ICONOCRAZIA

Cybersecurity: breve introduzione a una questione tecnica e politica fondamentale.

iconocrazia.it/cybersecurity-breve-introduzione-a-una-questione-tecnica-e-politica-fondamentale/

30 Giugno 2021

di Danilo Caivano Alfredo Ferrara e Giuseppe Cascione Iconocrazia 19/2021 - "Bivi europei e questioni tecno-politiche"

L'importanza assunta dalle ICT nelle società contemporanee ha reso la questione della cybersecurity una delle più rilevanti questioni con la quali governi, player privati e singoli cittadini devono confrontarsi quotidianamente. Come tanti altri fenomeni che caratterizzano la nostra contemporaneità, anche questo si è imposto assumendo rilevanza pubblica a livello globale con una tale velocità che nel momento stesso in cui le opinioni pubbliche hanno cominciato a rendersi conto della sua esistenza hanno dovuto anche constatare che era diventata una questione fondamentale ed estremamente complessa. Il presente contributo si propone di fornire alcune coordinate minime della cybersecurity sotto un triplice punto di vista: ricostruendo sotto un punto di vista storico la sua progressiva affermazione come questione fondamentale dei nostri tempi, affrontando la questione definitoria ed infine evidenziandone le implicazioni politiche. Questa breve ricognizione che proponiamo è basata su tre contributi pubblicati nell'ultimo decennio da Myriam Dunn Cavelty (2010), Michael Warner (2012) ed infine Dan Craigon, Nadia Diakun-Thibault e Randy Purse (2014).

Una trentennale preistoria

Sebbene il dibattito sulla cybersecurity abbia attirato l'attenzione di studiosi e decisori politici negli Stati Uniti soprattutto a partire dagli anni Novanta, come evidenzia Michael Warner esso ha avuto una preistoria trentennale che precede gli anni Novanta. Secondo l'ipotesi di periodizzazione proposta da Warner, tale preistoria può essere riassunta in quattro successive fasi culminanti proprio negli anni Novanta, basate ciascuna su un'intuizione che ha permesso alle élites tecniche e politiche, oltre che all'opinione pubblica, di metterne a fuoco un singolo aspetto; a partire da queste acquisizioni di consapevolezza sono state adottate poi specifiche iniziative politiche negli anni successivi.

Periodo	Intuizione	Iniziative

1	Anni Sessanta	"I computer possono perdere dati sensibili e devono essere protetti" (Warner, p. 782)	Istituzione di sistema federale di crittografia digitale: Digital Encryption Standard (DES) – 1976
2	Anni Settanta	"I computer possono essere attaccati e i dati rubati" (Ibidem)	Direttiva sulla decisione sulla sicurezza nazionale (NSDD) - 145 (1984) Legge sulla sicurezza informatica (1987) Direttiva sulla sicurezza nazionale (NSD)-42 denominata *Politica nazionale per la sicurezza della sicurezza nazionale Delle telecomunicazioni e dei sistemi informativi* (1990).
3	Anni Ottanta e Novanta	"Possiamo realizzare attacchi informatici con gli apparati militari" (Ibidem)	Istituzione di *Air Force Information Warfare Center* (1993), *Navy Information Warfare Activity* (1994) e Army Land Information Warfare *Activity* (1994).
4	Anni Novanta	"Altri potrebbero farlo a noi – e forse lo stanno già facendo" (Ibidem)	Esercitazione *Eligible receiver* (1997)

