Università
Ca'Foscari
Venezia

Corso di Laurea magistrale

in Economia e Finanza

Tesi di Laurea

Le obbligazioni catastrofali tra rischio nat-cat e rischio informatico

Relatrice
Ch.ma Prof.ssa Diana Barro

Correlatore
Ch. Prof. Paolo Pianca

Laureanda
Francesca Bertone
842694

Anno Accademico
2018 / 2019

Indice

Introduzione

In un contesto dominato da squilibri climatici e tecnologie dirompenti, la società si trova sempre più esposta a rischi catastrofali, tipologie di rischio legate ad eventi casuali naturali ed antropici che si manifestano con bassa frequenza ma che al loro verificarsi producono ingenti impatti al tessuto economico sociale. Il conseguente sentiment di insicurezza ha alimentato una domanda consistente di coperture contro i danni derivanti da questi eventi avversi, ponendo il settore (ri)assicurativo alla costante ricerca di modellistica, per catturare il più accuratamente possibile il profilo di tali rischi, e di strategie di liability hedging, funzionali alla gestione sostenibile di tale linea di business.

Il presente lavoro, partendo dalla modalità innovativa di gestione dei rischi catastrofali, la insurance securitization, una strategia che consente il trasferimento di tali rischi al mercato dei capitali, mediante l'emissione di strumenti finanziari detti Insurance Linked Securities (ILS), approfondirà in particolare, tra i prodotti della cartolarizzazione, i catastrophe bonds. Tali titoli rappresentano la categoria più diffusa di ILS e offrono all'impresa di assicurazione protezione contro i rischi di coda che potrebbero provocare l'insolvenza in caso di perdite superiori ai premi totali accumulati. Altresì, l'attenzione sarà posta sul sottostante di tali strumenti finanziari, il rischio catastrofale, e sul processo di modellizzazione di tali rischi. Infine, sarà esplorata la potenzialità dei cat bonds come strumenti di trasferimento del rischio informatico, un rischio che sta assumendo sempre più un ruolo centrale nella vita quotidiana, stante il processo in atto di digitalizzazione dell'economia e della conseguente pervasività delle tecnologie dell'informazione e delle telecomunicazioni che rendono la società nel suo complesso più esposta alla dimensione catastrofale del rischio informatico. Una dimensione, tra l'altro, esasperata dal fenomeno del silent cyber risk.

Nello specifico, nel primo capitolo, dopo una breve disamina dell'attuale contesto caratterizzato dai fenomeni del global warming e dell'informatizzazione dell'economia, l'attenzione sarà posta sulla dimensione gestionale del rischio, andando ad approfondire per quanto riguarda il rischio assicurativo non-life catastrofale, la riassicurazione tradizionale e la cartolarizzazione assicurativa, mettendone in luce caratteristiche e differenze.

Il secondo capitolo, invece, si focalizza sulla dimensione rischio. In particolare, sarà proposta la teoria dei valori estremi, schema statistico di modellizzazione degli eventi rari come le catastrofi, con un'applicazione empirica del metodo Block Maxima, e si

descriveranno i modelli catastrofali, frameworks risultanti dalla combinazione di modelli probabilistici e fisici.
Il capitolo 3 è incentrato sull'obbligazione catastrofale e sui fattori che ne determinano il profilo rischio-rendimento.
Infine, il capitolo 4, dopo una descrizione delle opportunità e delle problematiche strutturali del mercato assicurativo cyber, presenterà le funzioni copula come strumento di modellizzazione della struttura di dipendenza tra i rischi cyber a fini di pricing e le potenzialità di un cyber-cat bonds come strumento di gestione delle dimensioni catastrofale e silente del rischio informatico.

Capitolo 1

Mercato ILS vs. climate change e digitalizzazione

1.1 Il contesto di sviluppo: rischio nat-cat e rischio informatico

Con catastrofe si designa la conseguenza disastrosa di fenomeni eccezionali sfuggiti al controllo dell'uomo.

A questo termine si associano oltre che eventi naturali estremi come alluvioni, uragani, terremoti, tsunami, inondazioni, tornadi, siccità, eruzioni vulcaniche, incendi frane, gelo, precipitazioni intense, anche cedimenti di grandi strutture, guerre, insurrezioni, avarie, interruzioni di processi industriali, disastri fisico-tecnologici e ambientali associabili o ad errori umani o ad azioni intenzionali dell'uomo come, ad esempio, attacchi informatici e atti terroristici.

Infatti, quando si parla di rischio catastrofale non si fa riferimento solo alle catastrofi naturali ma, in linea con il processo di digitalizzazione e con le conseguenti nuove vulnerabilità a cui il sistema industriale, il sistema finanziario e l'intera umanità si trovano ad essere esposti, si include anche il rischio informatico ovvero il cosiddetto cyber risk che può considerarsi attualmente ma soprattutto in futuro un rischio sistemico e quindi classificato come un rischio catastrofale.

Dal punto di vista delle compagnie assicurative, i rischi legati a catastrofi naturali e a catastrofi cibernetiche sono collegati ad eventi che accadono con bassa frequenza (low frequency), irregolari, imprevedibili e con elevato impatto in termini di conseguenze (high severity).

Questi eventi infatti determinano danni in un'ampia zona territoriale coinvolgendo più soggetti e beni. Dunque, un singolo evento estremo può provocare una moltitudine di sinistri oggetto di altrettanti diversi contratti assicurativi. Di conseguenza tali rischi sono configurabili come rischi dipendenti e positivamente correlati.

I danni complessivi riconducibili all'evento catastrofale comprendono danni ad edifici, infrastrutture, veicoli ma comprendono anche danni dovuti ad interruzione di attività, furto e perdita di dati sensibili come indicato da Swiss Re (2008,2009).

Queste potenziali catastrofi naturali e cibernetiche determinano una crescente domanda di copertura assicurativa, per via della natura stessa del rischio nat-cat (natural catastrophe risk) e del rischio informatico, la compagnia assicurativa nel far fronte a questa domanda

potrebbe incorrere, durante la tariffazione, ad un errato prezzo in quanto non dispone di un'ampia banca dati e anche se tale banca dati fosse a disposizione non è detto che quei dati storici riescano a cogliere le tendenze in atto.

Un'errata tariffazione ha conseguenze dirette sulla stabilità finanziaria dell'assicuratore.

L'articolo 1912 del codice civile per quanto riguarda la copertura dei rischi "movimenti tellurici, guerra, insurrezione o tumulti popolari", rinvia all'autonomia delle parti, come sottolineato da Donati e Volpe Putzolu (2015), in quanto tale articolo in generale esclude tali rischi catastrofali dalle coperture nelle polizze danni salvo però patto contrario. Quindi tali rischi possono essere suscettibili di una copertura ad hoc perché è possibile il patto contrario. Inoltre, l'articolo 182 del Codice delle Assicurazioni Private obbliga la compagnia assicurativa ad inserire nella documentazione contrattuale e anche nella documentazione precontrattuale la clausola che prevede queste esclusioni, salva ovviamente diversa pattuizione.

Per quanto riguarda il rischio naturale catastrofale (nat-cat), com'è noto, il clima e le caratteristiche dell'ambiente incidono fortemente sui fenomeni naturali e di conseguenza sull'evoluzione della specie umana. Ogni comunità, infatti, vive all'interno di un ecosistema caratterizzato dalle specie animali e vegetali che ospita e dal clima, due elementi che incidono sull'esistenza della comunità stessa. Gli individui hanno sempre convissuto con i rischi legati a fenomeni naturali distruttivi come terremoti, alluvioni, uragani, incendi ed eruzioni vulcaniche. Eventi che si considerano essere difficili se non impossibili da predire. La comunità scientifica sostiene l'esistenza di una forte correlazione tra i cambiamenti climatici in atto e gli eventi metereologici estremi (Michel-Kerjan and Morlaye(2008), Johnson(2014)).

Di certo, l'antropizzazione dell'ambiente, ovvero quelle trasformazioni che l'uomo infligge all'ecosistema attraverso la costruzione di impianti produttivi sempre più inquinanti, la deforestazione e lo sfruttamento indiscriminato dei territori, mette a serio rischio la biodiversità del pianeta e contribuisce a questi stravolgimenti climatici che, a loro volta, concorrono alla manifestazione di catastrofi naturali.

Alcuni paesi europei, tra cui l'Italia, sfruttano e inquinano l'ambiente fino al 140% di quanto sarebbe consentito in termini di sostenibilità (European Consortium for modelling Air pollution annd climate strategies(2010).

Nell'ultimo secolo si è assistito ad un notevole innalzamento della temperatura media, come mostrato in figura 1, e stime effettuate dalla NASA[1] indicano un ulteriore incremento in futuro.

