federalismi.it
RIVISTA DI DIRITTO PUBBLICO ITALIANO, COMPARATO, EUROPEO

25 APRILE 2018

# La cyber sicurezza come nuova dimensione della difesa dello Stato: bene meritorio o bene pubblico?

di Mario De Benedetti
Laureato in Relazioni internazionali
LUISS "Guido Carli" – Roma

# La cyber sicurezza come nuova dimensione della difesa dello Stato: bene meritorio o bene pubblico? *

**di Mario De Benedetti**
Laureato in Relazioni internazionali
LUISS "Guido Carli" – Roma

**Sommario**: **1.** Introduzione; **2.** La cyber sicurezza: natura ed evoluzione di un bene; **3.** Considerazioni conclusive

## 1. Introduzione

La sicurezza nazionale sta espandendo sempre più i propri confini fisici, tralasciando la propria connessione con la territorialità degli Stati-Nazione e rivolgendo sempre più le proprie istanze verso la dimensione virtuale. Anche le minacce provenienti dall'esterno e mirate alla sottrazione di dati sensibili, siano esse di matrice terroristica o di stampo criminale, assumono quella caratteristica di liquidità che le libera dal loro collegamento con la dimensione fisica connessa alla materia tangibile.

Obiettivo di questo elaborato è di contribuire ad inquadrare un'impostazione teorica di stampo microeconomico della cyber sicurezza, che da bene valutabile sul mercato come bene meritorio può, in virtù delle trasformazioni subite dalla dimensione della sicurezza e apportate dalla rivoluzione cibernetica attualmente in atto, essere catalogato come una risorsa identificabile alla stregua di bene pubblico puro, alla cui tutela ed implementazione devono concorrere sia le istituzioni nazionali, sia gli operatori del settore privato.

Indispensabile, a questo punto, diviene una piccola introduzione dei concetti riguardanti la necessità dell'intervento pubblico nei casi in cui i meccanismi del libero mercato e dei prezzi non riescano ad assorbire le deviazioni dei processi di allocazione delle risorse.

Nell'ambito della teoria microeconomica generale, un bene pubblico è riconosciuto come una delle cause dei fallimenti del mercato, intesi come l'impossibilità dei mercati di poter raggiungere l'equilibrio economico generale in quanto non in grado di organizzare la produzione in maniera efficiente o di non allocare efficientemente beni e servizi ai consumatori[1].

* Articolo sottoposto a referaggio.

[1] I fallimenti del mercato rappresentano il venir meno delle ipotesi prese in considerazione dal primo Teorema dell'Economia del benessere, il quale stabilisce che per ogni allocazione iniziale delle risorse a disposizione, il sistema di mercato in concorrenza perfetta garantisce un'allocazione finale efficiente, tale da non poter migliorare le condizioni di un individuo senza peggiorare le condizioni di un altro individuo.

Un bene è considerato pubblico quando risponde a due caratteristiche fondamentali. Una prima caratteristica risiede nella indivisibilità o non rivalità, che ne permette il consumo da parte di una persona senza impedirne l'utilizzo da parte di un altro individuo. La seconda caratteristica di un bene pubblico è la non escludibilità, nel senso che i costi per escludere gli individui non paganti dalla possibilità di impiego del bene sarebbero troppo alti da sostenere per un'impresa privata che tenti di massimizzare i propri profitti nella ricerca di un'efficienza allocativa[2].

In mercati perfettamente concorrenziali, l'efficienza allocativa di risorse è determinata dall'incontro spontaneo tra la domanda e l'offerta, a loro volta scandite dalle scelte di consumo e di produzione degli attori economici, all'interno di un sistema statale in cui si dia per scontato che i cittadini operino le loro scelte sulla base di un calcolo razionale[3] incoraggiato dalla presenza di una forma di governo democratica, in cui la difesa dei diritti di proprietà e l'efficiente amministrazione della giustizia (*rule of law*) facciano percepire che la tutela delle libertà fondamentali sia una imparziale priorità da parte del legislatore.

L'equilibrio generale è, quindi, definibile come il punto in cui le decisioni indipendenti sia dei consumatori che massimizzano l'utilità, sia delle imprese che massimizzano i profitti si intersecano, conducendo all'inevitabile instaurazione di una situazione di equilibrio simultaneo di domanda e offerta in tutti i mercati e, conseguentemente, all'uguaglianza tra beneficio e costo marginale per ogni bene e servizio[4]. La concorrenza perfetta, in un mercato in equilibrio, si verifica quando: la libertà di ingresso nel mercato è piena; nessuna delle decisioni individuali di imprese e consumatori è in grado di influenzare i prezzi di

[2] La difesa nazionale, sia interna, sia esterna, rappresenta, forse, l'esempio più tipico di bene pubblico apportato dalla teoria economica; data la presenza simultanea delle caratteristiche di non rivalità e di non escludibilità nel consumo, la difesa nazionale appartiene, più precisamente, alla categoria dei beni pubblici puri.

[3] Nella teoria economica si assume che il consumatore conosca le proprie preferenze e che possa esercitare le proprie scelte attraverso combinazioni che siano in grado di soddisfare i suoi desideri, data la possibilità di azioni alternative che permettono al consumatore di agire in modo libero e non condizionato. Si dà per scontato, quindi, che il consumatore adotti le proprie preferenze in modo completo, riflessivo e transitivo. La completezza si concretizza nella capacità del consumatore di poter sostenere la propria preferenza di un bene A rispetto ad un bene B o viceversa, oppure se li preferisca entrambi; la riflessività comporta che un paniere di consumo debba essere almeno del medesimo valore di se stesso per poter essere preferito; la transitività significa che la scelta del paniere A rispetto a B e la scelta di B rispetto al paniere C, riflette il fatto che il paniere A sia preferibile al paniere C, impedendo la circolarità tra le preferenze individuali.

