazio, almeno in senso simbolico, in cui il trasgressore e la vittima si incontrano per procura, in maniera mediata dalla tecnologia, ma con sufficiente profondità di contatto, per applicare correttamente il modello delle attività di routine (Arntfield, 2015, p. 375). È bene ricordare come il modello proposto da Cohen e Felson presuppone che per la realizzazione di un'azione deviante sia

necessario che sussistano contemporaneamente tre condizioni minime, in assenza delle quali il crimine non si può consumare. Tali condizioni contemplano la presenza di una persona disposta a compiere l'azione, il criminale, l'attore deviante; un bersaglio appetibile, sia esso un bene da danneggiare, sottrarre ovvero un individuo da aggredire e, in ultimo ma fondamentale, l'assenza di un guardiano in grado di impedire tale condotta (Cohen, Felson, 1979). Il concetto di guardiano non deve essere ricondotto esclusivamente a quello di agenzia di controllo formale poiché questa funzione può essere esercitata sia da un soggetto che applica un controllo sociale informale sia, in maniera più generale, da un vincolo fisico o da una barriera efficace che si interpone a protezione del bene oggetto di interesse per il criminale. L'assenza di uno solo di questi elementi comporterà l'attuazione della condotta criminale. In base a tale approccio teorico un gruppo sociale o una singola persona, risulta a rischio di vittimizzazione quando si situa nelle vicinanze di un criminale potenziale, criterio di prossimità, costituisce un bersaglio interessante dal punto di vista economico o simbolico, criterio di remuneratività, e non è sufficientemente protetto, criterio di accessibilità (Scarscelli, Vidoni Guidoni, 2008). Nell'ambito dei crimini informatici queste tre condizioni si verificano con estrema frequenza. Si può infatti affermare come il bene appetibile, oggetto di attenzione da parte di attori devianti, sia costituito dal "dato", inteso nella sua accezione più ampia, quale singolo elemento computazionale che incorpora in sé il valore stesso dell'informazione: dato personale, finanziario, sanitario, segreto industriale o scientifico; ma anche come porzione di codice sorgente, software, che consente la gestione di dispositivi connessi alla rete, permettendo o impedendo determinate operazioni. È dunque il "dato" che, nella società dell'informazione, assume un valore incommensurabile ed una appetibilità tale da creare la necessità di domanda negli ambienti criminali. La frequente assenza di adeguati guardiani (*gatekeepers*) intesi come tecnologie e/o persone tecnologicamente preparate e l'enorme disponibilità di vittime "poco" consapevoli genera le necessarie condizioni per la realizzazione dell'azione criminale stessa.

L'analisi eziologica della criminalità informatica si può altresì inquadrare all'interno delle teorie della scelta razionale, nel più ampio paradigma criminologico della Scuola Classica, con particolare riferimento alla teoria economica sulla criminalità di Becker (1968). I teorici della scelta razionale individuano come un'azione venga considerata razionale quando l'attore sociale, di fronte a diversi corsi d'azione, intraprende quella che a suo giudizio fornirà il risultato migliore. In tal senso l'atto deviante diviene quel comportamento razionale che appare all'attore la scelta più adeguata a raggiungere i propri fini (Elster, 1993). La teoria economica del comportamento criminale considera quindi il deviante al pari di un consumatore all'interno del libero mercato (Becker, 1968). Il criminale in tal senso viene definito come quell'attore razionale mosso dal desiderio di massimizzare il proprio benessere.

Becker sintetizza la teoria economica del comportamento criminale attraverso l'ormai nota formulazione $Oj = Oj(pj, fj, uj)$, dove il numero dei reati commessi (O) da una persona in un particolare momento (j) è funzione della probabilità (p) di essere individuato, arrestato e condannato per il suo comportamento, della sanzione (f) prevista per quella tipologia di reato e da altra variabile cumulativa (u). Quest'ultima individua ad esempio l'utilità derivante dallo svolgimento di attività legali

o di attività non conformi, ma anche la volontà stessa di commettere quello specifico atto illegale (Becker, 1968). In base a quanto postulato da Becker, un aumento della probabilità (p) di essere individuato, ma anche un incremento dell'entità della sanzione (f) a seguito di condanna, produce la riduzione dell'utilità attesa nel compiere l'azione criminale.

Si deve considerare come il crimine informatico sia ontologicamente caratterizzato da una elevata rapidità nell'azione e da una forte componente di anonimato, oltre che da confini labili e frastagliati che limitano la possibilità di una rapida identificazione del criminale ed una adeguata e pronta azione di contrasto. La quasi totale assenza di una armonizzazione delle norme di diritto sostanziale a livello internazionale e le difficoltà operative di collaborazione tra forze di polizia di differenti paesi incide oltremodo sulla buona riuscita delle attività investigative, con una conseguente ricaduta a livello giudiziario.

Recenti studi sui fattori causali della criminalità nel cyberspazio hanno poi evidenziato che l'analisi della fenomenologia dei reati informatici necessita di una nuova e più ampia lettura in termini teorici. Jaishankar (2008) considera la criminalità informatica come una nuova forma di criminalità che si sviluppa in uno *spazio-non-spazio*, il cyberspazio appunto, che presenta caratteristiche e peculiarità differenti da quello che viene considerato lo spazio fisico (Jaishankar, 2007a, 2008). Il criminologo indiano proponendo la "*Space Transition Theory of Cyber Crime*" evidenzia come l'analisi di questa nuova tipologia di criminalità non può prescindere da sette postulati fondamentali, colonne portanti di quella che Egli definisce la "*Cybercriminology*": una nuova sub-disciplina inserita all'interno della più ampia cornice teorica della Criminologia[3]. La *Cybercriminology* o cybercriminologia viene intesa dallo studioso come "lo studio causale del crimine che si sviluppa nel cyberspazio ma che ha ricadute nello spazio fisico" (Jaishankar, 2007a, p. 1).