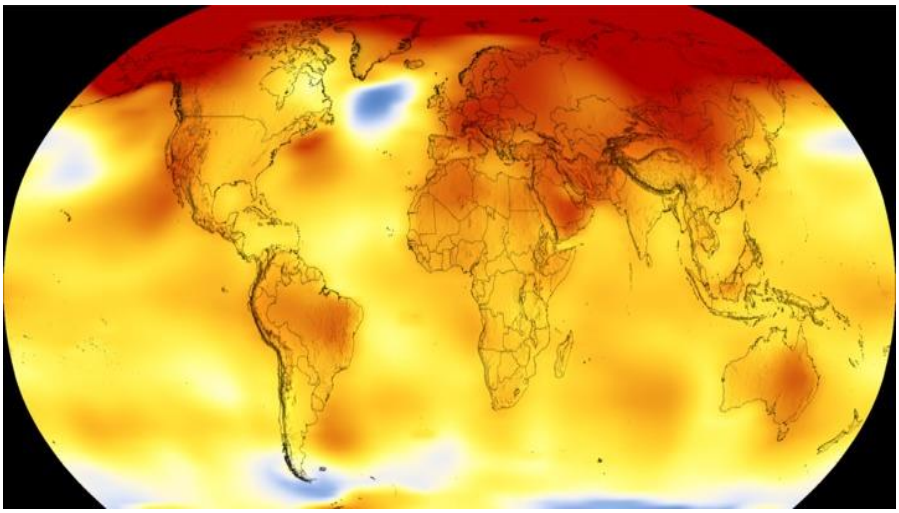

Figura 1*: Global warming (NASA)*

Tuttora i processi produttivi delle maggiori industrie utilizzano come fonte energetica combustibili fossili come il carbone e gas naturali che rilasciano nell'atmosfera sostanze tra cui l'anidride carbonica (CO_2).

La CO_2 assieme agli altri gas naturali, come ozono e metano, uniti al vapore acqueo causano l'effetto serra, portano cioè alla formazione di un involucro intorno alla terra che, invece di consentire la dispersione del calore dei raggi del sole nello spazio, lo trattiene nell'atmosfera garantendo così un clima mite. Ma negli ultimi anni la concentrazione nell'aria di anidride carbonica è cresciuta in modo spropositato, provocando un aumento dell'effetto serra e quindi un aumento della temperatura media. E questo incremento della CO_2 oltre ad essere causato dall'industria non green è causato anche dalla deforestazione che a sua volta porta alla riduzione delle aree verdi che contribuiscono all'assorbimento ed alla trasformazione di questo gas in ossigeno.

Questo continuo processo di riscaldamento della terra, il cosiddetto global warming, che porta al surriscaldamento degli oceani che produce, a sua volta, una forte evaporazione dell'acqua dei mari, è considerato essere la principale causa dell'incremento dell'intensità delle piogge e della manifestazione di fenomeni atmosferici estremi come uragani, alluvioni e tempeste. Calamità a cui, via via che la temperatura media del pianeta continuerà ad

[1] https://climate.nasa.gov/vital-signs/global-temperature/

innalzarsi, la società si troverà ad essere maggiormente più esposta. Inoltre, queste temperature elevate causano lo scioglimento dei ghiacciai in Antartide, le cosiddette fasi di ritiro, tale fenomeno a sua volta provoca l'innalzamento degli oceani a cui consegue la sommersione delle coste, zone che sono più densamente popolate.

In altre aree del pianeta invece, per via della circolazione globale atmosferica, si assiste ad una diminuzione della piovosità che accelera il fenomeno della siccità ed il processo di desertificazione che producono ingenti danni alle attività agricole e minano il sostentamento di numerosi popoli.

Tutti questi mutamenti sono intensificati anche dall'aumento della popolazione mondiale che, non essendo spesso supportato da politiche di sviluppo sostenibile e di tutela ambientale, determina un eccessivo sfruttamento e consumo delle risorse naturali.

L'Italia, ad esempio, è molto esposta al rischio idrogeologico, causato dal disboscamento e dall'alterazione del suolo attraverso la cementificazione[2]. Le aree definite ad alto rischio sono ben il 91%, esattamente pari a 7201 comuni.

La popolazione nel tempo si è concentrata nelle aree costiere, zone che sono considerate fortemente esposte a questi eventi, e le compagnie assicurative, in linea con il loro business, non hanno fatto altro che fornire coperture assicurative andando incontro ad ingenti perdite assicurate in seguito all'accadimento dell'evento avverso[3].

Negli Stati Uniti le compagnie assicurative hanno indennizzato tra il 2015 e il 2016 danni per 60 miliardi di dollari in seguito a calamità naturali conseguenti a repentini cambiamenti climatici *(Aon Benfield, 2016)*.

Secondo lo Swiss Re Institute (2018, 2019) in quell'anno gli eventi più disastrosi in termini di perdite umane ed economiche sono stati le alluvioni in Cina e l'Uragano Matthwe di categoria 5 tra Caraibi e Stati Uniti.

L'anno 2017, invece, ha visto protagonisti i distruttivi uragani di categoria 4+ Harvey, Irma e Maria che tra Agosto e Settembre hanno devastato diverse zone degli Stati Uniti e di altri paesi.

Il 2018 è stato anch'esso uno dei più costosi per il settore assicurativo ma comunque inferiore rispetto all'anno 2017. Esempi di devastanti catastrofi naturali del 2018 sono gli uragani Michael e Florence, i devastanti incendi in Europa ed in California, i terremoti in Giappone ed in Indonesia, infine le eruzioni vulcaniche nelle Hawaii.

[2] ISPRA (2018)
[3] Swiss Re (2019)

Come mostrato in figura 2, i sinistri dovuti a queste calamità sono costati al settore 79 miliardi di dollari US ed è stato coperto poco più del 50% di tutte le perdite economiche registrate. Invece nel 2017, il settore ha sopportato perdite pari a 150 miliardi di dollari.

	2018	2017	annual change	10-year average
Economic losses (total)	**155**	**350**	**-56%**	**220**
Nat cat	146	342	-57%	208
Man-made	9	8	9%	12
Insured losses (total)	**79**	**150**	**-47%**	**71**
Nat cat	71	143	-50%	63
Man-made	8	7	20%	8

Figura 2: *Perdite economiche totali e assicurate nel 2017 e nel 2018 in miliardi di dollari (Swiss Re Institute)*

Le calamità naturali, inoltre, hanno causato circa 11000 vittime.

In particolare, nel 2018, la compagnia riassicuratrice Swiss Re ha fatto fronte a 3 miliardi di dollari di danni provocati dalle numerose calamità naturali verificatesi, in particolare quelli derivati dagli uragani negli Stati Uniti e i tifoni in Giappone.

Nello stesso anno, terminati questi fenomeni, sono sopraggiunti gli incendi in California che hanno colpito aree boschive, residenziali e produttive. In questo caso, gli immobili e le attività commerciali sono stati colpiti da danni per oltre 7 miliardi di dollari.

Stante questo versante legato ai fenomeni naturali, il settore assicurativo e riassicurativo, si trova anche a cogliere le opportunità derivanti dalla nuova realtà che si è ormai delineata: una società ed un'industria sempre più digitalizzate[4].

Il dirompente processo di digitalizzazione di quest'epoca, legato alle tecnologie dell'informazione e della comunicazione, ICT, ha consentito alle aziende di ottenere una maggiore produttività e la possibilità di gestire e sfruttare un'elevata quantità di dati.

Inoltre, ha contribuito a nuove modalità di condivisione e comunicazione delle informazioni ed operativamente a nuove modalità di gestione aziendale, ad esempio, è possibile dirigere un team anche da remoto. Lo sviluppo dell''internet of things (IoT), che ha creato una realtà in cui diversi oggetti di uso comune, come tostapane o frigoriferi intelligenti, sono abilitati ad internet ed interconnessi tra loro. Oppure si pensi ai veicoli, droni e aerei completamente autonomi.

[4] Ania (2019), Banca D'Italia-Ivass (2018), Swiss Re (2017), Accenture, Ponemon Institute LLC (2017)

Questa realtà per l'industria assicurativa rappresenta un'importante occasione per sviluppare un'offerta di coperture assicurative contro il rischio di danni derivanti da incidenti informatici dolosi o accidentali. Infatti, la digitalizzazione oltre ad aver apportato benefici ha anche esposto a nuove minacce.

I settori sensibili al rischio informatico sono aumentati come anche la loro vulnerabilità.

Il Global risks report 2018 del World Economic Forum considera gli attacchi informatici come una delle principali fonti di danni economici dovuti ad interruzioni delle attività nei prossimi cinque anni e li posiziona, in termini di potenziali danni, subito dopo i disastri naturali e gli eventi metereologici estremi.

Col passare del tempo le aziende[5], hanno sempre più acquisito consapevolezza del potenziale rischio di un attacco informatico e quindi di possibili violazioni nei loro sistemi di sicurezza. Di conseguenza, oltre a dotarsi di presidi il più robusti possibili stanno creando un'importante domanda di coperture assicurative cyber. Tra l'altro, i costi complessivi per arginare questi crimini informatici sono in aumento ma spesso le strategie di sicurezza cibernetica adottate, per mettere al riparo reti e sistemi informativi da attacchi indesiderati, non si sono rivelate così efficaci, portando ad importanti perdite.