[4] Il comportamento dei consumatori relativamente ad un certo bene viene descritto dalla teoria economica tramite una curva di domanda individuale che ci informa su quanto bene verrebbe acquistato da un consumatore per ogni determinato livello di prezzo. Un curva di domanda di mercato di quel determinato bene ci informa invece sulla domanda che i consumatori effettuerebbero al variare del prezzo, sommando le diverse domande individuali per ogni dato livello di prezzo. Si definisce beneficio marginale il beneficio aggiuntivo ottenuto dall'incremento di una unità di prodotto, accompagnato dal costo aggiuntivo per l'aumento di questa unità di prodotto, che a sua volta prende il nome di costo marginale. Supponendo che il consumatore tenti di massimizzare il risultato delle proprie scelte, acquistando una unità di prodotto in più, egli percepirà un miglioramento del suo status iniziale se il beneficio marginale sia maggiore del costo marginale dovuto all'acquisto di quell'unità di prodotto in più. Il consumatore continuerà ad acquistare unità di prodotto, fino a quando il costo marginale dell'ultima unità di prodotto acquistata eguagli, o superi, il beneficio marginale.

mercato; vi sia omogeneità nel prodotto; non vi siano asimmetrie informative e, perciò, vi sia completa trasparenza del mercato[5].

L'intervento pubblico tenta di rimediare al fallimento di mercato nella fornitura di beni pubblici attraverso due correttivi generali: primo, provvedendo al sussidio della fornitura eventualmente privata del bene pubblico sia direttamente, sia indirettamente attraverso il sistema fiscale. Secondo, provvedendo esso stesso a fornire il bene pubblico pagandone il relativo prezzo di fornitura mediante le entrate raccolte da tassazione obbligatoria.

Le cause che conducono all'alterazione dell'equilibrio di mercato sono individuate, dalla teoria economica, non solo nei beni pubblici, ma anche nella presenza di monopoli, esternalità, asimmetrie informative e nei beni meritevoli di tutela pubblica (o beni meritori).

In presenza di un monopolio, l'offerta di beni e servizi è concentrata in un solo produttore-venditore, che in questo modo potrà esercitare la propria influenza condizionando la quantità di prodotto immessa sul mercato e incidendo, così, sull'andamento del prezzo.

Il monopolio può essere naturale, quando una sola impresa è in grado di poter produrre un bene a costi più bassi rispetto ai costi che sosterrebbero due o più imprese[6]; se l'efficienza produttiva è raggiunta quando una sola impresa soddisfa l'intera domanda di mercato, quest'impresa monopolistica potrà comunque utilizzare il proprio potere di mercato per fissare un prezzo superiore al costo marginale; questo genera una perdita di efficienza allocativa dovuta alla perdita secca di benessere sociale che si genera in questo caso. Se più imprese competono sul mercato caratterizzato come monopolio naturale, il prezzo diventa maggiormente allineato con il costo marginale di produzione, ma la produzione viene ad essere effettuata ad un costo maggiore di quello di un monopolista, perdendo quindi efficienza produttiva.

Quando è l'ordinamento giuridico ad assicurare, tramite riserva di legge, l'esercizio esclusivo dell'attività produttiva, allora il monopolio è definito legale. L'intervento pubblico, per correggere le inefficienze del monopolio, provvede ad instaurare un regime concorrenziale, oppure consente alla pubblica autorità di regolare strettamente i prezzi, lasciando che il monopolio continui a sussistere[7].

---

[5] G.NAPOLITANO – M.ABRESCIA, *Analisi economica del diritto pubblico,* Il Mulino, 2009; R.COOTER – U. MATTEI – P.G MONATERI – R. PARDOLESI – T. ULEN, *Il Mercato delle regole. Analisi economica del diritto civile*, vol. I, Il Mulino, 2006.

[6] Il monopolio naturale caratterizza numerosi settori produttori di pubblici servizi (telecomunicazioni, trasporti ferroviari, energia elettrica), essendo infatti connesso al controllo di risorse che non sono tecnicamente o economicamente replicabili.

[7] La regolazione del monopolio privato attraverso la concorrenza è alla base della legislazione *antitrust* di origine anglosassone e regolata dalla normativa europea attraverso gli artt. 101 e ss. del Trattato sul funzionamento dell'Unione europea (Tfue); in Italia, la regolamentazione *antitrust* attraverso la Legge n. 287 del 10 ottobre 1990.

Le esternalità sono collegate alla capacità di scambio operate dagli individui all'interno di un mercato secondo questo schema: coloro che sono prendono parte allo scambio ne ottengono i benefici sopportandone i costi; tuttavia, sia i benefici sia i costi degli scambi possono riversarsi su soggetti terzi alle parti coinvolte in esso.

Le esternalità, che possono essere sia negative, sia positive[8], rappresentano questi costi e benefici che ricadono nella sfera individuale di soggetti estranei alle attività poste in essere: il fallimento del mercato in presenza di esternalità si verifica per il fatto che colui che le genera non è soggetto a sanzioni, sentendosi libero in questo modo di esercitare uno scarso autocontrollo sulla propria attività. In termini economici, è possibile sostenere che si verifica una differenza tra costo marginale privato e costo marginale sociale, data dalla produzione di *output* eccessivo[9].

Per ottenere l'ottimo sociale in presenza di esternalità, l'intervento pubblico dovrebbe portare l'impresa privata ad «internalizzare» l'esternalità stessa, inducendo a restringere il livello di produzione privato al punto socialmente ottimo[10].

L'asimmetria informativa costituisce un'altra forma di distorsione del mercato che impedisce il raggiungimento dell'ottimo sociale raggiungibile attraverso gli scambi volontari, rendendo necessario l'intervento pubblico per correggere tale alterazione. Tra le ipotesi, infatti, di un mercato in concorrenza perfetta vi è anche quella dell'altrettanto perfetto livello di informazione tra gli operatori economici; un'asimmetria informativa si ha quando una delle parti del rapporto economico possiede maggiori informazioni rispetto alla controparte.