1. Negli anni Sessanta e negli anni Settanta i computer non erano ancora diventati un oggetto di consumo di massa ma erano dei grandi macchinari, rari e costosi, che venivano fittati dai pochi possessori ad agenzie e ricercatori che non potevano permettersene l'acquisto. La circostanza che uno stesso macchinario venisse usato da una pluralità di utenti sollecitò l'attenzione sulla sicurezza dei dati che ciascun utente inseriva ed elaborava. Tra gli utenti inoltre c'erano anche agenzie e operatori privati che operavano per conto del governo americano, lavorando pertanto su dati sensibili. La questione fu delegata sin da subito alla *National Security Agency* (NSA) che, come vedremo, avrà un ruolo fondamentale nel gestire la cybersecurity. Nell'Ottobre del 1967 il *Defense Science Board* (un comitato di esperti civili su questioni tecnico-scientifiche nominato dal Dipartimento della Difesa) affidò a Willis H. Ware il coordinamento di un gruppo di studio che esaminasse il problema; ne nacque un report – il cosiddetto *Rapporto Ware* (The RAND for the Office of the Director of Defense Research, 1970) nel quale, secondo il riassunto che ne propone Warner, emergeva l'impossibilità di "alcuna soluzione ingegneristica al problema della sicurezza informatica" (Warner, 2012, pp. 784-5). Nonostante questo approccio da parte delle istituzioni politiche, i produttori di computer cominciarono a sviluppare "una serie di innovazioni nella programmazione dei computer per migliorare la sicurezza". L'IBM ad esempio sviluppò "la crittografia dei dati

che scorrevano tra i computer" per proteggere le transazioni bancarie in risposta ad una call "per un sistema federale di crittografia digitale" lanciata nel 1974 dal *National Bureau of Standards*; nel1976 il Federal Information Processing *Standard* adottò un sistema federale di crittografia digitale che assunse il nome di Digital Encryption *Standard* (DES) (ivi, pag. 785).

2. La diffusione delle tecnologie informatiche ed il loro utilizzo da parte delle forze armate americane fece emergere sempre più “quanto i sistemi informativi fossero vulnerabili a intrusioni a distanza così come da abusi da parte di insiders” (ibid.). Nel 1972 un test su un database che avrebbe dovuto unire “i dati di diverse agenzie per permettere ai loro analisti un maggiore accesso” alle informazioni e ai dati della *Intelligence Community* ne mostrò la vulnerabilità, diffondendo scetticismo tra le autorità sulla possibilità di raggiungere un soddisfacente livello di sicurezza multi-livello. Nel 1979 un’esercitazione – o una presunta tale, visto che dalle ricostruzione emergono dubbi sulla possibilità che si sia trattato di un errore – avvenuta presso il *North American Air Defense Command* (NORAD) fece scattare l’allarme di un attacco missilistico reale. Sempre più report pubblici e articoli di giornale venivano dedicati in quegli anni alla cybersecurity, che cominciò a diventare anche oggetto dell’immaginario collettivo (ad esempio attraverso il film WarGames del 1983). Nel 1984 l’amministrazione Reagan promulgò la *National Security Decision Directive (NSDD) – 145* che “rese effettivamente la NSA responsabile della definizione di standard e linee guida, della conduzione di ricerche e del monitoraggio di tutti i ‘sistemi di telecomunicazione governativi e dei sistemi informativi automatizzati’” (Warner, 2012, pp. 787-8). Ad esso fece seguito l’attenzione del Congresso, che temeva che un iniziativa tutta in capo al Presidente ed un ruolo eccessivo attribuito alla NSA potessero rappresentare un pericolo per le libertà civili. Tra il 1985 e il 1987 il Congresso dibatté a lungo della cybersecurirty ospitando le udienze di vari portatori di interesse (American Bankers Association, American Civil Liberties Union ecc.); nel 1987 approvò il *Computer Security Act* che divise i compiti relativi alla cybersecurity tra NSA – a cui era demandato il compito di proteggere le reti di “sicurezza nazionale” – e il *National Bureau of Standards* (che si sarebbe invece occupato della sicurezza delle reti federali). Sotto la presidenza di George H.W. Bush, nel luglio del 1990 venne approvata attraverso la *National Security Directive (NSD)-42* la legge *National Policy for the Security of National Security Telecommunications and Information Systems* che esautorava la NSA dalla “protezione delle informazioni sensibili ma non classificate del governo degli Stati Uniti” e ne attribuiva il compito al *National Institute of Standards and Technology*, riaffermava “il primato del Dipartimento (e della NSA) nella protezione dei sistemi di sicurezza nazionale” ed autorizzava il direttore della NSA (DIRNSA) a “ispezionare le reti ‘.gov’ e ‘.mil’ che contenevano dati classificati di sicurezza nazionale” (ibidem, p. 789).