D'altro canto, garantire la sicurezza di dispositivi e relativi software, non è così facile, di fronte ad attacchi sempre più sofisticati ed in continua mutazione di pari passo con l'evoluzione digitale e tecnologica.

Nello specifico, il rischio informatico è quel rischio di azioni che, sfruttando le vulnerabilità di dispositivi che si avvalgono di queste tecnologie dell'informazione e della comunicazione, possono interrompere la continuità aziendale, accedere indebitamente a big data o compromettere l'integrità di dati sensibili.

Nella sua accezione comprende malfunzionamenti del sistema informatico, infezioni da malware, interruzioni, furti di dati sensibili, cancellazione o alterazione di dati propri o di terzi, frodi e sabotaggi *(Swiss Re Institute 201*7).

Nell'ultimo anno molte aziende hanno subito almeno un attacco ma molte violazioni passano addirittura inosservate.

Se prima i settori a rischio di attacco informatico erano la difesa o comunque gli internet service provider (ISP), ora, gli hacker, motivati meramente da finalità di profitto, attaccano aziende di ogni settore.

[5] Ania (2019)

Nel 2017, più del 50% dei sistemi di controllo di infrastrutture critiche, quali il settore difesa, il settore sanità, il settore dei trasporti ma anche il settore energetico, hanno subito attacchi informatici *(Accenture, 2017).*

Nel 2016, invece, negli Stati Uniti, l'FBI ha ricevuto circa 2500 attacchi ransomware[6].

Il ransomware è un malware diffuso per impedire l'accesso ad un sistema produttivo o a dati informatici fino a che le vittime non pagano una somma di denaro in Bitcoin.

Le aziende digitalizzate sono fortemente vulnerabili a questa estorsione perché la minaccia di interruzione di operazioni, che magari sono critiche e continue e se bloccate potrebbero causare esosi danni economici, induce le vittime a pagare il riscatto.

Proprio nel 2017, come riportato da *The Guardian* si è diffusa la notizia di WannaCry, un ransomware responsabile di un'epidemia su larga scala che ha infettato i sistemi informatici, basati sul sistema operativo Microsoft Windows, di numerose aziende ed organizzazioni in tutto il mondo tra cui numerosi ospedali. Questo malware, una volta criptati i file presenti sul computer, richiedeva, appunto, un riscatto in Bitcoin entro un lasso di tempo, pena la cancellazione di tutti i dati presenti nel computer.

Se in certe realtà industriali, l'interruzione delle attività, il cosiddetto business interruption (BI), o la perdita di dati cruciali per l'ordinario esercizio dell'attività può determinare importanti danni economici, invece, in realtà come gli ospedali, dove, ad esempio, è in aumento l'uso di robot nelle operazioni chirurgiche, un attacco hacker che provoca una business interruption può comportare ben più gravi conseguenze dei danni economici come la perdita di vite umane. Tra l'altro, alcuni dispositivi medici, come i pacemaker, che servono per regolare il battito cardiaco, o i distributori automatici di insulina sono risultati estremamente vulnerabili a cyber attacchi, tanto che alcuni di questi dispositivi sono stati ritirati dal mercato *(Wired, 2018).*

Gli incidenti di sicurezza informatica, i malfunzionamenti, i disservizi prolungati che causano perdite economiche elevatissime, ormai sono all'ordine del giorno. Con lo sviluppo del fintech, a esempio, il settore finanziario, le infrastrutture di mercato e i sistemi di pagamento sono diventati uno dei settori più sensibili al rischio informatico *(Accenture , 2017).* A titolo d'esempio, molti servizi finanziari sono erogati on line, si pensi all'home banking, ed episodi come il furto di credenziali dei conti tramite il phishing o il denial of service, che sovraccarica i server con milioni di richieste di dati per rendere inutilizzabili i servizi bancari, sono molto diffusi.

[6] Nbcnews

Negli anni 2016 e 2017 si sono verificati ripetuti attacchi al circuito SWIFT che hanno causato il furto di numerosi milioni da varie banche centrali e nel 2017 Unicredit è stata bersaglio di un attacco hacker che ha portato all'acquisizione indebita di dati anagrafici e codici IBAN relativi a 300 mila clienti, dati che potrebbero essere utilizzati per attacchi di phishing via email, come riportato da *Il Sole 24 ore (2017).*

Invece, a Febbraio di quest'anno, secondo il *Corriere di Malta,* anche la Bank of Valletta ha subito un pesante attacco attraverso il quale i cyber criminali hanno tentato di rubare circa 14 milioni tramite un trasferimento illecito verso banche situate in Hong Kong.

Come conseguenza di questo evento, la banca è stata costretta a sospendere tutte le funzioni, tutti i servizi ed a chiudere le filiali.

In tutti questi attacchi non c'è stata alcuna intrusione nei conti correnti ma questi eventi evidenziano come nessuno è ormai immune da questo rischio e le conseguenze potevano essere ben più importanti.

I danni al settore finanziario, dovuti a questi attacchi informatici, possono provocare crisi sistemiche. Oltre ai danni materiali diretti si deve tenere conto anche dei danni derivanti dalla diffusione di una percezione di insicurezza che può provocare sconvolgimenti nei mercati.

La spesa per dotarsi di avanzati sistemi di sicurezza informatica, la complessità e la sofisticazione degli attacchi stanno aumentando ma, come mostrato, le misure messe in atto da parte delle organizzazioni risultano spesso inefficaci.

Dietro a questi attacchi non c'è più l'hacker solitario ma spesso ci sono vere e proprie organizzazioni criminali. Infatti, se prima l'hacker era visto come una figura specializzata, isolata con competenze IT che agiva in proprio autofinanziando i propri attacchi guidato dalla fama, adesso sono comparse vere e proprie organizzazioni criminali che hanno accesso a risorse significative e che hanno scoperto quanto possa essere redditizio mettere a frutto un attacco.

Inoltre, spesso questi criminali sono addirittura finanziati da uno stato che desidera ad esempio perturbare un intero mercato, influenzare le elezioni politiche o addirittura possono essere finanziati da realtà aziendali con finalità di spionaggio in modo tale da mettere in pratica una concorrenza sleale, carpendo informazioni segrete per eliminare dal mercato il concorrente.

E' diffusa la vendita dei dati rubati sul mercato nero oppure la divulgazione di informazioni sensibili che possono ad esempio incidere sulle quotazioni azionarie. E sono proprio ad

essere più a rischio i dati sensibili ossia quei dati che sono conservati in forma digitale che possono essere sottratti, alterati o addirittura distrutti.

La sicurezza informatica, nella maggior parte dei casi, viene esternalizzata, ma il coinvolgimento di figure terze nell'erogazione dei servizi legati alla sicurezza dei sistemi informatici di un'azienda è anch'esso una fonte di rischio perché questi appaltatori potrebbero sfruttare indebitamente l'accesso a dati e processi critici.

Uno studio effettuato dalla Banca d'Italia (2017), contenuto nel documento *Cyber attacks: preliminary evidence from the Bank of Italy's business surveys,* ha evidenziato come un ente su tre dichiari di essere stato vittima di un attacco informatico nell'arco di un anno. Il problema è che spesso le imprese che non dichiarano attacchi potrebbero non essere consapevoli di aver subito un attacco, quindi il numero di attacchi potrebbe essere ben più alto di quanto registrato recentemente.

Le organizzazioni più esposte al rischio informatico sono soprattutto quelle di elevate dimensioni in quanto gestiscono una massa di dati più elevata rispetto a quelle di più piccole dimensioni. I costi di un attacco informatico potrebbero portare al fallimento dell'impresa in quanto causano enormi danni reputazionali che si traducono in ulteriori danni economici per la stessa per perdita di clienti e conseguenti rischio di liquidità e rischio legale.

Ci sono pressioni normative verso l'adozione di efficaci presidi del rischio informatico ed il riconoscimento delle responsabilità interne per i danni determinati da una violazione del sistema. Il nuovo regolamento UE sulla protezione dei dati, 2016/679, in vigore dal 2018, è stato introdotto proprio come "argine" del rischio informatico.

Questo regolamento impone a chi custodisce e tratta dati sensibili l'adozione di presidi atti alla salvaguardia ed alla protezione dei dati personali, obbligandoli ad una vera e propria mappatura dei potenziali rischi informatici, una formalizzazione dei protocolli interni e la formalizzazione delle diverse responsabilità nel processo finalizzato al trattamento dei dati personali che prevede la loro raccolta, elaborazione e conservazione. Inoltre, si accompagna ad un pesante apparato sanzionatorio.

Da un'analisi effettuata da *Artemis (2015)* le società potrebbero avere bisogno in futuro di polizze di assicurazione del rischio cyber che forniscano una copertura fino ad 1 miliardo. E questo numero è credibile se si pensa a multinazionali o comunque a realtà con una significativa quantità di dati sensibili oppure ai sistemi di pagamento elettronico che potrebbero essere compromessi.

Al momento però non esistono polizze di assicurazione che forniscano più di 300 milioni di copertura assicurativa. Ed i costi potenziali derivanti da un attacco hacker sono ben più alti e queste polizze dunque risultano insoddisfacenti.