Jaishankar osserva come il comportamento delle persone possa subire variazioni nel passaggio tra lo spazio fisico e quello virtuale. La *Space Transition Theory* è concepita quindi come la teoria che vuole evidenziare il mutare del comportamento del singolo soggetto nel passaggio tra lo spazio fisico e lo spazio cibernetico. Lo studioso rileva infatti che le persone che presentano un comportamento criminale represso all'interno dello spazio fisico abbiano la propensione a commettere azioni criminali nel cyberspazio, azioni che non avrebbero commesso nel mondo reale a causa del loro *status* o della loro posizione sociale. Jaishankar introduce poi il concetto di «*Identity Flexibility*», identità flessibile, inteso come un anonimato dissociativo tipico del cyberspazio, che comporta una mancanza di deterrenza nel passaggio tra lo spazio fisico e lo spazio virtuale, con conseguente propensione alla commissione di azioni devianti (Jaishankar, 2008). Il cyberspazio è quindi da considerarsi un nuovo *locus commissi delicti* all'interno del quale l'anonimato

[3] I sette postulati fondamentali proposti da Jainshnkar sono: "1.Persons, with repressed criminal behavior (in the physical space) have a propensity to commit crime in cyberspace, which, otherwise they would not commit in physical space, due to their status and position; 2.Identity Flexibility, Dissociative Anonymity and lack of deterrence factor in the cyberspace provides the offenders the choice to commit cyber crime; 3.Criminal behavior of offenders in cyberspace is likely to be imported to physical space which, in physical space may be exported to cyberspace as well; 4.Intermittent ventures of offenders in to the cyberspace and the dynamic spatio-temporal nature of cyberspace provide the chance to escape; 5.Strangers are likely to unite together in cyberspace to commit crime in the physical space; (5b) Associates of physical space are likely to unite to commit crime in cyberspace; 6.Persons from closed society are more likely to commit crimes in cyberspace than persons from open society; 7.The conflict of Norms and Values of Physical Space with the Norms and Values of cyberspace may lead to cybercrimes" (Jaishankar, 2007b, p.7).

produce un effetto inibitorio favorendo l'azione criminale[4].

3. Cosa si intende per cybercriminalità?

La multidisciplinarità che caratterizza lo studio dei fenomeni riguardanti la criminalità informatica, l'assenza di contatto tra criminale e vittima, l'evidente asincronia causa-effetto che impone una rimodulazione del concetto di spazio e di tempo comporta, dal punto di vista teorico, alcune disambiguità definitorie il cui risultato, talvolta, può limitare il campo d'analisi. La rapida evoluzione tecnologica e la sempre più stretta convergenza tra dispositivi elettronici e le reti di comunicazione hanno modificato nel tempo il concetto di criminalità, al punto tale che difficilmente una qualsiasi indagine criminale possa risultare scevra dalle evidenze digitali. Termini quali *computer crime*, *computer related crime*, *hight tech crime* o *net crime* vengono spesso utilizzati in letteratura per descrivere la medesima fenomenologia che vede coinvolti a vario titolo dispositivi e competenze ad alto impatto tecnologico. Numerosi autori, Clough (2010) tra tanti, ritengono che il termine più appropriato da utilizzare per definire tale fenomenologia criminale sia quello di *cybercrime*, richiamando per altro la nota classificazione a tre livelli fornita dal *US Departement of Justice* (US DOJ, 1997), che individua il *cybercrime* come quell'insieme di azioni criminali dove il computer o le reti di comunicazione possono essere l'obbiettivo dell'azione, lo strumento per poter attuare tale attività, ma anche tutte quelle situazioni nelle quali i dispositivi o le reti possono intervenire incidentalmente nell'attuazione o definizione dell'attività criminale. Ad oggi infatti, l'analisi delle tracce digitali permette di acquisire elementi di prova talvolta fondamentali per sviluppare nuovi approcci investigativi o proporre ipotesi accusatorie, anche in circostanze dove le tecnologie intervengono in maniera meramente marginale rispetto al fatto reato per cui si procede. Ne è un esempio l'analisi dei dati presenti nei tabulati telefonici, dei dispositivi gps, dei varchi autostradali, delle telecamere di sicurezza o delle connessioni alla rete, funzionali all'individuazione di un soggetto autore di un crimine comune (Tonellotto, 2015). La classificazione tripartita del Dipartimento di Giustizia americano si può riassumere perciò come *computer crimes*, *computer-facilitates crimes* e *computer-supported crimes* (Clough, 2010, p.10).

Il Consiglio d'Europa all'interno della Convenzione sul *Cybercrime* fatta a Budapest nel 2001, pur non fornendone una definizione puntuale, individua con il termine *cybercrime* tutte quelle attività criminali che possono incidere sulla sicurezza dei dati o sulle reti, ma anche quelle azioni che ledono il *copyright*, che favoriscono frodi tramite dispositivi elettronici ed in fine che abbiano come finalità lo sfruttamento sessuale di minori attraverso la rete.

Nella sintesi iniziale della norma viene evidenziato come "La Convenzione è il primo trattato internazionale sulle infrazioni penali commesse via internet e su altre reti informatiche, e tratta in particolare le violazioni dei diritti d'autore, la frode informatica, la pornografia infantile e le violazioni della sicurezza della rete. Contiene inoltre una serie di misure e procedure appropriate, quali la perquisizione dei sistemi di reti informatiche e l'intercettazione dei dati. Il suo obiettivo principale,

[4] Anche se per l'economia di questo articolo ci si riferisce esclusivamente all'approccio teorico di Jaishankar sulla cybercriminologia, è bene rilevare come l'influenza dell'anonimato sulla propensione al delinquere nel cyberspazio non sia un concetto nuovo, già altri autori in precedenza hanno rilevato come tale fattore riduca uteriormente il legame empatico autore-vittima favorendo quindi azioni devianti, *ex multis* Suler (2004), Saponaro e Prosperi (2007).

enunciato nel preambolo, è perseguire una politica penale comune per la protezione della società contro la cyber criminalità, in special modo adottando legislazioni appropriate e promuovendo la cooperazione internazionale."[5] (CoE, 2011).

Lo scopo della Convenzione è quello di fornire un'armonizzazione delle norme di diritto sostanziale e di diritto processuale, al fine di garantire una cooperazione internazionale per contrastare il cybercrime. La norma, in apertura, presenta definizioni che riassumono il complesso delle attività criminali che rientrano nel novero dei reati informatici. In particolare si evidenziano: a) i reati contro la riservatezza, l'integrità e la disponibilità dei dati, che contemplano l'accesso abusivo a sistema informatico, le intercettazioni non autorizzate, l'interferenza illecita su dati, programmi o sistemi informatici; b) i "*computer related crime*", che definiscono i concetti di falsificazioni informatiche e le frodi; c) i reati cd. di "contenuto", associati alla produzione, diffusione e detenzione di materiale pedopornografico; d) i reati connessi alla violazione del diritto d'autore.