3. Contestualmente alla consapevolezza sulla vulnerabilità causata dalla proliferazione delle tecnologie informatiche cresceva tra i teorici militari la consapevolezza di poter sfruttare questo elemento nel warfare americano. La guerra in Vietnam – “con la sua svolta verso munizioni a guida di precisione, sensori remoti sul campo di battaglia e l’elaborazione computerizzata di ogni sorta di dati logistici, amministrativi e operativi” – aveva messo in evidenza l’importanza dei flussi di informazione nei contesti di guerra (ivi,

p. 789). Da qui emergeva l'idea che fosse possibile "interrompere le funzioni di comando e controllo impiegate da un avversario" e che "i sistemi di comando e controllo computerizzati fossero un obiettivo promettente" (ivi, p. 790). La prima guerra in Iraq dette un grande impulso a questa idea, tanto da meritarsi l'appellativo – non privo di enfasi – di "prima guerra dell'informazione"; in questa categoria, fa notare Warner, venivano inclusi "tutti i modi non cinetici di colpire un nemico" (ibidem). In questo dibattito fu fondamentale il contributo di Colin Powel, allora *Chairman of the Joint Chiefs of Staff*, che nel 1993 pubblicò un memorandum sulle politiche militari in ambito cybernetico (Chairman of the Joint Chiefs of Staff, 1993). In quegli anni l'organizzazione delle forze armate americane si dotò di strutture finalizzate allo sviluppo del cyberwarfare: nel 1993 nacque l'*Air Force Information Warfare Center*, nel 1994 la *Navy Information Warfare Activity* e l'*Army Land Information Warfare Activity*. Queste iniziative stimolarono e avviarono il dibattito su cybersecurity e cyberwarfare anche in Russia e Cina, preoccupate non solo dalla riorganizzazione delle forze armate americane ma anche dalla diffusione di personal computer di produzione americana tra i propri cittadini (cfr. Warner, 2012, pp. 791-3).

4. Negli anni Novanta gli Stati Uniti – in particolar modo gli esperti della NSA – cominciarono a preoccuparsi della loro vulnerabilità legata a possibili cyberattacchi terroristici. In un report pubblicato nel 1991 dalla *National Academy of Sciences* possiamo leggere:

> *Siamo a rischio. L'America dipende sempre più dai computer. Controllano la fornitura di energia, le comunicazioni, l'aviazione e i servizi finanziari. Sono usati per immagazzinare informazioni vitali, dalle cartelle cliniche ai piani finanziari, fino ai casellari giudiziari* (National Academy of Science, Computer Science and Telecommunications Board, 1991).

La diffusione del *Morris worm* nel 1988 e l'isteria collettiva provocata dal virus Michelangelo nel 1992 mostrarono come la percezione della vulnerabilità digitale era diventata un fenomeno molto diffuso nell'opinione pubblica. Il 1995 fu un anno di "svolta concettuale" sulle questioni della cybersecurity: "i funzionari e i consulenti del governo degli Stati Uniti" infatti cominciarono ad adottare un approccio secondo il quale "le reti informatiche […] comprendevano solo una parte della vulnerabilità della nazione agli attacchi informatici"; il problema più grande risiedeva nei dati, attraverso la manipolazione dei quali gruppi terroristici o nazioni ostili potevano "distruggere le infrastrutture critiche dell'America" (Warner, 2012, p. 795). Tra gennaio e giugno 1995 la *RAND Corporation* su delega del Dipartimento della Difesa condusse una serie di esercitazioni che consistevano nel "creare finte risposte difensive del governo degli Stati Uniti a uno scenario di crisi in Medio Oriente che minacciava un intervento armato americano"; queste esercitazioni misero in evidenza la facilità con la quale era possibile "devastare le infrastrutture critiche negli Stati Uniti per mezzo di attacchi alla rete informatica" (ibidem). Il *General Accounting Office* riferì inoltre nel maggio 1996 che le reti del Dipartimento della Difesa "erano apparentemente attaccate (o, quasi certamente, sondate) circa 250.000 volte al giorno" (ibidem). Questa consapevolezza crebbe anche durante la Presidenza Clinton e nel giugno 1997 il *Joint Chiefs of Staff* (organo che riunisce i Capi di

