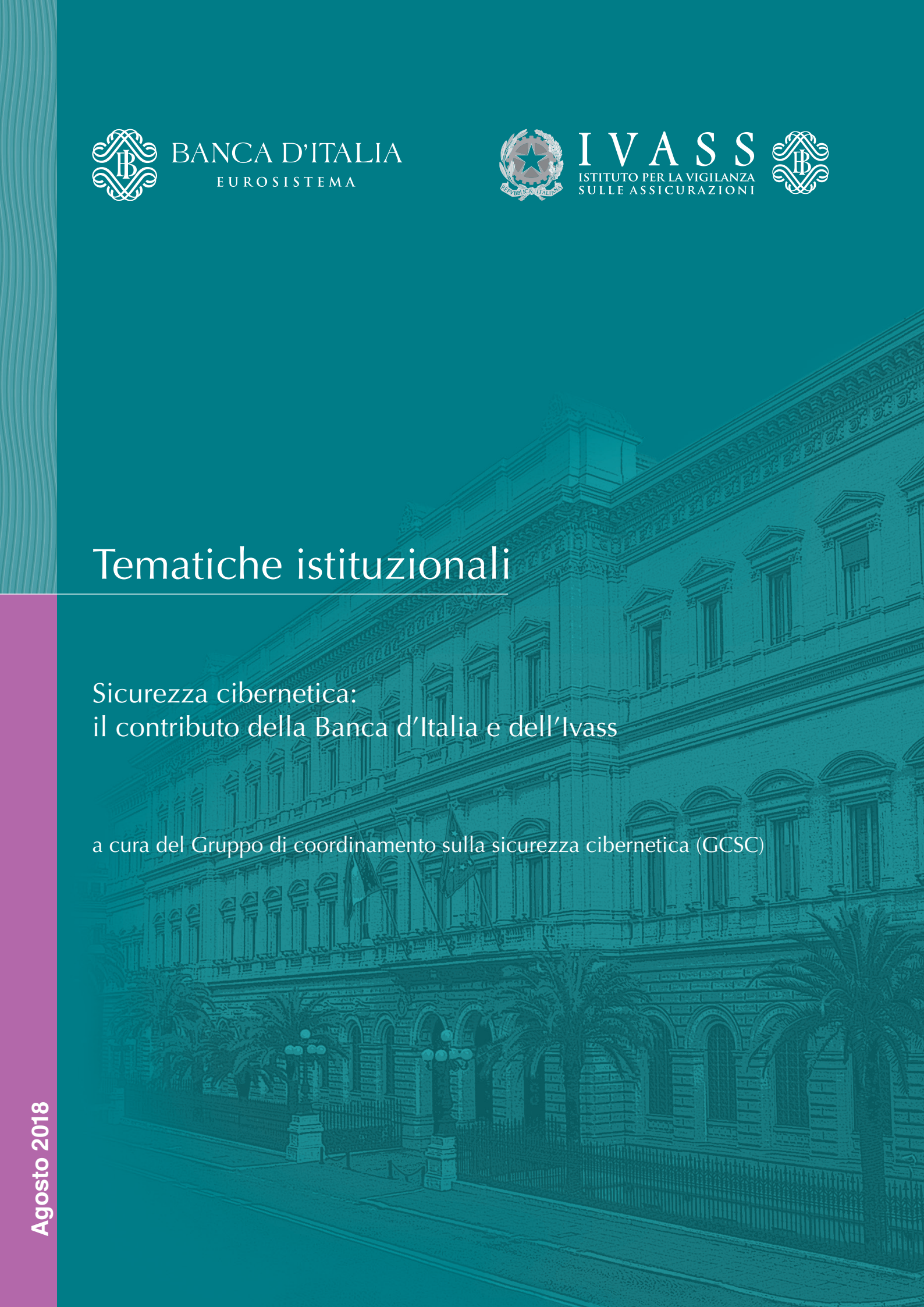
BANCA D'ITALIA
EUROSISTEMA

IVASS
ISTITUTO PER LA VIGILANZA SULLE ASSICURAZIONI



Tematiche istituzionali

Sicurezza cibernetica: il contributo della Banca d'Italia e dell'Ivass

a cura del Gruppo di coordinamento sulla sicurezza cibernetica (GCSC)

Agosto 2018

BANCA D'ITALIA
EUROSISTEMA

IVASS
ISTITUTO PER LA VIGILANZA SULLE ASSICURAZIONI

Tematiche istituzionali

Sicurezza cibernetica: il contributo della Banca d'Italia e dell'Ivass

a cura del Gruppo di coordinamento sulla sicurezza cibernetica (GCSC)

Agosto 2018

Questo lavoro è stato curato dal Gruppo di coordinamento sulla sicurezza cibernetica (GCSC).

Alla stesura del documento hanno contribuito:
per Banca d'Italia, Caterina Beccarini *e* Claudia Biancotti *(coordinamento),* Alessandro Campi, Antonio Credendino, Riccardo Cristadoro, Sabina Di Giuliomaria, Pasquale Digregorio, Antonino Fazio, Gino Giambelluca, Marilisa Guida, Sonia Guida, Giovanna Partipilo, Adriana Selvaggi*;*
per Ivass, Sergio Antonica *e* Pietro Franchini.

Gli aspetti editoriali sono stati curati da: Fabrizio Martello *e* Rosanna Visca *(Banca d'Italia).*

Per la pubblicazione cartacea: autorizzazione del Tribunale di Roma n. 290 del 14 ottobre 1983
Per la pubblicazione telematica: autorizzazione del Tribunale di Roma n. 9/2008 del 21 gennaio 2008

Indirizzo
Via Nazionale 91, 00184 Roma - Italia

Telefono
+39 0647921

Sito internet
http://www.bancaditalia.it

ISSN 2283-3226 (stampa)
ISSN 2283-3250 (online)

Aggiornato con i dati disponibili a maggio 2018, salvo diversa indicazione

Grafica e stampa a cura della Divisione Editoria e stampa della Banca d'Italia

INDICE

Premessa

Gli attacchi informatici sono una minaccia crescente per un'economia che sempre più si basa su tecnologie digitali. Il rischio cibernetico interessa molteplici attività produttive e di consumo; per sua natura oltrepassa i confini tra paesi e settori.

È necessaria una risposta globale e di sistema. In un mondo connesso, nessun dispositivo informatico – per quanto ben protetto – può dirsi interamente sicuro se l'ambiente circostante resta vulnerabile. È centrale la collaborazione tra autorità pubbliche e settore privato; la consapevolezza del rischio deve essere diffusa nell'intera società, non solo tra gli addetti ai lavori.

A livello internazionale ed europeo si vanno definendo principi, buone prassi, regole e standard tecnologici per rafforzare le capacità di prevenzione, difesa e reazione dei paesi, delle organizzazioni e delle imprese. A queste iniziative si affianca l'adozione di strategie nazionali di sicurezza cibernetica; anche l'Italia si è mossa in questa direzione.

La Banca d'Italia e l'Ivass sono in prima linea nel contrasto alla minaccia, in ragione delle competenze loro affidate in materia di sicurezza del sistema finanziario italiano. Quest'ultimo è un obiettivo privilegiato per i soggetti ostili, siano essi motivati dal semplice profitto o dall'intento di innescare una crisi di fiducia. Respingere le aggressioni è essenziale per tutelare il risparmio e per garantire l'ordinato funzionamento dell'economia.

I due Istituti hanno costituito un Gruppo di coordinamento sulla sicurezza cibernetica che riunisce esperti di informatica, vigilanza sugli intermediari bancari, finanziari e assicurativi, sorveglianza sul sistema di pagamenti e ricerca economica, con il fine di sviluppare un pensiero strategico sul rischio cibernetico e di assicurare una linea di azione coerente tra le varie funzioni.

Questo documento offre una visione di insieme di quanto congiuntamente realizzato per proteggere il settore finanziario dagli attacchi informatici.

Salvatore Rossi

Introduzione e sintesi

Il quadro di insieme

Le tecnologie dell'informazione e della comunicazione (*information and communication technology*, ICT)[1] sono in rapida espansione, grazie ai guadagni di produttività che il loro utilizzo comporta; ne dipende ormai completamente un numero crescente di settori vitali dell'economia e della finanza. Aumenta il valore delle grandi masse di dati (cosiddetti big data), da cui l'intelligenza artificiale trae informazioni complesse. Si ampliano anche la quantità e la tipologia degli oggetti connessi a internet, come ad esempio macchinari industriali, elettrodomestici, automobili, videocamere, impianti di illuminazione (internet delle cose).

Alle nuove tecnologie si accompagnano però nuovi rischi; tra questi particolarmente rilevante è quello cibernetico (*cyber risk*), legato ad azioni che sfruttano le vulnerabilità di un dispositivo ICT o del codice che ne consente il funzionamento, per interromperne l'operatività, per ottenere un indebito accesso ai dati che custodisce o per comprometterne l'integrità.

Fino a qualche anno fa il rischio cibernetico era di fatto circoscritto a pochi specifici settori, come la difesa, sia perché le tecnologie avanzate erano per lo più concentrate nei grandi centri di elaborazione di dati, sia perché sferrare attacchi informatici era molto costoso. Con l'espansione dell'accesso alle reti telematiche e con la diffusione di strumenti di attacco a basso costo, alle intrusioni cibernetiche con finalità politico-militari si sono affiancate quelle motivate dal profitto (cfr. il capitolo 1).

L'intensificarsi della minaccia cibernetica ha posto gli Stati di fronte a complesse sfide di policy. I software malevoli e gli altri mezzi di attacco informatico sono in grado di provocare danni ingenti alla sicurezza e all'economia, alla stregua delle armi tradizionali. Gli ordinamenti giuridici nazionali e il diritto internazionale si stanno adattando al nuovo scenario.

Fin dagli anni novanta in diversi paesi è stato introdotto il reato di accesso abusivo ai sistemi informatici. Dai primi anni duemila le principali economie avanzate ed emergenti hanno elaborato strategie più ampie, che contemplano la definizione di un'architettura istituzionale per la prevenzione e la gestione delle crisi, misure per il potenziamento della sicurezza delle Pubbliche amministrazioni e delle infrastrutture critiche, incentivi alla formazione di specialisti e alla collaborazione pubblico-privato, schemi di certificazione della sicurezza di software e hardware (cfr. il par. 2.1).

Le iniziative sul fronte della cooperazione internazionale, essenziali per fronteggiare una minaccia globale, sono ancora carenti. Si sono registrati progressi solo su temi specifici – come il coordinamento tra Forze di Polizia per la lotta ad alcuni crimini – e in contesti in cui cooperano paesi che condividono i principali obiettivi strategici in materia di sicurezza, come la NATO e il G7 (cfr. il par. 2.1). Fa

---

[1] Per i termini tecnici e le sigle presenti in questo lavoro, cfr. il Glossario e il Siglario nell'Appendice alla *Relazione annuale* sul 2017 della Banca d'Italia.

parziale eccezione il sistema finanziario, dove la cooperazione anche regolamentare su base allargata è favorita dall'esistenza di esperienze su altri fronti – primo tra tutti quello della stabilità finanziaria – e dalla dimensione globale di alcuni operatori chiave.

Le tecniche di attacco sono in rapida evoluzione: essere aggiornati sulle vulnerabilità dei sistemi informatici e sulle modalità con le quali queste vengono sfruttate dai soggetti ostili permette di operare in anticipo nella direzione di una difesa proattiva, molto più efficace di una meramente reattiva. La condivisione tempestiva di informazioni è dunque un elemento difensivo fondamentale. Tuttavia non sempre chi ha subito attacchi o identificato debolezze è disposto a condividere quanto appreso: sono pertanto necessarie garanzie di riservatezza e di reciprocità. In alcuni casi queste condizioni si creano spontaneamente all'interno di gruppi di operatori economici particolarmente sensibili al rischio cibernetico. Più spesso interviene l'autorità pubblica, che svolge un ruolo di stimolo e di creazione di fiducia.

I modelli di condivisione delle informazioni di maggior successo sono due: il primo si basa sugli *information and analysis centers* (ISAC), il secondo è fondato sui *computer emergency response teams* (CERT) e sui *computer security incident response teams* (CSIRT; cfr. il par. 2.1).