Gordon e Ford (2006) in maniera più ampia definiscono invece *cybercrime* "qualsiasi reato che è stato agevolato o commesso utilizzando un computer, una rete o un dispositivo hardware"[6] (Gordon & Ford, 2006 p. 2) in quanto, secondo il modello proposto, l'offesa può essere posta in essere sia su un computer, *computer alone,* sia nei confronti di qualsiasi altro luogo "non virtuale", *non-virtual location*. In tal senso il dispositivo hardware può essere considerato l'attore del crimine, *agent of crime*, lo strumento che agevola il crimine, *facilitator of the crime* ovvero, l'obbiettivo stesso della condotta criminale, *objective of the criminal conduct*. Gli studiosi poi individuano due tipologie di *cybercrime* che definiscono come Tipo I e Tipo II. La criminalità informatica di Tipo I dal punto di vista vittimologico è generalmente un evento singolare, spesso posto in essere utilizzando programmi malevoli (virus, malware, rootkit, ecc.) che sfruttano le vulnerabilità del sistema attaccato. Il Tipo II invece include attività plurioffensive come il *cyberstalking*, le molestie, lo sfruttamento sessuale di minori, l'estorsione, lo spionaggio industriale, la pianificazione o lo svolgimento di attività terroristiche online, ecc. (Gordon, Ford, 2006 p. 3). Appare evidente come risulti estremamente difficile fornire un'unica definizione di criminalità informatica ed in particolare definire una linea di demarcazione tra lo spazio fisico e lo spazio virtuale, anche in un'ottica di azioni di contrasto o di prevenzione.

Analizzando gli effetti della condotta illecita si può asserire come tutte quelle azioni dirette a colpire la confidenzialità delle comunicazioni, l'integrità e la disponibilità dei dati abbiano una diretta ricaduta sul mondo reale, in particolare sull'aspetto economico. Un accesso abusivo o ad un danneggiamento ad un sistema informatico deputato al controllo dell'erogazione di corrente elettrica, oppure ai server di gestione del sistema sanitario nazionale, produrrà effetti nefasti sia sui sistemi elettronici, ingenerando la non disponibilità di servizi computazionali, sia sulle persone, inibendo il normale accesso e fruizione dei servizi stessi. Analogamente un furto identità o un utilizzo fraudolento di codici di carta di credito colpirà le persone, titolari di questi sistemi di pagamento, ma anche il sistema bancario stesso,

[5] Recentemente, il 12 maggio 2022, in occasione della conferenza internazionale organizzata sotto la Presidenza italiana del Comitato dei Ministri del Consiglio d'Europa, è stato aperto alla firma il secondo protocollo addizionale alla Convenzione sulla criminalità informatica, con l'intento di rafforzare la cooperazione e la trasmissione delle prove elettroniche nel campo della lotta alla criminalità informatica.

[6] Per completezza si riporta il testo originale degli autori: "any crime that is facilitated or commited using a computer, network, or hardaware device".

comportando il blocco dei pagamenti, la sostituzione della carta di credito e influenzando in ultimo, anche il sistema assicurativo.

Sintetizzando al massimo si potrebbe comunque affermare come il *cybercrime* possa essere considerato una particolare espressione del crimine tradizionale ma orientato tecnologicamente: sono mutati gli strumenti ma le finalità sono analoghe, ovvero porre in essere comportamenti antisociali plurioffensivi il cui contrasto richiede una forte specializzazione da parte delle forze di polizia, una armonizzazione delle norme ed una elevata cooperazione internazionale (Brenner, 2004).

4. Fenomenologia, tipizzazione dei crimini informatici e attori

Bunch, Clay-Warner e Lei, in *Demographic characteristics and victimization risk: Testing the mediating effects of routine activities*, hanno dimostrato come le vittime della criminalità tradizionale siano spesso giovani, maschi, con un basso livello di istruzione e di reddito e con tendenze a trascorrere più tempo all'aperto (Bunch *et al.* 2012). Al contrario, Junger e Montoya (2017) hanno evidenziato come le vittime di *cybercrime* siano più simili al cittadino medio[7] rispetto alle vittime della criminalità tradizionale. In *Towards the normalization of cybercrime victimization: A routine activities analysis of cybercrime in Europe* (Junger *et al.* 2017) gli studiosi, rilevano come la condizione di vittimia in questo contesto sia trasversale al genere ed all'età, anche se, per le frodi *online* vi è un maggiore scostamento verso le donne di età più avanzata, rispetto alle vittime delle frodi tradizionali. Nello studio gli Autori introducono la nozione di "normalizzazione" delle vittime di cybercrime, concetto legato al fatto che i computer sono presenti ovunque e le persone trascorrono *online* una notevole quantità di tempo: persone di diverso status socioeconomico hanno le stesse possibilità di essere vittimizzate. La ricerca evidenzia poi come alcuni comportamenti possano aumentare il rischio di vittimizzazione, tra questi i principali sono il tempo trascorso *online*, la tendenza a fare "click" facilmente su collegamenti senza verificarne il contenuto o la spasmodica ricerca del "prezzo migliore" a discapito del rischio di incappare in truffe talvolta banali (Junger *et al.* 2017). Dunque la consapevolezza e la conoscenza degli strumenti, oltre al tempo di utilizzo, rappresentano enormi fattori di rischio di vittimizzazione (Pratt *et al.* 2010).

Ad esclusione dei fenomeni criminali che vedono la tecnologia in termini meramente strumentali alla commissione dell'illecito[8], la criminalità informatica *stricto sensu* può essere generalmente associata ad azioni devianti mosse principalmente da motivazioni economiche o ideologiche, intese nella loro accezione più ampia, ed hanno come fine ultimo l'arricchimento, l'acquisizione illecita di informazioni sensibili o strategicamente appetibili ovvero il danneggiamento dei sistemi (Friedman, Bouchard, 2015). A tal proposito, per una analisi fenomenologica di questa tipologia di criminalità nel cyberspazio appare necessario fornire una tipizzazione degli attori coinvolti. Analizzando motivazione, obbiettivi e *modus operandi*, alcuni ricercatori hanno sviluppato una classificazione dei criminali informatici basata su tre livelli: i cybercriminali, i *competitor* o agenti di cyber spionaggio e gli hacktivisti (Friedman, Bouchard,

[7] Seppur in termini astrattamente teorici la locuzione "cittadino medio" potrebbe dar adito ad ambigue interpretazioni, nell'articolo proposto da Junger e Montoya la si deve intrepretare come quel cittadino le cui condizioni socioeconomiche e culturali lo collocano nella media nazionale.

