BANCA D'ITALIA
EUROSISTEMA

Mercati, infrastrutture, sistemi di pagamento

(Markets, Infrastructures, Payment Systems)

Cyber resilience per la continuità di servizio del sistema finanziario

di Boris Giannetto e Antonino Fazio

Marzo 2022

Numero 18

BANCA D'ITALIA
EUROSISTEMA

Mercati, infrastrutture, sistemi di pagamento
(Markets, Infrastructures, Payment Systems)

Questioni istituzionali
(Institutional Issues)

Cyber resilience per la continuità di servizio del sistema finanziario

di Boris Giannetto e Antonino Fazio

Numero 18 – Marzo 2022

I lavori pubblicati nella collana "Mercati, infrastrutture, sistemi di pagamento" presentano documentazioni e studi su aspetti rilevanti per i compiti istituzionali della Banca d'Italia in tema di monitoraggio dei mercati finanziari e del sistema dei pagamenti, nonché di sviluppo e gestione delle relative infrastrutture. L'intento è quello di contribuire alla diffusione della conoscenza su questi argomenti e di favorire il dibattito tra le istituzioni, gli operatori economici, i cittadini.

I lavori pubblicati riflettono le opinioni degli autori, senza impegnare la responsabilità dell'Istituto.

La serie è disponibile online sul sito www.bancaditalia.it.

Copie a stampa possono essere richieste alla casella della Biblioteca Paolo Baffi: richieste.pubblicazioni@bancaditalia.it.

ISSN 2724-6418 (online)
ISSN 2724-640X (stampa)

Banca d'Italia
Via Nazionale, 91 - 00184 Roma - Italia
+39 06 47921

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

Cyber resilience per la continuità di servizio del sistema finanziario

di Boris Giannetto e Antonino Fazio*

JEL: F50, G38, K24, L50, O33.
Parole chiave: *cyber resilience*, analisi sistemiche di scenario, continuità di servizio, sistema finanziario, *cybersecurity*.

CONTENTS

* Banca d'Italia, Dipartimento Mercati e sistemi di pagamento.

SINTESI[1]

Il lavoro presenta le principali iniziative e misure in materia di *cyber resilience* volte a garantire la continuità di servizio del sistema finanziario.

Le minacce da fronteggiare sono sempre più variegate e ibride[2]: esse includono eventi *cyber*[3] e naturali, incendi, emergenze sanitarie, tensioni geopolitiche, attentati e altri fenomeni.

Nel comparto finanziario la necessità di intervenire tempestivamente per prevenire e contenere minacce di natura *cyber* è elevata, date le interconnessioni che lo caratterizzano: un evento su una singola infrastruttura, se non prontamente affrontato, può rapidamente propagarsi all'intero sistema, con impatti da reazione a catena. La diffusione di tecnologie digitali ha ampliato peraltro la superficie dei sistemi esposti a eventi *cyber*.

In questo contesto, la *cyber resilience* diviene strumento centrale per prevenire e gestire eventi che possono intaccare la continuità di servizio del sistema finanziario.

Il presente lavoro dopo avere descritto i principali elementi di contesto (capitoli 1, 2 e 3), espone le maggiori iniziative istituzionali avviate a livello nazionale (capitolo 4) e internazionale (capitolo 5) per rafforzare la *cyber resilience* nel sistema finanziario, comprese misure *ad hoc* adottate nel tempo dalla Banca d'Italia. Vengono poi presentati profili a carattere evolutivo (capitoli 6 e 7), prima di passare alle conclusioni.

---

1 Le opinioni qui riportate sono degli autori e non impegnano in alcun modo la Banca d'Italia.

2 Per una definizione di minaccia ibrida, Commissione UE, *Defense Industry and Space*: "*Hybrid threat – state or non-state actors seek to exploit the vulnerabilities of the EU to their own advantage by using in a coordinated way a mixture of measures (i.e. diplomatic, military, economic, technological) while remaining below the threshold of formal warfare*".

3 Per evento *cyber* si intende: "*Any observable occurrence in an information system. Cyber events sometimes provide indication that a cyber incident is occurring*". – Fonte: *Cyber Lexicon* del *Financial Stability Board* (FSB).

1. Evoluzione del contesto

La digitalizzazione dell'economia e della società rappresenta un indubbio elemento di progresso. Di pari passo con la sua diffusione, aumentano tuttavia i rischi e le minacce di natura *cyber*[4].

Il confronto geopolitico fra Stati rende il sistema finanziario, in virtù della sua apertura ai servizi *on-line* e alla natura transnazionale del cyberspazio, particolarmente esposto agli attacchi *cyber*.

Nuovi rischi – oltre alle indubbie opportunità – derivano inoltre dall'impiego di tecnologie informatiche e sistemi di telecomunicazione sempre più evoluti (l'utilizzo di algoritmi di intelligenza artificiale ne è un esempio) in nuovi prodotti e servizi finanziari.

Le interrelazioni tra sistema finanziario, nuove tecnologie e sicurezza stanno diventando sempre più rilevanti; non fa eccezione *Fintech*, termine con il quale si fa riferimento a prodotti e servizi finanziari che prevedono l'impiego di avanzate tecnologie dell'informazione e della comunicazione (ICT – su *Fintech* e sicurezza cfr. WEF, 2020 e Banca d'Italia, 2022).

Da tempo si assiste a crescenti fenomeni di disintermediazione delle entità finanziarie tradizionali (ne è un esempio la *DeFi – decentralized finance*), derivanti dall'impiego di tecnologie basate su sistemi decentralizzati[5].

COSA SI INTENDE COL TERMINE FINTECH?

Con il termine inglese *FinTech* ci si riferisce alla *Financial Technology*, ossia all'offerta di strumenti ad alta intensità tecnologica che comportano innovazione nel mercato dei servizi finanziari. Tali strumenti possono riguardare servizi di finanziamento, di pagamento, di investimento e di consulenza. In tale ambito, le Autorità pubbliche sono chiamate a svolgere un'attenta analisi dei fenomeni in atto, per identificare tempestivamente iniziative e interventi che salvaguardino l'interesse pubblico, garantendo in tal modo un adeguato equilibrio tra opportunità e rischi del processo innovativo.

L'evoluzione continua del mercato ICT richiede lo sviluppo di nuovi modelli di sicurezza (Ciocca, 2020) e di nuovi approcci regolamentari (Perrazzelli, 2021). Gli interventi vanno definiti non solo a livello nazionale, ma secondo un approccio *cross-authority* e *cross-border*.

Gli sforzi finalizzati ad assicurare adeguati controlli e livelli di sicurezza nella catena di fornitura dei servizi finanziari digitali stanno ponendo sfide crescenti

---

4 Per le definizioni di rischio e minaccia *cyber* si fa riferimento al *Cyber Lexicon* FSB, rispettivamente: "*The combination of the probability of cyber incidents occurring and their impact.*" e "*A circumstance with the potential to exploit one or more vulnerabilities that adversely affects cyber security*".

5 Le Autorità finanziarie – comprese quelle europee – hanno a più riprese messo in guardia dai rischi (volatilità, complessità delle tecnologie sottostanti, incertezza regolamentare e legale) connessi con investimenti in cripto-attività. Nel contempo, esse intraprendono azioni volte a governare il cambiamento, cercando di avviare iniziative innovative in ambito istituzionale.

alle istituzioni e agli operatori finanziari: i presìdi di difesa vanno continuamente adeguati, per fare fronte alla veloce e costante trasformazione tecnologica.

In tale contesto, la sicurezza non è più un aspetto ancillare; essa diviene un aspetto centrale per le infrastrutture e i servizi; la salvaguardia della resilienza operativa digitale assume rilievo strategico (BCBS, 2020a, 2020b).

Anche la collaborazione tra le istituzioni finanziarie, il settore privato, l'accademia e gli organi di *intelligence* e *law enforcement* riveste importanza, nell'ottica del potenziamento della *cyber resilience* a livello sistemico. Per fare questo, occorre non soltanto una *workforce* nazionale adeguata, ma anche un rapporto solido e strategico delle istituzioni con i soggetti privati (Baldoni, 2021a, 2021b).

2. La minaccia *cyber* nel sistema finanziario

Nel descrivere i *trend* che caratterizzano la minaccia *cyber* nel sistema finanziario, occorre prestare attenzione (*i*) alla natura della minaccia, (*ii*) alle organizzazioni *target*, (*iii*) agli attori della minaccia, (*iv*) ai possibili fini alla base delle operazioni malevole, (*v*) al tipo di campagne e di attacchi, (*vi*) al confronto statuale e alle principali misure di rafforzamento della sovranità *cyber* a disposizione delle autorità pubbliche.

IL FENOMENO DELLA MINACCIA IBRIDA

Con "minaccia ibrida" si indica una situazione nella quale attori statuali o non statuali cercano di sfruttare a proprio vantaggio le vulnerabilità di un *target* (per esempio, una infrastruttura finanziaria), utilizzando in modo coordinato una combinazione di misure (ad esempio diplomatiche, militari, economiche, tecnologiche), pur rimanendo al di sotto della soglia della guerra formale. Il fenomeno prevede in sostanza la deliberata volontà da parte degli attori di colpire uno o più obiettivi impiegando diversi mezzi.

La minaccia *cyber* è sempre più interconnessa con altri fenomeni, quali eventi naturali, cambiamento climatico, instabilità politica ed economico-finanziaria, precarietà sociale, migrazioni, tensioni geopolitiche, attacchi terroristici, epidemie e pandemie (WEF, 2021, 2022)[6].

La minaccia è spesso ibrida per sua stessa natura (Sørensen e Nyemann, 2018). Il fenomeno dell'interconnessione delle minacce si accompagna alla deliberata volontà da parte degli attori di perseguire scopi plurimi, colpendo diversi obiettivi e impiegando mezzi variegati (Treverton *et al.*, 2018). Tra questi, gli attacchi *cyber* sono tra gli strumenti preferiti, poiché essi sono spesso difficili da

[6] Ciò è stato reso particolarmente evidente dalla recente congiuntura emergenziale sul fronte sanitario. La rilevazione di connessioni tra minaccia pandemica, *cyber* e organizzazioni finanziarie rientrava invero nella normale attività di *threat modeling*, già prima che insorgesse il fenomeno COVID/Sars-Cov-2 (Bodeau, Mccollum e Fox, 2018). Con riguardo ad analisi predittiva sul fenomeno pandemico (Coats, 2019).

rilevare e gli autori sono raramente perseguibili a livello transnazionale, per mancanza di prove certe e conclusive o per questioni di giurisdizione.

Benché la minaccia *cyber* sia per sua stessa natura trasversale, investendo pressoché ogni comparto, il settore finanziario è senz'altro obiettivo privilegiato degli attacchi. I *target* di azioni malevole nel comparto finanziario includono banche centrali, banche commerciali, fornitori di sistemi di pagamento, *money transfer*, società per lo scambio di cripto-valuta, altre organizzazioni finanziarie e utenti.