Le forme principali di asimmetrie informative riconosciute dalla letteratura economica sono denominate: la selezione avversa, in cui il deficit informativo si presenta nella fase pre-contrattuale, quando la parte che possiede il maggior livello di informazioni riguardanti il livello dello scambio è in grado di influenzare gli effetti economici del contratto concluso[11]; l'azzardo morale, fenomeno di opportunismo post-

[8] Le esternalità sono negative quando l'attività di un individuo comporta un costo che ricade su un terzo estraneo (ad esempio, l'inquinamento atmosferico derivante da un'attività industriale); le esternalità sono positive quando l'attività posta in essere da un soggetto arreca un beneficio a terzi.

[9] Il costo marginale privato è il costo sostenuto dall'impresa che genera l'esternalità quando produce un'unità addizionale di prodotto; il costo marginale sociale è il costo che la società sostiene quando si produce un'unità addizionale di prodotto, dato dalla somma del costo marginale privato e dei costi marginali (danni) sopportati dai soggetti terzi per ogni unità addizionale prodotta.

[10] Il Governo può «internalizzare» un'esternalità imponendo una tassa (o un sussidio, in caso di esternalità positive) al produttore con l'obiettivo di sensibilizzare il privato sugli effetti esterni della propria attività e di ridurre la quantità di equilibrio fino alla quantità socialmente desiderata. Imposte di questo tipo, volte a correggere gli effetti delle esternalità (a rendere cioè il costo marginale privato uguale al costo marginale sociale) prendono il nome di imposte correttive, o di imposte pigouviane, ideate dall'economista inglese A.C.Pigou.

[11] L'agente, ossia colui che conosce pienamente tutte le caratteristiche dell'oggetto dell'accordo contrattuale, è i grado di ottenere maggiori benefici dalla stipula del contratto.

contrattuale, dove chi possiede il maggior bagaglio informativo agisce a proprio favore, ma a scapito di altri, non sopportandone tutte le conseguenze[12].

Le asimmetrie informative, sia *ex-ante* che *ex-post*, devono essere tenute in considerazione al momento dell'instaurazione del negozio giuridico, in ordine di prevenire eventuali comportamenti opportunistici. La necessità di un intervento pubblico risiede nella convinzione che, in assenza di tutela da parte dello Stato, molti mercati privi di perfetta informazione non rendono possibile la promozione di scelte economiche efficienti[13].

## 2. La cyber sicurezza: natura ed evoluzione di un bene

L'idea di beni di merito risale ad una intuizione dell'economista Richard Musgrave[14] nel trattare le possibili classificazioni dei compiti dei bilanci pubblici. Sono beni meritori quei beni che, pur essendo a domanda individuale, vengono erogati dalle istituzioni a tutti i cittadini i quali corrispondono un prezzo minimo come controprestazione; il motivo risiede nella loro capacità di apportare un vantaggio (esternalità positive) non solo ai soggetti che la consumano ma, indirettamente, a tutta la collettività[15].

Autorevole dottrina sostiene che la presenza di beni di merito costituisca un'ulteriore causa di fallimenti del mercato: la loro offerta esclusiva da parte del settore privato comporterebbe, perciò, una perdita di benessere sociale, poiché le imprese non potrebbero tenere in conto gli indiretti effetti benefici sui soggetti non direttamente coinvolti nello scambio (né, tantomeno, potrebbero sopportarne le conseguenze in termini di mancati guadagni)[16]. Va da sé che l'erogazione quasi gratuita di questi beni da parte delle Amministrazioni Pubbliche divenga quindi un mezzo per incrementare l'efficienza e la giustizia sociale.

---

[12] Tipico esempio di azzardo morale è il mercato assicurativo, in cui l'assicurato gode di un vantaggio informativo dettato dalla possibilità di poter compiere «azioni nascoste» o di poter sfruttare conoscenze non disponibili alla compagnia.

[13] Data l'appartenenza certa dell'informazione alla categoria dei beni pubblici puri, data la sua non rivale e non escludibile, il legislatore può intervenire imponendo obblighi informativi sull'offerta di alcuni beni e servizi (come l'obbligo di divulgare l'origine dei prodotti alimentari), oppure intervenire attraverso le istituzioni finanziarie pubbliche, come Consob o Banca d'Italia, svolgendo attività di monitoraggio e vigilanza mirata alla promozione della trasparenza informativa per le valutazioni poste in essere dagli operatori economici.

[14] R. MUSGRAVE, *A Multiple Theory of Budget Determination*, FinanzArchiv, 17, 1956 e *The Theory of Public Finance*, McGraw-Hill, 1958 nell'ambito della classificazione dei compiti del bilancio pubblico.

[15] Così, nella Costituzione italiana, si pone in capo alla fiscalità generale e al bilancio dello Stato il compito di assicurare servizi come la salute (art. 32 Cost.), l'istruzione (art. 33 Cost.) e la previdenza sociale (art. 38 Cost.), in quanto diritti fondamentali dell'individuo e oggetto di interesse collettivo. Vale, certamente, l'opposto in caso di bisogni considerati di "demerito", dove lo Stato può intervenire attraverso un'imposizione più marcata (come con gli alcolici o con le sigarette) o mediante la diretta proibizione del consumo dei beni connessi al loro soddisfacimento.

[16] J. STIGLITZ, *Economia del settore pubblico*, Hoepli, 2003.

Ma è possibile, attualmente, catalogare la cyber sicurezza come bene meritorio, o intravedere le basi teoriche e sostanziali di un bene pubblico puro?