I riferimenti normativi nazionali ed europei

Il quadro normativo italiano rispecchia la strategia di sicurezza cibernetica (*cybersecurity*) dell'Unione europea (UE), di cui la direttiva UE/2016/1148 sulla sicurezza delle reti e dei sistemi informativi (Directive on Security of Network and Information Systems, NIS) costituisce l'asse portante. Il legislatore europeo prevede che gli Stati membri si dotino di un'organizzazione in grado di vincolare gli operatori di servizi ritenuti essenziali per l'economia all'adozione di stringenti misure di protezione; istituisce inoltre un gruppo di cooperazione nell'ambito della UE per lo scambio di informazioni e migliori prassi (cfr. il par. 2.2 e il riquadro: *La direttiva NIS in Italia* del capitolo 2).

Per una varietà di soggetti, requisiti di sicurezza informatica discendono anche da altre due recenti disposizioni europee: il regolamento generale UE/2016/679 sulla protezione dei dati (General Data Protection Regulation, GDPR; cfr. il riquadro: *Il regolamento GDPR* del capitolo 2) e la direttiva UE/2015/2366 sui servizi di pagamento nel mercato interno (Revised Directive on Payment Services, PSD2; cfr. il riquadro: *La direttiva PSD2* del capitolo 3). Altri obblighi potrebbero derivare dall'approvazione del Cybersecurity Act, presentato nel 2017 dalla Commissione europea, che attribuisce all'Unione il potere di certificare la sicurezza dei dispositivi e dei relativi software.

L'architettura legislativa italiana in materia di sicurezza cibernetica si basa al momento su due provvedimenti:

a) il decreto del Presidente del Consiglio dei ministri del 17 febbraio 2017 (cosiddetto decreto Gentiloni), che attribuisce al Dipartimento delle informazioni per la sicurezza della Presidenza del Consiglio (DIS) la responsabilità di coordinare la prevenzione e gestione delle crisi cibernetiche mediante il Nucleo

per la sicurezza cibernetica (NSC), composto in via permanente dai ministeri che siedono nel Comitato interministeriale per la sicurezza della Repubblica (CISR): Difesa, Interno, Affari esteri, Economia e finanze, Sviluppo economico, Giustizia (cfr. il par. 2.3);

b) il D.lgs. 65/2018, in attuazione della direttiva NIS, che istituisce uno CSIRT pubblico nazionale, attribuisce al DIS il ruolo di punto di contatto con le istituzioni dell'Unione e individua le autorità responsabili dell'attuazione delle misure previste dalla direttiva per i settori economici considerati strategici.

La sicurezza cibernetica nel settore finanziario

Il sistema finanziario è un obiettivo privilegiato per gli attacchi informatici e, a causa delle numerose interdipendenze, i danni dovuti a queste aggressioni possono essere ingenti e provocare ricadute sistemiche.

Le banche centrali e le altre autorità di supervisione rivestono un ruolo cruciale nel garantire la sicurezza informatica del sistema finanziario; in molti paesi ne gestiscono componenti vitali, come i sistemi di pagamento; possono richiedere ai soggetti vigilati informazioni sugli attacchi subiti, imporre l'adozione di adeguati presidi difensivi e sanzionare gli inadempienti (cfr. il par. 3.1).

Nel settore finanziario la cooperazione internazionale, per quanto riguarda le infrastrutture di mercato e i sistemi di pagamento, ha come principale forum il Comitato sui sistemi di pagamento e sulle infrastrutture di mercato (Committee on Payments and Market Infrastructures, CPMI) della Banca dei regolamenti internazionali (BRI); in tema di vigilanza sono rilevanti il Senior Supervisors Group (SSG), il Consiglio per la stabilità finanziaria (Financial Stability Board, FSB) e il Comitato di Basilea per la vigilanza bancaria (Basel Committee for Banking Supervision, BCBS) della BRI. Il più importante documento di riferimento è la *Guidance on cyber resilience for financial market infrastructures* (in questo lavoro citata anche come Cyber guidance), pubblicata nel 2016 dal CPMI in collaborazione con il Board of the International Organization of Securities Commissions (Iosco; cfr. il par. 3.2).

Un ruolo centrale è rivestito anche dal Cyber Expert Group del G7 finanziario (G7-CEG), che attualmente è impegnato nella definizione di un protocollo di cooperazione internazionale tra autorità per la risposta a incidenti transfrontalieri.

All'interno della UE il Comitato europeo per il rischio sistemico (European Systemic Risk Board, ESRB) garantisce un raccordo di alto livello a fini di stabilità finanziaria tra la Commissione europea, le autorità di settore[2], l'Eurosistema e le autorità macroprudenziali nazionali. Per quanto riguarda la vigilanza bancaria, l'EBA ha emanato linee guida per il monitoraggio del rischio informatico delle banche da parte delle autorità competenti (cfr. il par. 3.3).

---

[2] Autorità bancaria europea (European Banking Authority, EBA), Autorità europea degli strumenti finanziari e dei mercati (European Securities and Markets Authority, ESMA), Autorità europea delle assicurazioni e delle pensioni aziendali e professionali (European Insurance and Occupational Pensions Authority, EIOPA).

Nell'ambito dell'Eurosistema la Banca centrale europea (BCE) garantisce, in collaborazione con le banche centrali nazionali, la sicurezza delle piattaforme TARGET2 e TARGET2-Securities; sviluppa inoltre regolamentazione in ambito cibernetico per i sistemi di pagamento e le infrastrutture di mercato gestite da terzi. Il Meccanismo di vigilanza unico (Single Supervisory Mechanism, SSM) verifica il rispetto di requisiti di sicurezza da parte degli intermediari, raccoglie le segnalazioni di gravi incidenti cibernetici e, in caso di crisi, ne coordina le procedure di gestione.

Nel 2017 il Consiglio direttivo della BCE ha approvato la strategia di supervisione per la resilienza cibernetica delle infrastrutture di mercato europee. Tale strategia prevede tra l'altro la costituzione di un forum di cooperazione pubblico-privato, denominato European Cyber Resilience Board (ECRB), istituito nel 2018 (cfr. il par. 3.3).

Accanto ai tradizionali strumenti di vigilanza e supervisione, l'Eurosistema sta sviluppando un quadro di riferimento in materia di test tecnici della sicurezza dei sistemi, che sarà ultimato entro quest'anno per le infrastrutture di pagamento e di mercato.

Il ruolo della Banca d'Italia e dell'Ivass

La Banca d'Italia svolge diverse attività per rafforzare sia la propria sicurezza informatica (in quanto infrastruttura critica, erogatrice di servizi digitali e custode di dati sensibili), sia quella del sistema finanziario nel suo complesso, in qualità di autorità di supervisione dei sistemi di pagamento e di altre infrastrutture di mercato, nonché di autorità di vigilanza bancaria e finanziaria (cfr. il capitolo 4).

Analogamente l'Ivass, in quanto autorità di vigilanza sul sistema assicurativo, conduce varie attività per monitorare e rafforzare la sicurezza informatica del sistema stesso (cfr. il capitolo 5).

La Banca d'Italia e l'Ivass operano mediante:

– la costituzione di adeguati presidi difensivi interni, che includono il CERT aziendale della Banca (CERTBI);

– la partecipazione a tavoli tecnici internazionali ed europei delle banche centrali e del settore finanziario;

– l'emanazione di regolamentazione nazionale per rafforzare la governance dei processi informatici e i presidi in materia di sicurezza cibernetica;

– la vigilanza e la supervisione di infrastrutture di mercato e operatori finanziari nazionali;

– la raccolta di informazioni sulle vulnerabilità e sugli incidenti informatici;

– lo scambio di informazioni e di ricerche con le altre istituzioni impegnate sul fronte della difesa da attacchi cibernetici;

– lo stimolo alla cooperazione pubblico-privato per la condivisione delle informazioni e per la creazione di capacità difensive, anche attraverso la gestione di un CERT del settore finanziario italiano (CERTFin), in collaborazione con l'Associazione bancaria italiana (ABI);

– il rafforzamento, per mezzo dell'attività di educazione finanziaria, della consapevolezza di giovani e adulti in merito all'utilizzo di servizi finanziari digitali;

– la raccolta e l'analisi di dati statistici sulla frequenza e sull'impatto economico degli attacchi informatici contro il settore privato italiano;

– la valutazione del rischio cibernetico in ambito assicurativo con riferimento ai prodotti, come ad esempio le polizze di assicurazione specifiche (*cyber insurance*), e alla loro distribuzione.

Per coordinare al meglio le attività nelle diverse sedi di lavoro, nel 2017 la Banca d'Italia e l'Ivass hanno istituito il Gruppo di coordinamento sulla sicurezza cibernetica (GCSC).

1. I fattori di contesto

La sicurezza informatica, considerata in passato un tema unicamente tecnico e legato alla continuità operativa di processi specifici, interessa oggi competenze e contesti sempre più numerosi. L'ampliamento dei settori coinvolti e delle conoscenze richieste è una conseguenza della digitalizzazione dell'economia e della dipendenza di numerose attività dai servizi digitali; molte azioni quotidiane si svolgono nel cosiddetto spazio cibernetico o cyberspace[3]. In prospettiva la crescita dell'internet delle cose, ossia l'insieme di dispositivi connessi in grado di svolgere operazioni nel mondo fisico, aprirà sia le attività domestiche sia quelle di produzione alla dimensione cibernetica, in modo qualitativamente diverso rispetto a quanto accade attualmente.

I dispositivi, il software e le connessioni di rete che compongono lo spazio cibernetico presentano vulnerabilità tecnologiche e organizzative che possono essere sfruttate in modo malevolo, come dimostra il moltiplicarsi degli attacchi informatici[4]. Uno spazio cibernetico non sicuro costituisce una debolezza grave in una società digitalizzata, non solo per i danni diretti che gli attacchi possono arrecare alle strutture colpite, ma anche perché una diffusa percezione di insicurezza può minare il funzionamento di quei mercati, ormai vitali per l'economia, che si basano sulla disponibilità, sull'integrità e sulla riservatezza di dati digitali. Nel medio termine inoltre gli attacchi informatici potrebbero rallentare l'adozione di nuove tecnologie, con riflessi negativi sulla produttività e sulla crescita[5].

La minaccia cibernetica – pervasiva, anonima, polimorfa, transnazionale, asimmetrica[6] – richiede una risposta "di sistema", anche perché debolezze di una parte del cyberspazio causano danni anche in altre (esternalità negative)[7]. Questo principio è espresso sia nel *Quadro strategico nazionale per la sicurezza dello spazio cibernetico* adottato dal Governo italiano (cfr. il par. 2.3), sia negli omologhi documenti dei principali paesi appartenenti all'OCSE. Una pluralità di soggetti pubblici e privati deve agire di concerto per garantire la sicurezza del cyberspazio nel suo complesso.

La consapevolezza del rischio non deve essere diffusa solo tra gli addetti ai lavori, ma deve estendersi all'intera società. Molti incidenti cibernetici infatti traggono origine da comportamenti imprudenti, come ad esempio l'uso di password troppo semplici. Non è sufficiente investire in programmi antivirus e in altre difese

---

3 Il cyberspace è definito come «l'insieme delle infrastrutture informatiche interconnesse, comprensivo di *hardware*, *software*, dati ed utenti nonché delle relazioni logiche, comunque stabilite, tra di essi. Include tra l'altro internet, reti di comunicazione, sistemi attuatori di processo ed apparecchiature mobili dotate di connessione di rete», cfr. Presidenza del Consiglio dei ministri (2013a).

4 Per una rassegna dei principali incidenti informatici resi pubblici nell'ultimo decennio, cfr. CSIS (2018).

5 Cfr. tra gli altri: World Economic Forum (2014) e CSIS (2018).

6 A. Fazio e A. Leotta (2015), p. 71.

7 T. Moore e R. Anderson (2012).

tecniche: è necessario un vero e proprio cambio di paradigma, che coinvolga anche aspetti culturali e organizzativi[8].