I principali attori della minaccia sono *hacker*, cyber-criminali, *hacktivisti* (*hacker* che agiscono per fini ideologici, politici, disobbedienza civile etc.), *cyber*-terroristi ed entità statuali (Maurer e Nelson, 2021). Gli attaccanti possono talvolta disporre di ingenti risorse e di capacità tecniche elevate, come nel caso degli APT (*advanced persistent threats*)[7].

Sempre più spesso le azioni malevole vengono attribuite (anche da parte di organi governativi) a specifiche unità *cyber* di agenzie di *intelligence*. Il fenomeno è da considerare con attenzione, per via delle avanzate dotazioni *cyber* e degli ampi poteri di ingaggio di queste unità.

Tuttavia, nell'attribuzione degli attacchi occorre esercitare estrema cautela, in un contesto in cui la disinformazione, l'anonimizzazione e l'offuscamento della fonte costituiscono fenomeni diffusi e spesso una delle componenti dell'attacco stesso[8]. Difficoltà di attribuzione possono ad esempio riscontrarsi in presenza di operazioni "*false flags*", condotte con l'intento di far incolpare di un attacco un altro attore (ad es. attraverso l'*infrastructure hijacking*[9]). Specularmente, il fenomeno del *name & shame* – con cui si accusa pubblicamente un attore della minaccia (ad esempio uno Stato) di un attacco *cyber* – può essere utilizzato anche per fini di depistaggio e deterrenza.

Quanto ai fini appunto, le azioni malevole cyber nel settore finanziario possono coprire l'intero asse patrimonio-compiti-reputazione: furto, frode, esfiltrazione

---

7 Secondo il *Cyber Lexicon* del FSB, un *APT* è: *"A threat actor that possesses sophisticated levels of expertise and significant resources which allow it to create opportunities to achieve its objectives by using multiple threat vectors."* L'*APT*: *"[…] pursues its objectives repeatedly over an extended period of time"*.

8 Quanto all'anonimizzazione, l'utilizzo di *virtual private networks* (VPNs) impedisce spesso di risalire la catena reale degli IP. Le tecniche di offuscamento rendono difficile il *reverse engineering* sugli artefatti; si pensi, tra l'altro, alla crittografia che mira al *fully undetectable malware* (FUD). Tecniche di steganografia (tecnica che mira a nascondere la comunicazione – o meglio l'esistenza stessa della comunicazione – tra due interlocutori; dal greco *στεγανός*, coperto e *γραφία*, scrittura) ed esfiltrazione avanzate – spesso prerogativa di *tiger teams* statuali – complicano il quadro. Super computer, computazione quantistica e crittografia post-quantistica possono cambiare alcuni scenari correnti.

9 In questo tipo di operazioni, un attaccante acquisisce il controllo, tramite un'azione *cyber* fraudolenta, degli strumenti utilizzati da un altro attore della minaccia (ad esempio la sua infrastruttura di *command-and-control* e i *software* usati per attacchi *cyber*), per mascherare la sua azione. La *false flag* si può tuttavia configurare anche come semplice imitazione delle tattiche, tecniche e procedure (TTPs), utilizzate da un altro attore.

o manipolazione di dati e informazioni[10], azioni dimostrative, spionaggio, azioni contro la reputazione e compromissione di infrastrutture.

A livello di sistema Paese, gli attacchi possono mirare a condurre azioni di disinformazione e *cyber espionage*[11] o addirittura ad alterare gli equilibri finanziari e geopolitici; i *cyber*-attacchi *nation state* e *state-sponsored* possono talvolta rientrare in più vaste campagne di *psychological operations* (PSYOP) e *information operations* (IO)[12].

Gli attacchi in ambito finanziario sono sempre più mirati allo sfruttamento di specifiche vulnerabilità e caratteristiche delle singole organizzazioni (ENISA, 2020a, 2020b) (vi è in questi casi una preventiva azione di profilazione e *social engineering*[13]). Tra i fenomeni in marcato aumento si possono menzionare: richieste di riscatto talvolta connesse con attacchi volti a rendere indisponibili i servizi o a compromettere le infrastrutture, frodi e furto (ad esempio presso ATM, *hacks* contro *exchanges* di cripto-valuta, *wallets*)[14], operazioni contro la catena di approvvigionamento, azioni contro l'immagine e il nome. In particolare, si assiste a un costante aumento di campagne *ransomware*, *data leaks*, *cryptojacking*, *DDoS* e *RDDoS*, *supply chain attacks*, disinformazione, oltre al *phishing* nelle sue varie declinazioni (EUROPOL, 2020, 2021; ENISA, 2021a, 2021b)[15].

Gli eventi *cyber* (attacchi, malfunzionamenti etc.) sono sempre più accompagnati da elevata velocità di propagazione di notizie (vere, parzialmente vere o false),

---

10 L'utilizzo del termine esfiltrazione è comune in questo ambito; esso deriva dalla locuzione inglese *data exfiltration*; in italiano viene talvolta reso anche con "estrusione di dati"; per semplificare, si può associare a un furto di dati. Sul fronte della possibile manipolazione di dati e informazioni, gli *adversarial machine learning attacks* – ossia tecniche volte a compromettere il corretto funzionamento di un sistema informatico che faccia uso di algoritmi di apprendimento automatico – possono avere effetti finanche più gravi rispetto all'esfiltrazione (gli impatti possono essere molto rilevanti per un'organizzazione finanziaria).

11 L'attività di raccolta attraverso l'utilizzo di strumenti informatici di informazioni segrete o sensibili per fini personali, economici, tecnologici o politici; i *target* possono essere persone fisiche, aziende, Istituzioni, Stati.

12 Anche il movente economico e il furto di denaro – contrariamente a quanto si potrebbe pensare – possono essere un *trigger* persino per alcune entità statuali. Le unità di *intelligence* degli Stati – al fine di massimizzare il risultato, minimizzando i costi – possono talvolta ricorrere a semplici ed economici mezzi reperibili *in the wild*, anche al fine di sviare circa la fonte dell'attacco. Tali unità sono ovviamente in grado di mettere in campo anche tecniche di *reconnaissance*, intrusione ed esfiltrazione avanzate, segrete e difficilmente rilevabili dai comuni sistemi in commercio, compresi quelli in uso nelle istituzioni e nelle organizzazioni finanziarie.

13 Per ingegneria sociale si intende (FSB, Cyber Lexicon): *"A general term for trying to deceive people into revealing information or performing certain actions"*.

14 In ambito *crypto*, i furti dai *wallets*, gli *hacks* verso *exchanges* e gli attacchi *ransomware* (con i relativi proventi illeciti) sono spesso associati a fenomeni riciclaggio di denaro (dal virtuale al fisico). Rileva anche il riciclaggio in senso opposto (dal fisico al virtuale), specie per fondi derivanti da attività di criminalità organizzata. In questo frangente rivestono importanza le misure di AML/CFT di livello nazionale e internazionale.

15 L'ENISA nel suo *Threat Landscape* 2021 offre una chiara definizione di *ransomware*, *cryptojacking* e *DDoS*, rispettivamente: *"Ransomware is a type of malicious attack where attackers encrypt an organisation's data and demand payment to restore access"; "Cryptojacking or hidden cryptomining is a type of cybercrime where a criminal secretly uses a victim's computing power to generate cryptocurrency"; "DDoS is one of the most critical threats to IT systems, targeting their availability by exhausting resources, causing decreases in performance, loss of data, and service outages"*.

vista anche l'incontrollabilità di fenomeni di viralità ed *echo chambers*[16] in rete (Giannetto e Paganini, 2020): questo aspetto è in grado di influenzare i mercati finanziari in modo particolarmente rapido. La gestione bilanciata e proporzionata delle notizie e dell'esposizione esterna può costituire un elemento centrale, tanto quanto la gestione resiliente degli eventi ai fini della continuità operativa.

Attacchi fisici e logici vanno sovente insieme; di qui la necessità del potenziamento di sistemi informatici in grado di interagire in modo continuo con il sistema fisico in cui opera (*cyber-physical systems*). Attacchi sempre più sofisticati e articolati sono accompagnati da attacchi semplici, che continuano a essere usati massivamente e diffusamente.

Ambienti tecnologici nuovi sono interessati da modalità e tipologie di attacco sia ordinarie (con relativi presìdi di *cybersecurity* classica), sia specifiche[17].

Quanto al confronto geopolitico tra Stati (con le conseguenti ripercussioni anche per il comparto finanziario), le operazioni *cyber* sono spesso sotto-soglia (*below-the-threshold*), ossia fatte con l'intento di non provocare una risposta o contro-offensiva da parte dell'attaccato. In questo caso, oltre al fine primario di non innescare una reazione, l'attore della minaccia riesce spesso anche a eludere la rilevazione di tali operazioni (in questo senso vi è anche un problema di *detection*)[18]. In un quadro di guerra ibrida, esse sono preferite a operazioni apertamente ostili, per via dei minori costi e rischi (Bilal, 2021). In altri casi, l'attacco di tipo statuale può essere volutamente sopra-soglia (*above-the-threshold*), in considerazione della difficoltà di perseguire e sanzionare a livello internazionale, nonché della possibilità di non risposta da parte del colpito e della comunità internazionale, che potrebbero non reagire per evitare reazioni a catena. In ambito *cyber*, a livello internazionale, vi sono tuttavia dibattiti aperti di natura tecnica, politica e giuridica sul concetto stesso di soglia e sulla sua precisa definizione (Schmitt, 2021).

In questo scenario, per far fronte alla minaccia *cyber*, gli Stati mettono in campo misure volte a rafforzare la loro autonomia strategica, l'indipendenza e la supremazia tecnologica, nonché la cosiddetta "*cyber sovereignty*": le misure adottate variano da paese a paese e comprendono aspetti geopolitici, giuridici, economici, finanziari e tecnologici. Tra queste misure, vi sono ad esempio: azioni di *public policy* in consessi multilaterali su *Internet governance*

---

16 La locuzione indica una situazione in cui le informazioni vengono amplificate attraverso una continua ripetizione all'interno di un sistema definito, con tendenza a escludere e censurare idee concorrenti e diverse. Il fenomeno è spesso legato a episodi di disinformazione.

17 Ad esempio, in tema di attacchi specifici per ambienti DLT e *blockchain*, si pensi ai *consensus attacks ("consensus",* insieme di regole di convalida che forniscono a partecipanti indipendenti la capacità di verificare la validità e l'integrità delle registrazioni delle transazioni su un libro mastro). Alcuni esempi ne sono il "*51% attack*" con controllo della maggioranza dei validatori su reti *permissionless* pubbliche o il "*regulator's exploitation attack*" su reti *permissioned* private. I meccanismi di manipolazione del *consensus* possono portare a trasferimenti non autorizzati di risorse digitali, censura non autorizzata delle transazioni, doppia spesa o interruzione operativa della convalida della transazione. Gli attacchi contro gli algoritmi che governano il *consensus* possono agire su diversi *entry points* come reti, nodi, utenti e codice.