Nella attuale configurazione della società, dominata da interazioni che trascendono la dimensione dei rapporti interpersonali mantenuti attraverso la comunicazione fisica, si assiste sempre più alla tessitura di relazioni che si intrecciano all'interno di un mondo privo di limiti sia fisici, sia spaziali, sia temporali, in grado di contenere l'enorme massa di informazioni che assume oggi il termine di *big data*[17].

Il cyber spazio diviene, quindi, luogo dove si manifestano le azioni quotidiane dei singoli ma replicate all'interno di un mondo privo delle limitazioni riscontrabili nella società civile dovute, in particolar modo, alla presenza coercitiva delle leggi il cui scopo è quello di mantenere l'equilibrio ed il rispetto delle reciproche libertà.

In questo mondo liquido, il tema della sicurezza contribuisce alla profonda revisione delle dinamiche tanto care agli Stati liberali e sopravvissute fino al secolo scorso: il concetto di sicurezza nazionale legato alla dimensione territoriale di difesa militare dello Stato, interna o esterna che sia[18].

Nel tentativo di approfondire l'analisi della sicurezza nel cyber spazio, deve essere fatta una constatazione di partenza: la cyber sicurezza si configura, a monte, come un bene di mercato, che i singoli sono comunque disposti a pagare, anche a determinati prezzi. Non è infrequente che bisogni meritevoli di tutela da parte dello Stato siano soddisfatti da beni erogati contemporaneamente dal settore pubblico e da quello privato.

Il problema sorge dal momento in cui si considera che essa sia costituita da un vario insieme di beni che operano sia in totale indipendenza gli uni dagli altri, sia in combinazioni interdipendenti; questi beni vengono, perciò, acquistati dai privati nello sforzo di ricercare un'efficace protezione delle reti telematiche, degli strumenti hardware, dei dati in transito o contenuti in *database* dai tentativi di intrusione, furto, dispersione o distruzione.

Date queste vaste forme di impiego della cyber sicurezza, non dovrebbe stupire il fatto che alcune possibili fonti di produzione di tale bene possano provenire dal settore privato: proprio come tante forme di sicurezza privata vengono fornite nel mondo fisico, anche nello spazio virtuale molti sistemi di sicurezza, come software antivirus o sistemi anti-intrusione, possono essere venduti sul mercato alla stregua di beni privati.

[17] Termine che indica una mole di dati così elevata in termini di volume, velocità, varietà e veridicità che implica tecnologie specifiche per gestirli ed analizzarli.

[18] Importante appare la definizione di cyber spazio inteso come sesto continente "invisibile" ad opera di K. OHMAE in *Il continente invisibile: oltre la fine degli Stati-nazione. Quattro imperativi strategici nell'era della rete e della globalizzazione*, Fazi, 2001.

In questo senso la sicurezza dello spazio cibernetico assume i caratteri di rivalità, in quanto il suo consumo si rivela accessibile solo a chi si può permettere di sostenere i relativi costi ed escludibile, in quanto i rispettivi proprietari possono escludere altri possibili fruitori dall'uso del bene.

Un aspetto rilevante è quello relativo ai livelli di informazione riguardanti le possibili minacce, passate, presenti e future e la vulnerabilità cui i sistemi di difesa sono sottoposti[19]; la diffusione al pubblico di informazioni riguardanti la debolezza della protezione offerta dal proprio sistema di difesa da cyber attacchi potrebbe comportare un costo troppo elevato da sostenere per il privato fornitore, il quale incorrerebbe anche nel rischio di danno alla propria reputazione dovuto alla diminuzione del livello di fiducia dei propri clienti, i quali sarebbero portati ad intentare cause di risarcimento per responsabilità da danno contrattuale.

Vanno considerati, in conseguenza di ciò, gli effetti negativi sui mercati finanziari che i produttori dovrebbero fronteggiare, fornendo prova di vulnerabilità sia ai mercati finanziari, sia ai criminali virtuali. Inoltre, i danni sofferti dall'imprenditore avrebbero conseguenze negative sulle carriere e sulla stabilità lavorativa dei propri dipendenti; i produttori continuerebbero, quindi, ad approfittare del vantaggio offerto dalla asimmetria informativa in merito all'efficacia dei propri servizi.

Creando incentivi per consentire maggiore accessibilità e trasparenza delle informazioni sul traffico di dati riguardanti la presenza di falle o punti deboli nei sistemi di sicurezza cibernetica e fornendo adeguata protezione attraverso la legge, l'intervento delle istituzioni impedirebbe l'alterazione dei livelli di informazione disponibili. Si garantirebbe, così, sia la non rivalità, in quanto l'accesso ai dati da parte di un individuo non limiterebbe la possibilità di accesso ad altri individui, sia la non escludibilità, perché tutti usufruirebbero allo stesso modo delle informazioni disponibili.

La fornitura di un bene privato, inoltre, è passibile di generare esternalità sia positive, sia negative; molte attività di cyber sicurezza sono suscettibili di produrre esternalità positive[20]. Tuttavia, la possibilità che si manifestino effetti negativi nel rapporto produttore-consumatore finale è altrettanto probabile per diversi ordini di ragioni.

Una prima considerazione va fatta tenendo presente che se il livello di protezione da attacchi informatici di un determinato soggetto sia particolarmente elevato, ciò potrebbe creare un effetto di deviazione di tali attacchi su soggetti dotati di sistemi di protezione meno efficienti. Una seconda osservazione deve

[19] Ampiamente dibattuta è l'attuale configurazione di un'economia criminale collegata allo spazio cibernetico come controparte dell'economia digitale, che coinvolge lo spionaggio politico ed istituzionale, lo spionaggio industriale, il traffico di informazioni in ambito borsistico e finanziario, i dati in ambito previdenziale e sanitario, le informazioni militari e di intelligence, gli investimenti in strutture e tecnologie difensive.