Il rischio cibernetico non è nuovo: nelle fasi iniziali del processo di digitalizzazione tuttavia erano in numero limitato sia le potenziali vittime sia gli attori della minaccia. Solo pochi settori, come la difesa e le telecomunicazioni, erano abbastanza informatizzati da essere vulnerabili agli attacchi cibernetici; inoltre le conoscenze e le risorse necessarie per progettare e sferrare tali aggressioni esistevano quasi esclusivamente in ambito militare e in alcuni centri di ricerca. Negli anni l'uso di dispositivi informatici e l'accesso alle reti telematiche si sono enormemente estesi, moltiplicando il numero di obiettivi; inoltre le competenze necessarie per programmare codici malevoli (malware) sono ormai a disposizione di molte organizzazioni criminali, che sviluppano strumenti offensivi e talvolta li offrono a basso costo a un'ampia platea di clienti. Sebbene gli attacchi con finalità politico-militari giochino ancora un ruolo cruciale, sono diventati molto numerosi quelli sferrati da privati e motivati dal profitto.

Il settore finanziario, data la sua centralità nel sistema produttivo, rappresenta un obiettivo primario sia per gli aggressori motivati dal profitto sia per quelli intenzionati a compromettere l'ordinato funzionamento dell'economia. La superficie aggredibile è ampia in ragione dell'uso intensivo di tecnologie informatiche da parte dell'industria finanziaria, che è stata tra le più rapide a sfruttare i nuovi strumenti digitali; ancor più oggi, in quanto, con lo sviluppo del FinTech, i servizi finanziari ad alto contenuto tecnologico sono erogati per lo più online.

Un esempio di obiettivo critico è la rete SWIFT. Questa connette più di 11.000 soggetti in 200 paesi: il suo sistema di messaggistica è usato da banche, gestori di infrastrutture di mercato e autorità pubbliche nelle attività di intermediazione finanziaria. Negli ultimi anni ha subito numerosi attacchi, che in alcuni casi hanno anche coinvolto banche centrali[9].

---

[8] Benoît Cœuré, membro del Comitato esecutivo della BCE, ha parlato di paradigm shift, sottolineando che «we have to accept that cyberattacks are inevitable and that attackers are persistent. Consequently, we have to establish how – in case of persistent attacks – we prioritise our operations and resources, protect our key assets and restore functionalities. Cyber resilience goes beyond technology, it also encompasses governance, company culture and business processes» (B. Cœuré, 2017). Questo cambio di paradigma è richiamato anche in A. Fazio e F. Zuffranieri (2018).

[9] Nel 2016 l'uso non autorizzato di messaggi SWIFT da parte di un gruppo criminale ha portato alla sottrazione di circa 80 milioni di dollari dalla Banca centrale del Bangladesh; nel 2017 è stata colpita allo stesso modo una banca privata di Taiwan, con un danno di circa 60 milioni di dollari (poi in gran parte recuperati). Un episodio analogo, ma di dimensioni molto più contenute, ha riguardato recentemente la Banca centrale russa.

2. Il quadro istituzionale e normativo

2.1 Le strategie nazionali di sicurezza cibernetica e la cooperazione internazionale

L'intensificarsi della minaccia cibernetica ha posto gli Stati di fronte a complesse sfide di policy; gli attacchi informatici sono infatti in grado di dispiegare effetti lesivi dei diritti dei cittadini e degli Stati stessi, alla stregua delle armi tradizionali.

In diversi paesi le norme del diritto penale sono state aggiornate fin dagli anni novanta e sono stati introdotti reati come l'accesso abusivo ai sistemi informatici. Dai primi anni duemila le economie avanzate e i principali paesi emergenti hanno elaborato strategie più ampie per rafforzare la sicurezza cibernetica come parte della sicurezza nazionale.

Tali strategie, pur mostrando un diverso livello di sviluppo, presentano tratti comuni quali:

– la definizione di un'architettura istituzionale per la prevenzione e la gestione delle crisi;

– misure per il potenziamento della sicurezza delle Pubbliche amministrazioni e delle infrastrutture critiche;

– incentivi alla cooperazione pubblico-privato e alla formazione di specialisti;

– schemi di certificazione della sicurezza di software e hardware.

Nelle strategie nazionali assume quasi sempre particolare rilievo la condivisione di informazioni sugli attacchi e sulle minacce (*information sharing*). Poiché le tecniche di intrusione sono in rapida evoluzione, essere aggiornati sulle vulnerabilità dei sistemi informatici e sulle modalità con le quali soggetti ostili le sfruttano segna il discrimine tra una difesa efficace e una inefficace. Le imprese che hanno subito attacchi sono però riluttanti a svelarli per timore di ricadute reputazionali; sono disposte a condividere dati solo in contesti che garantiscono riservatezza e reciprocità. Talvolta gruppi di operatori economici particolarmente sensibili al rischio cibernetico (ad esempio i gestori di infrastrutture critiche) si aggregano volontariamente; più spesso è necessario un intervento del settore pubblico, che svolge una funzione di garanzia e aiuta a creare e a mantenere un clima di fiducia.

I modelli di *information sharing* di maggior successo sono due. Il primo si basa sugli *information and analysis centers* (ISAC), piattaforme che consentono a un gruppo di soggetti interessati di mettere in comune informazioni e capacità di analisi. Il secondo è fondato su reti di *computer emergency response teams* (CERT) e di *computer security incident response teams* (CSIRT)[10], squadre di "pronto intervento" costituite all'interno

[10] Un CERT ha in teoria un mandato più generale rispetto a uno CSIRT: il primo interviene in occasione di qualsiasi emergenza che mette a rischio il funzionamento di un sistema informatico (incluse ad esempio quelle causate da guasti ed eventi naturali), mentre il secondo si attiva solo nel caso di violazioni di sicurezza. Nei fatti i due acronimi vengono spesso usati per riferirsi alle stesse attività; in questo lavoro sono considerati equivalenti.

di Amministrazioni pubbliche, aziende e associazioni di categoria[11], che si collegano tra loro per condividere informazioni, capacità di analisi e capacità operative di difesa (cfr. il riquadro: *L'origine e l'evoluzione delle reti di CERT/CSIRT*)[12].

L'origine e l'evoluzione delle reti di CERT/CSIRT

Già negli anni ottanta del secolo scorso le amministrazioni militari dei principali paesi avanzati avevano strutture organizzative dedicate alla sicurezza informatica; in alcuni casi, soprattutto negli Stati Uniti, queste collaboravano anche con il mondo accademico per analizzare l'evoluzione della minaccia e per sviluppare mezzi di difesa. Alcune grandi aziende ad alta tecnologia destinavano risorse alla protezione cibernetica già molti anni prima che questa espressione divenisse di uso comune.

All'epoca non era ancora diffusa la consapevolezza che un attacco informatico potesse colpire simultaneamente molti obiettivi: le intrusioni erano per lo più isolate (nel 1986, ad esempio, alcuni hacker della Germania occidentale reclutati dai servizi di informazione sovietici avevano sottratto segreti dalle reti della Difesa americana). Non era quindi percepita come urgente la collaborazione tra le vittime nelle attività di analisi e di contrasto di un attacco.

Lo scenario cambiò nel 1988, quando lo studente di informatica Robert Morris (attualmente docente presso il Massachusetts Institute of Technology), allo scopo di misurare quanto fosse estesa la rete internet, programmò un software che, sfruttando una vulnerabilità del sistema operativo UNIX, si replicava automaticamente su tutti i terminali connessi in rete in un determinato momento, rinviando allo stesso Morris informazioni su ciascun terminale. Per un errore di programmazione questo software, benché concepito per non interferire con l'attività dei computer contagiati, finì per renderli inutilizzabili; secondo l'International Telecommunications Union, un'agenzia delle Nazioni Unite, bloccò circa il 10 per cento dei 6.000 computer a quel tempo collegati a internet.

I ricercatori della Defense Advanced Research Projects Agency (DARPA), l'ente militare americano cui si deve la creazione di internet, rilevarono che le vittime del cosiddetto *Morris worm* avevano per lo più affrontato il problema separatamente: ciascuno aveva speso risorse per identificare il problema, capire come combatterlo e ripristinare i sistemi danneggiati. Un approccio collaborativo, fondato sulla condivisione delle informazioni e degli strumenti di difesa, avrebbe consentito significativi risparmi economici e guadagni di tempestività.

Il governo statunitense si fece quindi promotore della costituzione del Computer Emergency Response Team (CERT) Coordination Center presso l'Istituto

---

[11] Ogni CERT/CSIRT svolge attività a favore di una specifica comunità di riferimento, nota come *constituency*: essa può essere definita in termini di utenti o di beni tecnologici tutelati.

[12] Le principali reti internazionali di CERT sono: (a) il Forum of Incident Response and Security Teams (FIRST), con sede negli Stati Uniti. È una confederazione internazionale di CERT, istituita nel 1990, che raggruppa oltre 300 organizzazioni di differenti nazionalità e settori; (b) la rete Trusted Introducer (TI), costituita nel 2000 dalla comunità dei CERT europei, che conta più di 100 organizzazioni.

di ingegneria del software della Carnegie Mellon University di Pittsburgh: fu questo il primo utilizzo ufficiale dell'acronimo CERT. Oggi le attività di coordinamento dei CERT statunitensi sono demandate a enti federali, ma è ancora attivo – ed è considerato di eccellenza – un CERT presso la Carnegie Mellon University.

Mentre, in linea generale, le iniziative di respiro nazionale e regionale (ad esempio a livello europeo) hanno prodotto risultati significativi, quelle sul fronte della cooperazione internazionale – essenziali per fronteggiare una minaccia globale – sono ancora carenti. Si sono registrati progressi solo su temi specifici, come il coordinamento tra Forze di Polizia per la lotta ad alcuni crimini, e in contesti in cui cooperano paesi che condividono i principali obiettivi strategici in materia di sicurezza, come la NATO e il G7.

L'Assemblea delle Nazioni Unite non è riuscita finora a raggiungere un accordo sull'applicazione del diritto internazionale ai conflitti nello spazio cibernetico. In particolare persistono differenze tra paesi circa le condizioni sotto cui un attacco informatico sponsorizzato da uno Stato possa essere considerato come un atto di guerra, e possa quindi legittimare l'autodifesa dello Stato colpito (ai sensi dell'art. 51 dello Statuto delle Nazioni Unite)[13] o innescare un intervento militare multilaterale (art. 42)[14].

2.2 La strategia di sicurezza cibernetica dell'Unione europea

I primi atti normativi dell'Unione europea in materia di *cybersecurity* risalgono agli inizi degli anni duemila e si sono concentrati sul contrasto alla criminalità. In questa fase disposizioni sulla sicurezza delle reti, non limitate ad aspetti di polizia, hanno riguardato solo il settore delle telecomunicazioni. Negli anni successivi è stata sottolineata la necessità di garantire in generale la sicurezza delle informazioni, in quanto ritenuta funzionale agli obiettivi di promozione dei valori di libertà e democrazia. Nel 2008, con la direttiva CE/2008/114 sulla protezione delle infrastrutture critiche, sono state introdotte misure minime di protezione anche rispetto alle minacce di origine tecnologica per le infrastrutture critiche europee.

Nel 2013 l'Unione è giunta alla formulazione di una strategia organica sulla sicurezza informatica[15]. Per quanto attiene alla difesa civile, l'asse portante di tale strategia

---

[13] «Nessuna disposizione del presente Statuto pregiudica il diritto naturale di autotutela individuale o collettiva, nel caso che abbia luogo un attacco armato contro un Membro delle Nazioni Unite, fintantoché il Consiglio di Sicurezza non abbia preso le misure necessarie per mantenere la pace e la sicurezza internazionale».

[14] «Se il Consiglio di Sicurezza ritiene che le misure previste nell'articolo 41 [intervento non armato] siano inadeguate o si siano dimostrate inadeguate, esso può intraprendere, con forze aeree, navali o terrestri, ogni azione che sia necessaria per mantenere o ristabilire la pace e la sicurezza internazionale. Tale azione può comprendere dimostrazioni, blocchi ed altre operazioni mediante forze aeree, navali o terrestri di Membri delle Nazioni Unite».