18 La capacità di rilevazione (*detection*) delle attività malevole è sicuramente un fronte da potenziare, lungo tutto l'arco che va dalla *reconnaissance* all'*exfiltration*, secondo la nota matrice MITRE ATT&CK (*https://attack.mitre.org*); si veda anche *https://d3fend.mitre.org/* (*https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/2665993/nsa-funds-development-release-of-d3fend/*).

e *cyber operations*; emanazione di disposizioni nazionali in materia di sicurezza nazionale (ivi compresi obblighi specifici per le aziende private di condividere informazioni con l'*intelligence*); *golden power*; limitazioni all'utilizzo di piattaforme di *file sharing* e *social networks*; approntamento di *DNS* (*domain name system*), *servers*, reti Internet e *cloud* nazionali; controllo su cavi sottomarini e transoceanici; produzione autonoma di componenti e infrastrutture tecnologiche; verifica su *supply chain* e infrastrutture tramite centri di valutazione e certificazione nazionali; predisposizione di *standard* tecnici in tema *cyber*; operazioni *cyber* difensive e offensive; attività di censura su Internet, oscuramento di siti *web*, blocco di *VPN*, *geoblocking* (blocco geografico, ovvero limitazione dell'accesso ai contenuti Internet in base alla posizione geografica dell'utente) (Giannetto, 2019, 2021).

A fronte di un contesto di minaccia *cyber* sempre più mutevole e complessa, organismi governativi, deputati alla prevenzione e alla gestione della sicurezza nel cyberspazio, potenziano modelli adattativi ed evolutivi in accordo a un approccio *zero trust*, partendo dal presupposto che un attore della minaccia può avere già penetrato il perimetro dell'organizzazione (NSA, 2021a, 2021b)[19].

Viene ritenuto cruciale pertanto monitorare su base costante tutto il perimetro, adottando schemi di autenticazione forte a più fattori (*multi-factor authentication* – MFA) (ENISA, 2022). Ciononostante, pur mettendo in campo le migliori strategie di prevenzione e difesa, è evidente che il rischio sistemico non potrà mai essere annullato (Baldoni, 2021b).

La difficoltà per singoli operatori, organizzazioni e istituzioni, di dotarsi di difese *cyber* adeguate o quantomeno al livello di uno Stato estero, impone che essi operino in stretta cooperazione con gli organi di *intelligence/law enforcement* nazionali, in particolare in una fase storica che vede la costituzione o il rafforzamento a livello statuale di speciali unità interforze dedite a diversificate attività nel cyberspazio.

3. *Cyber resilience* e sistema finanziario

Il termine "resilienza", mutuato dalla scienza dei materiali e dalla psicologia, è ormai impiegato diffusamente in vari campi. In sintesi, indica la capacità di reagire, adattarsi ed evolvere a fronte di eventi di varia natura, noti e non noti. A questo si aggiunge la capacità di prevenire tali eventi avversi e, più in generale, le situazioni di crisi.

Secondo una definizione consolidata in ambito BCE, la locuzione *cyber resilience*[20] ha diretta correlazione con il fenomeno degli attacchi *cyber*: *"Cyber resilience refers to the ability to protect electronic data and systems from*

---

19 Dati, persone, dispositivi, reti, infrastrutture non dovrebbero mai essere considerati sicuri; una verifica è sempre opportuna. La minaccia non è più solamente esterna (al netto di *insider threats*, talpe, malfunzionamenti ed errori umani).

20 In Italia, è invalso da anni anche l'aggettivo "cibernetico"; si veda ora l'impiego in ambito istituzionale del termine "cybersicurezza" (di derivazione anglo-italiana, per evitare l'utilizzo di "cibernetica", che in effetti indica altra branca). Per analogia potrebbe essere introdotto in ambito nazionale il neologismo "cyber-resilienza".

cyberattacks, as well as to resume business operations quickly in case of a successful attack"[21].

IL CONCETTO DI CYBER RESILIENCE

Dello stesso tenore, è una definizione data dal *Cyber Lexicon* del *Financial Stability Board* (FSB): *"The ability of an organisation to continue to carry out its mission by anticipating and adapting to cyber threats and other relevant changes in the environment and by withstanding, containing and rapidly recovering from cyber incidents"*[22].

La *cyber resilience* è la capacità di un'organizzazione di continuare a svolgere la propria attività anche a fronte di eventi avversi sia di tipo *cyber* sia di altra natura (approccio adattativo), con un rapido ritorno a livelli normali di operatività.

Il sistema finanziario si contraddistingue per la complessità delle interdipendenze tra gli elementi che lo compongono; ne consegue che piccoli eventi e minime perturbazioni di tipo *cyber*, anche solo a carattere locale, hanno la capacità di provocare ricadute di grande portata a livello sistemico, a volte con dinamiche di tipo caotico (Visco, 2013).

Nel concreto, il sistema in questione è essenzialmente costituito da istituzioni, mercati e infrastrutture (finanziarie e tecnologiche). Vi operano un insieme articolato e interconnesso di attori e di elementi: datori di fondi e prenditori di fondi (ad es. famiglie e imprese); intermediari finanziari (ad es. banche, assicurazioni, società di gestione del risparmio, società di intermediazione mobiliare, etc.); mercati (monetario, finanziario, cambi, etc.); infrastrutture, piattaforme e sistemi di pagamento; prodotti e servizi scambiati sui mercati; Autorità di vigilanza, supervisione e sorveglianza (ad es. Banca d'Italia, IVASS, CONSOB, COVIP, AGCM – cfr. Banca d'Italia, 2019).

Le numerose e profonde interconnessioni fisiche e logiche tra le diverse componenti del sistema finanziario travalicano i confini nazionali, estendendosi a una dimensione globale e dando luogo a una fitta rete di interdipendenze sia operative che economico-finanziarie. La crescente digitalizzazione amplifica tali relazioni[23]. Un attacco *cyber* su larga scala contro punti nodali del sistema finanziario può pertanto innescare una crisi sistemica a livello globale (Zhang,

---

21 BCE, 2018b.

22 Si veda FSB, 2018. Sul tema generale, si veda anche WEF, 2018.

23 Una spinta ulteriore al processo di digitalizzazione diffusa è stata data dai piani europei e nazionali volti a promuovere la ripresa economica e la resilienza a fronte dell'emergenza pandemica (Consiglio Europeo, 2020 e Signorini, 2021).

2020). Uno degli aspetti da rafforzare è l'*information sharing*[24], per promuovere una pronta e completa condivisione delle informazioni da parte degli operatori impattati.

Al fine di predisporre difese efficaci, è ovviamente essenziale che le entità finanziarie – e in particolare gli operatori di rilevanza sistemica e i gestori di infrastrutture centrali – sviluppino una adeguata conoscenza circa la capacità degli attaccanti di aggirare i presìdi di sicurezza e di difesa, adottando anche misure proattive (Fazio e Zuffranieri, 2018).

Un ulteriore aspetto da sottolineare è il carattere *time critical* del sistema finanziario: le transazioni devono concludersi il più rapidamente possibile, e comunque entro un tempo massimo predeterminato. Ciò assicura da un lato la definitività di un'operazione finanziaria (ad es. una disposizione di pagamento) e in ultima analisi la certezza e la fiducia degli operatori; al contempo, ne discende una debolezza intrinseca legata alla rapidità con cui un evento anomalo o fraudolento può contagiare l'intero sistema.

ATTORI ED ELEMENTI DEL SISTEMA FINANZIARIO

Il sistema finanziario è costituito da istituzioni, mercati e infrastrutture (finanziarie e tecnologiche). I principali attori ed elementi che lo costituiscono sono: datori di fondi e prenditori di fondi (ad es.: famiglie e imprese); intermediari finanziari (ad es.: banche, assicurazioni, società di gestione del risparmio, società di intermediazione mobiliare, etc.); mercati (monetario, finanziario, cambi, ecc.); infrastrutture, piattaforme e sistemi di pagamento; prodotti e servizi scambiati sui mercati; Autorità di vigilanza, supervisione e sorveglianza (ad es.: Banca d'Italia, IVASS, CONSOB, COVIP, AGCM).

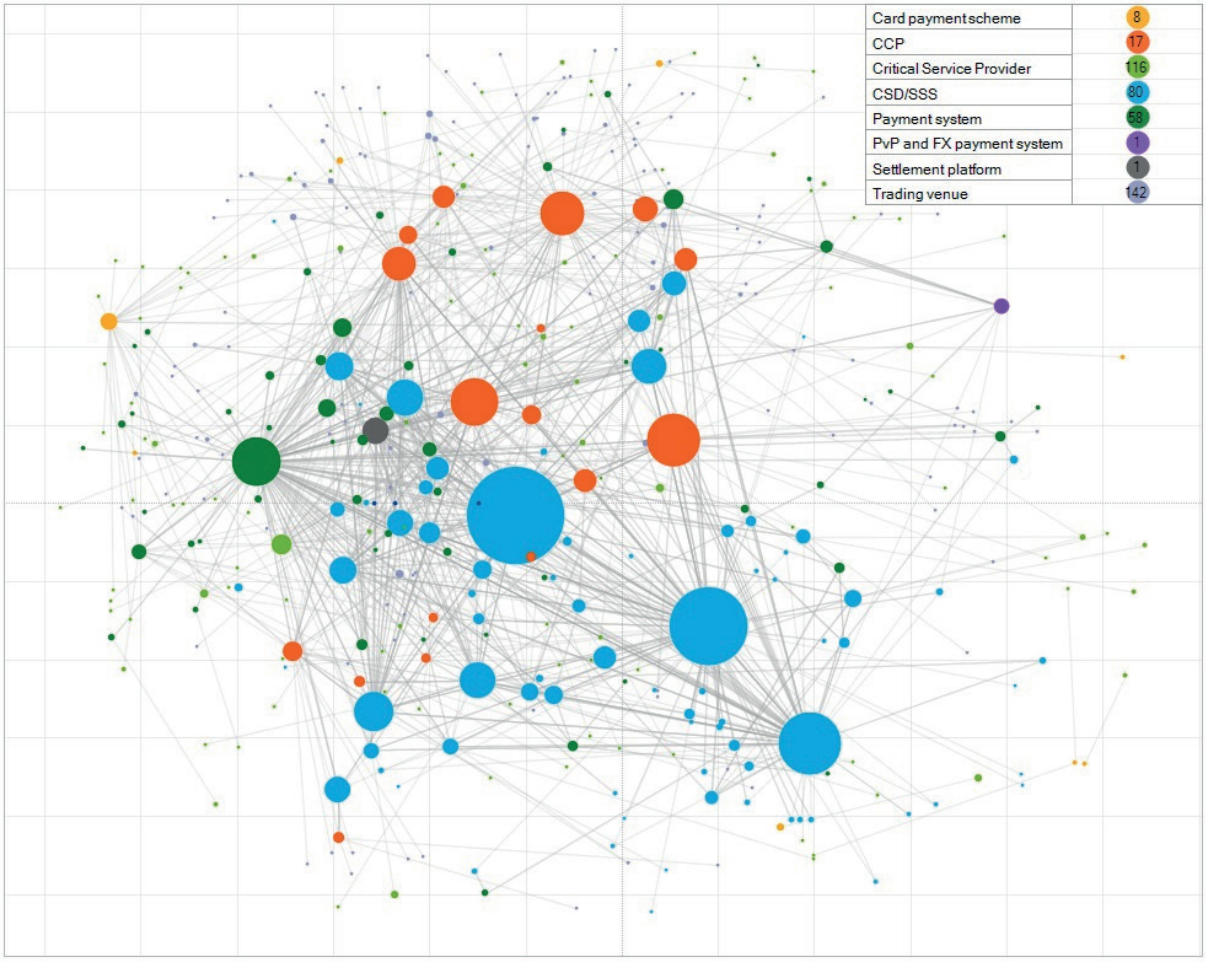
La figura 1 (il cui grafo aggiornato su base costante è utilizzato anche a fini di monitoraggio dinamico) mostra, per l'ambito europeo, la stretta interconnessione tra diversi attori del sistema finanziario (la grandezza dei nodi indica il loro peso in funzione di diversi parametri; la distribuzione dei nodi nello spazio del grafo e il loro colore seguono un criterio di raggruppamento per tipologia di attori).