[20] Ad esempio, rendere un computer sicuro da virus o intrusioni esterne garantirebbe la sicurezza delle azioni compiute nella rete da quel terminale con ricadute positive sulla sicurezza di altri computer operanti nella medesima rete. Una maggior sicurezza della rete alzerebbe, quindi, i costi degli attacchi e delle intrusioni illegali dall'esterno.

essere rivolta sulla parte che davvero sopporta i costi della vulnerabilità e della inefficienza dei sistemi di sicurezza informatica: in un sistema di mercato, un produttore privato spesso non riesce ad «internalizzare» i costi dell'inefficienza allocativa della fornitura di una protezione cibernetica efficace.

In questo caso, se un *firewall* non garantisce la prevenzione da eventuali intrusioni o se un *service provider* non impedisce puntualmente un attacco da *malware*, chi ne soffrirebbe di più, dovendone sopportare totalmente i costi, sarebbero gli utenti finali di questi servizi.

Si configurano, così, dei casi classici di esternalità negative che accompagnano la produzione dei beni privati, in quanto le spese derivanti dall'inefficienza e inefficacia dei sistemi di sicurezza acquistati costituiscono un costo finale non facilmente considerabile dai consumatori del servizio al momento dell'acquisto[21].

Nel contesto della cyber sicurezza, quindi, potendo svolgere un'analisi costi-benefici della fornitura privata di tale servizio rispetto all' intervento pubblico, si potrebbe constatare che i costi sostenuti dai privati per la prevenzione da eventuali minacce cibernetiche sarebbero più elevati rispetto a quelli sostenuti mutualmente dall'intera collettività, comprendendo in questa valutazione anche il comportamento opportunistico dei soggetti non disposti a partecipare ai costi di produzione di s*oftware* utili alla difesa da attacchi informatici che non sarebbe comunque possibile evitare[22].

Nel caso si volessero introdurre delle imposte correttive, lo Stato dovrebbe essere in grado di disporre di sufficiente informazione riguardo i costi marginali sociali delle esternalità, per poter modulare l'imposta in modo tale da riflettere tale onere e da creare un sistema in grado di ottenere un risultato allocativo efficiente. Lo Stato, quindi, imporrebbe un'imposta su ogni unità aggiuntiva prodotta, pari al danno indotto dal livello di produzione efficiente, creando un mercato dove il prezzo verrebbe determinato dal Governo piuttosto che dalla domanda e dall'offerta.

Questa soluzione, sebbene efficace, non appare risolutiva del problema delle esternalità, in quanto vincolata alla capacità governativa di determinare più o meno con precisione il livello di prezzo socialmente ottimale: se il prezzo viene fissato in modo errato, le esternalità continuerebbero a persistere.

Per correggere gli effetti negativi delle esternalità nel mercato cibernetico, lo Stato potrebbe intervenire attraverso politiche di *soft regulation* costruendo, innanzitutto, un sistema di incentivi in grado di indurre i soggetti economici privati a collaborare con le istituzioni, per creare forme di cooperazione allo scopo di

[21] P.ROSENZWEIG, "*Cyberwarfare: How Conflicts in Cyberspace are Challenging America and Changing the World*", Praeger, 2012.

[22] Il discorso si potrebbe estendere anche ad altri servizi collegati tramite *networks* come: dorsali informatiche, fornitori di servizi internet; telecomunicazioni; settore finanziario e bancario; servizio sanitario nazionale.

internalizzare gli effetti distorsivi che accompagnano la produzione di mercato dei sistemi di sicurezza informatica.

Un valido supporto alla creazione di incentivi che lo Stato dovrebbe essere in grado di ideare in un sistema di *governance* multilivello, sarebbe dato dalla capacità delle istituzioni, in quanto in possesso di un miglior livello di informazioni circa le incidenze e le tipologie degli attacchi informatici e le connesse vulnerabilità del sistema, di esercitare delle «spinte gentili»[23] per indirizzare i mercati verso una più efficiente creazione di infrastrutture dedicate alla cyber sicurezza.

Successivamente, una collaborazione tra poteri pubblici e organizzazioni rappresentanti il mondo dell'industria e della finanza potrebbe adoperarsi per la stesura di *best practices* o *frameworks* sulla sicurezza cibernetica strutturati su vari livelli di possibilità opzionali[24], facilmente permeanti entrambi i settori, pubblico e privato.

Nell'ottica di una avvertita necessità di un generale ridisegno dell'architettura istituzionale della protezione informatica, dettata in precedenza dal decreto Monti del 23 gennaio 2013[25], un ulteriore incentivo alla

[23] Il termine si riferisce alla traduzione non letterale del termine anglosassone *nudge*, coniato da un lavoro congiunto dell'economista R.H.THALER e del giurista C.R.SUNSTEIN, entrambi statunitensi, nell'ambito degli studi afferenti all'economia e al diritto comportamentali. Secondo questi autori i poteri pubblici dovrebbero comportarsi come «architetti delle scelte», nel senso di poter indirizzare in modo non coercitivo le decisioni dei soggetti, siano essi economici, politici o sociali, al fine di razionalizzare e migliorare il proprio modo di operare. Da questa collaborazione è nato il termine, ossimorico in apparenza, di «paternalismo libertario», ossia un intervento dei pubblici poteri regolativo, ma non invasivo della capacità di scelta degli individui e molto apprezzato nel mondo anglosassone (Regno Unito e negli Stati Uniti d'America). In particolare, v. *Nudge. Improving decisions about health, wealth and happiness*, Yale University Press, 2008 e *Why Nudge? The politics of Libertarian Paternalism*, Yale University Press, 2014. E. RIGHINI, in *Behavioural Law and Economics: problemi di policy, assetti normativi e vigilanza* collega il *nudging* all' *empowerment*, ossia ad un processo volto a sviluppare nelle persone e nei gruppi una maggiore capacità di prendere decisioni razionali e di trasformarle in azioni e obiettivi desiderati; processo impiegabile anche nello sviluppo di una cultura istituzionale della *cybersecurity*.