Stato maggiore) diresse un'esercitazione che rappresenta lo spartiacque per la consapevolezza contemporanea sulla cybersecurity: l'esercitazione denominata *Eligible receiver*. Finalizzata a testare "la capacità del Dipartimento di lavorare con altri rami del governo per rispondere a un attacco informatico alle infrastrutture critiche della nazione", l'esercitazione prevedeva che un *red team* interpretasse un nemico impegnato ad orchestrare un cyberattacco agli Stati Uniti utilizzando normali pc in commercio e software facilmente scaricabili da internet. L'esercitazione dimostrò che con questi pochi mezzi era possibile mandare in tilt il sistema elettrico americano. Altri attacchi informatici avvenuti nel 1998 confermarono ciò che l'anno precedente *Eligible receiver* aveva già dimostrato.

Cosa è la Cybersecurity

Dalla seconda metà degli anni Novanta quindi il dibattito sulla cybersecurity raggiunge la base del grado di maturazione a partire dalla quale si sviluppa anche ai giorni nostri. Un problema rilevante in questo dibattito, ricorrente in numerosi scritti degli studiosi che se ne sono occupati, è cosa si intenda per cybersecurity: le definizioni sono infatti molteplici, come è facile aspettarsi per un oggetto di ricerca recente e in perenne evoluzione. Gli studiosi Dan Craigen, Nadia Diakun-Thibault e Randy Purse aprono un articolo intitolato *Defining cybersecurity* con una significativa citazione del filosofo analitico Charles Leslie Stevenson: "scegliere una definizione significa perorare una causa" (Craigen et alii., 2014, p. 13). Come ci insegna la filosofia del linguaggio infatti, definire i concetti non è mai un'operazione neutra e comporta sempre delle conseguenze sugli usi legittimi e illegittimi di un concetto. Gli autori del saggio evidenziano come "l'assenza di una definizione concisa e ampiamente accettabile, che colga la multidimensionalità della cybersecurity, inibisce potenziali progressi tecnologici e scientifici, rafforzando una visione prevalentemente tecnica della cybersecurity e separando le discipline che invece dovrebbero agire di concerto per risolvere le sfide complesse della cybersecurity"; a questo approccio essi ne contrappongono uno che invece prenda atto della "vera natura interdisciplinare della cybersecurity", permettendo così di evidenziare come essa coinvolga dimensioni organizzative, economiche, sociali e politiche che finirebbero per essere trascurate adottando un approccio esclusivamente tecnico. Partendo da questa consapevolezza i tre studiosi hanno passato in rassegna le principali definizioni di cybersecurity presenti nella letteratura per evidenziarne gli aspetti più rilevanti, per poi sottoporre a "un gruppo multidisciplinare di professionisti della cybersecurity, accademici e laureati" la questione definitoria al fine di "sviluppare una definizione più olistica che collochi meglio la cybersecurity come attività interdisciplinare, facendo consapevolmente un passo indietro rispetto alla visione tecnica predominante attraverso l'integrazione di molteplici" (Craigen et alii., 2014, pp. 13-4).

Un importante punto di partenza per comprendere la cybersecurity è decostruirne il termine. Il prefisso cyber "connota il cyberspazio e si riferisce alle reti elettroniche di comunicazione e alla realtà virtuale" e indica un "ambiente informativo", una "ecosistema dinamico, in evoluzione e multilivello di infrastrutture fisiche, software, regolamenti, idee,