[8] In tal senso, in questa sede, ci si riferisce ad esempio alla pedopornografia, al (cyber)stalking, al (cyber)bullismo o comunque a tutte quelle fattispecie che si perfezionano attraverso la rete ma le cui condotte potrebbero essere poste in essere anche al di fuori dei confini virtuali.

2015). A prescindere dalla tipologia dei soggetti coinvolti il fattore motivazionale risulta sempre riconducibile o comunque strettamente correlato a finalità di carattere economico finanziario oppure a motivazioni di tipo ideologico-politico. In linea di principio l'universo criminale nel cyberspazio può dunque essere ripartito tra tre tipologie di attori principali, le cosiddette *cyber gang*, i *competitor* o *state-sponsored* e gli hactivisti.

I primi sono riconducibili a gruppi criminali che perseguono illecitamente un arricchimento finanziario: utilizzano tecniche di *hacking* con il fine di acquisire ed esfiltrare informazioni a fini estorsivi, oppure per carpire e gestire in maniera fraudolenta i sistemi di pagamento delle singole vittime. Molto spesso sfruttano il fattore umano con tecniche di *social engineering*[9], come il *phishing*[10] distribuito (*spear phishing*), per poi inoculare software malevoli che vengono utilizzati per danneggiare o rendere inservibili i sistemi colpiti, chiedendo successivamente un riscatto per permetterne il ripristino. Gli attacchi di tipo *ransomware* o *cryptolocker*[11] hanno visto negli ultimi periodi un'impennata enorme: a livello globale nel 2021 sono stati registrati oltre 623 milioni di attacchi *ransomware*, con un incremento del 105% rispetto al 2020 e del 232% rispetto al 2019 (Crowdstrike, 2022).

I *competitor* o *state-sponsored* mirano invece ad ottenere un vantaggio competitivo sul piano economico, industriale, commerciale, politico o militare (Friedman, Bouchard, 2015 p. 14). Sono orientati ad acquisire informazioni strategiche, proprietà intellettuali, dati o informazioni, carpendo illecitamente credenziali di accesso dei sistemi informatici concorrenti o installando software malevoli che ne permetto il controllo da remoto, l'intercettazione delle comunicazioni ed il danneggiamento irreversibile dei dati. Il *modus operandi* e gli strumenti utilizzati sono molto simili a quelli in uso ai cybercriminali (*cyber gang*) ma hanno motivazioni differenti, maggiori risorse ed *expertise* tecniche. Utilizzano metodologie e approcci di tipo APT, *Advanced Persistent Threat,* stabiliscono una presenza illecita e duratura, una persistenza, all'interno del sistema avversario, con l'obiettivo di acquisire informazioni riservate, esfiltrare dati o prendere il controllo dell'infrastruttura attaccata. Con l'acronimo APT si identificano anche gli stessi gruppi criminali *state-sponsored* che sfruttano tali metodologie di attacco[12]. Questi gruppi fanno ampio uso di tecniche di *social engineering*, poiché il fattore umano è sicuramente l'anello più debole

[9] In linea generale per *social engineering* si devono intendere tutte quelle tecniche che sfruttano il fattore umano per acquisire informazioni o dati sensili dalla vittima, approfittando delle debolezze delle persone attraverso manipolazioni emotive. La casistica più classica è rappresentata dall'impersonificare uno specifico ruolo o una qualifica particolare presentandosi alla vittima come la persona che ha detiene prerogative per richiedere determinate informazioni altrimenti riservate.

[10] Il *phishing* si annovera nelle tecniche di social engineering, nella maggioranza dei casi viene attuato attraverso invio di messaggi di posta elettronica, sms, etc. artefatti in modo tale che la vittima, nel credere di ricevere comunicazioni ufficiali da parte di soggetti quali istituti di credito, corrieri, enti governativi etc. aderisce all'invio di informazioni, fornendo all'aggressore dati personali come codici di carte di pagamento, password di accesso al servizio di home banking, ecc. ovvero eseguendo procedure tali che consentono l'attivazione di software malevoli, solitamente offuscati all'interno dei messaggi stessi.

[11] Con il termine *ransomware* si fa riferimento ad una tipologia di *malware* (software dannoso) che ha lo scopo di bloccare o inibire l'accesso al sistema colpito. Per poter ripristinare le funzionalità i cybercriminali richiedono alle vittime il pagamento di un riscatto in denaro (tipicamente in cryprovaluta). Il *cryptolocker* o *crypto-ransomware* invece, una volta attivato sul sistema vittima, inizia a cifrare con chiave asimmetrica tutti i dati presenti: documenti, file di backup, progetti, etc, rendendoli completamente inutilizzabili senza però interferire con le funzioni di base del computer. Anche in questo caso vi è la richiesta di un riscatto che, se perfezionato, attiverà l'invio alla vittima della chiave di decodifica dei file per poterli utilizzare nuovamente.

[12] Gli attacchi di tipo APT vengono supportati e ricevono indicazioni sugli obbiettivi da attaccare da Governi o Stati Nazionali. Il loro principale scopo è quello di carpire dati sensibili e/o danneggiare o distruggere infrastrutture di rilevanza strategica utilizzando differenti tecniche e strumenti di attacco, a riguardo si rimanda a FireEye (2016) p. 3.