In virtù della forte e crescente interconnessione fisica e logica tra diversi sistemi e piattaforme, il comparto finanziario presenta una potenziale superficie di attacco molto estesa, con innumerevoli punti critici di accesso, quali istituti di credito di rilevanza internazionale, infrastrutture di mercato per la negoziazione e il regolamento di strumenti finanziari (ad es. controparti centrali), sistemi di pagamento all'ingrosso di rilevanza sistemica (cd. SIPS), fornitori globali di servizi tecnologici e di rete (ad es. rete SWIFT).

[24] Per il concetto di *information sharing*, si veda il *Cyber Lexicon* FSB: "*An exchange of data, information and/or knowledge that can be used to manage risks or respond to events*". Nel presente lavoro si fa riferimento, quindi, alla condivisione di informazioni di tenore generale e livello istituzionale, con particolare riguardo agli impatti, non soltanto all'*information sharing* di tipo tecnico e *peer-to-peer* tra CERT, basato sullo scambio di indicatori di compromissione, artefatti e vulnerabilità. Sul tema, in ambito istituzionale, basti citare fruttuose esperienze cooperative e di settore quali CIISI-EU e CERTFin, che vedono coinvolte diverse tipologie di attori (si veda oltre, nel presente lavoro).

Figura 1 - Principali interdipendenze nel sistema finanziario europeo, 2021

grafo basato su dati reali (nodi e link anonimizzati)



Fonte: *Market Infrastructure and PAyments Committee* (MIPC) – *European Central Bank*.

Una specifica funzione esercitata dall'Autorità impegnata ad assicurare la continuità di servizio[25] del sistema finanziario è il potere di sorveglianza sul sistema dei pagamenti che, unitamente ai poteri di supervisione sulle infrastrutture finanziarie e al potere di vigilanza bancaria e finanziaria, mira a garantire la *business continuity* in ambito finanziario. Il potere di sorveglianza sul sistema dei pagamenti da parte della Banca d'Italia trova fondamento nell'articolo 146 del Testo Unico Bancario (TUB), il cui comma 1 recita: *"La Banca d'Italia esercita la sorveglianza sul sistema dei pagamenti avendo riguardo al suo regolare funzionamento, alla sua affidabilità ed efficienza nonché alla tutela degli utenti di servizi di pagamento".*

25 Per quanto concerne la locuzione "continuità di servizio", qui viene intesa in un'accezione estesa, come capacità delle istituzioni, delle organizzazioni e dei fornitori di servizi tecnologici critici del sistema finanziario nel suo complesso di erogare regolarmente prodotti o servizi, anche a fronte di eventi avversi. Questa definizione include anche l'approntamento preventivo di istruzioni o procedure, che descrivono come saranno sostenuti i processi di un'organizzazione durante e dopo un'interruzione significativa. Su questo ultimo punto, si veda: *https://csrc.nist.gov/glossary/term/business_continuity_plan*. Su continuità del sistema finanziario, si veda anche Bank of England, 2021.

Tale disposizione va letta in combinato disposto con la previsione contenuta nell'art. 127 comma 2 del Trattato sul Funzionamento dell'Unione Europea (TFUE), laddove si statuisce, tra l'altro, che tra i compiti fondamentali da assolvere tramite il Sistema Europeo di Banche Centrali (SEBC) vi è quello di *"promuovere il regolare funzionamento dei sistemi di pagamento"*.

La Banca d'Italia assolve a tali compiti nei confronti dei soggetti che: emettono, gestiscono o prestano strumenti di pagamento; gestiscono sistemi di scambio, di compensazione e di regolamento; gestiscono infrastrutture tecnologiche. Essa – di concerto con la CONSOB – vigila inoltre sui sistemi di regolamento dei titoli e su infrastrutture che agevolano gli scambi in attività finanziarie, quali il depositario centrale Monte Titoli S.p.A. e la controparte centrale Cassa di Compensazione e Garanzia S.p.A. (CCG). La Banca d'Italia esercita altresì la supervisione sull'efficienza e sull'ordinato funzionamento del mercato all'ingrosso dei titoli di Stato (MTS). I poteri di sorveglianza, vigilanza e supervisione sui mercati e sulle infrastrutture a supporto delle negoziazioni sono ripartiti tra la Banca d'Italia e la CONSOB[26].

Le attività di sorveglianza e di vigilanza nell'ambito del sistema dei pagamenti comprendono quelle sui sistemi di scambio e regolamento al dettaglio nazionali ed europei (come BI-Comp e STEP2-T), quelli all'ingrosso (come TARGET2 o il sistema privato europeo Euro1) e, a livello internazionale, il sistema di regolamento per i pagamenti multi-valutari interbancari (CLS). L'attività di sorveglianza è stata inoltre estesa alle piattaforme europee di regolamento dei pagamenti istantanei, di più recente realizzazione (RT1 e *Target Instant Payment Settlement*, TIPS).

La Banca d'Italia è interessata anche al buon funzionamento dei circuiti di pagamento utilizzati dalla clientela finale, come quelli su cui operano le carte di debito e di credito e le varie forme di pagamento digitale. Sono soggetti a controllo anche fornitori di servizi strumentali tecnologici o di rete rilevanti per il sistema dei pagamenti, che espletano attività sul mercato nazionale o a livello transnazionale. Tra questi ultimi, ad esempio, rileva l'infrastruttura SWIFT, soggetta come il sistema CLS a un regime di sorveglianza cooperativa da parte dei paesi del G10, inclusa l'Italia.

L'obiettivo delle misure descritte nel seguito di questo lavoro comprende la resilienza dell'intero complesso delle infrastrutture e istituzioni finanziarie sopra descritte, nonché quella dei fornitori di servizi tecnologici critici, in quanto la continuità operativa di questi ultimi è considerata condizione essenziale per la salvaguardia della stabilità del sistema finanziario.

[26] Secondo un criterio di vigilanza per finalità, la CONSOB è responsabile della trasparenza e della tutela degli investitori, la Banca d'Italia della stabilità e del contenimento dei rischi di sistema.

4. Iniziative istituzionali a livello nazionale

Nel corso degli anni la Banca d'Italia ha avviato diverse attività volte a promuovere l'innovazione e la resilienza del settore finanziario italiano[27]. Le azioni intraprese, nel solco delle linee strategiche concordate nell'Eurosistema, hanno comportato una costante interazione con le altre Autorità nazionali di settore (in particolare, CONSOB, IVASS e MEF) e con altre strutture governative.

Tra le misure specifiche volte a raggiungere la *cyber resilience*, la Banca d'Italia ha promosso interventi volti: all'innalzamento della resilienza di ogni singola entità finanziaria, all'efficace cooperazione transnazionale nello spazio finanziario europeo, alla pronta condivisione delle informazioni in ambito pubblico e privato, al potenziamento della capacità di analisi e reazione verso eventi *cyber* e di altra natura, alla definizione di adeguate *partnership* pubblico-privato e cooperazione intra-settoriale, all'idoneo scambio di *know how* inter-settoriale, allo sviluppo di un efficiente contesto regolamentare, all'accrescimento della consapevolezza dei rischi *cyber*. Alcune di queste misure sono già consolidate, altre sono in fase di sviluppo, altre ancora hanno un carattere evolutivo, stante il necessario e costante adattamento a uno scenario della minaccia mutevole e complesso.

Fin dall'emanazione del DPCM 17 febbraio 2017 (cd. Decreto Gentiloni) e del Piano nazionale per la protezione cibernetica e la sicurezza informatica nazionali del marzo 2017[28], la Banca d'Italia, quale Autorità di sorveglianza sui sistemi di pagamento e sulle infrastrutture di mercato, ha progressivamente consolidato la sua attività in materia di *cybersecurity* e di *cyber resilience*.

L'Istituto negli ultimi anni ha presidiato, con diversi livelli di coinvolgimento, varie iniziative e provvedimenti che hanno interessato specificatamente l'ambito *cyber*.

Già nel 2017 il settore delle infrastrutture finanziarie era stato incluso nel perimetro degli interessi essenziali (strategici) del nostro Paese, ai fini dell'esercizio di poteri speciali in base al c.d. *golden power*[29]; le misure in merito sono state aggiornate e integrate con il decreto-legge n. 23 dell'8 aprile 2020.

Sempre in materia di protezione degli *asset* strategici e in connessione col tema del *golden power*, sono attualmente in fase di implementazione e sperimentazione le misure previste nel complesso normativo-regolamentare sul Perimetro di Sicurezza

---

27 Specifiche previsioni erano contenute anche nel Piano Strategico 2017-2019, che includeva i due piani d'azione seguenti: 1.3 Promuovere l'innovazione e la resilienza del settore finanziario italiano – anche accrescendo la sicurezza e la continuità di servizio del settore finanziario italiano attraverso l'attuazione di una strategia di *cyber resilience* per le infrastrutture di mercato italiane; 4.4 Rafforzare la *cybersecurity* della Banca in relazione a nuovi scenari di rischio – anche attraverso la costituzione e lo sviluppo del *Computer Emergency Response Team*, CERTBI.

28 Il decreto ha, tra l'altro, istituito il Nucleo di Sicurezza Cibernetica (NSC); il Piano ha disegnato l'architettura nazionale *cyber*.

29 Segnatamente, giusta l'articolo 14 del decreto-legge 16 ottobre 2017, n. 148 (convertito dalla legge 4 dicembre 2017, n. 172, recante Disposizioni urgenti in materia finanziaria e per esigenze indifferibili) che ha inserito il comma 1-ter all'art. 2 del decreto-legge 15 marzo 2012, n. 21, recante disciplina sul *golden power*, convertito, con modificazioni, dalla legge 11 maggio 2012, n. 56.

Nazionale Cibernetica (legge 133 del 2019 che ha convertito il D.L. n. 105 del 2019) e successive disposizioni collegate (decreti attuativi).