[15] Essa individua cinque priorità: aumentare la resilienza cibernetica dell'Unione, ossia la capacità di respingere attacchi informatici e di recuperare rapidamente se si viene colpiti; ridurre drasticamente il crimine informatico; sviluppare una politica di difesa militare nello spazio cibernetico e le necessarie capacità operative nel quadro della Politica di sicurezza e di difesa comune; sviluppare risorse industriali e tecnologiche in materia di *cybersecurity*; stabilire linee di politica internazionale riguardo all'azione degli Stati nello spazio cibernetico.

è rappresentata dalla direttiva UE/2016/1148 sulla sicurezza delle reti e dei sistemi informativi (direttiva NIS), emanata nel 2016 con obbligo di recepimento da parte degli Stati membri entro maggio del 2018. Il legislatore europeo ha previsto che gli Stati membri si dotino di un'organizzazione nazionale in grado di vincolare a stringenti misure di protezione i maggiori operatori di servizi essenziali per l'economia (energia, trasporti, finanza, sanità, erogazione di acqua potabile, smistamento del traffico telematico) e di servizi digitali (motori di ricerca, mercati online, fornitori di servizi di cloud computing). La direttiva ha introdotto a carico di questi operatori un obbligo di notifica alle autorità degli incidenti con "effetti negativi rilevanti"; la definizione dei criteri per individuarli è demandata agli Stati membri.

La direttiva ha istituito anche un gruppo di cooperazione in ambito UE per lo scambio di informazioni e migliori prassi. Il gruppo mira a potenziare le capacità di reazione alle crisi introducendo l'obbligo per ogni paese di dotarsi di uno CSIRT pubblico; quest'ultimo, nel caso di incidenti transfrontalieri, deve collaborare con gli omologhi team costituiti presso gli altri Stati membri.

Dal 2018 trova applicazione un ulteriore provvedimento comunitario denominato General Data Protection Regulation (GDPR), relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali. La nuova disciplina, che si applica a soggetti pubblici e privati, impone a chi custodisce e tratta dati personali l'adozione di standard di sicurezza più elevati rispetto al passato (cfr. il riquadro: *Il regolamento GDPR*).

Il regolamento GDPR

Il regolamento UE/2016/679 (General Data Protection Regulation, GDPR) è entrato in vigore il 25 maggio 2018; si applica al trattamento dei dati personali negli Stati membri dell'Unione europea e segna il passaggio da una concezione formale di protezione dei dati a una sostanziale. Le nuove regole si fondano sul principio della *data protection by default and by design*: le modalità di trattamento dei dati personali devono essere concepite con l'obiettivo primario di tutelare il diritto alla riservatezza degli interessati. A questo fine devono essere adottate sia misure tecniche, anche di sicurezza cibernetica, sia modelli organizzativi che minimizzino la probabilità di accessi indebiti alle informazioni.

Viene enfatizzata la responsabilità (*accountability*) dei cosiddetti titolari del trattamento dei dati personali (ad esempio i datori di lavoro verso i dipendenti, i fornitori di servizi nei confronti dei clienti): a loro compete l'accertamento del rispetto dei principi stabiliti nella norma. I titolari hanno l'obbligo di notificare all'autorità di controllo eventuali violazioni della riservatezza dei dati (*data breach*); devono anche informare i diretti interessati qualora ne derivi un rischio per i loro diritti e libertà. Tale innovazione è particolarmente importante perché espone al rischio di azioni legali una platea molto ampia, ossia tutti i titolari del trattamento di dati personali; potrebbe stimolare un generalizzato rafforzamento della sicurezza informatica e lo sviluppo del mercato assicurativo.

Il regolamento è sostenuto da un severo apparato sanzionatorio. Le sanzioni pecuniarie possono raggiungere i 20 milioni di euro nei casi più gravi, oppure il 4 per cento del fatturato (qualora questo sia superiore a 20 milioni).

Completano il quadro alcuni provvedimenti settoriali (per quelli relativi al sistema finanziario, come ad esempio la direttiva sui servizi di pagamento nel mercato interno, cfr. il par. 3.3 e il riquadro: *La direttiva PSD2* del capitolo 3).

Nel 2017 la Commissione europea ha presentato la proposta di regolamento Cybersecurity Act. Se approvato, quest'ultimo comporterebbe l'introduzione di una certificazione unica europea della sicurezza cibernetica di hardware e software e avrebbe un impatto potenzialmente molto rilevante, trasponendo in campo informatico gli stringenti standard già applicati alla sicurezza fisica dei beni prodotti nella UE. Responsabile delle certificazioni sarebbe l'Agenzia europea per la sicurezza delle reti e dell'informazione (European Network and Information Security Agency, ENISA)[16], che vedrebbe fortemente rafforzato il suo ruolo finora limitato a compiti tecnico-operativi (ad esempio l'organizzazione di esercitazioni), di studio e di consulenza per gli Stati membri.

2.3 La strategia di sicurezza cibernetica dell'Italia

In Italia, come nell'Unione europea, le prime iniziative sulla *cybersecurity* sono state incentrate sul contrasto alla criminalità; negli anni novanta sono stati introdotti nel Codice penale i reati informatici e il compito di contrastarli è stato affidato alla Polizia postale e delle comunicazioni[17].

Nei primi anni duemila è stato imposto alle Pubbliche amministrazioni di innalzare i propri livelli di sicurezza informatica[18]. Poco dopo sono state rafforzate le competenze in materia cibernetica del sistema di intelligence, mirando soprattutto alla protezione delle informazioni riservate o coperte da segreto di Stato[19]. Nel 2008 sono state censite le infrastrutture critiche informatizzate nazionali[20] ed è stato istituito il Centro nazionale anticrimine informatico per la protezione delle infrastrutture critiche (CNAIPIC); successivamente sono stati introdotti i primi meccanismi formali di gestione degli eventi cibernetici rilevanti per la sicurezza nazionale. Un approccio organico alla materia ha preso corpo tra il 2012 e il 2014. In particolare, nel 2013 la Presidenza del Consiglio dei ministri ha pubblicato due documenti: (a) il *Quadro strategico nazionale per la sicurezza dello spazio cibernetico*, con lo scopo di individuare strumenti e procedure per potenziare le capacità cibernetiche del Paese; (b) il *Piano nazionale per la protezione cibernetica e la sicurezza informatica*, che traduce in indirizzi operativi le previsioni del Quadro strategico. Sono inoltre stati istituiti un CERT nazionale al servizio di

---

16 Collaborando ad alto livello al network per la sicurezza delle informazioni all'interno dell'Unione, l'ENISA, che ha sede in Grecia, opera dal 2004 come centro di expertise sulla sicurezza cibernetica, allo scopo di svilupparne la cultura e la conoscenza per un corretto funzionamento del mercato interno. L'Agenzia coopera strettamente con gli Stati membri e il settore privato in tre diverse aree: raccomandazioni, attività di supporto per la definizione e l'implementazione delle policy, attività pratiche di collaborazione diretta con i team operativi come gli CSIRT.

17 L. 547/1993 e L. 269/1998.

18 Direttiva del Presidente del Consiglio dei ministri del 16 gennaio 2002.

19 DL 144/2005, convertito dalla L. 155/2005.

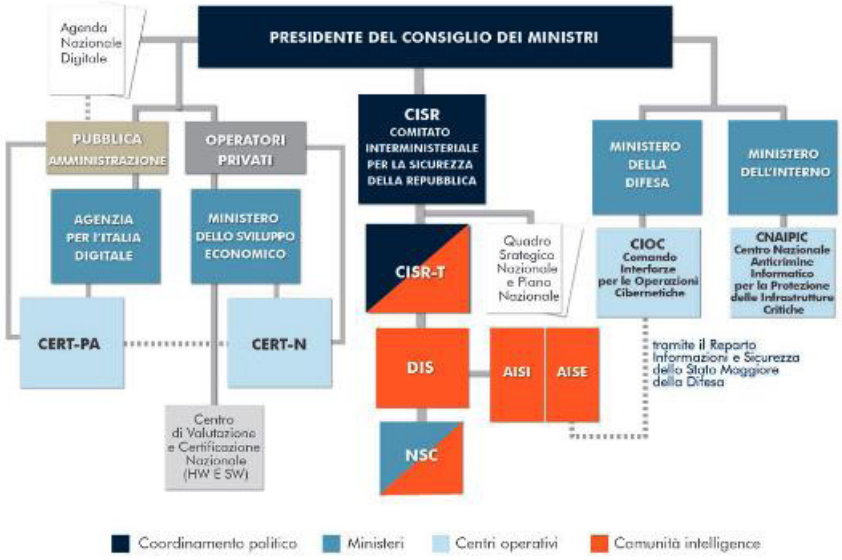
20 DM del Ministero dell'Interno 9 gennaio 2008, in attuazione del DL 144/2005.

cittadini e imprese, all'interno del Ministero dello Sviluppo economico[21], e un CERT della Pubblica amministrazione all'interno dell'allora neocostituita Agenzia per l'Italia digitale (AgID)[22]. È stata infine potenziata la capacità di raccolta informativa in materia cibernetica da parte degli organismi di informazione e sicurezza[23].

Il decreto del Presidente del Consiglio dei ministri del 17 febbraio 2017 (cosiddetto decreto Gentiloni) ha razionalizzato l'architettura istituzionale di sicurezza cibernetica, riconducendo direttamente tutte le responsabilità in materia alla Presidenza del Consiglio dei ministri (fig. 1).

Figura 1

ARCHITETTURA NAZIONALE DELLA SICUREZZA INFORMATICA DISEGNATA DAL DECRETO GENTILONI



Fonte: Presidenza del Consiglio dei ministri (2018).

La Presidenza impartisce l'indirizzo politico mediante il Comitato interministeriale per la sicurezza della Repubblica (CISR), di cui fanno parte alcuni ministeri (Difesa, Interno, Affari esteri, Economia e finanze, Sviluppo economico, Giustizia). Le attività operative sono coordinate dal Dipartimento delle informazioni per la sicurezza (DIS) della Presidenza stessa, che assume anche la direzione del Nucleo per la sicurezza cibernetica (NSC), responsabile per la gestione delle crisi (fig. 2).

Al decreto Gentiloni è seguita la pubblicazione della seconda edizione del Piano nazionale per la protezione cibernetica e la sicurezza informatica, che aggiorna gli

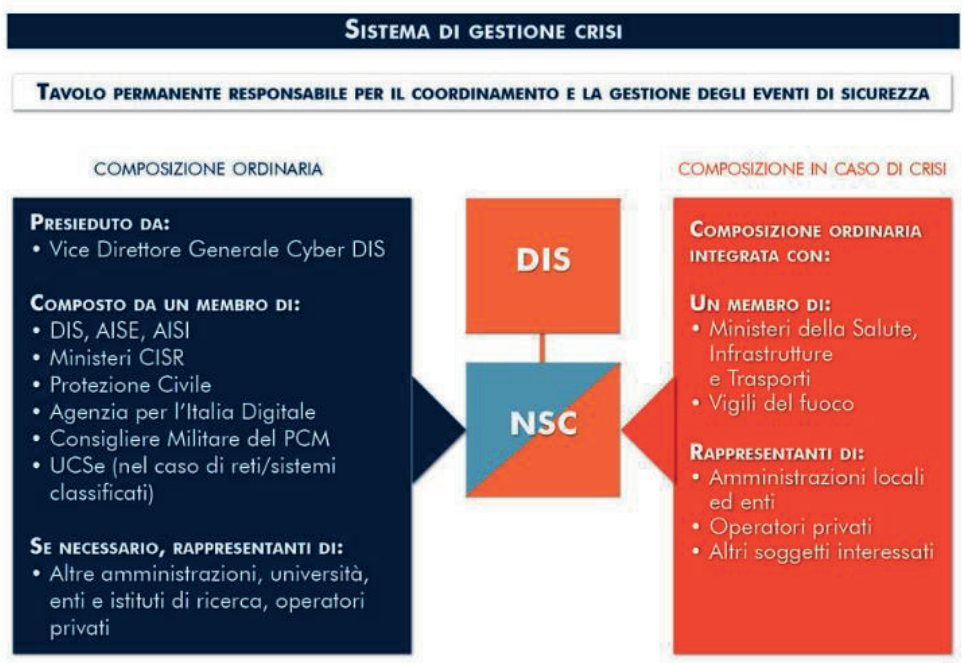
[21] D.lgs. 70/2012.