[24] L'*Italian Cyber Security Report 2015*, realizzato dal Cis-Sapienza e dal Laboratorio nazionale di Cyber Security è un framework nazionale a cui hanno partecipato enti pubblici, università ed importanti operatori del settore privato e realizzato per offrire alle organizzazioni pubbliche e private, piccole, medie e grandi, un approccio omogeneo per affrontare la cyber security, al fine di ridurre il rischio legato alle minacce provenienti dal cyber spazio. Ispirato al *Framework for improving critical infrastructure Cyber security* del *National Institute of Standards and Technology* (Nist) del governo statunitense, il cui scopo consisteva nell'aumentare la resilienza delle infrastrutture critiche, il documento si pone come punto di riferimento per offrire delle linee guida su come aumentare il livello di cyber sicurezza per le piccole e medie imprese italiane, oltre a fornire raccomandazioni per sensibilizzare il management pubblico e privato su come organizzare al meglio i processi di *risk management* della sicurezza cibernetica.

[25] La recente *Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionali*, di cui al DPCM 17 febbraio 2017, pubblicato in G.U. N. 83 del 13 aprile 2017, sostituisce *in toto* il precedente decreto Monti e traccia la nuova strada che il Governo desidera intraprendere per strutturare il sistema cibernetico di difesa nazionale, valorizzando l'interazione istituzionale tra pubblico e privato ed evidenziando con maggior vigore la funzione di bene pubblico svolta dalla cyber sicurezza. Esso si compone di undici indirizzi operativi, le cui tematiche investono un raggio d'azione che spazia da misure di potenziamento del ruolo dell'*intelligence* e delle forze armate e di polizia nell'architettura istituzionale della prevenzione dei crimini informatici alla elaborazione di strategie nazionali di *cyber risk management*, finalizzati alla definizione delle soluzioni da applicare per rendere operativo il Quadro Strategico Nazionale; gli indirizzi operativi relativi al "Potenziamento dell'organizzazione e delle modalità di coordinamento

*partnership* tra pubblico e privato dovrebbe prendere in considerazione esperienze maturate nell'ambito internazionale sulla scorta, ad esempio, del sistema tedesco di partenariato relativo alla cyber sicurezza, dove il settore privato riveste un duplice ruolo: quello di collaboratore diretto e fattuale nella creazione di sistemi di protezione informatica per le infrastrutture critiche e quello di sviluppatore e certificatore di tecnologie specifiche per la sicurezza nazionale[26].

Occorre tuttavia tenere in conto che, agli albori del XXI secolo, la capacità di una Nazione di potersi difendere da qualsiasi tentativo di attacco deve essere in grado anche di superare il limite fisico correlato al carattere territoriale della sicurezza per poter rispondere alle minacce provenienti dallo spazio digitale[27]. In questa veste la cyber sicurezza si delinea come un'ulteriore espressione della più classica forma di sicurezza garantita dallo Stato ed esplicata attraverso l'azione delle varie forze armate e di polizia presenti nel Paese e, come tale, ricollegabile alla teoria economica dei beni pubblici.

La garanzia di un'efficace ed efficiente tutela da cyber attacchi di stampo terroristico o nel trattamento di dati sensibili dalle possibilità di intrusione dall'esterno a scopi criminali, esplicantisi in tentativi di spionaggio militare o industriale, oppure di sottrazione ed uso fraudolento di dati personali, può essere fornita soltanto attraverso un intervento dello Stato che assume la funzione di regolatore nell'erogazione di questo servizio[28].

---

e di interazione a livello nazionale tra soggetti pubblici e privati" ed alla "Promozione della cultura della sicurezza informatica" appaiono essere i settori sicuramente più adatti alla diffusione di strumenti di regolazione strategica «gentile» per la diffusione di pratiche condivise dalla *governance* pubblica e privata.

[26] In Italia, il partenariato pubblico privato trova espresso riferimento normativo nell'art. 3, c.1, lett. eee) del nuovo Codice dei contratti pubblici, di cui al d.lgs. n. 50 del 2016. Nell'ambito della cyber sicurezza italiana, è già in atto una collaborazione tra Leonardo-Finmeccanica e la *joint venture* statunitense Forcepoint, che collabora con il Dipartimento della Difesa americano, per fornire servizi mirati alla prevenzione e gestione degli incidenti informatici e per l'analisi delle vulnerabilità delle componenti *hardware* e *software* dei sistemi informativi della Pubblica Amministrazione, applicabili sia agli ambienti *cloud* centralizzati e condivisi, sia alle singole amministrazioni. Importante da sottolineare è anche la partnership tra l'azienda italiana Yarix, con sede a Montebelluna e le realtà governative ed economiche israeliane, per la realizzazione in Italia del *Security Operation Center 4.0*, un sistema operativo su scala globale risultante dai lavori di una *task force* costituita da esperti informatici dell'azienda trevigiana, ricercatori universitari italiani ed analisti provenienti dalle aziende israeliane leader del settore, che sia in grado di monitorare, rilevare e rispondere alle minacce cibernetiche più evolute.

[27] N. CHOUCRI, in *Cyberpolitics in International Relations*, The MIT press, Cambridge, 2012, teorizza la difesa nazionale come funzione di quattro diverse ma interconnesse dimensioni: sicurezza esterna; sicurezza interna; sicurezza dell'ambiente; cyber sicurezza. La difesa da minacce provenienti dallo spazio virtuale assurge, così, alla dignità di *high politics*, cioè di attività di importanza critica per la tutela degli interessi dello Stato, il cui studio assurge alla stessa dignità accordata dalla scienza politica ad altri temi come l'organizzazione istituzionale, le politiche pubbliche e le scienze strategiche e di intelligence.