Il Decreto Legislativo 18 maggio 2018, n. 65 ha recepito la Direttiva NIS 2016/1148 (*Network and Information Security Directive*), che prevede una serie di misure mirate a creare un livello comune di sicurezza delle reti e dei sistemi informativi all'interno dell'Unione Europea. A livello europeo, sono tuttora in corso lavori per rendere più armoniche – pur con margini di tolleranza relativamente ampi – le implementazioni nazionali della Direttiva NIS, in linea con alcuni principi delineati nelle proposte della NIS 2[30].

Anche la creazione del Centro di competenza europeo per lo sviluppo industriale, tecnologico e della ricerca in materia di *cybersecurity* ha avuto ricadute sul piano nazionale, per via dei collegamenti con la rete dei Centri nazionali di coordinamento (DIS, 2021a, 2021b).

A livello nazionale, un ruolo centrale in tema di *cyber resilience* è ora svolto dall'Agenzia per la Cybersicurezza Nazionale (ACN)[31], dipendente dalla Presidenza del Consiglio dei Ministri. All'ACN spetta la direzione e la responsabilità generale delle politiche in tema di cybersicurezza e *cyber resilience*. Nell'Agenzia è confluito anche lo CSIRT Italia (*Computer Security Incident Response Team*), precedentemente incardinato nel DIS.

A livello di strategia nazionale in ambito *cyber* sono degni di nota anche l'"*Italian Position Paper on International Law and Cyberspace*" e la "Strategia Cloud Italia" entrambi del 2021[32].

Sui temi della continuità operativa e delle infrastrutture critiche, in ambito nazionale è stata anche adottata una specifica disposizione (art. 211 bis del D.L. 19.05.2020, n. 34) concernente l'adozione e l'aggiornamento di piani di sicurezza, con specifiche misure atte a garantire una migliore gestione di crisi derivanti da emergenze sanitarie.

Sempre in ambito nazionale, a livello di iniziative specifiche nelle quali è coinvolta la Banca d'Italia, è stato costituito nel 2003 il Comitato per la continuità di servizio della piazza finanziaria italiana (Codise), presieduto dalla Banca d'Italia. Vi partecipano la CONSOB, operatori del settore finanziario rilevanti sul piano sistemico (principali banche, operatori del sistema dei pagamenti e infrastrutture di mercato) e altre Autorità. L'attività di *information sharing* è uno dei punti fondamentali nella prevenzione e nella gestione di tali crisi.

Nel concreto, il Codise si occupa dello scambio tempestivo di informazioni e del coordinamento delle misure necessarie in caso di eventi che possono mettere a rischio la continuità di servizio degli operatori finanziari critici

---

30 Altri filoni di intervento avviati dalla Commissione europea e aventi ricadute in ambito nazionale (tra i quali la proposta di Direttiva sulla resilienza delle *critical entities* del 16 dicembre 2020 – cfr. Commissione Europea, 2020d e 2020e – e il pacchetto regolamentare del settembre 2020 – cfr. Commissione Europea, 2020b e 2020c) verranno affrontati nel capitolo successivo.

31 Istituita con DECRETO-LEGGE 14 giugno 2021, n. 82; Legge 109/2021.

32 I documenti sono consultabili rispettivamente ai seguenti *link*: *https://www.esteri.it/mae/resource/doc/2021/11/italian_position_paper_on_international_law_and_cyberspace.pdf*; *https://cloud.italia.it/strategia-cloud-pa/*.

e il regolare funzionamento dei servizi finanziari essenziali. Il Comitato, tramite un rappresentante della Banca d'Italia, partecipa inoltre al Comitato operativo della Protezione Civile e interagisce con la Commissione tecnica interministeriale di Difesa Civile, coordinata dal Ministero degli Interni.

Il Codise si raccorda altresì con il CERTFin (*Computer Emergency Response Team Finanziario Italiano*), iniziativa cooperativa pubblico-privato istituita nel 2017 in collaborazione con l'ABI, cui partecipano, su base volontaria, gli operatori del settore bancario e finanziario nazionale[33]. Tale raccordo permette di attivare procedure condivise in occasione di eventi *cyber* e crisi, segnalati dal singolo operatore, dalla Banca d'Italia o dal CERTFin. Il Codise svolge periodiche esercitazioni per verificare l'adeguatezza delle procedure in caso di emergenza, attraverso il collaudo dei sistemi interni per la gestione della continuità operativa.

Oltre alla dimensione nazionale, il Comitato costituisce un punto di contatto con il SEBC, in caso di crisi a livello europeo. Sempre in ambito *cyber*, il Comitato è attivo nell'organizzazione e nello svolgimento di esercitazioni anche in ambito internazionale (ad es. G7), che prevedono la simulazione di attacchi *cyber*, sia in scenari *table-top*, con simulazione di situazioni di emergenza, basata su discussione di possibili eventi (*discussion-based*) o con simulazione di operazioni in scenari verosimili (*operation-based*)[34]. A tale riguardo, è degno di menzione il Protocollo di intesa CIRP (*Cyber Incident Response Protocol*) siglato in ambito G7: tale accordo coinvolge le Autorità finanziarie del G7 per la gestione di incidenti *cyber cross-border* nel settore finanziario. Il Protocollo prevede una serie di procedure e interventi da mettere in campo in caso di necessità; in tale evenienza, il Codise costituisce la sede nazionale per il coordinamento delle crisi operative a livello G7.

Il Codise cura infine analisi e ricerche su tematiche di continuità di servizio del sistema finanziario, inclusi gli aspetti di *cyber resilience*, attraverso la promozione di eventi e pubblicazioni.

Il citato CERTFin, la cui Presidenza è condivisa tra la Banca d'Italia e l'ABI (Associazione Bancaria Italiana)[35], mira a innalzare la capacità di risposta alla minaccia *cyber* degli operatori finanziari e la *cyber resilience* del sistema finanziario nazionale nel suo insieme.

Le attività svolte dal CERTFin hanno carattere sia operativo sia strategico: vanno dalla prevenzione delle crisi *cyber*, alla risposta agli attacchi informatici e agli incidenti di sicurezza.

---

33 *Provider* di servizi di pagamento, intermediari bancari e finanziari, imprese di assicurazione, gestori di infrastrutture di mercato. Possono partecipare ai lavori del CERTFin anche altre Autorità e associazioni di categoria del settore finanziario, sulla base di accordi *ad hoc*.

34 Cfr. *G-7 fundamental elements of cyber exercise programmes* – Ottobre 2020.

35 Il CERTFin ha il suo fulcro nel Comitato Strategico, che ha il compito di definire linee di indirizzo e sviluppo. Nel Comitato Strategico, oltre alla Banca d'Italia e all'ABI, sono presenti l'IVASS e l'ANIA per il settore assicurativo e la CONSOB per il settore finanziario. Tra gli organi vi sono anche la Direzione Operativa e un *Team* Virtuale, coinvolto perlopiù in attività tecnico-tattiche.

Tra gli obiettivi del CERTFin vi sono, ad esempio, la costituzione di un punto unico di contatto per la segnalazione e la gestione di eventi *cyber* nel settore finanziario; la promozione della cooperazione pubblico-privato e intersettoriale; lo scambio di informazioni su eventi *cyber*; la realizzazione di campagne di *awareness*.

In tema di collaborazione inter-istituzionale sulle questioni attinenti alla *cybersecurity* e alla *cyber resilience*, è da rilevare la costante collaborazione tra Banca d'Italia, MEF e CONSOB. Con quest'ultima, la Banca d'Italia ha definito negli ultimi anni sia una strategia congiunta per la supervisione delle infrastrutture finanziarie nazionali (sistemi di pagamento, mercati e *post-trading*), sia una strategia per la *cyber resilience* del sistema finanziario[36].

La Banca d'Italia ha adottato inoltre al proprio interno un "*Governance Framework* per la *Cyber Resilience*", che riguarda la resilienza dei sistemi interni al perimetro dell'Istituto.

5. Iniziative internazionali ed europee: EU, G7, G20, FSB, BIS

Uno dei primi tasselli nello sviluppo di una *policy* in materia di *cyber resilience* a livello internazionale è costituito dalla pubblicazione nel 2016 della "*Guidance on cyber resilience for financial market infrastructures*" da parte del *Committee on Payments and Market Infrastructures* (CPMI) e della *International Organization of Securities Commissions* (IOSCO), nel contesto della Banca dei regolamenti internazionali (BRI o *Bank for International Settlements*, BIS).

In seguito, dopo l'adozione di una strategia di *cyber resilience* dell'Eurosistema nell'ambito del *Market Infrastructure and Payments Committee* (MIPC), la Banca centrale europea (BCE o *European Central Bank*, ECB) ha istituito nel giugno 2017 lo *Euro Cyber Resilience Board for pan-European Financial Infrastructures*, forum cooperativo pubblico-privato deputato alla definizione e alla promozione di una politica di *cyber resilience*.

Nel 2018 il Consiglio per la Stabilità Finanziaria (*Financial Stability Board*, FSB), costituito dal G20 in seno alla BRI, ha pubblicato il cosiddetto *Cyber Lexycon*. Il 2018 è anche l'anno di pubblicazione del Framework versione 1.1 del NIST (*U.S. National Institute of Standards and Technology* – cfr. NIST, 2018) e del *Framework for Threat Intelligence-based Ethical Red Teaming* (TIBER-EU) della BCE (cfr. BCE, 2018a). Quest'ultimo strumento, mutuato dall'originale TIBER-NL, prevede schemi e procedure di *testing*. A seguire vi è stata la costituzione di un *TIBER-EU Knowledge Center* (TKC). Ad oggi, il TIBER-EU è stato adottato da diversi paesi dell'Unione Europea (sul tema TIBER-EU e TIBER-IT, si veda oltre).

---

[36] Incentrata in particolare su alcuni filoni normativi europei (ad es. DORA , *Digital Operational Resilience Act* e NIS, *Network and Information Security Directive*) e su un piano d'azione congiunto che prevede, tra l'altro, l'adozione di metodologie e strumenti di supervisione e *testing*, quali le CROE e il TIBER-EU (su questo punto si veda oltre nel presente lavoro).

Sempre nel 2018 la BCE ha varato un altro strumento in materia di *cyber resilience*, il *Cyber Resilience Oversight Expectations* (CROE), che fornisce una metodologia di valutazione del grado di *cyber resilience* per le entità finanziarie ed è prevalentemente rivolto ai gestori di sistemi di pagamento e alle infrastrutture di mercato. Tale strumento è stato sviluppato nell'ambito dell'Eurosistema, a beneficio delle Autorità competenti per lo svolgimento di *assessment* tematici sulla gestione del rischio *cyber* dei soggetti sorvegliati. La metodologia può essere altresì utilizzata autonomamente dalle entità finanziarie, per l'autovalutazione e l'interlocuzione strutturata con controparti del proprio ecosistema.