[22] DL 22 giugno 2012, convertito con modificazioni dalla L. 134/2012.

[23] L. 133/2012.

Figura 2

SISTEMA DI GESTIONE DELLE CRISI PREVISTO DAL DECRETO GENTILONI



Fonte: Presidenza del Consiglio dei ministri (2018).

strumenti operativi di contrasto al rischio e sottolinea tra l'altro la necessità di migliorare il coordinamento pubblico-privato.

Nel maggio 2018 con il recepimento della direttiva NIS sono stati delineati ulteriori interventi di rafforzamento del "sistema Paese"; è stata prevista l'istituzione di uno CSIRT italiano presso la Presidenza del Consiglio dei ministri, nel quale confluiranno il CERT nazionale e quello della Pubblica amministrazione (cfr. il riquadro: *La direttiva NIS in Italia*). Sul versante regolamentare, il Parlamento ha conferito apposita delega al Governo per l'adeguamento dell'ordinamento italiano in tema di misure per la sicurezza dei dati personali (regolamento GDPR).

La direttiva NIS in Italia

Il D.lgs. 65/2018, emanato in attuazione della direttiva UE/2016/1148 sulla sicurezza delle reti e dei sistemi informativi (Directive on Security of Network and Information Systems, NIS), disegna un sistema di responsabilità articolato. In coerenza con l'architettura definita dal decreto del Presidente del Consiglio dei ministri del 17 febbraio 2017 (decreto Gentiloni), al vertice del sistema è posta la Presidenza del Consiglio dei ministri, cui vengono affidati i compiti di indirizzo politico e di coordinamento previsti dal legislatore comunitario: la definizione della strategia nazionale di *cybersecurity*, il raccordo con l'Unione europea e con gli altri Stati

membri mediante il Dipartimento delle informazioni per la sicurezza della Presidenza del Consiglio (DIS), la raccolta centralizzata di informazioni sugli incidenti e il monitoraggio delle minacce attraverso il *computer security incident response team* (CSIRT) italiano.

Con il decreto vengono inoltre individuate le autorità competenti di settore, che hanno il compito di specificare gli operatori di servizi essenziali, definire le misure di sicurezza minime, vigilare sulla loro applicazione anche mediante ispezioni, comminare sanzioni. Le autorità coinvolte sono:

- il Ministero dello Sviluppo economico per il settore energetico, per le infrastrutture di scambio del traffico telematico[1] (le cosiddette infrastrutture digitali) e per i servizi digitali;
- il Ministero dei Trasporti e delle infrastrutture per il settore dei trasporti;
- il Ministero dell'Economia e delle finanze, in collaborazione con la Banca d'Italia e con la Commissione nazionale per le società e la borsa (Consob), per il settore bancario e delle infrastrutture dei mercati finanziari[2];
- il Ministero della Salute e, per quanto di competenza, le Regioni e le Province autonome di Trento e Bolzano per l'attività di assistenza sanitaria;
- il Ministero dell'Ambiente e, per quanto di competenza, le Regioni e le Province autonome di Trento e Bolzano per il settore di fornitura e distribuzione dell'acqua potabile.

---

[1] Il settore delle telecomunicazioni è escluso dall'ambito di applicazione della NIS in quanto già destinatario di disciplina specifica. Rientrano invece tra gli operatori essenziali NIS i gestori degli *internet exchange points* (IXP, ossia le infrastrutture che consentono lo scambio di dati tra i vari provider di servizi internet), dei servizi *domain name system* (DNS, le infrastrutture che consentono di instradare il traffico di rete trasformando un indirizzo di rete nel formato *universal resource locator*, URL, ad esempio www.bancaditalia.it, nell'indirizzo IP del server di destinazione), e dei servizi *top level domain* (TLD), ossia le infrastrutture che gestiscono l'assegnazione dei suffissi di dominio come ".it" o ".com" ai siti internet.

[2] Non sono ricompresi i sistemi di pagamento e regolamento; la direttiva non incide sul regime previsto dal diritto dell'Unione per la sorveglianza dell'Eurosistema su tali sistemi (cfr. il considerando 14 della direttiva e il parere della Banca centrale europea del 25 luglio 2014).

Per quanto riguarda la Pubblica amministrazione, l'AgID ha emanato le *Misure minime di sicurezza ICT per le pubbliche amministrazioni*, intese come insieme ordinato e ragionato di "controlli", ossia azioni puntuali di natura tecnica e organizzativa[24] volte a prevenire il rischio di attacchi informatici e a contenerne gli effetti negativi. È stato inoltre adottato il *Piano triennale per l'informatica nella Pubblica amministrazione 2017-2019*, che definisce il modello di riferimento per lo sviluppo dell'informatica pubblica italiana e la strategia operativa di trasformazione digitale del Paese. Il Piano prevede la razionalizzazione delle risorse ICT come metodo prioritario per aumentare il livello di sicurezza attraverso la riduzione della superficie esposta agli attacchi informatici.

---

[24] Circolare AgID 2/2017.

3. La sicurezza cibernetica del sistema finanziario e il ruolo delle autorità di settore

3.1 Gli attacchi al sistema finanziario

Il sistema finanziario costituisce un obiettivo preferenziale per gli attori della minaccia, che siano motivati dal profitto o interessati a impedire l'ordinato funzionamento del sistema economico per motivi politici. Già nel 2014 un attacco coordinato contro numerose banche statunitensi condusse, tra l'altro, al furto dei dati personali di 80 milioni di clienti di JP Morgan Chase. Negli anni successivi si sono moltiplicati episodi simili; quasi nessuna delle grandi istituzioni finanziarie private è rimasta immune e sono state colpite anche alcune banche centrali[25].

Gli attacchi al sistema finanziario sono talvolta condotti con metodi molto semplici, come il furto di credenziali di accesso ai conti mediante il phishing, o il *denial of service*, che, sovraccaricando i server con milioni di richieste simultanee di dati, rende inutilizzabili i servizi bancari erogati via rete. Altre volte le intrusioni sono condotte con metodi complessi e portano alla sottrazione di fondi o di dati su larga scala.

La difesa del sistema finanziario è assai complessa: il settore è altamente digitalizzato, è interconnesso a livello globale mediante un piccolo numero di infrastrutture che possono presentare vulnerabilità, è attaccabile attraverso possibili comportamenti imprudenti di centinaia di milioni di utenti di servizi finanziari online. Un attacco che va a buon fine può essere particolarmente dannoso anche se condotto su piccola scala: alcuni processi centrali del sistema finanziario, come quelli legati al regolamento dei pagamenti, dipendono fondamentalmente dalla tempestiva disponibilità dei dati; un ritardo anche modesto si traduce in costi elevati.

Le autorità di settore sono state tra le prime, al di fuori dell'ambito della difesa e della sicurezza nazionale, a prestare attenzione al rischio cibernetico, intuendone il potenziale impatto negativo non solo sui singoli operatori colpiti, ma anche sulla fiducia del pubblico nei confronti del sistema finanziario. Con lo sviluppo di malware in grado di diffondersi molto rapidamente, dando vita a vere e proprie epidemie, assume maggiore rilevanza anche il rischio sistemico derivante dall'alto livello di interconnessione dei processi e dei sistemi finanziari (cfr. il riquadro: *Due esempi di attacco cibernetico su scala globale: WannaCry e NotPetya*).

Due esempi di attacco cibernetico su scala globale: WannaCry e NotPetya

Nei primi mesi del 2017 un gruppo di hacker noto come Shadow Brokers ha diffuso in rete un codice malevolo che è stato utilizzato da gruppi criminali per realizzare strumenti di attacco particolarmente virulenti.

Questo codice ha la caratteristica di replicarsi molto velocemente mediante artifici inediti e sofisticati, ideati proprio per facilitare il più possibile il contagio tra computer.

---

[25] Cfr. nota 9.

Tale meccanismo è stato alla base di due tra le più importanti crisi cibernetiche dei tempi recenti. Nel maggio 2017 centinaia di migliaia di utenti del sistema operativo Windows sono stati colpiti da WannaCry, un programma che blocca il funzionamento di un computer cifrando i dati e che chiede un "riscatto" (*ransomware*) in Bitcoin per decifrarli; in alcuni ospedali britannici è stato necessario rinviare visite e operazioni per indisponibilità dei sistemi informatici.

Nel giugno 2017 è stato sferrato un altro attacco attraverso la diffusione di NotPetya, software ancora più pericoloso in quanto cifra i dati ma non dà la possibilità di decifrarli, di fatto distruggendo i contenuti dei dispositivi colpiti. La multinazionale danese Møller-Mærsk ha dichiarato danni per circa 300 milioni di dollari; anche altri gruppi industriali, pur non indicando un ammontare preciso, hanno rivelato di aver subito conseguenze significative[1]. Secondo fonti giornalistiche l'impatto globale di NotPetya ha superato un miliardo di dollari.

Le due campagne di attacco hanno sfruttato vulnerabilità già note, presenti nelle piattaforme più comuni. Il numero delle vittime, seppure elevato, è rimasto contenuto grazie al fatto che molte aziende avevano aggiornato per tempo i propri sistemi.

---

[1] C. Biancotti e R. Cristadoro (2018).

Anche quando non hanno responsabilità di regolamentazione e vigilanza sugli intermediari, le banche centrali nella maggior parte dei paesi rivestono un ruolo di primaria importanza nel guidare il processo di rafforzamento del sistema finanziario; esse infatti spesso gestiscono direttamente o hanno responsabilità di supervisione su infrastrutture vitali, come i sistemi di pagamento.

Il rischio cibernetico riguarda anche il settore assicurativo, le cui aziende hanno ampia esposizione in ragione della catena del valore in cui sono inserite[26] e della connessione con le altre componenti del sistema finanziario (banche e conglomerati). I profili tipici di operatività nei rami vita, danni e salute, che comportano un'intensa interazione online con gli assicurati, espongono gli operatori ai rischi legali connessi con la sottrazione di informazioni riservate.

D'altro canto, per il settore assicurativo il presidio del rischio cibernetico costituisce un'opportunità di mercato, con lo sviluppo e l'offerta a imprese e a individui di prodotti di copertura contro gli effetti avversi degli attacchi informatici (cfr. il par. 5.3). Questo mercato presenta ancora una certa immaturità a livello globale[27]; si sta però sviluppando rapidamente e le autorità di settore hanno un ruolo

---

[26] Vi partecipano soggetti con dimensioni operative e presidi organizzativi molto eterogenei (agenzie, broker, singoli agenti).

[27] Secondo stime dell'OCSE, negli Stati Uniti – dove è concentrato più dell'80 per cento del mercato globale – la quota di imprese con copertura specifica sarebbe tra il 20 e il 35 per cento. Ancora inferiori sono le percentuali nel Regno Unito, secondo mercato al mondo, e nell'Europa continentale; cfr. in proposito OCSE (2017).

centrale nel garantire che le caratteristiche del rischio cibernetico, per l'elevata correlazione tra eventi e la rilevanza dei grandi incidenti, non si trasformino in una minaccia per la solvibilità delle imprese assicurative.

3.2 Le risposte in ambito internazionale

Nel settore finanziario la cooperazione internazionale in materia di sicurezza cibernetica ha raggiunto risultati apprezzabili anche in contesti allargati, almeno in termini di definizione di linee guida e migliori prassi. Ciò è stato facilitato dall'esistenza di precedenti su altri fronti, primo tra tutti quello della stabilità finanziaria, e dalla dimensione globale di alcuni operatori chiave.

Al contrario di quanto è accaduto in ambito politico, le banche centrali, le autorità di supervisione sui mercati e quelle sugli intermediari bancari e finanziari hanno raggiunto un consenso su alcuni documenti fondamentali, coinvolgendo anche paesi con agende strategiche molto diverse: l'esempio più rilevante è rappresentato dalla *Guidance on cyber resilience for financial market infrastructures* pubblicata nel 2016 dal CPMI-Iosco[28]. In coerenza con i principi internazionali di supervisione[29], la Cyber guidance indica metodi e strumenti per garantire la continuità operativa delle infrastrutture di mercato in caso di attacchi cibernetici; anche se rivolta a una specifica categoria di operatori, è diventata una pubblicazione di riferimento per l'intero sistema finanziario.