1.2 Il ruolo delle ILS nella gestione del rischio assicurativo non-life[7]

Negli anni 90', dopo il terremoto di Northbridge, Stati Uniti, che provocò 40 miliardi di perdite assicurate[8], le imprese di riassicurazione posero un freno all'offerta di copertura riassicurativa in quella zona così ad alto rischio, creando un vero e proprio "collo di bottiglia". L'offerta assicurativa di conseguenza si ridusse notevolmente, non trovando copertura sul mercato riassicurativo. E le esigue coperture assicurative reperibili sul mercato erano offerte in cambio di premi elevatissimi.

Da questo contesto si diffonde tra i partecipanti al mercato assicurativo, proprio per un'esigenza operativa, la tecnica di cartolarizzazione dei rischi considerati sistemici.

Attraverso la cartolarizzazione, le compagnie di assicurazione dirette ed indirette possono ampliare la loro capacità di assunzione di questi rischi e al tempo stesso liberare capitale trasferendo le loro esposizioni al mercato finanziario.

La cartolarizzazione[9], infatti, in questo caso permette il trasferimento dei rischi puri da un mercato all'altro attraverso "l'atomizzazione" ovvero la riduzione in piccole parti dei rischi sistemici ed il successivo trasferimento di questi all'esterno del settore assicurativo.

Questa tecnica, che si è affermata nel settore assicurativo proprio come soluzione a colli di bottiglia nel mercato riassicurativo, ramo danni in particolare, è diventata popolare dapprima nel settore bancario americano, attraverso l'emissione dei mortgage backed securities, la cartolarizzione dei mutui ipotecari più rischiosi attraverso il pooling dei crediti relativi a queste attività illiquide e la loro trasformazione in titoli negoziabili sul mercato dei capitali.

La cartolarizzazione assicurativa si differenzia però dalla cartolarizzazione bancaria tradizionale in quanto in ambito assicurativo non vengono cartolarizzati dei crediti ma vengono cartolarizzati dei veri e propri rischi puri. Quindi si accosta maggiormente alla cartolarizzazione sintetica che produce le credit linked notes che inglobano il solo rischio di credito, al contrario della cartolarizzazione tradizionale che trasferisce direttamente il credito inglobante tale rischio.

---

[7] Albertini, Bareue (2009), OECD(2005)
[8] Eguchi et al. (1998)
[9] Borsa Italiana, glossario finanziario

L'output della insurance e reinsurance securitization è la nascita di una nuova categoria di asset class denominata Insurance Linked Securities.

Questa categoria di strumenti favorisce la copertura assicurativa delle tipologie di rischio che stanno emergendo con lo sviluppo tecnologico e con il cambiamento climatico ovvero il rischio nat-cat ed il rischio informatico.

Le ILS, come indicato dalla letteratura, in particolare Holzheu., Karl and Helfenstein (2006), Cummins (2007), Edesess(2014) e MacMinn (2009), sono prodotti negoziabili che consentono ad assicuratori e riassicuratori, quest'ultimi attuando un'innovativa retrocessione dei rischi, attraverso il trasferimento del rischio assicurativo sul mercato dei capitali, di ricavare quei fondi utili per procedere agli indennizzi relativi a quei sinistri derivanti da catastrofi naturali e da altri eventi calamitosi.

Il mercato delle ILS ha visto una costante crescita dal 1990 al 2007 e attualmente può considerarsi non ancora maturo ma in costante espansione *(Albertini and Bareau 2009).*

Nei rami danni la forma di cartolarizzazione che ha avuto una maggiore penetrazione nel mercato dei capitali è sicuramente il catastrophe bond, un titolo obbligazionario, legato al verificarsi di sinistri di natura catastrofale, che incorpora un'opzione call il cui sottostante però non è negoziabile come invece risulta essere quello dei derivati tradizionali *(Cummins, 2007).*

Le obbligazioni catastrofali sono strutturate proprio in forma di "asset" backed securities[10] **,** ma in questo caso sono liability backed securities, ovvero sono strumenti finanziari emessi a fronte di operazioni di cartolarizzazione.

L'impetuoso affermarsi della digitalizzazione e dello sviluppo tecnologico ha reso oggetto di cartolarizzazione e trasferimento al mercato non più soltanto il rischio catastrofale legato ai disastri naturali ma anche il rischio operativo incorporante il rischio informatico, come dimostrato anche dalle recenti transazioni.[11]

Tradizionalmente, ad esempio, il rischio informatico viene incluso nel novero dei rischi operativi oggetto di costosi presidi, molti dei quali risultando inefficaci, procurano perdite esose a imprese non finanziarie e finanziarie che quindi ne domandano la copertura al mercato assicurativo.

[10] Cummins(2008)

[11] Artemis:

- *Credit Suisse's Operational Re transaction (2016)*
- *Baltic PCC Limited (2019*), in questo caso è stato trasferito mediante cat bond di tipo indemnity il rischio terrorimo, incluso il cyber terrorismo

Nel 2016 la banca d'affari Credit Suisse tramite la compagnia assicurativa Zurich si è rivolta al mercato delle ILS per garantirsi una copertura assicurativa e riassicurativa dei propri rischi operativi tra i quali spicca il rischio informatico.

La forma di cartolarizzazione scelta è proprio un catastrophe bond che trasferisce ai sottoscrittori di questo titolo una parte dell'esposizione al rischio operativo di Credit Suisse.

Il cyber risk offre opportunità di crescita al mercato delle ILS maggiori di quelle che offre il nat-cat risk, quindi in un prossimo futuro si vedranno sul mercato maggiori volumi di cyber catastrophe bond, ovvero cat bond che trasferiscono direttamente il rischio informatico stand alone. Fino ad oggi non ci sono ancora state emissioni di questo tipo.

In Italia la *securitization* è disciplinata dalla legge numero 130 del 1999 e questo processo permette appunto alla società di scorporare dal bilancio parte dei rischi che vengono impacchettati o atomizzati e ceduti sul mercato per mezzo di una società veicolo.

In questa operazione il risk protection seeker, colui che è in cerca all'esterno di una copertura del rischio è denominato cedente o sponsor.

Il cedente non necessariamente è una compagnia assicurativa o riassicurativa ma può essere qualsiasi agente economico che utilizza questa tecnica per trasferire il rischio ad un altro mercato.

Ad esempio,[12] la Oriental Land Company che è proprietaria di Tokyo Disneyland ha usato questa tecnica per proteggersi dai danni che avrebbe potuto provocare un terremoto.

Oppure la FIFA, la Federazione Internazionale delle associazioni calcistiche, che ha utilizzato questa tecnica emettendo (indirettamente perché l'emittente diretto in ogni operazione è una società giuridicamente diversa) un'obbligazione catastrofale per un valore di 260 milioni di dollari per coprirsi contro l'eventualità che il campionato mondiale di calcio dei mondiali del 2002, svoltosi in Corea del Sud ed in Giappone, potesse essere cancellato a causa di attacchi terroristici. Anche la Metropolitan Transportation Authority di New York, società pubblica responsabile del trasporto, ha fatto ricorso all'emissione di un catastrophe bond per un valore di 200 milioni di dollari per proteggere il sistema metropolitano dal rischio di alluvioni, in quanto le assicurazioni si sono rifiutate di assumersi tale rischio per via della mancanza di coperture riassicurative.

Per quanto riguarda, invece, le compagnie assicurative e riassicurative, Allianz ad esempio nel 2013 ha emesso un catastrophe bond per un valore di 275 milioni di euro per proteggersi dai rischi di perdite per danni collegati sia agli uragani negli Stati Uniti, nei Caraibi e nel Messico sia ai terremoti in Canada e negli Usa. UnipolSai, invece, nel 2015 ha emesso

[12] European Commission, Derris (2016*)*

indirettamente catastrophe bonds per 200 milioni di euro per coprirsi dal rischio sismico in Italia e nei paesi limitrofi. Operando in questo modo, gli assicuratori riescono ad eliminare quel rischio residuo che non sono riusciti a coprire attraverso il tradizionale pooling dei rischi.
Nel mercato delle Insurance Linked Securities gli sponsor creano l'offerta di titoli e gli investitori istituzionali tra cui fondi specializzati, fondi hedge, banche, fondi pensione e compagnie assicurative e riassicurative generano la domanda. E' un mercato over the counter quindi ci sono problemi di trasparenza.
Questi titoli vengono sottoscritti dagli investitori nel mercato dei capitali e sono quindi proprio gli investitori a fornire "indirettamente" la copertura, assumendo il ruolo di protection seller.
I cash flow legati a questi titoli dipendono dall'accadimento o meno dell'evento assicurativo sottostante che può essere ad esempio una calamità naturale come un terremoto, uno tsunami, le alluvioni oppure il sottostante può essere un rischio operativo che ingloba il rischio informatico. Se l'evento predefinito contrattualmente e sottostante lo strumento non si verifica entro un determinato periodo di tempo, gli investitori ricevono il rimborso del capitale a scadenza e durante il periodo di esposizione al rischio ricevono un flusso di pagamenti, dette cedole. Se invece si verifica l'evento, il valore nominale dello strumento viene utilizzato per coprire le perdite subite dalla compagnia e l'investitore perde gli interessi e/o il capitale.
L'emissione di ILS aumenta ogni qualvolta si verificano eventi che provocano colli di bottiglia nel mercato riassicurativo. Esempi[13] di questa connessione sono mostrati nel 2001 dopo l'attacco al World Trade Center di New York che ha ridotto enormemente la disponibilità di capacità riassicurativa del ramo danni determinando un aumento delle emissioni pari a 2 miliardi di dollari.
Nel 2007, invece, a seguito dell'uragano Katrina l'emissione è raddoppiata fino a raggiungere il picco pari 7 miliardi di dollari.
Solo nel 2008, anno centrale della crisi finanziaria globale, i volumi di emissione si sono pesantemente ridotti per via della sfiducia da parte degli investitori verso il mercato globale in seguito a questo evento.