Nel febbraio 2020, lo *Euro Cyber Resilience Board* ha lanciato l'iniziativa *Cyber Information and Intelligence Sharing Initiative* (CIISI-EU), che vede la cooperazione di attori pubblici e privati: infrastrutture finanziarie attive a livello europeo, banche centrali (tra cui la Banca d'Italia), fornitori di servizi critici, ENISA ed EUROPOL. Esso mira a costituire un *trusted network* per lo scambio informativo.

A settembre 2020, nell'ambito della *Digital Finance Strategy*, la Commissione Europea ha proposto tra l'altro un Regolamento dedicato al tema della resilienza operativa (DORA – *Digital Operational Resilience Act* – cfr. Commissione Europea, 2020a). A dicembre dello stesso anno la Commissione ha pubblicato il documento sulla nuova *Cybersecurity Strategy for the Digital Decade*.

L'obiettivo di questo insieme di iniziative è rafforzare la resilienza collettiva dello spazio *cyber* europeo e assicurare la piena e affidabile fruibilità di servizi e strumenti digitali da parte di cittadini e imprese. Tale obiettivo viene perseguito anche attraverso l'armonizzazione del quadro normativo, lo sviluppo del mercato unico dei servizi digitali, il rafforzamento della resilienza operativa degli operatori di servizi essenziali.

Sul fronte G7, l'elemento più rilevante nell'ambito della cooperazione tra istituzioni finanziarie è stata la costituzione nel 2015 di un gruppo di esperti (CEG – G7 *Cyber Expert Group*), incaricato di definire principi di alto livello non vincolanti, finalizzati a rafforzare la *cyber resilience* dei sistemi finanziari dei Paesi coinvolti. Il CEG è inoltre dedito allo sviluppo di metodologie e protocolli per facilitare il coordinamento e la comunicazione tra le Autorità finanziarie e gli operatori privati.

Nel 2016, il G7 emana i "*G7 fundamental elements of cybersecurity for the financial sector*", un insieme di princìpi mirati a fornire al settore pubblico e al settore privato un quadro di riferimento comune per lo sviluppo di strategie di *cybersecurity* (G7, 2016).

Nel 2019 è stato organizzato il G7 *Cybersecurity Exercise*, che ha visto il coinvolgimento di 24 Autorità finanziarie dei Paesi del G7, impegnati in un attacco *cyber* simulato transfrontaliero contro il settore finanziario.

A livello G20, in seguito alla dichiarazione dei Capi di Governo del luglio 2017, la *cybersecurity* è divenuta una priorità nelle agende delle varie Presidenze di turno. In seno al G-20 *Finance Track*, si è dunque assistito a un crescente impegno da parte del *Financial Stability Board* (FSB); nel 2020 è stato varato un pacchetto di linee guida per la risposta efficace verso eventi *cyber* (*Cyber Incident Response*

and Recovery Toolkit, 2020). Questo impegno di armonizzazione transfrontaliera sta proseguendo con un filone di lavoro incentrato sulla riduzione dell'attuale frammentazione in materia di segnalazione di incidenti *cyber*; sul tema è stato pubblicato un recente rapporto che analizza gli schemi segnaletici regolamentari esistenti a livello G20 e individua alcuni interventi per favorirne una maggiore convergenza a livello internazionale[37].

Altri temi al centro delle discussioni e dei lavori dei gruppi attivi in ambito G20 e FSB sono il potenziamento delle capacità *cyber* e l'inclusione finanziaria. Il primo si esplica innanzitutto in una serie di attività volte a promuovere la sicurezza dei servizi. A questo si connette il tema del rafforzamento delle capacità *cyber* di paesi con dotazioni meno avanzate, al fine di scongiurare che singoli eventi possano intaccare l'intero sistema finanziario. Di pari passo, in questi organismi viene promossa – anche da parte dei rappresentanti e delle funzioni competenti della Banca d'Italia – l'educazione finanziaria dell'intera cittadinanza[38]: tale aspetto è essenziale per la costruzione di un contesto *cyber* resiliente; l'alfabetizzazione finanziaria, unitamente alla tutela dei consumatori e alle infrastrutture digitali, è un elemento che può contribuire a costruire un ecosistema finanziario resiliente e inclusivo (Visco, 2021).

Nel contesto della Banca dei Regolamenti Internazionali i *benchmark* da tenere presenti sono la *Cyber Guidance for Financial market Infrastructures* (2016) e la *Wholesale Payment Security Strategy* (2018), che hanno dato impulso a una serie di iniziative e documenti a livello internazionale, europeo e nazionale. Le misure per il rafforzamento della *cyber resilience* del sistema finanziario definite dal Comitato sui pagamenti e le infrastrutture di mercato (CPMI) sono supportate da altri comitati internazionali. Il CPMI è impegnato nell'attuazione di una strategia volta a rafforzare la *cyber resilience* delle infrastrutture finanziarie di mercato e dei relativi ecosistemi, con particolare riferimento ai sistemi di pagamento all'ingrosso. Le iniziative più rilevanti in tale ambito, oltre alla citata *Cyber Guidance*, riguardano infatti azioni mirate a ridurre il rischio di frode dei sistemi di pagamento all'ingrosso e a innalzare il grado di *cybersecurity* dei punti terminali del sistema finanziario. Inoltre la BRI, anche in collaborazione con Università e altre istituzioni, è impegnata nello sviluppo di una base dati per la conduzione di analisi e la pubblicazione di lavori di ricerca sulla quantificazione dei rischi *cyber*, sia per le perdite riconducibili agli incidenti *cyber*, sia per le potenziali ricadute sistemiche e la stabilità finanziaria.

6. *Threat Intelligence*, TIBER-EU e TIBER-IT

Il *Cyber Lexicon* dell'FSB, riprendendo una definizione del NIST, si riferisce alla locuzione *threat intelligence* come: *"Threat information that has been aggregated, transformed, analysed, interpreted or enriched to provide the necessary context for decision-making processes"*. La *threat intelligence*, qui intesa sia come acquisizione informativa sia come analisi sulla minaccia

37 FSB, 2021.

38 In merito all'educazione finanziaria e all'alfabetizzazione finanziaria, si veda https://economiapertutti.bancaditalia.it.

in genere, può essere considerata come un sotto-insieme dell'attività di *intelligence tout court*[39].

In tema di *threat intelligence* – e segnatamente per le capacità di prevenzione e rilevamento della minaccia *cyber* – rilevano senz'altro le attività di *testing* TIBER-EU e le sue declinazioni nazionali (in ambito italiano, il TIBER-IT, in fase di definizione) ne sono un ottimo esempio[40].

Il TIBER-EU, pubblicato dalla BCE nel 2018, è un *framework* europeo per *red-teaming* etico basato su *threat intelligence*. È in sostanza un complesso di linee guida, a livello europeo, su attori, processi e responsabilità nelle attività di *testing*, finalizzate al potenziamento della *cyber resilience* delle organizzazioni a fronte di un attacco informatico[41].

I test TIBER-EU imitano le tattiche, le tecniche e le procedure (TTPs) degli attori della minaccia nella vita reale (siano essi Stati, singoli *hacker*, *cybercrime*, *hacktivisti*, cyber-terroristi etc.). Le prove sono ideate su misura per la singola organizzazione, così da simulare un attacco alle funzioni critiche, ai sistemi, alle persone, ai processi. Il test ha lo scopo di rivelare i punti di forza e di debolezza dell'entità testata – in termini di prevenzione, rilevamento e risposta – consentendole di raggiungere alla fine dell'esecuzione un livello più elevato di *cyber resilience*.

I principali attori coinvolti in un test TIBER-EU sono ripartiti in diversi *team*, a seconda del loro ruolo e delle loro responsabilità:

- *blue team* (BT): le persone dell'organizzazione oggetto del test preposte alla difesa da attacchi *cyber*; esse non sono a conoscenza del test;
- *threat intelligence provider* (TI): l'azienda che esamina la gamma di possibili minacce e supporta l'organizzazione nella fase di acquisizione informativa e analisi;
- *red team* (RT): l'azienda che esegue l'attacco simulato tentando di compromettere le funzioni critiche dell'entità, imitando le tattiche, le tecniche e le procedure di un reale attore della minaccia;

---

39 Su questa linea, si veda Digregorio e Giannetto, 2019, pag. 14. In taluni ambiti, si tende tuttavia a sovrapporre la locuzione *threat intelligence* con quella di *cyber threat intelligence*; qui viene considerata anche questa impostazione.

40 ECB – TIBER-EU FRAMEWORK – *How to implement the European framework for Threat Intelligence-based Ethical Red Teaming* – Maggio 2018. TIBER-EU è stato sviluppato congiuntamente dalla BCE e da banche centrali nazionali dell'UE, approvato dal Consiglio direttivo della BCE e pubblicato nel maggio 2018.

41 Il TIBER-EU è stato ispirato e tiene conto di iniziative avviate in precedenza in alcuni paesi come il Regno Unito (CBEST) e i Paesi Bassi (TIBER-NL). TIBER-EU era inizialmente ricompreso in un *cyber resilience supervision toolkit* sviluppato dall'Eurosistema, in attuazione della propria strategia di supervisione per la *cyber resilience* dei sistemi di pagamento e delle infrastrutture di mercato. Il *toolkit* comprendeva anche una *Cyber resilience survey* (strumento di "prima diagnosi" in forma di questionario a risposte multiple) e le *Cyber resilience Oversight Expectations* (CROE). Tale strumento integrato era messo a disposizione delle Autorità competenti per lo svolgimento di *assessment* tematici sulla gestione del rischio *cyber* dei soggetti sorvegliati. In ambito europeo, anche la regolamentazione sulle sedi di negoziazione (MiFID2/MiFIR), quella sulle CCP (EMIR) e quella sui depositari centrali di titoli (CSDR) contengono previsioni in materia di rischio operativo anche in materia *cyber*. Sempre in ambito Eurosistema, è stata poi definita una strategia regolamentare (approvata dal Consiglio Direttivo della BCE) sui SIPS (*Sistemically Important Payment Systems*).

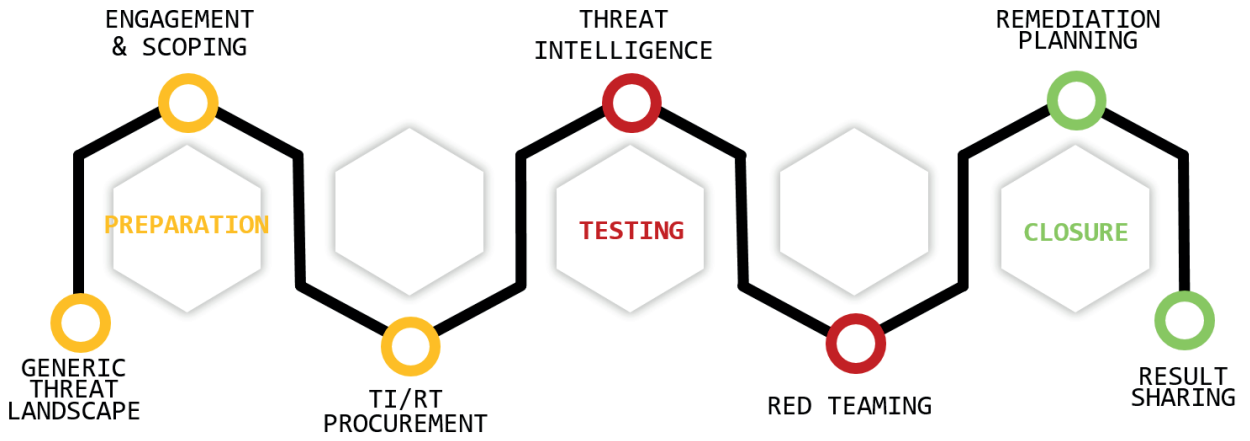
- *white team* (WT): un *team* all'interno dell'organizzazione *target* che è responsabile dell'intero processo di test; è a conoscenza del test; guida e gestisce il test in collaborazione con il TIBER *cyber team*;
- *TIBER cyber team* (TCT): il *team* all'interno dell'Autorità che facilita l'interazione tra i diversi attori coinvolti nel test; supervisiona l'esecuzione del test e assicura il rispetto dei requisiti del framework TIBER.