innovazioni e interazioni influenzate da una popolazione di utilizzatori in espansione" (Iidem, p. 14). Questo aspetto della cybersecurity sollecita una sua trattazione tecnica: per intervenire con consapevolezza nell'ambito della cybersecurity occorrono conoscenze tecniche sulle questioni ad essa connesse, alle vulnerabilità, ai rischi e alle soluzioni potenziali. La parola security apre invece il dibattito a implicazioni che travalicano l'ambito tecnico, ed infatti questa seconda parte del concetto è quella più problematica. Citando Buzan, Wæver e Wilde (1998), i tre autori evidenziano come "i discorsi sulla sicurezza includono necessariamente e cercano di capire chi mette in sicurezza, su quali questioni (minacce), da chi (l'oggetto di riferimento), perché, con quali risultati e in quali condizioni" (Iidem). Il concetto di sicurezza è un "contested term" (iidem), perché implica un giudizio di valore (politico, etico, sociale ed economico) su cosa sia la sicurezza. Tale richiamo alla complessità tuttavia, evidenziano i tre autori citando Baldwin (1997), non può tradursi in una rinuncia a formulare ipotesi definitorie.

Dalla ricognizione della letteratura disponibile e dal lavoro con il gruppo multidisciplinare i tre studiosi hanno formulato la seguente definizione di cybersecurity:

> *Cybersecurity is the organization and collection of resources, processes, and structures used to protect cyberspace and cyberspace-enabled systems from occurrences that misalign de jure from de facto property rights (Craigen et alii., 2014, p. 17).*

Il riferimento all'organizzazione e all'insieme di risorse, processi e strutture evidenzia le "dimensioni multiple, intrecciate e la complessità intrinseca della sicurezza informatica"; il livello di astrazione di questo riferimento, che non specifica quali risorse, strutture ecc., permette alla definizione di non essere prescrittiva, di non limitare l'ambito di azioni e le risorse della cybersecuirty a quelli disponibili in un determinato contesto e momento storico, riconoscendone invece la "natura dinamica". Il riferimento alla protezione del cyberspace e dei sistemi abilitati al cyberspace estende l'ambito da proteggere anche ai "sistemi di controllo del computer" ed ai "sistemi cyber-fisici", "ai beni e alle informazioni di interesse all'interno del cyberspazio e dei sistemi connessi". Il riferimento agli "eventi" riconosce invece che la cybersecurity deve affrontare molteplici tipi di minacce (intenzionali, accidentali ecc.) (ibidem). Il riferimento al disallineamento tra diritti di proprietà *de jure* e *de facto* parte invece dalla consapevolezza che i dati che la cybersecurity ha il compito di proteggere rispondono a una doppia logica: quella della proprietà e quella del controllo. I diritti di proprietà, come evidenziano Ostrom e Hess (2007, p. 17), soprattutto in virtù della proliferazione delle risorse informative elettroniche, sono diventati una materia più complessa che conosce molteplici tipologie: accesso ("il diritto di entrare in un'area fisica definita e di godere di benefici non sottrattivi"), contributo ("il diritto di contribuire al contenuto" della risorsa stessa), estrazione ("il diritto di ottenere unità di risorse o prodotti di un sistema di risorse"), rimozione ("il diritto di rimuovere i propri artefatti dalle risorse"), gestione/partecipazione ("il diritto di regolare i modelli d'uso interni e di trasformare la risorsa apportando miglioramenti"), esclusione ("il diritto di determinare chi avrà i diritti di accesso, contribuzione, estrazione e rimozione e come questi diritti possono essere trasferiti") e alienazione ("il diritto di vendere o affittare i diritti di gestione ed esclusione") (iidem). Qualsiasi evento o attività che disallinei la condizione

reale (*de facto*) dei diritti di proprietà in una di queste sei tipologie da quella giuridicamente legittima (*de jure*) – sia che ciò avvenga intenzionalmente o per caso – costituisce un problema di cybersecurity.

Le implicazioni politiche della cybersecurity

Gli attacchi informatici sono oggi parte di quello che Myriam Dunn Cavelty chiama "triplice minaccia" (2010, p. 154) per la sicurezza nazionale costituita per l'appunto dai rischi connessi alla cybersecurity, dagli attacchi biologici e da quelli nucleari. Il cyberspace è allo stesso stesso da un lato un ecosistema virtuale e immateriale – essendo popolato da interazioni digitali – e dall'altro materiale – perché tali interazioni sono rese possibili e permettono il controllo di apparati e infrastrutture materiali. La cybersecurity "si occupa di rendere sicuro questo 'ambiente bioelettronico'" (p. 155). Le minacce che essa fronteggia – e che nella definizione affrontata nel paragrafo precedente abbiamo qualificato come "eventi" – possono essere di triplice tipo: guasti ("causati da carenze nel sistema o in un elemento esterno da cui il sistema dipende" che "possono essere dovuti a errori di progettazione del software, degrado dell'hardware, errore umano o dati corrotti"), incidenti (che "includono l'intera gamma di eventi che si verificano casualmente e potenzialmente dannosi, come i disastri naturali") o attacchi ("orchestrati da un nemico") (eadem).