[13] Albertini and Bareau (2009)

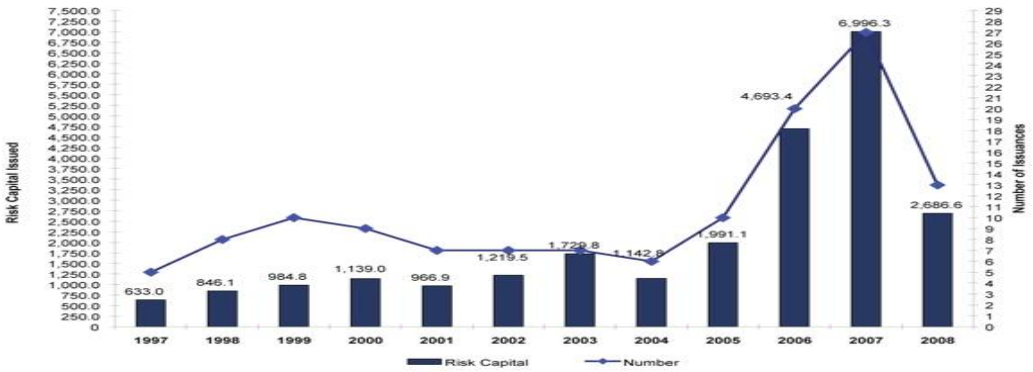

Figura 3: *Numero annuale di transazioni e size dell'emissione in milioni di dollari (GC Securities Proprietary Database)*

La flessione nei volumi di vendita tra il 2007 e il 2008 è riportata in figura 3.

Poi nel 2014, come mostrato in figura 4, sono state effettuate nuove operazioni per una raccolta complessiva di oltre 7 miliardi di dollari. Nello stesso anno il volume totale delle emissioni ha raggiunto quasi i 10 miliardi di dollari, superando l'ammontare complessivo del 2013 pari a 6,7 miliardi. Dalla nascita del mercato al 2014 il volume complessivo delle emissioni era pari a 65 miliardi di dollari.

La massa di titoli ILS nel 2018 è ulteriormente aumentata, Willis Re ILS (2019) stima che il volume complessivo di ILS si sta rapidamente avvicinando alla soglia dei 100 miliardi di dollari.

Figura 4: *Valore dei CAT bonds in circolazione in miliardi di dollari (Willis RE, 2019)*

La cartolarizzazione assicurativa è diventata ormai una strategia di risk management molto diffusa sia perchè fornisce maggiori risorse attraverso la creazione delle Insurance Linked Securities sia perché l'output, rappresentato dalle ILS, si configura come una categoria di strumenti che non sono correlati all'andamento dei mercati finanziari.

Offrono, di solito, un elevato rendimento corretto per il rischio maggiore rispetto a quelli di mercato. L'indice che misura la performance dei catastrophe bonds è lo Swiss Re Cat Bonds Index.

Il tasso di rendimento è composto dal Libor oppure Euribor, il risk free rate garantito da uno swap, e da un risk premium o spread legato al rischio assunto cioè l'accadimento incerto dell'evento che dipende da una probabilità di avveramento di difficile stima.

Presentano una correlazione con gli altri potenziali asset in portafoglio molto bassa. Ciò permette di sfruttare la proprietà di diversificazione e quindi di migliorare il profilo rischio-rendimento del portafoglio. La bassa correlazione è dovuta al fatto che i rendimenti delle ILS dipendono innanzitutto dall'accadimento o meno delle catastrofi naturali o informatiche, si pensi ad esempio al rischio per cui una parte significativa dell'ITC sia fuori uso, e non hanno generalmente alcuna relazione con i fattori che influenzano ad esempio il rendimento di azioni o di corporate bonds. Di conseguenza l'inserimento di questi titoli in portafoglio sposta verso l'alto la frontiera efficiente, come dimostrato dalla figura 5, frutto di un'analisi prodotta da Artemis[14]. E questo consente l'ottenimento di un migliore rendimento del portafoglio a parità di rischio oppure una diminuzione del rischio del portafoglio a parità di rendimento.

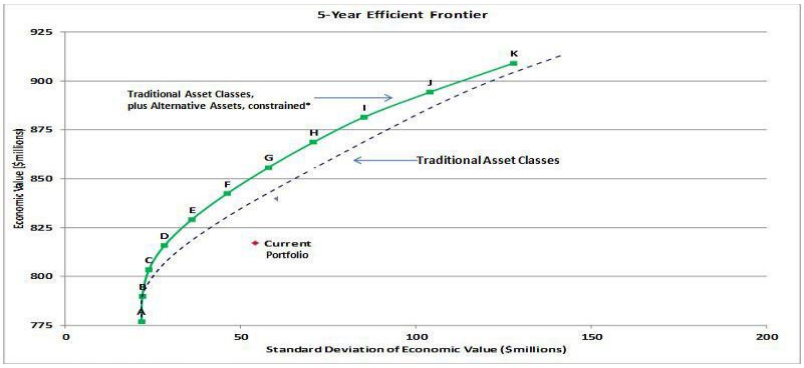

Figura 5: *Impatto dovuto all'inserimento in portafoglio di strumenti ILS (Conning Advise, ERM analysis)*

Però se a livello macro si può sostenere ad esempio che le calamità naturali non causino turbolenze finanziarie e viceversa, invece a livello micro potrebbero esserci delle correlazioni.

Ad esempio, se si verificasse un terremoto in Giappone, è molto probabile che questo abbia impatti negativi su alcuni titoli giapponesi.

[14] Artemis (2015)

Un uragano potrebbe danneggiare gli impianti utilizzati nella lavorazione del petrolio e questo ovviamente causerebbe un rialzo del prezzo del greggio e a sua volta ciò causerebbe altri impatti a catena sui titoli dei produttori di questa materia prima e sui titoli collegati ai settori altamente dipendenti da questa risorsa. Oppure, se si verificasse un terremoto nella Silicon Valley, questo potrebbe comportare un certo impatto negativo sui titoli legati al settore ICT. Quindi è comunque necessario puntare su una diversificazione a livello internazionale cioè anche a livello geografico, per far sì che gli eventi metereologici sottostanti a questi strumenti abbiano effettivamente una bassa correlazione con le altre asset class in portafoglio.
Questi strumenti innovativi non devono essere inquadrati dal punto di vista strategico come sostituti delle tradizionali modalità di trasferimento del rischio ma come strumenti integrativi della riassicurazione e della retrocessione in quanto forniscono alle imprese assicurative e riassicurative maggiori capacità di assunzione del rischio.

1.3. Riassicurazione e cartolarizzazione assicurativa a confronto[15]

Non sempre la compagnia assicurativa riesce ad ottenere una diversificazione tale da ridurre il rischio dal portafoglio.
Ci sono, infatti, coperture assicurative che presentano una correlazione significativa in quanto certi eventi oppure la stessa innovazione normativa possono incidere simultaneamente su molte polizze.
A titolo d'esempio, le polizze di assicurazione da responsabilità civile, seppur diversificate geograficamente su un paese, una volta che è intervenuta una modifica legislativa sulla responsabilità, ne sono influenzate simultaneamente tutte.
L'assicurazione da catastrofi naturali o antropiche, in particolare rischio catastrofale informatico, presentano una più alta correlazione con gli altri rischi, le polizze tradizionali che coprono danni a beni diversi potrebbero, infatti, essere tutte colpite da uno stesso evento sistemico, la calamità naturale o un attacco informatico su larga scala.
Questi rischi, quindi, da cui scaturiscono i sinistri, non sono indipendenti e quindi l'ente assicurativo non riesce né a diversificare né a fare operare la legge dei grandi numeri.
La prima permette di ridurre notevolmente, se non azzerare, il rischio marginale assunto e inserito all'interno di un portafoglio di asset, nel caso, infatti, di asset dipendenti,

[15] Albertini and Bareue (2009), Donati, Volpe Putzolu (2015), Paci (2018), Braun and Weber (2017)

l'unexpected loss di portafoglio, invece di essere minore della somma delle singole unexpected loss marginali imputate ai singoli rischi stand alone, risulterà uguale a tale somma. Al contrario, se il portafoglio fosse costituito da asset indipendenti allora si otterrebbe un'unexpected loss a livello di portafoglio minore della somma suddetta e quindi un minore rischio complessivo.