nella cosiddetta catena della sicurezza: sistemi, procedure e persone. Utilizzano poi le vulnerabilità dei sistemi non correttamente aggiornati ovvero le vulnerabilità ancora non del tutto conosciute, *exploit zero days*, per garantirsi la persistenza all'interno dell'infrastruttura attaccata. Nel 2021 i tentativi di *exploit* per la vulnerabilità denominata "Log4j" sono stati oltre 142 milioni in sei settimane. Il numero di varianti malware inedite sviluppate su tale vulnerabilità ha segnato un +65% (Crowdstrike, 2022). I gruppi *state-sponsored* sviluppano in maniera metodica un elevato numero di agenti software malevoli, sfruttano tecniche di dns *hijacking*[13] per intercettare e dirottare le comunicazioni della vittima, oltre che *tool* di tipo RAT (*remote access trojan*) per garantire, una volta installato sul sistema attaccato, la persistenza, il controllo e l'esfiltrazione di dati e delle informazioni sensibili. Il *Threat Analysis Group* (TAG) di Google ha pubblicato un report relativo ai tentativi di *hacking* commissionati da governi non occidentali nel terzo quadrimestre del 2019, dallo studio emerge che si sono identificati oltre 270 gruppi con legami con i governi di più di 50 paesi. Gruppi specializzati nella raccolta di informazioni, nel furto di proprietà intellettuali ovvero in attacchi informatici ai danni di dissidenti politici, giornalisti e attivisti scomodi. Gli stessi gruppi agiscono anche attraverso coordinate attività di disinformazione, disseminando in rete di notizie non veritiere, del tutto false o forvianti nei confronti di avversari politici (TAG, 2019).

Gli obiettivi tipici di questi attacchi sono rappresentati da istituzioni straniere, enti governativi e grandi gruppi industriali, mentre le finalità sono legate all'acquisizione di informazioni strategiche ed alla compromissione e sabotaggio di intere infrastrutture critiche o di siti produttivi. Gli APT si differenziano dagli attacchi informatici tradizionali per il grado di sofisticazione, decisamente più elevato, ma anche per la loro durata, ovvero la permanenza all'interno del sistema attaccato. In un recente studio presentato da Mediant, società di *threats intelligence*[14], si evidenzia come il cosiddetto *dwell time* o tempo di permanenza media di un attaccante all'interno di un sistema informatico, prima che venga riconosciuta e rimossa la minaccia, varia tra i 30 ed i 140 giorni (Mediant, 2021).

Gli hacktivisti sono invece spinti da motivazioni ideologiche con lo scopo di screditare o danneggiare una istituzione, un governo, un gruppo industriale, un'azienda (Friedman, Bouchard, 2015). Agiscono per ragioni etiche o politiche. Tipicamente le azioni dei cyber-attivisti sono orientate a screditare la vittima con attività di divulgazione sulla rete di informazioni o dati sensibili illecitamente esfiltrati, ovvero contrastare l'operatività del sistema attaccato attraverso azioni di tipo *denial of service* (DOS). Il *denial of service*, letteralmente negazione del servizio, viene generalmente effettuato attraverso l'invio massiccio di pacchetti di dati artefatti verso la rete o il sistema informatico attaccato, allo scopo di sovraccaricare i sistemi colpiti e di impedirne, anche solo temporaneamente, il regolare funzionamento. Le finalità sono di tipo quasi esclusivamente dimostrativo, spesso causano danni temporanei o

[13] Il *DNS Hijacking* o anche *DNS cache poisoning* è una tipologia di attacco informatico che ha lo scopo di modificare la *cache* dei *name server* in modo da alterare l'associazione indirizzo IP / nome di dominio; in questa maniera è possibile per l'attaccante dirottare il traffico della vittima verso falsi server DNS e dunque verso indirizzi IP / siti web malevoli. Con questa tipologia di attacco si possono carpire informazioni sensibili o indurre una potenziale vittima ad accedere a servizi malevoli o che presentano dati o informazioni artefatte.

[14] Per (cyber) *Threat Intelligence* si deve intendere la capacità di raccogliere, elaborare ed analizzare informazioni, notizie ma anche tecniche, tattiche e proceure (tactics, techniques, and procedures, TTPs) utilizzate dai cybercriminali per poter improntare un sistema di difesa adeguato e gestire in maniera efficacie le minacce in ambito cyber.

rallentamenti ai singoli sistemi attaccati. L'hacktivista, da iscrivere all'interno di movimenti di matrice ideologico-culturale, può operare in maniera isolata o collaborare con gruppi più o meno organizzati e strutturati di individui che condividono intenti, ideologie, credenze ed obiettivi. Organizzazioni come Anonymous, ad esempio, sono diventate famose già dal 2008 con l'Operazione Chanology: un attacco contro la chiesa di Scientology. Da allora sono molti gli attacchi che sono stati attribuiti a questo gruppo e che hanno visto colpire diversi obiettivi con differenti finalità politico-ideologiche (Tonellotto, 2020). È importante notare come, anche se alcuni autori includono l'hacktivismo all'interno del *cybercrime*, altri sostengono che questo approccio sia discutibile: a seconda della situazione o delle finalità, i gruppi di cyber hacktivisti, come il citato Anonymous, possono essere alternativamente visti come criminali o protettori dei diritti civili (George & Leidner, 2019). Quello che è certo è che le azioni dei cyber hacktivisti producono un impatto importante su differenti soggetti: individui, governi o istituzioni, con devastanti conseguenze economiche, politiche e sociali. Esiste dunque un forte legame tra *cybercrime* e *hacktivismo,* inteso come condotta multi-offensiva con risvolti *high tech*.

5. Quali attività di contrasto? Cooperazione internazionale, armonizzazione normativa, partnership pubblico-privato

Si è detto come il *cybercrime* si distingua rispetto alla criminalità reale poiché non prevede un contatto diretto tra autore e vittima (Brenner, 2004), in quanto risulta sempre necessaria la mediazione del mezzo tecnologico per l'attuazione della condotta deviante. È noto poi come in linea generale un elemento che facilita la commissione di un crimine risulti essere l'anonimato. Si consideri però che dal punto di vista meramente tecnico una qualsiasi attività svolta attraverso sistemi informatici lascia sempre elementi che possono essere ricostruiti, analizzati e tracciati, permettendo dunque di individuare origine e destinatario di una comunicazione[15]. Esiste però un anonimato *de facto* dettato, in particolare, dalle difficoltà di una pronta cooperazione giudiziaria internazionale da parte delle forze di polizia. Tentativi di armonizzazione delle normative a livello internazionale, come la già citata *Convenzione sul Cybercrime* del Consiglio d'Europa, hanno lo scopo di colmare tali limiti, ma si scontrano comunque con l'estrema velocità dell'azione criminale oltre che con la fragilità e la rapidità di dispersione delle evidenze digitali. Brenner (2004) evidenzia infatti come a livello locale le strategie di contrasto al *cybercrime* sono sviluppate per combattere crimini all'interno del territorio e della giurisdizione nazionale anche se, molto frequentemente, le azioni criminali sono originate o hanno ricadute al di fuori dei confini dei singoli Stati. Sempre di più dunque vi è la necessità di politiche di contrasto comuni che esulino dal concetto di giurisdizione nazionale. Politiche orientate a favorire una puntuale attività preventiva, mettendo a fattore comune competenze, attività info-investigative o di intelligence, che prevedano condivisione e scambio informativo costante, promuovendo una fattiva cooperazione internazionale e facilititando accordi di partenariato pubblico-privato. La definizione di politiche comuni ed il partenariato pubblico-privato diviene fondamentale nella gestione della tutela delle infrastrutture critiche o delle attività sensibili. Si