Altre iniziative di cooperazione su base molto ampia sono quelle avviate dall'FSB su mandato del G20. Le principali riguardano:

– la definizione di un glossario per il settore finanziario in materia di sicurezza e resilienza cibernetica. Il Cyber lexicon, che sarà pubblicato entro la fine del 2018, ha lo scopo di eliminare le ambiguità terminologiche e supportare iniziative internazionali coerenti, riducendo la difformità tra regolamentazioni nazionali che spesso aggrava l'onere di compliance dei soggetti vigilati;

– le analisi di scenario condotte dallo Standing Committee on Assessment of Vulnerabilities (SCAV) per valutare il potenziale impatto sistemico di attacchi informatici;

– l'inclusione del rischio cibernetico nel programma di allarme preventivo (*early warning exercise*) condotto in collaborazione con il Fondo monetario internazionale.

Nel 2016 l'Associazione internazionale degli organi di vigilanza nel settore assicurativo (International Association of Insurance Supervisors, IAIS) ha diffuso un documento ricognitivo[30] sull'evoluzione del rischio cibernetico, sulle pratiche di mitigazione e sugli approcci adottati dalle autorità. L'OCSE, secondo cui la diffusione di polizze assicurative a copertura del rischio cibernetico è fondamentale per aumentare la sicurezza

---

[28] Ai lavori ha partecipato, con un ruolo consultivo, anche il Comitato di Basilea per la vigilanza bancaria.

[29] CPSS-Iosco (2012).

[30] IAIS (2016).

dell'economia, ha pubblicato raccomandazioni destinate a imprese di assicurazione e ad autorità di supervisione[31].

Il consenso globale raggiunto su linee guida e standard tecnici non è stato invece conseguito su temi con più forti legami con la sicurezza nazionale, come la condivisione di informazioni, il coordinamento tra paesi nel reagire a crisi cibernetiche con impatto transfrontaliero e le metodologie di test delle difese degli operatori finanziari privati (cfr. il riquadro: *L'*intelligence-led red team testing*: caratteristiche e criticità*).

Su queste materie si sono registrati progressi solo all'interno del G7, il cui Cyber Expert Group (G7-CEG) ha delineato dei principi non vincolanti di alto livello per i test dei sistemi informativi[32] e sta elaborando un protocollo di comunicazione e cooperazione internazionale tra autorità finanziarie, da seguire in caso di crisi transfrontaliera. Questo protocollo verrà sperimentato nel 2019 all'interno di un esercizio di simulazione. Il G7-CEG ha anche istituito un tavolo di confronto con il settore privato per individuare strategie di scambio di informazioni e interventi regolatori appropriati.

L'*intelligence-led red team testing*: caratteristiche e criticità

Per valutare le difese cibernetiche di un'impresa non è sufficiente verificare il rispetto degli obblighi normativi, ma è opportuno simulare attacchi il più possibile realistici. Uno dei modelli ritenuti più efficaci al riguardo è costituito dall'*intelligence-led red team testing* (o *red teaming*). Per misurare la qualità delle difese di un'impresa target viene in primo luogo chiesto a un gruppo di investigatori (*threat intelligence providers*) di valutare le modalità attraverso le quali soggetti ostili potrebbero sfruttare le vulnerabilità organizzative, procedurali e tecnologiche dell'organizzazione, e di descrivere tali vulnerabilità in un *targeted threat intelligence report*. Sulla base di tale rapporto, un secondo gruppo indipendente di "pseudo-attaccanti" (denominato *red team*, secondo un'espressione mutuata dalle esercitazioni militari) pianifica ed esegue appositi esercizi di simulazione allo scopo di valutare le difese dell'obiettivo dell'aggressione.

Poiché il *red team* può scoprire vulnerabilità dell'impresa target o può entrare in possesso di informazioni riservate, tali esercizi – se condotti da persone non affidabili e senza opportune garanzie – sono a loro volta fonte di ulteriori rischi. Nel settore finanziario questi aspetti sono ancora più rilevanti, per cui alcuni governi e autorità finanziarie, con il supporto del settore privato, hanno introdotto quadri di riferimento per lo svolgimento controllato di tali simulazioni, prevedendo il ricorso a schemi di certificazione e accreditamento dei fornitori di servizi di *threat intelligence* e di *red teaming*.

---

31 OCSE (2017).

32 G7-CEG (2016) e (2017).

3.3 Il contesto europeo: sviluppi recenti

L'elevata globalizzazione del sistema finanziario fa sì che le iniziative regionali, almeno nei paesi avanzati, siano in generale coerenti con quelle internazionali. Ciò è vero soprattutto per le infrastrutture di mercato e di pagamento. La Cyber guidance emanata dal CPMI-Iosco (cfr. il par. 3.2) è il principale riferimento adottato nel Sistema europeo di banche centrali (SEBC) e nell'Eurosistema.

Anche in materia di vigilanza bancaria le riflessioni sul rischio cibernetico attualmente in corso in ambito UE e nell'Eurosistema si raccordano con quelle internazionali; rimangono però importanti differenze regionali e nazionali, conseguenza del forte legame che i sistemi bancari mantengono con i contesti economici e istituzionali locali.

Il Comitato europeo per il rischio sistemico (European Systemic Risk Board, ESRB) garantisce un raccordo di alto livello a fini di stabilità finanziaria tra Commissione europea, autorità di supervisione finanziaria europee (EBA, ESMA, EIOPA), Eurosistema e autorità macroprudenziali nazionali. Al suo interno è istituito lo European Cyber Risk Group (ECRG) che analizza i potenziali impatti sistemici degli attacchi cibernetici con particolare riferimento all'economia europea.

3.3.1 Le infrastrutture di mercato e di pagamento

A marzo del 2017, su proposta del Market Infrastructures and Payments Committee (MIPC), il Consiglio direttivo della BCE ha approvato la strategia di supervisione per la resilienza cibernetica delle infrastrutture di mercato europee, sviluppata da una task force – formata da rappresentanti di 14 banche centrali e di altre autorità europee – con il fine di assicurare un'applicazione comune e coerente con la Cyber guidance emanata dal CPMI-Iosco nell'Eurosistema.

La strategia, che troverà piena attuazione entro il 2019, individua tre obiettivi: il rafforzamento delle singole infrastrutture di mercato, con specifico riferimento ai sistemi di pagamento; il rafforzamento del settore nel suo complesso; la promozione della cooperazione pubblico-privato a livello europeo.

Per conseguire questi obiettivi il MIPC ha sviluppato:

a) un questionario e un modello di analisi per raccogliere e valutare informazioni relative alla conformità delle infrastrutture di mercato europee con le previsioni della Cyber guidance;

b) un quadro di riferimento per l'esecuzione di test avanzati sui sistemi informativi (*European threat intelligence-based ethical red teaming*, Tiber-EU)[33];

[33] La guida metodologica del Tiber-EU è stata approvata dal Consiglio direttivo della BCE e pubblicata a maggio del 2018. A completamento del *framework*, entro la fine del 2018 saranno pubblicate due linee guida: (a) *Tiber-EU Threat Intelligence and Red Teaming Services Procurement Guide*; (b) *Tiber-EU White Team Guide*.

c) un insieme di *oversight expectations*, che costituiscono uno strumento di autovalutazione per i soggetti regolati e una base per l'interazione tra questi ultimi e le autorità.

Nel 2018 è stato inoltre istituito lo European Cyber Resilience Board (ECRB) quale forum di discussione strategica per facilitare e sostenere la cooperazione pubblico-privato in tema di resilienza cibernetica del sistema finanziario europeo[34].

3.3.2 La vigilanza sugli intermediari bancari e finanziari

Nel contesto europeo i principi di fondo per la vigilanza bancaria in materia cibernetica sono delineati dall'EBA, che definisce requisiti di sicurezza per i soggetti vigilati e regole di supervisione armonizzate per le autorità degli Stati membri; a tale scopo ha emanato linee guida nell'ambito dei servizi di pagamento, come previsto dall'aggiornamento della direttiva UE ad essi relativa (cfr. il riquadro: *La direttiva PSD2*).

L'EBA nel 2017 ha inoltre diffuso raccomandazioni sull'esternalizzazione dei servizi di cloud computing nel settore finanziario e linee guida per le autorità di vigilanza sulla valutazione del rischio informatico, che comprende anche quello legato agli attacchi cibernetici. Si tratta di strumenti che consentono di uniformare e integrare le prassi di supervisione nei paesi dell'Unione.

La direttiva PSD2

La direttiva UE/2015/2366 sui servizi di pagamento nel mercato interno (Revised Directive on Payment Services, PSD2), che sostituisce la precedente direttiva UE/2007/64, è entrata in vigore nei paesi membri nel gennaio 2018 e prevede norme per la gestione della sicurezza dei prestatori di servizi di pagamento. Questi sono tenuti ad adottare misure di attenuazione del rischio nella gestione interna, nell'interazione con la clientela (ad esempio l'autenticazione "forte") e in quella con altri prestatori di servizi di pagamento (ad esempio la comunicazione sicura con i nuovi operatori FinTech abilitati ad accedere ai conti bancari).

La direttiva introduce inoltre un obbligo di notifica degli incidenti gravi (art. 95), da individuare seguendo le linee guida dell'Autorità bancaria europea (European Banking Authority, EBA). La notifica deve essere indirizzata all'autorità competente dello Stato membro di origine del prestatore di servizi di pagamento; l'autorità competente a sua volta fornirà all'EBA, alla Banca centrale europea e alle altre autorità nazionali eventualmente interessate i dettagli dell'accaduto (art. 96). L'introduzione degli obblighi di notifica persegue due obiettivi: (a) prevenire eventi che per loro natura possono produrre

[34] L'ECRB è presieduto dalla BCE ed è composto da operatori dei sistemi di pagamento e delle altre infrastrutture di mercato, *critical service providers* e circuiti di pagamento di rilevanza europea. I membri sono identificati e designati dalla BCE e durano in carica un biennio. L'ECRB è formato da sette banche centrali in via permanente e tre banche centrali a rotazione. Sono inoltre invitati a partecipare in qualità di osservatori: ESMA, ENISA, EUROPOL, EBA, ECB/SSM e Commissione europea.

effetti a catena sul sistema finanziario; (b) migliorare la capacità di reazione a livello sistemico a fronte di tali eventi.

Nel 2017 l'EBA ha introdotto alcune importanti innovazioni, pubblicando degli standard di riferimento (*regulatory technical standards*) relativi alla sicurezza informatica per i prestatori di servizi di pagamento (banche, poste, istituti di moneta elettronica e altri istituti di pagamento).

Per quanto riguarda l'Europa, è centrale il ruolo del Meccanismo di vigilanza unico (Single Supervisory Mechanism, SSM), che dal 2015 si è dotato di un *framework* per la collaborazione tra la BCE e le autorità nazionali al fine di garantire una gestione condivisa, efficace ed efficiente di eventuali attacchi informatici contro banche significative. È stata istituita una base dati degli incidenti – alimentata da notifiche obbligatorie da parte delle banche – e la gestione operativa delle crisi è stata affidata a un'apposita task force.

In funzione di specifici indicatori di rischio derivanti da segnalazioni di incidenti o da debolezze riscontrate nell'attività di controllo *offsite*, l'SSM avvia ispezioni dedicate all'analisi del rischio cibernetico.

3.3.3 Il settore assicurativo

Nel settore assicurativo il processo di armonizzazione di regolamentazione e supervisione è coordinato dall'EIOPA. Il *framework* regolamentare Solvency II prevede, con riferimento al sistema di governance, che le imprese assicurative garantiscano la continuità delle loro attività, anche con lo sviluppo di piani di continuità che includano una componente relativa ai rischi informatici.

L'EIOPA ha inoltre promosso uno studio sulla diffusione delle polizze assicurative a copertura del rischio cibernetico in Europa, che sarà concluso entro il 2018.