Per quanto riguarda la seconda, la compagnia assicurativa riesce a sfruttare la legge dei grandi numeri solo se opera secondo il principio del pooling dei rischi e quindi se conclude contratti assicurativi che permettono l'assunzione di rischi tra loro omogenei, cioè rischi con probabilità di accadimento ed entità del danno simili, ed indipendenti.

Solo queste due proprietà riproducono proprio il tendere all'infinito del numero delle prove che attivano la legge statistica che permette alle imprese di assicurazione di giungere alla stima della perdita con una certa precisione che cresce all'aumentare del numero dei rischi assunti e, di conseguenza, determinano correttamente il premio cioè il prezzo che gli assicurati devono pagare per coprirsi dal rischio.

La compagnia assicurativa è messa, comunque, nelle condizioni di assumere questi rischi adottando diverse strategie di esternalizzazione di questi come la cartolarizzazione e la riassicurazione tradizionale.

L'entrata in vigore di Solvency II, come indicato da Braun and Weber (2017), ha spinto verso il canale alternativo della cartolarizzazione, infatti è possibile tenere conto nel calcolo del coefficiente di solvibilità degli strumenti ILS in modo tale da ridurre il requisito patrimoniale proprio come permette un tradizionale contratto di riassicurazione.

La cartolarizzazione e la riassicurazione sono operazioni molto simili in quanto basate su un meccanismo di trasferimento dei rischi. Ma ciò che le rende due differenti modalità di risk management è il fatto che l'output della cartolarizzazione è un distinto asset negoziabile sul mercato e ciò quindi rende più debole il legame tra cedente e sottoscrittore del rischio, rispetto alla riassicurazione che può prevedere invece dei legami duraturi formalizzati in trattati. Infatti, l'investitore in Insurance Linked Securities, al contrario di ciò che accade per la compagnia riassicurativa, può vendere il bond nel mercato secondario in cui sono negoziati questi titoli che hanno come sottostante i rischi assicurativi. Invece la compagnia riassicurativa può solo tentare una retrocessione del rischio stesso.

La riassicurazione è un'attività prettamente indiretta, cioè un'attività "all'ingrosso" in quanto consiste nell'assunzione sistematica di rischi non della clientela retail ma di imprese di assicurazione. Quindi il rapporto è tra imprese.

Il contratto di riassicurazione prevede la cessione dei rischi assunti dall'impresa di assicurazione, che assume la posizione di riassicurato, ad un riassicuratore.
La riassicurazione può quindi considerarsi uno strumento di hedging per la compagnia.
Il riassicuratore non ha alcun rapporto con l'assicurato o con il beneficiario della compagnia riassicurata. Al verificarsi del sinistro, la compagnia assicurativa liquida il danno al beneficiario mentre l'impresa di riassicurazione rimborsa l'assicuratore per la parte pattuita e collegata al rischio trasferito.
Grazie alle sue grandi dimensioni la compagnia riassicurativa riesce a raggiungere un elevato livello di diversificazione che le permette l'assunzione di maggiori rischi.
Nel mercato, infatti, prevalgono operatori specializzati che esercitano esclusivamente attività riassicurativa, in quanto è necessaria una certa dimensione per poter realizzare la legge debole dei grandi numeri.
L'impresa di assicurazione, se ha a disposizione un'ampia offerta riassicurativa è messa nelle condizioni di poter assumere rischi sistemici come i rischi nat-cat ed informatico, perché il riassicuratore si assume parte di questi rischi. Ma la compagnia riassicurativa pur avendo la capacità e le risorse per assumersi tali rischi non sempre offre capacità riassicurativa perché non riesce ad assumere tanti e indipendenti rischi e quindi, per gli stessi problemi mostrati precedentemente, non riesce a realizzare quella vitale diversificazione che a maggior ragione nemmeno la compagnia assicurativa diretta riesce a realizzare.
La compagnia riassicurativa ha comunque più possibilità di ottenere una diversificazione maggiore assumendo rischi in diverse aree geografiche, ad esempio, rispetto ad una compagnia assicurativa che opera a livello di singolo territorio.
La riassicurazione tradizionale, come modalità di gestione del rischio, diventa indispensabile, soprattutto, quando il portafoglio di rischi è ridotto e quindi l'impresa di assicurazione primaria è di piccole dimensioni oppure in occasione di nuove coperture assicurative richieste dal mercato come la richiesta attuale di copertura assicurativa cyber.
Si distinguono due modalità di riassicurazione, quella proporzionale e quella non proporzionale.
La riassicurazione proporzionale consiste in una vera e propria ripartizione proporzionale dei rischi in termini di "affari" secondo una quota proporzionale prestabilita mentre quella non proporzionale in una ripartizione dei danni. La proporzionale, quindi, si distingue da quella non proporzionale per il fatto di prevedere il trasferimento dei premi.

La riassicurazione proporzionale, a sua volta, viene distinta in riassicurazione per quota e per eccedente.
La cessione per quota consiste in un trasferimento di una percentuale prestabilita di premi e di futuri risarcimenti relativi ad un ramo.
Invece, nella cessione per eccedente l'assicuratore conserva i rischi assicurati fino ad un determinato ammontare e solo sulla quota eccedente viene applicata la percentuale fissata.
La riassicurazione non proporzionale, invece, prevede esclusivamente la ripartizione dei soli sinistri e non dei premi e si distingue a sua volta in eccedente per singoli sinistri, excess loss, e per eccesso di perdita, stop loss.
Nel primo caso, si fissa una soglia per cui se uno specifico sinistro è superiore ad un certo valore allora interviene la copertura riassicurativa per le perdite eccedenti.
Nel secondo caso, si fa riferimento ad un portafoglio di rischi o un ramo, quindi il riassicuratore copre una perdita relativa alla gestione assicurativa e non più relativa ad un singolo evento.
Solvency II, nel calcolo del requisito patrimoniale, tiene conto del ricorso alla copertura riassicurativa e quindi questa modalità di gestione del rischio ha importanti riflessi sul capitale da detenere, di conseguenza ha valenza strategica.
La riassicurazione è stata la forma di copertura più utilizzata per il rischio catastrofale fino agli anni 90, quando, diversi eventi naturali estremi hanno causato numerose insolvenze tra i riassicuratori che a catena hanno contagiato l'intero settore.
Come conseguenza di questo, la riassicurazione è divenuta molto costosa e l'offerta sul mercato si è notevolmente ridotta.
Quando il mercato riassicurativo non è più disponibile ad assumere rischi sistemici, per le ragioni precedentemente esposte, si ricorre alla copertura alternativa, frutto dell'innovazione finanziaria, ossia alla cartolarizzazione assicurativa che porta alla creazione delle ILS.
Gli strumenti ILS sono molto più flessibili rispetto ai contratti di riassicurazione.
Intanto, la riassicurazione presenta potenzialmente un rischio di credito e un rischio di moral hazard molto elevati ed un rischio base nullo. Invece, le ILS, a seconda della struttura alla base del prodotto, quindi questo non vale per tutti gli strumenti, possono considerarsi strumenti a rischio di credito e rischio di moral hazard nulli e con un rischio base elevato.
Il rischio di moral hazard è presente nei contratti di riassicurazione quando, essendoci una copertura riassicurativa, l'assicurato-impresa di assicurazione non assume un atteggiamento volto a ridurre la probabilità di richieste di indennizzo e quindi assume un comportamento negligente. Ad esempio, una volta stipulato il contratto di riassicurazione, la

compagnia di assicurazione, nella sottoscrizione delle polizze, potrebbe offrire coperture in zone ad elevato rischio oppure potrebbe essere eccessivamente generosa nel processo di liquidazione dei sinistri per evitare costose controversie legali e perdita di clienti. Infatti, il moral hazard sorge anche quando, dopo l'accadimento del sinistro, l'assicuratore gestisce in modo negligente il processo di liquidazione in quanto, ad esempio, non controlla le richieste di indennizzo che potrebbero essere delle vere e proprie frodi messe in atto dagli assicurati.

Tali abusi in aggiunta ai danni causati dagli eventi possono portare addirittura all'insolvenza del riassicuratore.

Quest'ultimo, per tutelarsi da questo rischio di azzardo morale, aumenta ex-ante i premi riassicurativi rendendo quindi spesso questa strategia di hedging inaccessibile alle imprese di più piccole dimensioni. Invece, nelle ILS, generalmente questo tipo di rischio viene ridotto in misura maggiore in quanto prevedono diversi presidi contro l'azzardo morale come l'indicizzazione del pagamento alle perdite dell'intero settore assicurativo (industry losses) che elimina del tutto il moral hazard rispetto ad un pagamento strettamente legato alle perdite effettive sostenute dal singolo sponsor.