[28] U. GORI, *L'inarrestabile sviluppo delle armi cibernetiche*, in U. GORI − S. LISI (a cura di), *Cyber Warfare. Armi cibernetiche, sicurezza nazionale e difesa del business*. L'A. sostiene che la condotta all'interno del cyber spazio sarà sempre più contrassegnata dal conflitto che dalla collaborazione, sia negli scontri tra Stati, sia negli scontri tra Stati e criminalità/terrorismo. È da notare che il Governo italiano ha presentato, durante l'incontro G7 di Taormina nel mese di maggio 2017, una nuova strategia nazionale sulla cyber sicurezza concretizzata in un Codice di condotta internazionalmente condiviso, allo scopo di definire un piano di "territorializzazione" del cyber spazio,

Così inquadrata, la cyber sicurezza è configurabile alla stregua di un bene pubblico puro, dotato delle caratteristiche di non escludibilità e di non rivalità, il cui costo marginale per la produzione di un'unità aggiuntiva di fornitura è pari a zero[29] e dal cui godimento non è possibile escludere nessuno.

In questi casi diviene, in tal modo, difficile definire precisamente i diritti di proprietà o di uso relativi, come avviene per i beni privati, mancando le condizioni necessarie perché essi possano essere venduti a prezzo di mercato e facendone venir meno gli incentivi alla produzione esclusiva da parte di fornitori privati.

Nell'ipotesi, ad esempio, che vi sia la necessità di difendere la Nazione, ma lo Stato non fornisca il servizio di difesa, il finanziamento di tale servizio sarebbe appannaggio di investitori privati dai cui benefici, però, non sarebbe possibile escludere chi non sia disposto a pagare per usufruire di tale vantaggio.

Si manifesta così il fenomeno del *free rider*, cioè di colui che non è incentivato a pagare per il servizio offerto perché consapevole di ottenerne i benefici indipendentemente dalla propria partecipazione ai relativi costi.

Il problema fondamentale per il fornitore privato di un bene pubblico si sostanzierebbe nel sostenere alti costi per escludere dalla fornitura del servizio di difesa i soggetti non paganti; a questo punto, come risultato della sommatoria tra presenza di *free riders* ed elevati costi dovuti alla differenziazione tra beneficiari paganti e non paganti si avrebbe la enorme difficoltà delle aziende private, uniche fornitrici che tentano di massimizzare il profitto, di stimolare l'acquisto del servizio di difesa, fornendo così un ammontare troppo esiguo di commercializzazione di tale bene[30].

Il potere pubblico risolve il problema del *free riding* agendo in modo autoritativo: attraverso l'imposizione fiscale o, come nel caso dell'obbligatorietà del servizio militare, attraverso forme di prestazione personale imposta, diventa possibile far pagare tutti i beneficiari del bene o del servizio, anche obbligandoli in modo coercitivo[31].

riconosciuto al summit Nato di Varsavia del luglio 2016 come dominio operativo assimilabile a terra, mare, aria e spazio extra-atmosferico e perciò assimilabile ad un campo di battaglia. L'obiettivo dell'Italia è quello di raggiungere una militarizzazione condivisa della dimensione cibernetica, per raggiungere la quale occorre la formulazione di regole di base comuni per regolare i rapporti informatici tra gli Stati e per creare un arsenale di armi informatiche come deterrente contro la proliferazione dei cyber criminali.

[29] Difendere un individuo in più non comporterebbe, cioè, costi marginali aggiuntivi allo Stato.

[30] In un'ottica derivante dalla teoria dei giochi e dal «dilemma del prigioniero», si verificherebbe una situazione di non cooperazione, in quanto i cittadini non paganti il servizio non hanno il minimo stimolo o interesse a contribuire alla spesa in difesa sostenuta dai cittadini paganti, perché ne subirebbero lo stesso i benefici. Dall'altra parte, l'esclusione dal godimento del bene sarebbe inefficiente, in quanto la presenza di un'unità aggiuntiva di bene non ne aumenta i costi marginali di produzione. I *free riders*, in questo caso, seguirebbero una strategia definibile come dominante.

[31] L'art. 23 della Costituzione italiana regola la determinazione dei casi e delle modalità per obbligare i cittadini a prestazioni personali e patrimoniali attraverso la legge.

Garantendo la necessaria provvista finanziaria attraverso il prelievo fiscale, il bene pubblico può essere erogato gratuitamente.

### 3. Considerazioni conclusive

L'impostazione che sta alla base di questo elaborato parte da una visione del fenomeno cyber sicurezza in chiave evolutiva: come si comportano attualmente lo Stato e le pubbliche istituzioni nei confronti di una società sempre più interconnessa e dipendente dai mezzi elettronici e telematici di comunicazione, come tale soggetta a pericoli provenienti da soggetti privi di identità e difficili da individuare? E quale sarà l'atteggiamento che gli operatori pubblici implementeranno in un futuro molto prossimo?

Considerata l'attuale fase storica, caratterizzata da una ancora incompiuta accettazione del controllo delle attività digitali a scopo preventivo e repressivo, appare oltremodo condivisibile l'intervento dello Stato, del Governo e dei servizi informativi della Repubblica italiana mirato a creare quel consenso e quella sensibilità condivisa nei riguardi della sicurezza del *cyberspazio*.

In questo contesto la sicurezza informatica sembra rientrare in uno dei contesti generali attraverso cui Musgrave giustificava la presenza e l'applicazione del concetto di beni meritori: ossia l'accettazione di quei valori comunemente condivisi dalla collettività, anche se contrastanti con le preferenze individuali e le scelte dei singoli consumatori, mediante la quale avviene il superamento del criterio paretiano secondo cui l'individuo è il miglior giudice del proprio interesse e la sua sostituzione mediante l'interposizione paternalista delle istituzioni pubbliche tra l'individuo e le proprie scelte[32].