3.4 Il quadro legislativo italiano

La normativa europea di settore descritta nel paragrafo precedente si applica anche al sistema finanziario italiano. Oltre a questa normativa, valgono le disposizioni nazionali emanate dalla Banca d'Italia, dall'Ivass e dalla Consob.

Con l'entrata in vigore della direttiva NIS, la protezione cibernetica degli enti creditizi e delle infrastrutture di mercato di maggiore rilevanza è inserita nella più ampia cornice nazionale (cfr. il par. 2.3 e il riquadro: *La direttiva NIS in Italia* del capitolo 2), con l'istituzione tra l'altro di un raccordo formale tra le autorità di settore e quelle governative.

4. Il ruolo della Banca d'Italia

4.1 La sicurezza cibernetica della Banca d'Italia

La Banca d'Italia svolge da lungo tempo un ruolo di stimolo nel processo di digitalizzazione del sistema finanziario, riservando una particolare attenzione al tema della sicurezza informatica. In passato questa funzione si manifestava principalmente attraverso il presidio dei rischi operativi e della continuità di servizio (*business continuity*), ed è proprio in quest'ambito che si è inizialmente sviluppata una sensibilità nei confronti della minaccia cibernetica.

La Banca presiede il Comitato per la continuità di servizio della piazza finanziaria italiana (Codise), istituito nel 2003 per gestire il coordinamento delle eventuali crisi operative della piazza stessa. Al Comitato partecipano gli operatori del settore finanziario rilevanti sul piano sistemico e la Consob[35]. Il Codise svolge periodicamente simulazioni di crisi a scopo di esercitazione; già nel 2008 queste contemplavano l'eventualità di attacchi informatici.

Con l'evoluzione della tecnologia e la proliferazione degli attacchi, alla tematica della continuità operativa se ne sono aggiunte altre. Attualmente la Banca d'Italia conduce numerose attività che mirano a rafforzare la sicurezza informatica interna (cfr. il par. 4.2) e del sistema finanziario (cfr. il par. 4.3). Svolge inoltre attività di ricerca in tema di sicurezza informatica dell'economia nel suo complesso, poiché vulnerabilità in altri settori potrebbero compromettere anche la sicurezza del sistema finanziario (cfr. il par. 4.4).

Il Piano strategico per il triennio 2017-19 mette in evidenza l'importanza del tema cyber con due piani di azione: (a) "Rafforzare la *cyber security* della Banca in relazione a nuovi scenari di rischio", nell'ambito dell'obiettivo "Essere più innovativi ed efficienti"; (b) "Promuovere l'innovazione e la resilienza del settore finanziario italiano", quale parte dell'obiettivo "Promuovere in Italia e in Europa servizi di pagamento innovativi, efficienti e sicuri".

Per rispondere alla minaccia cibernetica devono essere considerati congiuntamente profili tecnologico-operativi, normativi, di sorveglianza e vigilanza ed economici. Per coordinare al meglio le attività nelle diverse sedi di lavoro, nel 2017 la Banca d'Italia e l'Ivass hanno istituito un Gruppo di coordinamento sulla sicurezza cibernetica (GCSC).

4.2 La Banca d'Italia come infrastruttura critica

La Banca d'Italia deve mantenere un livello molto elevato di sicurezza informatica interna in quanto:

---

[35] Il Codise coopera con autorità governative e altre istituzioni pubbliche e private coinvolte nella gestione delle crisi e nella continuità di servizio delle infrastrutture critiche nazionali. Attraverso il Codise, la Banca partecipa a esercitazioni di comunicazione e gestione delle crisi a livello europeo e internazionale (ad esempio il *TITUS exercise* presso la BCE). Dal 2014 il ruolo del Codise è esplicitamente richiamato nella normativa di vigilanza bancaria e finanziaria e nelle linee guida per la continuità operativa delle infrastrutture di mercato.

– è individuata come gestore di infrastruttura critica informatizzata di interesse nazionale definita dal DM 9 gennaio 2008 del Ministero dell'Interno (cfr. il par. 2.3). In questa veste collabora al contrasto delle minacce cibernetiche con il Centro nazionale anticrimine informatico per la protezione delle infrastrutture critiche (CNAIPIC) del Servizio centrale della Polizia postale e delle comunicazioni;

– eroga servizi digitali a favore dell'Eurosistema (ad esempio mediante le piattaforme TARGET2 e TARGET2-Securities) e servizi a favore di enti governativi nazionali quali la tesoreria dello Stato, le aste del debito pubblico, il Sistema informativo delle operazioni degli enti pubblici (Siope);

– è titolare del trattamento di dati personali in formato elettronico ai sensi del regolamento GDPR.

I presidi di difesa informatica della Banca sono stati recentemente rafforzati mediante:

– l'elaborazione di una strategia di resilienza cibernetica dell'Istituto, sulla base delle linee guida e delle migliori prassi settoriali e internazionali;

– la creazione del CERT della Banca d'Italia (CERTBI), di un *security operations center* (SOC) e di un *network operations center* (NOC);

– la pianificazione di un programma di difesa cibernetica che prevede investimenti in risorse informatiche, anche per aggiornare e migliorare le misure di difesa dinamica;

– l'introduzione di innovazioni organizzative e tecniche per l'adeguamento dell'Istituto in base alla nuova disciplina europea in materia di privacy (cfr. il riquadro: *Il regolamento GDPR* del capitolo 2).

La Banca contribuisce alla stesura di una proposta per la realizzazione di un'offerta comune di servizi di sicurezza per il SEBC.

4.3 La sicurezza cibernetica del sistema finanziario

La Banca è competente in materia di sicurezza cibernetica del sistema finanziario:

– in quanto autorità di sorveglianza sul sistema dei pagamenti e di supervisione sulle altre infrastrutture di mercato; nell'Eurosistema condivide tale responsabilità con la BCE e con le altre banche centrali nazionali. L'obiettivo perseguito è l'innalzamento della resilienza cibernetica delle infrastrutture del mercato finanziario. Esponenti della Banca hanno partecipato alla stesura delle principali linee guida internazionali (cfr. il par. 3.2) e seguono lo sviluppo della strategia dell'Eurosistema (cfr. il par. 3.3). Nell'ambito della sorveglianza cooperativa su SWIFT, la Banca d'Italia collabora al monitoraggio del *Customer Security Programme* (SWIFT-CSP), che consiste in una serie di requisiti e controlli di sicurezza richiesti agli utenti a seguito dei recenti attacchi informatici su scala globale;

– in qualità di autorità di vigilanza sul sistema bancario e finanziario in ambito nazionale, ha introdotto requisiti specifici per la gestione dei sistemi informativi delle banche con la revisione della circolare 285/2013 (Disposizioni di vigilanza

per le banche). Tali requisiti includono misure legate alla sicurezza informatica dei soggetti vigilati nonché l'obbligo di segnalare gravi incidenti informatici, compresi gli attacchi cibernetici. All'interno dell'SSM la Banca d'Italia partecipa all'attività di valutazione del rischio cibernetico delle banche significative, che ha avuto inizio nel 2015 con la distribuzione agli intermediari di un questionario di autovalutazione volto a identificare quelli maggiormente esposti da sottoporre eventualmente a verifiche più accurate *onsite* e *offsite*. Inoltre, sempre nel contesto europeo, l'Istituto partecipa alla redazione delle linee guida dell'EBA sulla sicurezza informatica per gli intermediari bancari e finanziari. A livello internazionale, nell'ambito del Senior Supervisory Group e del Comitato di Basilea per la vigilanza bancaria, collabora alla definizione delle migliori prassi sulla sicurezza cibernetica.

Nel 2017 è iniziata l'attività del *computer emergency response team* del settore finanziario italiano (CERTFin), iniziativa promossa dalla Banca d'Italia in stretta collaborazione con l'ABI per sostenere la condivisione di informazioni sulle minacce cibernetiche e di competenze sulle tecniche di risposta agli attacchi subiti dagli intermediari. L'esperienza del CERTFin è un esempio di successo di partenariato pubblico-privato, riportato anche nella *Relazione sulla politica dell'informazione per la sicurezza* a cura del DIS[36]. I maggiori attori del sistema finanziario nazionale (intermediari e infrastrutture di mercato) vi hanno aderito su base volontaria, così come numerosi soggetti di dimensione più ridotta. Nel 2017 il CERTFin ha analizzato e condiviso con i soggetti aderenti circa 1.000 segnalazioni su possibili attacchi, compromissioni e vulnerabilità tecnologiche, di cui oltre due terzi hanno riguardato minacce di aggressioni tra cui campagne di diffusione di malware e tentativi di frode.

Tenuto conto dell'importanza del comportamento prudente degli utenti dei servizi finanziari online per contrastare la minaccia cibernetica, la Banca è anche impegnata, mediante il programma di educazione finanziaria, a rafforzare la consapevolezza di giovani e adulti nell'utilizzo di servizi finanziari digitali.

La tavola 1 mette in evidenza come le attività di protezione del settore finanziario, incluse quelle cui partecipa direttamente la Banca d'Italia, si inseriscano nel più ampio contesto nazionale e internazionale.

---

[36] Presidenza del Consiglio dei ministri (2018), p. 10.

Tavola 1

ATTIVITÀ DI PROTEZIONE DEL SISTEMA FINANZIARIO NEL CONTESTO NAZIONALE E INTERNAZIONALE

Ambiti di intervento	Indirizzi di policy	Settore finanziario
INTERNAZIONALE: regole di comportamento nello spazio cibernetico; resilienza dei settori strategici; cooperazione	– Dichiarazioni dei leader G7/G20 – Rapporti del Group of Governmental Experts delle Nazioni Unite (fino al 2015)	– G7-CEG: principi non vincolanti di alto livello (Fundamental elements) – G20/FSB: censimento regolamentazione e prassi di vigilanza; Cyber lexicon – CPMI-Iosco: Cyber guidance – Ricognizioni IAIS e OCSE sul settore assicurativo
EUROPEO: sicurezza e accessibilità del cyberspazio per lo sviluppo dell'economia digitale europea	– EU Cybersecurity strategy (2013) – Proposta UE Cybersecurity Act (2017) – Direttiva NIS – Regolamento GDPR	– Infrastrutture di mercato: Eurosystem cyber resilience strategy – Prestatori di servizi di pagamento: direttiva PSD2; linee guida dell'EBA – Vigilanza SSM su banche significative; ispezioni mirate sul rischio cibernetico – Prescrizioni Solvency II per la continuità operativa delle imprese assicurative
NAZIONALE: protezione del "sistema Paese" dalla minaccia cibernetica	– DPCM 17 febbraio 2017 – D.lgs. 65/2018 – *Quadro strategico nazionale per la sicurezza dello spazio cibernetico*; *Piano nazionale per la protezione cibernetica e la sicurezza informatica*	– CERTBI; CERTFin (Banca d'Italia/ABI) – Regolamentazione/vigilanza Banca d'Italia/Ivass in ambiti di competenza nazionale, inclusa l'attuazione della NIS – Piano strategico della Banca d'Italia 2017-19

4.4 La sicurezza cibernetica del sistema economico nel suo complesso

La Banca d'Italia offre un contributo anche sotto il profilo della raccolta di dati statistici e della ricerca economica. In un'economia digitalizzata la sicurezza del cyberspazio rappresenta un fattore essenziale per lo sviluppo e la competitività di un paese. La letteratura di settore[37] mostra che il mercato non garantisce livelli ottimali di protezione per la presenza di esternalità e di asimmetrie informative. Sono quindi necessari interventi di policy, che a loro volta richiedono due elementi essenziali: dati credibili e un'adeguata comprensione teorica delle dinamiche microeconomiche del mercato della sicurezza informatica.

Esistono significative carenze da entrambi i punti di vista. La letteratura teorica, ancorché in rapida crescita, risulta ancora immatura; quella empirica sconta il fatto che i dati di alta qualità sulla frequenza e sul costo degli attacchi sono scarsi. La maggior parte delle statistiche citate dai media è prodotta da società commerciali che vendono sistemi difensivi; per quanto tali informazioni possano avere comunque un valore, soprattutto laddove segnalino l'emergere di nuove minacce, non sono pienamente affidabili perché viziate da un potenziale conflitto di interesse.