Cavelty evidenzia come in questa triplice tipologia di eventi, gli attacchi e le intrusioni ostili sono la minaccia più pericolosa. Se infatti un intruso prende il pieno controllo del sistema "può ritardare, interrompere, corrompere, sfruttare, distruggere, rubare e modificare le informazioni" ed il loro flusso (p. 156). Citando i lavori di Dhillon (2007) e Stoneburner (2001), Cavelty sottolinea come, di fronte a questo rischio, i fini della cybersecurity sono triplici: assicurare riguardo ai dati ed alle informazioni riservatezza (garantire la "protezione delle informazioni dalla divulgazione a soggetti non autorizzati"), integrità (garantire la "protezione delle informazioni dall'essere modificate da soggetti non autorizzati") e disponibilità (assicurare che le informazioni siano "disponibili a soggetti autorizzati quando richieste") (Cavelty, 2010, p. 156).

La tesi più rilevante che Cavelty sostiene nel suo saggio è che la sicurezza nazionale e la cybersecurity siano due ambiti della sicurezza che originariamente erano distinti e che successivamente si sia realizzata una progressiva sovrapposizione tra di essi. Partiamo da una ricognizione del perché inizialmente questi rappresentavano due ambiti distinti.

	Caratteristiche comuni	Differenze
Cybersecurity	Ambiscono a realizzare una condizione libera dal pericolo.	Portata: difendere la sicurezza degli ecosistemi digitali Attori coinvolti: esperti informatici Misure tecniche finalizzate ad assicurare che le informazioni e i dati circolino come dovrebbero

National security	Si confrontano con gli stessi soggetti che pongono una minaccia: terroristi o stati nemici.	Portata: difesa della sicurezza nazionale sotto tutti i punti di vista (monetario, sicurezza personale degli invidui ecc.) Attori coinvolti: professionisti della sicurezza Misure assicurate da una pluralità di piani tra cui il mantenimento delle forze armate, dei servizi di intelligence ecc.

Sebbene – coerentemente con la periodizzazione di Werner che abbiamo riproposto nel primo paragrafo – questo processo abbia avuto inizio negli anni Settanta, Cavelty evidenzia che la "fusione delle due nozioni" (Cavelty, 2010, p. 156) sia avvenuta negli Stati Uniti negli anni Novanta. In quel decennio divenne infatti palese che l'estrema diffusione delle tecnologie informatiche esponeva il paese a una vulnerabilità senza pari nel contesto internazionale. Se infatti gli Stati Uniti, soprattutto dopo il 1989, avevano conquistato una supremazia militare tale per cui non c'era nessun attore capace di piegarli o colpirli militarmente, quegli stessi attori sebbene più deboli potevano colpire attraverso un cyberattacco le infrastrutture critiche americane (acquedotti, trasporti, sistemi elettrici ecc.). Come evidenzia Cavelty:

> *Con la crescita e la diffusione delle reti informatiche in sempre più aspetti della vita, l'oggetto della protezione era cambiato. Mentre prima consisteva in limitate reti governative, ora riguardava l'intera società. In questo modo, le minacce informatiche diventavano una minaccia ai valori fondamentali della società e al benessere economico e sociale dell'intera nazione – e la cybersecurity come garanzia di protezione delle infrastrutture critiche diventava un compito chiave della sicurezza nazionale (Eadem, p. 159).*