Nella tradizionale riassicurazione, il rischio di credito è molto alto, in quanto, al verificarsi dell'evento catastrofale, probabilmente questo scatenerà una serie di richieste di indennizzi su molti dei contratti in capo alla compagnia riassicurativa che potrebbe, quindi, non essere in grado di onorare le sue obbligazioni. Ad esempio, il contratto di riassicurazione stop loss, secondo il quale al verificarsi dei sinistri di un ramo o di una parte di esso oltre un certo importo determina l'intervento del riassicuratore, espone la compagnia assicurativa ad un elevato rischio di credito in quanto l'intervento del riassicuratore avviene nel momento in cui il livello di perdite è nella parte più a destra della loss distribution dell'assicuratore, quindi si tratta di coprire un elevato valore di perdita, e quindi l'accadimento di tali eventi estremi potrebbe causare numerose insolvenze in capo a riassicuratori ed assicuratori, se l'impresa riassicurativa non ha capitale sufficiente da coprire tali perdite trasferite. Ed il numero di insolvenze, ovviamente, aumenta all'aumentare della dimensione della perdita trasferita.

Invece, gli strumenti ILS, garantiscono in modo efficace la responsabilità dello special purpose vehicle[16], la società emittente i titoli, perché l'operazione è strutturata in modo tale

[16] "Per società veicolo si intende l'impresa, diversa da un'impresa di assicurazione o di riassicurazione, che assume i rischi ceduti da imprese di assicurazione o di riassicurazione e che finanzia integralmente la sua esposizione a tali rischi mediante l'emissione di strumenti finanziari, il cui rimborso ai detentori è subordinato agli obblighi di riassicurazione della società veicolo".
Tali società necessitano di un'autorizzazione per l'esercizio di questa attività, in quanto tale società seppur esercitante un'attività di "cartolarizzazione", consistente nel collocamento di strumenti finanziari, può

da garantire il pagamento dovuto dal cessionario, in quanto i proventi, derivanti dall'emissione, sono vincolati in un conto fiduciario o fondo garanzia o separati mediante un trust ed investiti in free risk assets o comunque titolo con alto rating.

Inoltre, la riassicurazione è un contratto in generale bilaterale in cui viene trasferito il rischio sulla base di certe condizioni dove è necessaria una disclosure, una condivisone di informazioni e di valutazioni effettuate da entrambe le parti.

Quindi, se le parti, ad esempio, non hanno aspettative simili sull'output del modello catastrofale interno e sulle perdite, non si riesce a trovare un accordo, di conseguenza il contratto di riassicurazione non viene stipulato e la compagnia assicurativa probabilmente ridurrà l'offerta di copertura.

Invece, per quanto riguarda le ILS, la misurazione del rischio è spesso generata, quindi garantita, da società indipendenti, esterne. Ciò, rende più accettabili e condivisibili gli output. E gli stessi output sono ulteriormente valutati, come anche la robustezza del modello catastrofale stesso, dalle agenzie di rating. Quindi viene garantita una certa affidabilità ed una maggiore trasparenza.

Nella riassicurazione, invece, non è rilevabile il rischio base, quel rischio per cui il pagamento derivante dalla copertura non corrisponde alla reale perdita subita e quindi sussiste la mancanza di un perfetto hedging. Al contrario, in un catastrophe bond con un attachment point di tipo industry loss trigger, il pagamento è basato sulle perdite del settore piuttosto che sulle perdite particolari dello sponsor e quindi è presente il rischio base in una certa misura. L'entità di tale rischio dipenderà dalla correlazione esistente tra perdita del settore e perdita dello sponsor: più bassa è questa correlazione e più alto sarà il rischio base. Molti studiosi, tra cui Neil A. Doherty (2000), individuano una certa correlazione negativa tra rischio base e rischio di moral hazard: più alto è il rischio base e più basso sarà il rischio di azzardo morale. Inoltre, è stato riscontrato un legame tra il livello dello spread che va a comporre assieme all'Euribor il rendimento del catastrophe bond e il costo della riassicurazione. La definizione dello spread è correlata positivamente al costo della riassicurazione nel momento in cui viene emesso il bond.

I prezzi della riassicurazione dipendono dalle condizioni del mercato: se la capacità di assunzione dei rischi si riduce, perché ad esempio gli indennizzi si sono rivelati superiori alle attese riducendo notevolmente il capitale a disposizione delle compagnie riassicurative, allora si verificherà un incremento dei prezzi. Se il costo delle coperture aumenta, anche gli

considerarsi esercitante un'attività pressochè riassicurativa nei confronti delle cedenti il rischio. (Donati, Volpe Putzolu (2012)

spread dei cat bonds aumenteranno, se invece si assiste ad un ciclo opposto cioè ad una diminuzione del costo delle coperture allora conseguirà un decremento degli spread. Tra il 2017 e il 2018, come mostrato nella figura 6 tratta dal report di Aon Benfield(2018), il mercato della riassicurazione tradizionale si è ridotto a causa dell'aumento dei premi dovuti ai numerosi eventi metereologici estremi del 2017 come gli uragani atlantici Harvey, Irma, Maria e Ophelia.

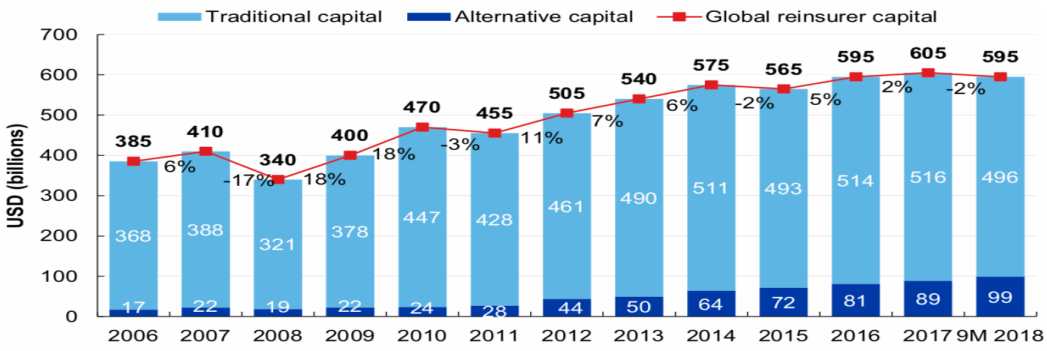

Figura 6 Capitale complessivo da riassicurazione in miliardi di dollari nel 2018 (AON)

Il capitale complessivo da riassicurazione si è ridotto del 2 % nel 2018 ma nonostante questo restringimento comunque il mercato rimane piuttosto capitalizzato.

Invece, il capitale derivante dagli strumenti ILS è cresciuto fino a raggiungere i 99 miliardi a fine 2018.

In definitiva, ciò che si può trarre è il fatto che cartolarizzazione e riassicurazione sono due canali di trasferimento del rischio che possono coesistere, infatti l'assicuratore può trasferire parte della sua esposizione all'impresa di riassicurazione ad esempio contro il pagamento di un premio ed il riassicuratore può a sua volta trasferire il rischio attraverso la retrocessione oppure la cartolarizzazione, trasferendo quindi il rischio sul mercato dei capitali.

Il riassicuratore emetterà questi strumenti alternativi solo se questi gli permettono di trasferire la parte di rischio non diversificabile. Quindi, in entrambi i settori la cartolarizzazione è inquadrata come un complemento ai canali tradizionali.

Capitolo 2

Misurazione e gestione del rischio nat-cat

2.1 Teoria dei valori estremi (ETV)

In questo capitolo presentiamo un approccio, noto come Teoria dei Valori Estremi, per l'analisi di eventi rari quali le catastrofi naturali.
Per una presentazione estensiva di questo argomento si rinvia a Mcneil et al. (2005) ed Embrechts et al. (1997).
Gli eventi considerati estremi, in quanto causanti una perdita significativa, sono rari, con conseguente mancanza di dati empirici.
Per sopperire a questa mancanza si utilizzano metodi simulativi attraverso i quali si crea un catalogo di eventi sintetici detto *ensemble* su cui fare inferenza.
Questo metodo consente una visione probabilistica della perdita dovuta a eventi catastrofali, oltre a fornire informazioni sui presidi idonei a mitigare tali rischi.
La simulazione di tali rischi è effettuata attraverso il modello catastrofale, un framework risultante dalla combinazione di diversi modelli statistici e fisici orientato alla produzione di stime probabilistiche sui fenomeni stocastici naturali e man made.
Input iniziali del processo di inferenza e modellizzazione del rischio sono i dati storici sui parametri fisici dell'evento naturale, in particolare ciò che rileva per le catastrofi sono i valori estremi, ad esempio il massimo valore delle precipitazioni o il massimo valore della velocità del vento, e quindi le code della distribuzione di una variabile casuale.
Tale analisi iniziale è supportata dalla Extreme Value Theory, uno schema statistico, che permette la modellizzazione di questi eventi rari ed estremi attraverso due approcci alternativi: il metodo block maxima ed il metodo Peak Over Threshold (POT).
E' una teoria che può essere considerata complementare al teorema del limite centrale, secondo cui la somma di v.a. i.i.d. standardizzata converge per n che tende all'infinito alla distribuzione normale indipendentemente dalle funzioni di probabilità delle v.a. considerate nella somma, in quanto individua la distribuzione limite a cui converge la distribuzione dei valori massimi, cioè degli eventi estremi, di una sequenza di variabili aleatorie X_i iid, indipendentemente dalla loro $f(x)$.