[15] In tal senso ci si riferisce alle metodiche di *incident response* e *digital forensics*, *ex multis*: Johansen Gerard, *Digital forensics and incident response: incident response techniques and procedures to respond to modern cyber threats*, Packt Publishing Ltd., Birmingham, 2020.

pensi al settore energetico, a quello dei trasporti o delle telecomunicazioni ed alle inevitabili ricadute sul sistema paese e sull'economia nazionale nel caso di attacchi informatici mirati a tali strutture. La storia recente ha evidenziato come le minacce alle infrastrutture sensibili o critiche siano concrete e di estrema attualità e come, in assenza di una stretta collaborazione pubblico-privato, le aziende possono ben poco nei confronti di situazioni emergenziali, che hanno riflessi anche sulla sfera geopolitica internazionale (Tonellotto, 2017).

Negli ultimi anni l'Unione Europea e gli Stati Uniti hanno compreso la necessità della cooperazione internazionale e dell'armonizzazione normativa a favore della gestione della protezione della sicurezza delle informazioni. Gli Stati Uniti e l'UE cooperano in numerose contesti e assemblee in materia di sicurezza informatica. Gli Stati Uniti hanno per altro siglato la Convenzione del Consiglio d'Europa sulla criminalità informatica e collaborano nel settore della sicurezza informatica in organizzazioni multilaterali. L'Unione Europea nel 2016 ha emanato la direttiva sulla sicurezza delle reti di informazione (direttiva NIS, *Network and Information Security*) ed il regolamento generale sulla protezione dei dati personali (GDPR). La Direttiva UE NIS[16], ha come scopo principale quello di aumentare e migliorare, per ogni singolo Stato membro dell'Unione, la propria capacità di gestire la sicurezza delle reti. Gli Stati europei in maniera concertata devono elevare gli standard di sicurezza e di scambio informativo in relazione ai cosiddetti "incidenti informatici". La direttiva prevede che ogni Stato membro sia obbligato ad adottare una strategia a livello nazionale in materia di cyber sicurezza, avendo il compito di nominare autorità competenti, nonché entità investite dalla responsabilità di monitorare gli incidenti informatici. I tal senso sono stati istituiti i CSIRT nazionali: *Computer Security Incident Response Team*. I CSIRT hanno il compito di monitorare gli incidenti informatici a livello nazionale, diramare preallarmi e allerte, inviare comunicazioni sul territorio, favorire lo scambio informativo tra le parti interessate in merito a rischi e alle minacce, intervenire in caso di incidente, analizzandone la dinamica e gestire i rapporti tra gli altri Stati membri dell'UE eventualmente coinvolti. Ai sensi della direttiva NIS gli Stati membri devono adottare una strategia nazionale di *cybersecurity* che garantisca elevati livelli di sicurezza per i sistemi e le reti informatiche, con particolare riguardo a quelli ritenuti essenziali, designando autorità competenti per monitorare a livello nazionale l'applicazione della direttiva ed individuando un unico punto di contatto per la cooperazione tra i singoli Stati. La norma ha poi definito il ruolo degli operatori di servizi essenziali (OSE), ovvero soggetti pubblici o privati che forniscono servizi direttamente dipendenti dalle reti di comunicazioni o da sistemi informatici e che sono essenziali per il mantenimento di attività sociali o economiche e per i quali un eventuale incidente informatico potrebbe avere ripercussioni rilevanti sulla fornitura dei servizi stessi e sulla collettività. Rientrano in questa classificazione le realtà pubbliche o private che operano in vari settori, in particolare quello dei trasporti, delle infrastrutture deputate alla produzione, erogazione e fornitura di energia elettrica, gas ed idrocarburi, gli enti creditizi, il settore sanitario, etc[17].

[16] Direttiva 2016/1148 del Parlamento Europeo e del Consiglio del 6 luglio 2016, Recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione.

[17] L'allegato II del d.lgs. n. 65 del 2018, norma che recepisce la Direttiva NIS in Italia, prevede l'elenco dei soggetti classificati come operatori di servizi essenziali (OSE). Con la medesima norma, all'art. 4, è stato istituito presso il Ministero dello sviluppo economico un elenco nazionale

L'Italia ha dato attuazione alla direttiva NIS recependola con il decreto legislativo 18 maggio 2018, n. 65, pubblicato sulla Gazzetta Ufficiale n. 132 del 9 giugno 2018. Con l'art.12, rubricato "obblighi in materia di sicurezza e notifica degli incidenti", viene previsto come gli OSE siano tenuti ad adottare misure tecniche e organizzative adeguate e proporzionate alla gestione dei rischi alla sicurezza delle reti e dei sistemi informativi. Tali misure devono essere adeguate a prevenire e minimizzare l'impatto di incidenti a carico dei sistemi informativi e applicate al fine di assicurarne la continuità operativa. Vi è poi l'obbligo da parte degli Operatori di Servizi Esenziali di notifica al CSIRT italiano e all'Autorità NIS di tutti gli incidenti con impatto rilevante. La rilevanza dell'impatto di un incidente viene definita a livello normativo sulla base di specifici parametri quali, il numero degli utenti coinvolti dal malfunzionamento dei sistemi, la durata dell'incidente, la diffusione geografica, etc. A seguito della ricezione della notifica di incidente, il CSIRT può informare i singoli Stati membri interessati nel caso in cui l'evento abbia causato un impatto rilevante sulla continuità dei servizi essenziali in quella specifica area geografica.