Tuttavia, riferendosi ad un contesto internazionale dove il concetto di *cyber warfare*[33] è del tutto condiviso ed affermato, è quasi impossibile trascurare il fatto che la sicurezza informatica possa essere intesa come ulteriore manifestazione della difesa nazionale e come tale divenire oggetto di qualsiasi tipo di transazione dato che, per definizione, i benefici collegati ad un bene pubblico puro si estendono indistintamente a

[32] Richard Musgrave riteneva che le scelte degli individui fossero parziali ed alterabili in quanto formatesi in situazioni di informazione incompleta o imperfetta e in stato di immaturità o incapacità o dipendenza. L'intervento dell'autorità pubblica era, quindi, preferibile perché più informata e più razionale. Appare utile richiamare, accanto all'impostazione teorica del citato autore e del summenzionato e più *soft* impianto del paternalismo libertario afferente al *nudging*, la teoria paternalistica di ispirazione illuminista facente capo alla scuola italiana di finanza pubblica di metà Novecento denominata degli "*assetti tutori*", tramite la quale venne elaborato un concetto alternativo di utilità collettiva, inteso come una valutazione delle utilità dei singoli individui effettuata forzosamente dal Governo al fine di renderle più omogenee e confrontabili. I soggetti pubblici intervengono sul mercato veicolando obbligatoriamente le scelte dei cittadini, operando un bilanciamento tra scelte private e preferenze collettive, al fine di ottimizzare la tutela dei loro bisogni "reali". Sul punto v. C. COSCIANI, *Scienza delle finanze*, Utet, 1991 e G. CAMPA, *Lezioni di Scienza delle finanze*, Utet, 2013.

[33] Gli attacchi cibernetici si possono manifestare in forma di: attacco ad infrastrutture critiche (comunicazioni, servizi idrici ed energetici; vandalismo web; le attività militari che si esplicano attraverso satelliti o computer sono ampiamente soggette a tale tipo di attacchi; violazione di dati sensibili e riservati; propaganda politica e religiosa (i recenti e non sporadici atti di terrorismo in Europa sono stati frutto di attività di radicalizzazione *on line*)

tutti, non potendo essere erogati selettivamente o con un livello di qualità differenziato da settore a settore[34].

È quanto mai utile, in questo approccio alla cyber sicurezza, sfruttare l'impianto fornito dalla teoria dello *Stato innovatore*, ossia lo Stato visto non come antagonista del settore privato o come soggetto chiamato in causa nel caso in cui il libero mercato fallisca nel suo compito redistributivo, ma come motore principale dello sviluppo economico della società nella sua interezza[35].

Con uno sguardo rivolto all'immediato futuro, tenendo conto che le Amministrazioni Pubbliche italiane sono sempre più in prima linea sulla strada per la integrazione digitale della fornitura dei servizi che esse erogano[36], si può intravedere la strada per la diffusione e l'accettazione della sicurezza informatica come un bene di natura indiscutibilmente pubblica.

Una volta completato e perfezionato, infatti, il processo di accesso ai servizi pubblici in rete, si renderà necessariamente indispensabile tutelare i cittadini da attacchi cibernetici attraverso l'*enforcement* delle tecnologie a disposizione delle forze dell'ordine e dei servizi di sicurezza, stante l'estrema delicatezza dei dati a quel punto disponibili in rete[37].

È importante, con ciò, che si evidenzi il necessario ruolo dello Stato e delle sue amministrazioni nel creare una percezione diffusa sia a livello istituzionale, sia a livello sociale dell'importanza della sicurezza informatica come ulteriore declinazione della difesa nazionale, anticipando *ex ante* le istanze che deriveranno dalla definitiva trasposizione cibernetica delle attività quotidiane degli esseri umani; a tal fine, destinare una parte della spesa pubblica per finanziare anche l'attività di ricerca e sviluppo delle università e degli istituti di ricerca, sia in ambito civile, sia in ambito militare, con l'obiettivo di creare una interazione di scopo tra l'attività di regolazione pubblica e la capacità di produzione di innovazione tipica del settore privato, consentirebbe la creazione di un sistema virtuoso che partendo dalle università, attraverso la creazione di indirizzi di studio e di attività di ricerca, si riverserebbe nell'ambito lavorativo privato ritornando, infine, al settore pubblico in forma di personale, tramite l'assunzione di esperti esterni alle

[34] Come nel caso dell'istruzione, i cui livelli di prestazione possono differire in qualità a seconda che essi siano erogati da istituti pubblici o da istituti privati.

[35] M. MAZZUCATO, *The Entrepreneurial State*, Anthem Press, 2013. È illuminante gli esempi che l'Autrice apporta nel descrivere l'utilità delle tecnologie cc.dd. "*dual use*", ossia tecnologie impiegate in ambito militare e poi introdotte nel settore civile tra cui, su tutti, il progetto *ARPANET*, finanziato dalla *Defence Advanced Research Projects Agency* (*DARPA*) ed unanimemente riconosciuto come progenitore della rete Internet.

[36] Si fa riferimento al *Sistema pubblico di identità digitale* (SPID), sistema unico di accesso ai servizi *on line* pubblici e dei privati aderenti.

[37] Si pensi alle dichiarazioni dei redditi *on line* o ad altre informazioni riguardanti dati sensibili dei cittadini.

amministrazioni pubbliche o di servizi, mediante l'impiego di sistemi di sicurezza informatica da destinare alla protezione dei siti istituzionali[38].

[38] Sul punto, v. M.F. GRADY−F. PARISI, *Law and Economics of Cybersecurity*, Cambridge University Press, 2005 e B.H. KOBAYASHI, *An Economic Analysis of the Private and Social Costs of the Provision of Cybersecurity and other Public Security Goods*, Supreme Court Econoomic Review, vol.14, 2005.