La Banca ha condotto, per la prima volta nel nostro paese, una rilevazione sull'incidenza e sull'impatto economico degli attacchi informatici al settore privato non

[37] Cfr. ad esempio R. Anderson (2001) e C. Biancotti et al. (2017).

finanziario[38]. I primi risultati, che riguardavano la frequenza e la distribuzione delle aggressioni per area, settore e classe dimensionale, sono stati pubblicati nel febbraio 2017; sei mesi dopo sono state diffuse stime sulla spesa sostenuta dalle imprese per la difesa da attacchi cibernetici, sui danni e sui costi legati a tali aggressioni[39]. Questi dati sono essenziali sia per guidare l'analisi economica sia per definire adeguati meccanismi di intervento pubblico (cfr. al riguardo anche il capitolo 16: *Il rischio cibernetico nell'economia italiana* nella *Relazione annuale* sul 2017).

[38] Dati analoghi di fonte ufficiale esistono, per il momento, solo per il Regno Unito. Sono stati raccolti con l'indagine *Cyber security breaches survey*, condotta per la prima volta nel 2016.

[39] C. Biancotti (2017a) e (2017b).

5. Il ruolo dell'Ivass

5.1 La sicurezza cibernetica dell'Ivass

I temi di sicurezza informatica e di rischio cibernetico sono rilevanti per l'Ivass (d'ora innanzi anche Istituto in questo capitolo) in termini di:

a) continuità e sicurezza delle funzioni e dei processi istituzionali (una dimensione che interessa anche la riservatezza dei flussi informativi);

b) sicurezza informatica delle aziende assicurative;

c) impatto dello sviluppo del settore delle polizze assicurative a copertura del rischio cibernetico sulla stabilità del sistema assicurativo.

Per quanto riguarda il punto a), l'operatività dell'Ivass fa riferimento in larga parte all'architettura, alle piattaforme, ai sistemi e ai servizi forniti dalla Banca d'Italia, sulla base delle linee di integrazione tecnologica tra le due istituzioni delineate nella legge istitutiva dell'Ivass e nell'Accordo quadro del 2014. Tali interventi hanno consentito, per le diverse attività sin qui realizzate, di far evolvere i requisiti di continuità e di sicurezza cibernetica (infrastrutture, procedure, servizi, posti di lavoro e dispositivi informatici personali) dell'Ivass in modo analogo a quanto avvenuto in Banca d'Italia.

Le questioni inerenti alla sicurezza informatica e al rischio cibernetico sono trattati nell'ambito del processo di valutazione dei rischi operativi (*Operational Risk Management*, ORM), che include la valutazione dei rischi in essere e delle possibili misure di gestione delle vulnerabilità. Le iniziative formative per gli addetti sono state rivolte a migliorare la conoscenza dei temi di sicurezza cibernetica, tra cui la governance e i processi di sicurezza.

5.2 La sicurezza cibernetica delle imprese assicurative

Sin dal 2014 l'Istituto monitora lo stato di esposizione al rischio cibernetico del comparto assicurativo, anche attraverso un questionario nell'ambito delle rilevazioni trimestrali delle vulnerabilità e dei rischi[40] delle imprese; ha inoltre svolto indagini sulla sicurezza di agenti e broker.

Sulla base della rilevazione condotta sugli intermediari assicurativi, nel 2017 l'Ivass ha inviato al mercato una lettera con l'indicazione di misure e raccomandazioni

---

[40] Le maggiori imprese assicurative indicano di aver avviato processi di mitigazione per la continuità di servizio (*business continuity*), di controllo e di gestione del rischio, proporzionati alla natura, dimensione e complessità operativa. Sono presenti processi di *business impact analysis* per identificare circostanze critiche da prevenire con più attenzione e gestire anche attraverso specifici *contingency plans*. I maggiori operatori riferiscono l'attivazione di programmi di prevenzione, monitoraggio e gestione del rischio cibernetico, supportati da una governance IT – che in alcuni casi prevede specifici comitati o funzioni quali il Chief Information Security Officer – e dall'applicazione di standard di sicurezza. La cooperazione nella gestione del rischio cibernetico prevede l'adesione a organizzazioni per la sicurezza informatica a vario livello (anche governativo) e lo scambio di informazioni con la Polizia postale e con associazioni di imprese (anche per ricostruire una serie storica delle perdite economiche dovute a rischi tecnologici).

per il rafforzamento della sicurezza informatica, preannunciando una nuova indagine nel 2019.

In linea con l'evoluzione regolamentare e del contesto operativo del settore assicurativo, l'Istituto è impegnato nella revisione della normativa di riferimento per imprese e intermediari. Nel luglio 2018 è stato emanato il nuovo regolamento sul governo societario delle imprese e dei gruppi assicurativi, che disciplina anche i presidi in materia di rischio cibernetico nell'ambito delle regole sulla governance aziendale.

In raccordo con l'EIOPA sono state avviate ulteriori iniziative per:

– rafforzare la resilienza del settore assicurativo, sia sul versante della continuità operativa sia su quello del rischio cibernetico, anche con iniziative informative[41];

– promuovere la realizzazione di attività di sistema da parte delle imprese assicurative anche mediante il partenariato pubblico-privato, da far confluire nelle iniziative già avviate per il settore bancario-finanziario.

5.3 L'impatto della diffusione delle polizze a copertura del rischio cibernetico sulla stabilità del settore assicurativo

L'Ivass ha avviato iniziative per monitorare l'esposizione al rischio cibernetico dell'industria assicurativa italiana e il mercato delle polizze a copertura di tale rischio; per queste ultime, alcune iniziative sono state svolte in collaborazione con la Banca d'Italia. Il monitoraggio sull'evoluzione del mercato avviene anche nell'ambito dell'attività dell'Ivass sui nuovi prodotti assicurativi.

Per quanto riguarda la diffusione delle polizze assicurative, il mercato italiano presenta andamenti in parte analoghi a quelli europei; la commercializzazione dei prodotti di copertura specializzati – su cui negli anni precedenti si riscontrava molta prudenza – mostra segnali di sviluppo, con un maggior numero di imprese attive, seppure con volumi ancora molto contenuti[42]. Secondo i dati pubblicati dall'ANIA nel 2017, la diffusione di coperture specifiche per le imprese italiane è molto limitata (5 per cento)[43]; i risultati delle rilevazioni condotte dalla Banca d'Italia sulle imprese industriali e dei servizi privati non finanziari mostrano le piccole dimensioni di questo mercato per le imprese. Una recente indagine condotta dall'Ivass, cui hanno partecipato cinque grandi

---

41 *InsurTECH: l'innovazione tecnologica nel mercato assicurativo* (2017).

42 I prodotti non solo includono la copertura del rischio cibernetico nell'ambito degli oneri connessi con azioni e con procedimenti civili e penali, ma prevedono anche la protezione dell'integrità del patrimonio per aspetti legati al furto di identità e alla responsabilità civile per i danni derivanti dalla violazione della normativa sulla privacy. Lo sviluppo del mercato risente comunque di alcuni limiti – riconducibili anche alla complessità di questo tipo di rischio e delle sue componenti di valutazione tecnica in continua evoluzione – sia dal lato dell'offerta (basso livello di penetrazione, difficoltà di un corretto *pricing* del rischio e mancanza di dati storici sul fenomeno, assenza di coperture riassicurative) sia dal lato della domanda (scarsa consapevolezza ed elevato moral hazard, difficoltà legate all'adeguamento della rete distributiva e delle competenze aziendali nonché delle infrastrutture di supporto).

43 Cfr. l'intervento di C. Savino, *Cyber risk, assicurazioni e PMI*, Milano, 7 marzo 2017.

gruppi assicurativi, conferma anche dal lato dell'offerta la limitata dimensione del mercato italiano delle polizze a copertura del rischio cibernetico[44].

Informazioni più aggiornate e dettagliate si potranno desumere dalle analisi in corso presso l'EIOPA sulle principali imprese assicurative europee (rassegna tematica sull'utilizzo dei big data nonché sulla diffusione e sui rischi dell'innovazione tecnologica).

[44] Sono state individuate tre tipologie di contratti, dedicati a: clientela retail (circa 2.000 contratti con importo assicurato medio pari a 300 euro, con un massimo di 150.000 euro); *small business* (circa 5.000 contratti con importo assicurato medio pari a 30.000 euro, con un massimo di 250.000 euro); *large corporate* (meno di 50 contratti con importo assicurato medio tra 3 e 20 milioni di euro, con un massimo di 50 milioni di euro).

Bibliografia

AgID (2017), *Piano triennale per l'informatica nella Pubblica amministrazione 2017-2019*.

Anderson, R. (2001), *Why information security is hard. An economic perspective*, in *17th Annual Computer Security Applications Conference*, atti del convegno tenutosi a New Orleans, LA, 10-14 dicembre 2001, Los Alamitos, CA, IEEE Computer Society, pp. 358-365.

BCE (2018), *Tiber-EU Framework. How to implement the European framework for Threat Intelligence-based Ethical Red Teaming*.

Biancotti, C. (2017a), *Cyber attacks: preliminary evidence from the Bank of Italy's business surveys*, Banca d'Italia, Questioni di economia e finanza, 373.

Biancotti, C. (2017b), *The price of cyber (in)security: evidence from the Italian private sector*, Banca d'Italia, Questioni di economia e finanza, 407.

Biancotti, C. e R. Cristadoro (2018), *The machine stops: the price of cyber (in)security*, in "VoxEU.org", 17 gennaio 2018.

Biancotti, C., R. Cristadoro, S. Di Giuliomaria, A. Fazio e G. Partipilo (2017), *Cyber attacks: an economic policy challenge*, in "VoxEU.org", 23 giugno 2017.

CSIS (2018), *Significant cyber incidents*.

Cœuré, B. (2017), *Introductory remarks*, intervento introduttivo tenuto in occasione dell'*High-level meeting on cyber resilience*, Francoforte sul Meno, 19 giugno 2017.

CPMI-Iosco (2016), *Guidance on cyber resilience for financial market infrastructures*.

CPSS-Iosco (2012), *Principles for financial market infrastructures*.

Department for Digital, Culture, Media & Sport [UK Government], Ipsos MORI e University of Portsmouth (2018), *Cyber security breaches survey 2018*.

Fazio, A. e A. Leotta (2015), *Attacchi informatici e* cyber-security, in *La continuità di servizio dei sistemi informatici. Il data centre incontra gli utenti*, atti del convegno tenutosi presso la Banca d'Italia, Roma, 22 aprile 2015, pp. 71-88.

Fazio, A. e F. Zuffranieri (2018), *Interbank payment system architecture from a cyber security perspective*, Banca d'Italia, Questioni di economia e finanza, 418.

G7-CEG (2016), *G7 fundamental elements of cybersecurity for the financial sector*.

G7-CEG (2017), *G7 fundamental elements for effective assessment of cybersecurity in the financial sector*.

IAIS (2016), *Issues paper on cyber risk to the insurance sector*.

InsurTECH: l'innovazione tecnologica nel mercato assicurativo (2017), atti del convegno organizzato dall'Ivass, Roma, 15 dicembre 2017.

Moore, T. e R. Anderson (2012), *Internet security*, in Peitz, M. and J. Waldfogel (a cura di), *The Oxford handbook of the digital economy*, Oxford, Oxford University Press, pp. 572-599.

OCSE (2017), *Enhancing the role of insurance in cyber risk management*.

Presidenza del Consiglio dei ministri (2013a), *Il linguaggio degli organismi informativi. Glossario intelligence*, in "Gnosis. Rivista italiana di intelligence", numero monografico.

Presidenza del Consiglio dei ministri (2013b), *Piano nazionale per la protezione cibernetica e la sicurezza informatica*.

Presidenza del Consiglio dei ministri (2013c), *Quadro strategico nazionale per la sicurezza dello spazio cibernetico*.

Presidenza del Consiglio dei ministri (2017), *Piano nazionale per la protezione cibernetica e la sicurezza informatica*.

Presidenza del Consiglio dei ministri (2018), *Relazione sulla politica dell'informazione per la sicurezza 2017*.

World Economic Forum (2014), *Risk and responsibility in a hyperconnected world*.

Gli accessi alle pubblicazioni online sono stati verificati al 30 agosto 2018.