L'art. 8 d.lgs. n. 65/2018 istituisce il CSIRT Nazionale o *Gruppo di Intervento per la Sicurezza Informatica*, che ha compiti di definire le procedure per la prevenzione e la gestione degli incidenti informatici, ricevere e gestire le notifiche di incidenti inviate dai fornitori dei servizi essenziali e garantire la "collaborazione effettiva, efficiente e sicura" nella rete di CSIRT europea.

A seguito dell'approvazione della Direttiva NIS nel 2016 sono state adottate, a livello comunitario, ulteriori misure con lo scopo di rafforzare la sicurezza cibernetica nell'Unione. Il Cybersecurity Act del 2019[18] si prefigge lo scopo di definire un quadro comune europeo per la certificazione della sicurezza informatica dei prodotti ICT e dei servizi digitali, oltre che quello di rafforzare il ruolo dell'Agenzia dell'Unione europea per la sicurezza delle reti e dell'informazione (ENISA). Il Cybersecurity Act costituisce un tassello fondamentale della nuova strategia dell'UE per la sicurezza cibernetica che ha l'obbiettivo di rafforzare la resilienza degli Stati membri agli attacchi informatici oltre che a sviluppare un mercato unico della sicurezza cibernetica in termini di prodotti, servizi e processi. Recentemente il Consiglio e il Parlamento Europeo hanno poi concordato un pacchetto di misure con lo scopo di migliorare ulteriormente le capacità di risposta agli incidenti del settore pubblico e privato, tale protocollo aggiornerà l'attuale direttiva NIS al fine di predisporre la nuova direttiva, NIS2, che avrà l'obiettivo di definire ulteriormente le misure di gestione del rischio di cybersecurity e gli obblighi di segnalazione in tutti i settori coperti dalla nuova direttiva, come l'energia, i trasporti, la salute e le infrastrutture digitali (EC, 2022).

In Italia, con il D.L. 14 giugno 2021, n. 82, è stata altresì istituita l'Agenzia Nazionale per la Cybersicurezza (ACN), che ha il compito di garantire l'implementazione della strategia nazionale di cybersicurezza adottata dal Presidente del Consiglio, promuovere un quadro normativo coerente nel settore delle nuove tecnologie, oltre che esercitare funzioni ispettive e sanzionatorie nel caso di soggetti inottemperanti alle linee di indirizzo del Governo in materia di cybersicurezza. L'Agenzia

degli operatori di servizi essenziali. Tale elenco deve essere riesaminato almeno a cadenza biennale a cura delle autorità competenti NIS e comunicato al MISE.

[18] Regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio, del 17 aprile 2019, relativo all'ENISA, l'Agenzia dell'Unione europea per la cibersicurezza, e alla certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione.

deve poi sviluppare collaborazioni a livello internazionale con agenzie omologhe ed assicurare il coordinamento tra soggetti pubblici per la realizzazione di azioni pubblico-private, volte a garantire la sicurezza e la resilienza cibernetica. In ultimo, il recentissimo decreto del Presidente della Repubblica n. 231 del 19 novembre 2021, entrato in vigore il 14 gennaio 2022, concernente "L'organizzazione degli uffici centrali di livello dirigenziale del Ministero dell'Interno" ha istituito, nell'ambito del Dipartimento di Pubblica Sicurezza, la nuova Direzione Centrale per la Polizia Scientifica e la Sicurezza Cibernetica, nella quale sono confluite le attribuzioni sinora svolte dal Servizio Polizia Scientifica e dal Servizio Polizia Postale e delle Comunicazioni. La Direzione Centrale assumerà la gestione del *Computer Emergency Response Team* (CERT) del Viminale. La nuova organizzazione del Dipartimento di P.S. prevede poi l'istituzione dei Centri Operativi per la Sicurezza Cibernetica, C.O.S.C., in sostituzione dei Compartimenti Polizia Postale e delle Comunicazioni. Questi Centri, alle dirette dipendenze della Direzione Centrale per la Polizia Scientifica e la Sicurezza Cibernetica, avranno competenza regionale. Lo stesso Decreto ha poi previsto la trasformazione anche delle Sezioni Polizia Postale che, con competenza provinciale, assumeranno la nuova denominazione di Sezioni Operative per la Sicurezza Cibernetica (S.O.S.C.).

La nuova riorganizzazione ha lo scopo di potenziare le capacità di intervento in caso di eventi di sicurezza informatica complessa e prevede l'istituzione, all'interno dei Centri C.O.S.C., di Nuclei Operativi per la Sicurezza Cibernetica (N.O.S.C.) che svolgeranno anche le funzioni di Organo periferico del Ministero dell'Interno per la regolarità dei servizi di telecomunicazione. Ai N.O.S.C. sono state attribuite specifiche competenze operative e di intervento rapido in caso di eventi informatici avversi e con criticità variabile, compiti info-investigativi e di *threat intelligence* funzionali al contrasto di reati informatici che coinvolgono infrastrutture critiche e sensibili del territorio.

6. Conclusioni

Si è visto come la criminalità informatica stia diventando una delle principali sfide alla sicurezza globale. Per contrastare e contenere la rapida evoluzione delle tecniche adottate dai cyber-criminali sono necessarie politiche internazionali integrate e comuni ma anche adeguata consapevolezza da parte di chi, quotidianamente, fa uso delle nuove tecnologie. Tale sfida richiede una collaborazione senza precedenti tra le parti interessate: governi, aziende, stakeholders, istituti di ricerca e mondo accademico. La necessità di una maggiore e più stretta collaborazione tra pubblico e privato appare attualmente la soluzione più auspicabile: azioni congiunte tra realtà differenti ma con medesimi scopi, come già pronunciato nel 2006 dall'Assemblea Generale delle Nazioni Unite con la risoluzione A/RES/60/288 del 20 settembre 2006 in tema di lotta al terrorismo internazionale. A livello europeo la strategia comune è quella della condivisione di intenti e responsabiltà sia tra i singoli Stati membri, sia coinvolgendo le realtà pubbliche e private che operano nei settori di intaresse strategico e che forniscono servizi esenziali, al fine di elevare i livelli di sicurezza per i sistemi e le reti informatiche.