A questi gruppi, il TIBER-EU prevede possa essere affiancato il cosiddetto *purple team* (PT), formato da membri del BT e del RT, con l'obiettivo di massimizzare i benefici del test attraverso una più profonda e strutturata cooperazione tra attaccanti e difensori[42].

Il TIBER-EU Framework mira ad armonizzare e standardizzare l'approccio al *red-teaming* etico basato sulla *threat intelligence* in tutta l'UE. Per raggiungere questo obiettivo, i vari framework TIBER nazionali dovrebbero seguire le linee guida fornite nel TIBER-EU.

Le fasi principali di un test *end-to-end* del tipo TIBER-EU sono preparazione, test e chiusura (*preparation*, *testing* e *closure*). Una sinossi del processo di *testing* TIBER-EU (e TIBER-IT) è rappresentata nella figura 2.

Figura 2 - Fasi del processo TIBER-EU e TIBER-IT



A monte del test, vi può essere una fase di profilazione dello scenario di minaccia (con il *Generic Threat landscape* – GTL). All'interno del processo si possono distinguere lo *scoping* (definizione obiettivi e portata), il *procurement* (ingaggio/approvvigionamento dei team di TI e RT), la *threat intelligence* (acquisizione informativa e analisi), il *red teaming* (attività di attacco simulato), la *remediation* (azioni di bonifica e rimedi tecnici) e il *result sharing* (condivisione dei risultati). I test si concludono con un *summary* report (sintesi riepilogativa) e un'attestazione.

[42] Di norma il *purple team* interviene alla fine della fase di attacco per consolidare i risultati e le lezioni apprese. Può anche essere attivato nel corso della fase di attacco qualora il BT individui le azioni del RT e le attribuisca a un test di sicurezza. Sono tuttora in corso, a livello europeo, lo sviluppo di metodologie e *best practices* evolutive riguardo al *testing* basato sul *threat intelligence* e l'esame di avanzate pratiche di *purple teaming*.

Il framework TIBER-EU è progettato per le Autorità nazionali e le entità che costituiscono FMIs (*financial market infrastructures*), comprese quelle le cui attività transfrontaliere rientrano nel mandato regolamentare di diverse Autorità. È applicabile sia a entità del settore finanziario, sia a organizzazioni di altri settori critici.

Oltre a una serie di requisiti obbligatori, il framework include anche opzioni che possono essere adattate alle specificità delle diverse giurisdizioni. Ciò facilita il riconoscimento reciproco e riduce l'onere sia per le Autorità che per le entità sottoposte ai test.

Le linee guida TIBER-EU sul *procurement* forniscono dettagli su come selezionare fornitori di *red-teaming* e acquisire i servizi di *threat intelligence*[43]. La TIBER-EU *White Team Guidance* spiega come impostare il team che gestisce il test TIBER dall'interno dell'entità *target*.

A gennaio 2020 la Banca d'Italia e la CONSOB hanno adottato un Piano di azione congiunto per la *cyber resilience* del settore finanziario italiano, che prevede, tra l'altro, lo sviluppo del framework di *testing* TIBER-IT, in linea con la strategia di *cyber resilience* dell'Eurosistema e in collaborazione con altre Autorità e *stakeholder* nazionali di settore (ad es. CERTFin).

Il TIBER-IT è in fase di sviluppo: esso potrebbe tenere conto delle specificità nazionali, sia dal punto di vista finanziario sia da quello giuridico, nonché delle sinergie istituzionali con altre Autorità, al fine di offrire uno strumento armonizzato e coordinato per gli operatori del sistema finanziario nazionale.

Come già positivamente sperimentato in altri Paesi, il TIBER-IT potrebbe essere applicato a tutte le entità finanziarie, potendo fungere anche da metodologia di riferimento per successive evoluzioni in materia (anche sul fronte della regolamentazione e della supervisione).

In linea con le migliori prassi adottate in altre giurisdizioni, lo sviluppo del TIBER-IT potrebbe essere orientato ai princìpi seguenti: partecipazione degli operatori finanziari su base volontaria; ambito di applicazione preferibilmente riferito agli operatori critici per la piazza finanziaria italiana; applicazione progressiva.

7. *Cyber resilience* nel sistema finanziario: profili evolutivi

Le misure di seguito elencate riflettono alcune tendenze emerse negli ultimi anni a livello internazionale in materia di *cyber resilience*: *capacity-building* per le organizzazioni e gli Stati; specializzazione delle risorse impiegate nella *cybersecurity*; promozione di un ambiente normativo e regolamentare solido

[43] Per garantire che i fornitori di servizi di *threat intelligence* e *red-teaming* soddisfino *standard* appropriati per condurre un test TIBER-UE, le organizzazioni sottoposte a test dovrebbero eseguire *due diligence*, per assicurarsi che il proprio fornitore selezionato possegga tutti i requisiti stabiliti nelle linee guida sul *procurement* del TIBER-UE. In futuro, le organizzazioni dovrebbero fare ricorso soltanto ai servizi di fornitori che hanno ottenuto la certificazione e l'accreditamento formale TIBER-UE. Attualmente, non esiste in Europa un'agenzia di certificazione e accreditamento preposta a questo scopo.

e condiviso per il cyberspazio; evoluzione delle capacità di monitoraggio e analisi; cooperazione inter-istituzionale.

Lo sviluppo di professionalità e capacità multidisciplinari in ambito *cyber* è un elemento chiave per la resilienza del sistema finanziario (Maurer e Nelson, 2020). Al fine di inquadrare le risultanze di investigazioni tecniche nel contesto in cui sono maturate e individuare plausibili motivazioni e attori della minaccia, occorrono competenze complementari rispetto alle sole conoscenze tecnico-informatiche. Sviluppare nel concreto unità e gruppi di lavoro composti da persone con competenze variegate è una delle misure che possono aiutare nella definizione e applicazione di politiche di *cyber resilience*.

IL RUOLO DELL'ANALISI PER LA RESILIENZA SISTEMICA

Le attività di analisi relative a minacce e fenomeni di varia natura (geopolitica, finanziaria, economica, tecnologica, di *intelligence*) svolgono un ruolo centrale nel perseguimento di una condizione di *cyber resilience* per la continuità di servizio del sistema finanziario. Tali attività vanno precedute e accompagnate da un lavoro continuo di acquisizione informativa e monitoraggio, secondo un'ottica di sistema e di scenario.

Il presidio regolamentare è un altro punto fondamentale per lo sviluppo e l'implementazione di politiche di *cyber resilience*, a livello nazionale, europeo e internazionale. L'obiettivo a cui tendere è la promozione di un ambiente normativo e regolamentare bilanciato (tra pubblico e privato) per il cyberspazio. Un corollario, sempre a livello regolamentare, è la promozione di un contesto *level playing field*, che preveda inoltre gradualità e proporzionalità degli interventi.

Un altro aspetto evolutivo riguarda le attività di analisi. La *cyber resilience* per la continuità operativa del sistema finanziario richiede un lavoro continuo di acquisizione informativa, monitoraggio e analisi su eventi *cyber*, minacce e fenomeni di varia natura (geopolitica, finanza, economia, tecnologia, *intelligence*). Non è quindi sufficiente la sola attività di *threat intelligence*, che si occupa in sostanza di minacce, ma occorre mettere in campo analisi sistemiche di scenario (SSA) (Giannetto, 2020, 2021), per scrutinare sinotticamente e simultaneamente una gamma di fenomeni molteplici e interconnessi.

Infine, una misura supplementare ma non meno importante per lo sviluppo di politiche di *cyber resilience*, è sicuramente l'interazione tra le istituzioni finanziarie e gli organismi di *intelligence* e di *law enforcement* (es. forze dell'ordine). Il potenziamento di tale cooperazione può in prospettiva rivelarsi particolarmente fruttuosa, anche per la trattazione congiunta e sinergica di temi strategici di *cybersecurity*.

Conclusioni

Il lavoro sintetizza le principali iniziative istituzionali avviate a livello nazionale e internazionale per rafforzare la *cyber resilience* e favorire la continuità di servizio del sistema finanziario. Esse comprendono le misure adottate dalla Banca d'Italia – alcune già consolidate, altre in fase di sviluppo – nel solco tracciato dalle linee strategiche dell'Istituto e dell'Eurosistema, nonché l'ampia gamma di iniziative messe a punto da diversi organismi internazionali. Dalla ricerca emerge la necessità di adattare e far evolvere su base costante le azioni finalizzate a rafforzare la *cyber resilience* a livello nazionale e internazionale, per poter far fronte al contesto di riferimento in costante evoluzione e sempre più complesso.

Riferimenti bibliografici

Baldoni, R. (2021a), Intervento al Convegno "Dalla sicurezza aziendale alla sicurezza collettiva", Roma, 15 ottobre 2021.

Baldoni, R. (2021b), Intervento al "36° Convegno Giovani Imprenditori di Confindustria", Napoli, 23 ottobre 2021.

Banca Centrale Europea (2018a), *How to implement the European framework for Threat Intelligence-based Ethical Red Teaming*, Tiber-Eu Framework, maggio 2018.

Banca Centrale Europea (2018b), *Cyber resilience oversight expectations for financial market infrastructures*; dicembre 2018.

Banca d'Italia (2019), *La Banca d'Italia. Funzioni e obiettivi,* dicembre 2019.

Banca d'Italia (2022), *Canale Fintech*, sito istituzionale.

Bank of England (2021), *CBEST Threat Intelligence-Led Assessments*, gennaio 2021.

Basel Committee on Banking Supervision (2020a), *Principles for Operational Resilience*, BIS, marzo 2021.

Basel Committee on Banking Supervision (2020b), *Consultative Document Principles for operational resilience*, BIS, agosto 2020.

Bilal, A. (2021), *Hybrid Warfare – New Threats, Complexity, and 'Trust' as the Antidote*, NATO Review, 20 novembre 2021.

Bodeau, J.D., C.D. Mccollum, D.B. Fox (2018), *Cyber Threat Modeling: Survey, Assessment and Representative Framework*, MITRE, novembre 2018.