Tale sovrapposizione tuttavia non implicava che le modalità e le forme per garantire sicurezza nazionale e cybersecurity fossero le stesse: la specificità della sicurezza da garantire rendeva infatti diverso l'impegno per garantirla. La diffusione delle ICT nell'ambito economico rendeva più poroso e complesso il sistema da difendere; e inoltre, contrastare i cyber-attacchi significa in primo luogo indagarne l'origine e la natura (vandalismo, atto di terrorismo, di guerra ecc.), rendendo necessario estendere sotto un punto di vista giuridico le prerogative di forze dell'ordine e autorità di sicurezza; al contrario la sicurezza nazionale fino ad allora si era basata sulla capacità di deterrenza e prevenzione degli attacchi. Inoltre l'ondata di privatizzazioni partita negli anni Ottanta aveva fatto sì che gran parte delle infrastrutture critiche passibili di un cyberattacco erano proprietà o gestite dal settore privato. Se quindi era chiaro sin da subito che l'iniziativa in merito alla cybersecurity spettasse allo Stato, era altrettanto chiaro che in quella struttura socio-economica questi non poteva gestirlo da solo. Lo Stato aveva una sola opzione per assicurare la sicurezza cybernetica: "cercare di convincere il settore privato a condividere parte della responsabilità" (ivi, p. 160), trattando quest'ultimo come "partner paritario"

(eadem) e convincendolo dell'utilità e della necessità di condividere questa responsabilità, in nome del fatto che gli interessi in materia di sicurezza del settore privato e dello Stato coincidevano.

Questa consapevolezza assunta dalla politica e sollecitata nel settore privato, come evidenzia Cavelty, è riscontrabile nel documento *Critical Foundations: Protecting America's Infrastructures* emanato dalla *President's Commission on Critical Infrastructure Protection* ancora una volta nel 1997 (PCCIP, 1997), lo stesso anno spartiacque di *Eligible receiver*. In questo documento veniva sostenuta la linea secondo la quale "la natura interdipendente delle infrastrutture crea un ambiente di rischio condiviso" tra autorità politiche e attori privati e che pertanto, in presenza di rischi condivisi (come ad esempio "il terrorismo, lo spionaggio industriale e il crimine organizzato") devono essere condivise anche le responsabilità nell'affrontarli. Tale appello al settore privato muoveva anche dall'idea che proprietari e gestori privati delle infrastrutture critiche devono essere "in prima linea negli sforzi di sicurezza, poiché sono i più vulnerabili agli attacchi informatici" (p. 161). Allo stesso tempo nell'affrontare i problemi di cybersecurity quindi la difesa nazionale non era più "una prerogativa esclusiva del governo", e "la sicurezza economica non riguardava più solo il mondo degli affari" (eadem). Il report invocava una strategia cooperativa della "sicurezza distribuita" (eadem) e della "condivisione delle informazioni", ispirata a una situazione win-win: le autorità politiche dispongono di informazioni su gruppi e nazioni potenzialmente autrici di atti ostili, gli attori privati dispongono di informazioni tecnologiche preziose nell'affrontare la questione; solo la condivisione di queste informazioni può garantire un'efficace strategia di cybersecurity.

L'idea di sicurezza subiva anch'essa una metamorfosi in virtù dell'emergere dell'esigenza di proteggere il cyberspace: la diffusione delle ICT e la pluralità di attori esposti alla vulnerabilità cybernetica rendeva infatti obsoleta l'idea di produrre una sicurezza assoluta secondo una logica binaria che separa la sicurezza dall'insicurezza. Emergeva invece una zona grigia che produce perennemente rischi e vulnerabilità e l'unica logica per affrontarla efficacemente era quella della "gestione del rischio", dell'accettazione di questa presenza costante di insicurezza e della necessità di affrontarla in maniera continuativa e sempre in aggiornamento. Come evidenzia Cavelty, "l'atto tradizionalmente sovrano di rendere sicura la società si è spostato nello spazio domestico", e pertanto l'assicurarla richiedeva il coinvolgimento di tutti gli attori coinvolti e la consapevolezza che una tale disseminazione del bisogno di sicurezza non poteva mai essere colmato in maniera definitiva (p. 161).