Vi è infine da sottolineare come numerosi attacchi informatici si basino in primo luogo sulla cosiddetta ingegneria sociale: una metodologia di raccolta delle informazioni che sfrutta quello che viene definito

l'anello più debole della sicurezza, il fattore umano. Le tecnologie possono aiutare a definire e sviluppare un ambiente sicuro, le *policy* di sicurezza possono mitigare azioni malevoli ma senza la consapevolezza del rischio associato all'uso non corretto di tali tecnologie, le minacce saranno sempre estremamente attuali e produrranno enormi danni. Il fattore umano è la componente fondamentale ed è dunque importante promuovere a tutti livelli il concetto di *attenzione consapevole* (Balloni, 1998) come risorsa necessaria per limitare i rischi di vittimizzazione anche nel dominio delle nuove tecnologie. Consapevolezza, cultura della *cybersecurity*, tecnologie affidabili, procedure comuni, competenze, armonizzazione del diritto e cooperazione internazionale sono dunque le parole chiave per vincere questa sfida globale nel cyberspazio.

Bibliografia

1. Balloni A., «Il criminologo dell'organizzazione della sicurezza: problemi di formazione ed esigenze di professionalità», Balloni A. (dir.), *Criminologia e sicurezza*, Franco Angeli, Milano, 1998, pp. 13-21.
2. Becker G., «Crime and Punishment: An Economic Approach», *Journal of Political Economy*, vol. 76, n. 2, 1968, pp. 169-217.
3. Brenner S. W., «Cybercrime metrics: Old wine, new bottles?», *Virginia Journal of Law and Technology,* vol. 9, n. 13, 2004.
4. Bunch J., Clay-Warner J., Lei M.-K., «Demographic characteristics and victimization risk: Testing the mediating effects of routine activities», *Crime and Delinquency*, 6, 2012, pp. 1181-1205.
5. Clough J., *Principles of Cybercrime*, University Press, Cambridge, UK, 2010.
6. Friedman J., Bouchard M., *Definitive Guide to Cyber Threat Intelligence*, MD: CyberEdge Group, LLC, Annapolis, 2015.
7. George J. Leidner D., «From Clicktivism to Hacktivism: Understanding Digital Activism», *Information and Organization*, vol. 29, n. 3, 2009.
8. Gordon S., Ford R., «On the Definition and Classification of Cybercrime», *Journal in Computer Virology*, vol. 2, n. 1, 2006, pp. 13-20.
9. Jaishankar K., «Cyber criminology: Evolving a novel discipline with a new journal», *International Journal of Cyber Criminology*, vol. 1, n.1, 2007a, pp. 1-6.
10. Jaishankar K., «Establishing a theory of cyber crimes», *International Journal of Cyber Criminology*, vol. 1, n. 2, 2007b, pp. 7-9
11. Jaishankar K., «Space Transition Theory of Cyber Crimes» in Schmallager F., Pittaro M. (ed.), *Crimes of the Internet*, Upper Saddle River, NJ: Prentice Hall, 2008, pp. 283-301.
12. Jaishankar K., *Cyber Criminology: Exploring Internet Crimes and Criminal Behavior*, CRC, Bca Raton, 2011.
13. Junger M, Montoya L., Hartel P, Heydari M., «Towards the normalization of cybercrime victimization: A routine activities analysis of cybercrime in Europe», *2017 International Conference On Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA)*.10.1109/CyberSA.2017.8073391, 2017.
14. Johansen G., *Digital forensics and incident response: incident response techniques and procedures to respond to modern cyber threats*, Packt Publishing Ltd., Birmingham, 2020.
15. Pratt T. C., Holtfreter K., Reisig M. D., «Routine online activity and internet fraud targeting: Extending the generality of routine activity theory», *Journal of Research in Crime and Delinquency*, vol. 47, n. 3, 2010, pp. 267-296.
16. Scarscelli D., Vidoni Guidoni O., *La devianza. Teorie e politiche di controllo*, Milano, Carrocci, 2008.
17. Suler J., «The online disinhibition effect», *CyberPsychology & Behavior*, vol. 7, n. 3, 2004, pp. 321-326.
18. Saponaro A., Prosperi G. (2007), «Computer crime, virtualità e cybervittimologia», in Pitasi A. (a cura di), *Webcrimes. Normalità, devianze e reati nel*

cyberspace, Angelo Guerrini e Associati, Milano, 2007.
19. Tonellotto M., *Computer forensics: l'acquisizione della prova informatica*, MD: EAI, Chisinau, 2015.
20. Tonellotto M., *La sicurezza nelle organizzazioni. Un approccio socio-criminologico alla security aziendale*, FrancoAngeli, Milano, 2017.
21. Tonellotto M., «Crime and Victimization in Cyberspace», in Balloni A., Sette R. (ed.), *Handbook of Research on Trends and Issues in Crime Prevention, Rehabilitation, and Victim Support,* IGI GLOBAL, Hershey, pp. 248-264, 2020.
22. U.S. DOJ., *Computer Crime & Intellectual Prop. Section*, U.S. Dep't of Justice Criminal Div., Legislative Analysis of the 1996 National Information Infrastructure Protection Act, 2 Electronic Info.Pol'y & L. Rep., 240, 240, 1997.
23. Wall D. S., *Cybercrime: The transformation of crime in the information age*, Polity Press, Malden, MA, 2007.

Sitografia

1. Crowdstrike, *2022 Global Threat Report,* disponibile all'indirizzo: https://go.crowdstrike.com/global-threat-report-2022.html
2. Datareportal, *Digital around the world*, 2019, disponibile all'indirizzo: https://datareportal.com/global-digital-overview
3. E.C., «Commission welcomes political agreement on new rules on cybersecurity of network and information systems», *European Commission Press Corner*, 2022, disponibile all'indirizzo: https://ec.europa.eu/commission/presscorner/detail/en/IP_22_2985
4. FireEye, *Advanced persistent threat (APT) groups. A field guide to state sponsored cyber attackers, 2016,* disponibile all'indirizzo: www.fireeye.com/offers/apt-handbook.html
5. Mediant, *M-trends 2021 Insights into Today's Top Cyber Trends and Attacks*, 2021 disponibile all'indirizzo: www.mandiant.com/resources/m-trends-2021
6. Intelligence, G. S. M. A., *Definitive data and analysis for the mobile industry,* 2021, disponibile all'indirizzo: www.gsmaintelligence.com
7. Internet World Stats, *World Internet Users and 2021 Population Stats,* 2021 disponibile all'indirizzo: www.internetworldstats.com/stats.htm