Ciocca, P. (2020), *Dati e finanza: nuove opportunità e nuove vulnerabilità. La necessità di cambiare paradigma*, intervento del Commissario Consob, Roma, 18 novembre 2020.

Coats, D.R. (2019), *Worldwide Threat Assessment of the US Intelligence Community*, 29 gennaio 2019.

Commissione Europea (2020a), *Consultation Document – Digital Operational Resilience Framework for financial services: Making the EU financial sector more secure*, 24 settembre 2020.

Commissione Europea (2020b), *Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL amending Directives 2006/43/EC, 2009/65/EC, 2009/138/EU, 2011/61/EU, EU/2013/36, 2014/65/EU, (EU) 2015/2366 and EU/2016/2341*, Brussels, 24 settembre 2020.

Commissione Europea (2020c), *Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014 and (EU) No 909/2014*, Brussels, 24 settembre 2020.

Commissione Europea (2020d), *Joint Communication to the European Parliament and the Council – The EU's Cybersecurity Strategy for the Digital Decade*, Brussels, 16 dicembre 2020.

Commissione Europea (2020e), *Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the resilience of critical entities*, Brussels, 16 dicembre 2020.

Committee on Payments and Market Infrastructures, Board of the International Organization of Securities Commissions (2016), *Guidance on cyber resilience for financial market infrastructures*, BIS, giugno 2016.

Consiglio Europeo (2020), *Next Generation EU*, Bruxelles, 21 luglio 2020.

Digregorio, P. e Giannetto B. (2019), *Development of a cyber threat intelligence apparatus in a central bank,* Banca d'Italia, QEF 517, 11 ottobre 2019.

Dipartimento delle informazioni per la sicurezza (2021a), *Relazione sulla politica dell'informazione per la sicurezza 2020*, 1 marzo 2021.

Dipartimento delle informazioni per la sicurezza (2021b), *Italian Position Paper on International Law and Cyberspace*, 4 novembre 2021.

Dipartimento per la trasformazione digitale, Agenzia per la cybersicurezza nazionale (2021), *Strategia Cloud Italia*, settembre 2021.

European Union Agency for Cybersecurity (2020a), ENISA Threat Landscape – Emerging Trends, 20 ottobre 2020.

European Union Agency for Cybersecurity (2020b), Artificial Intelligence Cybersecurity Challenges, 15 dicembre 2020.

European Union Agency for Cybersecurity (2021a), EU Cybersecurity Initiatives in the Finance Sector, 5 marzo 2021.

European Union Agency for Cybersecurity (2021b), *ENISA Threat Landscape 2021*, 27 ottobre 2021.

European Union Agency for Cybersecurity, CERT-EU (2022), *Joint Publication – Boosting your Organisation's Cyber Resilience,* 14 febbraio 2022.

Europol (2020), *Internet Organized Crime Threat Assessment (IOCTA) 2020*, 5 ottobre 2020.

Europol (2021), *Internet Organised Crime Threat Assessment (IOCTA) 2021*, 11 novembre 2021.

Fazio, A. e F. Zuffranieri (2018), *Interbank payment system architecture from a cyber security perspective,* Banca d'Italia, QEF 418, 29 gennaio 2018.

Financial Stability Board (2018), *Cyber Lexicon*, 12 novembre 2018.

Financial Stability Board (2021), *Cyber Incident Reporting: Existing Approaches and Next Steps for Broader Convergence*, ottobre 2021.

Gazzetta Ufficiale (2021), *Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale,* DECRETO-LEGGE 14 giugno 2021, n. 82, convertito in Legge 109/2021.

Giannetto, B. (2019), *Cyber Governance & Cyber Threat Intelligence*, Security Summit, 5 giugno 2019.

Giannetto, B. (2020), *All-Source Intelligence: Reshaping an Old Tool for Future Challenges*, Security Affairs, 18 dicembre 2020.

Giannetto, B. (2021), *Innovazione Tecnologica e Cybersecurity nel Sistema Finanziario*, Cyber Security Virtual Conference, 26 maggio 2021.

Giannetto, B. e Paganini P. (2020), *Mastering Communication in Cyber Intelligence Activities: A Concise User Guide*, Cyber Defense Magazine, 21 aprile 2020.

G7 (2016), *G7 fundamental elements of cybersecurity for the financial sector*, 11 ottobre 2016.

Maurer, T. e A. Nelson (2020), *International Strategy to Better Protect the Financial System against Cyber Threats*, CARNEGIE, 18 novembre 2020.

Maurer, T. e A. Nelson (2021), *The Global Cyber Threat*, IMF, marzo 2021.

MITRE, *ATT&CK Matrix for Enterprise*, *D3FEND*.

National Institute of Standards and Technology (2018), *Cybersecurity Framework*, Version 1.1, 16 aprile 2018.

National Security Agency (2021a), *Embracing a Zero Trust Security Model*, febbraio 2021.

National Security Agency (2021b), *NSA Funds Development, Release of D3FEND*, 22 giugno 2021.

Perrazzelli, A. (2021), *Le iniziative regolamentari per il Fintech: a che punto siamo?,* intervento della Vice Direttrice Generale della Banca d'Italia, Università degli Studi dell'Insubria, Laboratorio di Finanza Digitale, 4 maggio 2021.

Schmitt, M.N. (2021), *Terminological Precision and International Cyber Law*, Articles of War, 29 luglio 2021.

Signorini, L.F. (2021), *Economic Outlook, Public Finances and the Next Generation EU*, Banca d'Italia, 10 marzo 2021.

Sørensen, H. e D.B. Nyemann (2018), *Going beyond resilience – A revitalized approach to countering hybrid threats*, Hybrid CoE Strategic Analysis 13, novembre 2018.

Treverton, G.F., A. Thvedt, A.R. Chen, K.Lee e M. McCue (2018), *Addressing hybrid threats*, SDU, CATS, Hybrid CoE, 2018.

Visco, I. (2013), *Economia e finanza dopo la crisi,* Conferenza a Classi Riunite del Governatore della Banca d'Italia, Accademia Nazionale dei Lincei, 8 marzo 2013.

Visco, I. (2021), *Considerazioni finali del Governatore, Relazione annuale*, Banca d'Italia, Roma, 31 maggio 2021.

World Economic Forum (2018), *Cyber Resilience Playbook for Public-Private Collaboration*, gennaio 2018.

World Economic Forum (2020), *Systems of Cyber Resilience: Secure and Trusted FinTech*, luglio 2020.

World Economic Forum (2021), *The Global Risks Report*, gennaio 2021.

World Economic Forum (2022), *The Global Risks Report*, gennaio 2022.

Zhang, T. (2020), *Building Cyber Resilience*, (Virtual) IMF Cybersecurity Workshop, 9 dicembre 2020.

Pubblicazioni della collana Mercati, infrastrutture, sistemi di pagamento

n. 1 TIPS - TARGET Instant Payment Settlement – The Pan-European Infrastructure for the Settlement of Instant Paymentsi, *by Massimiliano Renzetti, Serena Bernardini, Giuseppe Marino, Luca Mibelli, Laura Ricciardi and Giovanni M. Sabelli* (Institutional Issues)

n. 2 Real-Time Gross Settlement systems: breaking the wall of scalability and high availability, *by Mauro Arcese, Domenico Di Giulio and Vitangelo Lasorella* (Research Papers)

n. 3 Green Bonds: the Sovereign Issuers' Perspective, *by Raffaele Doronzo, Vittorio Siracusa and Stefano Antonelli* (Research Papers)

n. 4 T2S - TARGET2-Securities – The pan-European platform for the settlement of securities in central bank money, *by Cristina Mastropasqua, Alessandro Intonti, Michael Jennings, Clara Mandolini, Massimo Maniero, Stefano Vespucci and Diego Toma* (Institutional Issues)

n. 5 The carbon footprint of the Target Instant Payment Settlement (TIPS) system: a comparative analysis with Bitcoin and other infrastructures, *by Pietro Tiberi* (Research Papers)

n. 6 Proposal for a common categorisation of IT incidents, *by Autorité de Contrôle Prudentiel et de Résolution, Banca d'Italia, Commissione Nazionale per le Società e la Borsa, Deutsche Bundesbank, European Central Bank, Federal Reserve Board, Financial Conduct Authority, Ministero dell'Economia e delle Finanze, Prudential Regulation Authority, U.S. Treasury* (Institutional Issues)

n. 7 Inside the black box: tools for understanding cash circulation, *by Luca Baldo, Elisa Bonifacio, Marco Brandi, Michelina Lo Russo, Gianluca Maddaloni, Andrea Nobili, Giorgia Rocco, Gabriele Sene and Massimo Valentini* (Research Papers)

n. 8 The impact of the pandemic on the use of payment instruments in Italy, *by Guerino Ardizzi, Alessandro Gambini, Andrea Nobili, Emanuele Pimpini and Giorgia Rocco* (Research Papers) (in Italian)

n. 9 TARGET2 – The European system for large-value payments settlement, *by Paolo Bramini, Matteo Coletti, Francesco Di Stasio, Pierfrancesco Molina, Vittorio Schina and Massimo Valentini* (Institutional Issues) (in Italian)

n. 10 A digital euro: a contribution to the discussion on technical design choices, *by Emanuele Urbinati, Alessia Belsito, Daniele Cani, Angela Caporrini, Marco Capotosto, Simone Folino, Giuseppe Galano, Giancarlo Goretti, Gabriele Marcelli, Pietro Tiberi and Alessia Vita* (Institutional Issues)

n. 11 From SMP to PEPP: a further look at the risk endogeneity of the Central Bank, *by Marco Fruzzetti, Giulio Gariano, Gerardo Palazzo and Antonio Scalia* (Research Papers)

n. 12 TLTROs and collateral availability in Italy, *by Annino Agnes, Paola Antilici and Gianluca Mosconi* (Research Papers) (in Italian)

n. 13 Overview of central banks' in-house credit assessment systems in the euro area, by L*aura Auria, Markus Bingmer, Carlos Mateo Caicedo Graciano, Clémence Charavel, Sergio Gavilá, Alessandra Iannamorelli, Aviram Levy, Alfredo Maldonado, Florian Resch, Anna Maria Rossi and Stephan Sauer* (Institutional Issues)

n. 14 The strategic allocation and sustainability of central banks' investment, by *Davide Di Zio, Marco Fanari, Simone Letta, Tommaso Perez and Giovanni Secondin* (Research Papers) (in Italian)

n. 15 Climate and environmental risks: measuring the exposure of investments, by *Ivan Faiella, Enrico Bernardini, Johnny Di Giampaolo, Marco Fruzzetti, Simone Letta, Raffaele Loffredo and Davide Nasti* (Research Papers)

n. 16 Cross-Currency Settlement of Instant Payments in a Multi-Currency Clearing and Settlement Mechanism, by *Massimiliano Renzetti, Fabrizio Dinacci and Ann Börestam* (Research Papers)

n. 17 What's ahead for euro money market benchmarks?, by *Daniela Della Gatta* (Institutional Issues) (in Italian)