La specificità delle infrastrutture critiche e il loro statuto proprietario inoltre rendeva l'attività di metterle in sicurezza oggetto di una perenne negoziazione tra attori pubblici e privati, producendo rilevanti conseguenze politologiche che Cavelty riassume nella formula "queste pratiche sono espressione e causa della rottura delle distinzioni politiche fondamentali tra interno/esterno, pubblico/privato, civile/militare e normale/eccezionale" (p. 162). La cybersecurity prima ancora di confrontarsi con le minacce di un nemico si confronta con una consapevolezza della vulnerabilità sociale ed economica di uno Stato:

la sicurezza che persegue è “incorporata nelle routine e nelle tecnologie quotidianamente usate da attori che non sono nemmeno necessariamente professionisti della sicurezza” (eadem).

Conclusioni

Con questa breve ricognizione abbiamo delineato i tratti fondamenti del dibattito sulle cybersecurity evidenziando alcuni aspetti della sua rilevanza politica. Il campo di ricerca della sicurezza informatica è un campo estremamente ampio e per il quale è prevedibile che nei prossimi anni acquisirà una sempre maggiore rilevanza pubblica. Comprenderne la portata è una sfida non solo per analisti, esperti informatici e decisori politici ma per la tenuta stessa della democrazia.

Il saggio è frutto della piena collaborazione tra i due autori e ogni contenuto è condiviso nel merito. Per la stesura, il paragrafo “Una trentennale preistoria” è attribuibile a Danilo Caivano, mentre i paragrafi “Cosa è la Cybersecurity” e “Le implicazioni politiche della cybersecurity” ad Alfredo Ferrara.

Bibliografia

Baldwin, D. A. 1997. The Concept of Security. Review of International Studies, 23(1): 5-26.

Buzan, B., Wæver, O., & De Wilde, J. 1998. Security: A New Framework for Analysis. Boulder, CO: Lynne Rienner Publishers.

Cavelty, M. D. 2010. Cyber-Security. In J. P. Burgess (Ed.), The Routledge Handbook of New Security Studies: 154-162. London: Routledge.

Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining cybersecurity. Technology Innovation Management Review, 4(10), pp. 13-21.

Dhillon, G. (2007) Principles of Information Systems Security: Text and Cases, New York: John Wiley & Sons.

Chairman of the Joint Chiefs of Staff (1993), *‘Command and Control Warfare’*, Memorandum of Policy 30, 8 March 1993 http://dodreports.com/pdf/ada389344.pdf.

National Academy of Science, Computer Science and Telecommunications Board (1991), *Computers at Risk: Safe Computing in the Information Age,* National Academy Press, Washington 1991; http://www.nap.edu/openbook.php?record_id¼1581&page¼74

Ostrom E. e Hess C. (2008), Private and Common Property Rights, in Encyclopedia of Law & Economics. Northampton, MA: Edward Elgar, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1304699

PCCIP, President’s Commission on Critical Infrastructure Protection (1997) Critical Foundations: Protecting America’s Infrastructures, Washington, DC: US Government Printing Office.

Stoneburner, G. (2001) Computer Security: Underlying Technical Models for Information Technology Security. Recommendations of the National Institute of Standards and Technology, NIST Special Publication 800-33, Washington, DC: US Government Printing Office.

The RAND for the Office of the Director of Defense Research (1970), *Report of the Defense Science Board Task Force on Computer Security, Security Controls for Computer Systems* [the Ware Report], 11 February 1970 http://seclab.cs.ucdavis.edu/projects/history/papers/ware70.pdf

Warner M. (2012), Cybersecurity: A Pre-history, in Intelligence and National Security, 27, 5, pp. 781-799, DOI: 10.1080/02684527.2012.708530

Danilo Caivano Alfredo Ferrara e Giuseppe Cascione

More Posts

Category: Iconocrazia 19/2021 - "Bivi europei e questioni tecno-politiche" | RSS 2.0
Responses are currently closed, but you can trackback from your own site.

No Comments

Comments are closed.

Iconocrazia Rivista scientifica semestrale di scienze sociali e simbolica politica ISSN 2240-760X | Aut. Trib. di Bari n. 3690//2011 - num Reg. Stampa 42 Bari © 2012 | designed by POOYA