2.1.1 Metodo Block Maxima

Finalità del metodo parametrico Block Maxima è l'identificazione della distribuzione del massimo.

Questo approccio prevede la suddivisione di un campione di n osservazioni in sottocampioni o blocchi disgiunti, in base ad esempio ad un periodo temporale che può essere l'anno, e la successiva identificazione per ogni sottocampione dei massimi che sono considerati realizzazioni degli extreme values della distribuzione $F(x)$ non nota.

In modo formale ciò può essere formulato nel seguente modo: sia $X_{1,} \dots \dots X_n$ una sequenza di variabili aletatorie iid ossia identicamente e indipendentemente distribuite con stessa funzione di ripartizione pari a $F(x)$. Per ogni blocco si individua la variabile aleatoria M_n che rappresenta il massimo valore.

La sequenza di massimi è la seguente: $M_n = \max(X_{1,} \dots \dots X_n)$, *dove* n= dimensione del blocco considerato. Per l'ipotesi di variabili casuali iid, in particolare per l'indipendenza, la funzione di ripartizione dei massimi sarà pari a:

$$M_n(x) = F(x) = \prod_{i=1}^{n} P(X_i \leq x) = F^n(x)$$

I valori estremi tendono ad un valore detto "right-end point", cioè un estremo destro superiore della funzione di ripartizione F quando $n \to \infty$, tale estremo è pari a:

$$x_F = \sup[x \in \mathbb{R}: F(x) < 1]$$

e può essere anche definito come il valore minimo per cui fdr assume valore 1. Quindi asintoticamente i massimi tendono a questo estremo ossia $M_n \to x_F$, converge in probabilità.

Se infatti $x_F < \infty$ all'aumentare di n si avrebbe la convergenza di $F^n(x)$ a 0 per ogni $x < x_F$ ottenendo una massa di probabilità concentrata appunto su x_F.

Non conoscendo il tipo di distribuzione a cui converge M_n , si ricorre al concetto di dominio di attrazione dei massimi, secondo il quale, una distribuzione F è detta essere nel dominio di attrazione della distribuzione generalizzata dei valori estremi, se esistono delle costanti

$b_n > 0$ e $a_n \in \mathbb{R}$ che consentono la normalizzazione del massimo in modo tale che, per $n \to \infty$, questi massimi normalizzati tendono appunto ad una distribuzione limite.

Quindi, queste costanti di normalizzazione consentono la convergenza della distribuzione del massimo standardizzato $\frac{M_n - b_n}{a_n}$ alla distribuzione limite GEV[17] ovvero realizzano il fatto che la distribuzione sia nel dominio di attrazione della GEV.

Questo risultato deriva dal teorema di Tippet e Fisher (Tippet, Fisher; 1928, Embrechts et al.; 1997):

Data una successione di variabili aleatorie iid, se esistono due successioni di costanti b_n e $a_n > 0$, che permettono la normalizzazione ed evitano la convergenza di M_n su x_F , ed una funzione di ripartizione non degenere H tale che:

$$\lim_{n\to\infty} P\left(\frac{M_n - b_n}{a_n} \leq x\right) = \lim_{n\to\infty} P\left(M_n \leq a_n \cdot x + b_n\right) = \lim_{n\to\infty} F^n(a_n \cdot x + b_n) = H(x)$$

dove b_n e a_n sono costanti di normalizzazione, allora la distribuzione F è nel dominio di attrazione della Generalized Extreme Value distribution H con la seguente forma:

$$H_{\xi,\mu,\sigma}(x) = \begin{cases} e^{\left\{-\left(1+\xi\frac{x-\mu}{\sigma}\right)^{-\frac{1}{\xi}}\right\}} & se\ \xi \neq 0 \\ e^{\left\{-\exp\left(-\frac{x-\mu}{\sigma}\right)\right\}} & se\ \xi = 0 \end{cases}$$

Per n che va ad infinito, quindi, la distribuzione degli estremi converge a questa distribuzione.

La GEV, H, è una famiglia di distribuzioni, caratterizzata da tre parametri: $\mu\ e\ \sigma$ che sono rispettivamente i parametri di posizione e di scala mentre $\xi = \frac{1}{\alpha}$, da cui discende $\alpha = \frac{1}{\xi}$ è il parametro di shape della coda detto "tail index". Quindi μ indica dove la distribuzione è centrata mentre σ ne esprime la dispersione. A seconda del valore che assume ξ si individuano tre tipi di distribuzioni estreme particolari:

1) Se $\xi > 0$, distribuzione GEV di tipo *Fréchet*:

$$G(x) = \begin{cases} 0 & x \leq 0 \\ e^{-\left(\frac{x-\mu}{\sigma}\right)^{-\alpha}} & x > 0, \quad \alpha > 0 \end{cases}$$

[17] Generalized Extreme Value Distribution

2) Se $\xi < 0$, distribuzione GEV di tipo *Weibull*:

$$G(x)=\begin{cases}1 & z > 0\\ e^{-[-(\frac{x-\mu}{\sigma})^{\alpha}]} & x \leq 0, \alpha > 0\end{cases}$$

3) Se $\xi = 0$, distribuzione GEV di tipo *Gumbel*:

$$G(x) = e^{[-e^{[-(\frac{x-\mu}{\sigma})]}} \qquad -\infty < x < \infty$$

Queste tre distribuzioni sono i limiti della distribuzione del massimo standardizzato per n che tende ad infinito. Ciò che le contraddistingue è la forma della loro coda destra, di conseguenza per questa ragione modellizzano in modo diverso i valori estremi.
Ad esempio, la distribuzione Weibull ha un limite superiore finito, "finite upper bound", e quindi i valori estremi o massimi non possono superare tale limite, invece le distribuzioni Fréchet e Gumbel sono illimitate superiormente, $x_F = \infty$.
Per la Gumbel i valori massimi assumono valori infinitamente grandi, in quanto "two-side unbounded", con la coda o le probabilità che seguono una dinamica esponenziale cioè decrescono in modo esponenziale e per questo motivo è detta "light-tailed distribution".
Invece, nella Fréchet i valori massimi hanno probabilità più alte di quelle che presentano i massimi della Gumbel, si dice infatti che le probabilità decrescano in maniera polinomiale. Per questa ragione è detta "heavy-tailed distribution".
Non è necessario scegliere a priori una delle tre distribuzioni ma sarà sufficiente utilizzare il modello generale GEV lasciando che siano i dati ad indicare la forma, quindi è sufficiente fare inferenza sul parametro di forma ξ, senza dover fare ipotesi a priori, per trovare a quale di questi tipi di distribuzioni si riduce la GEV e quindi trovare a quale famiglia appartiene la distribuzione del massimo, cioè la coda della distribuzione, infatti se il tail index:

1) $\xi = \frac{1}{\alpha} > 0$ allora è una distribuzione di Fréchet
2) $\xi = \frac{1}{\alpha} < 0$ cioè $\xi = -\frac{1}{\alpha}$ allora è una distribuzione Weibull
3) $\xi = 0$ allora si trova la Gumbel

Quindi ξ individua quale tra i tre tipi di distribuzione specifica meglio i valori massimi in esame.

Per fare inferenza sui parametri della GEV si utilizzano diversi metodi, il più utilizzato è il metodo della massima verosimiglianza in quanto permette la sua estensione al modello GEV con trend, permettendo quindi di ipotizzare la non stazionarietà degli estremi e quindi in questo caso il parametro di locazione μ varia nel tempo.
Sotto l'ipotesi di variabili iid con distribuzione dei valori estremi generalizzata, la log-verosimiglianza per i parametri della distribuzione è la seguente:

$$l(\mu,\sigma,\xi) = -mlog\sigma - \left(1+\frac{1}{\xi}\right)\sum_{i=1}^{m} ln\left[1+\xi\left(\frac{x_i-\mu}{\sigma}\right)\right] - \sum_{i=1}^{m}[1+\xi\,(\frac{x_i-\mu}{\sigma})]^{-\frac{1}{\xi}}$$

$per\ \xi \neq 0,\ con\ 1+\xi(\frac{x_i-\mu}{\sigma}) > 0$ altrimenti la verosimiglianza assume un valore pari a zero e la log-verosimiglianza va ad $-\infty$.
Massimizzando $l(\mu,\sigma,\xi)$ rispetto ai parametri μ,σ,ξ si giunge alla stima della massima verosimiglianza per la GEV .
Ci sono poi stimatori per il parametro forma $\xi = \frac{1}{\alpha} > 0$ come lo stimatore Hill (Embrechts et al.; 1997) e lo stimatore di Pickands per $\xi \to 0$ (Dekkers et al; 1989, Hosking et al.;1985).
E' possibile anche calcolare dalla funzione di distribuzione della GEV i quantili.
Ad esempio, la probabilità che la quantità di interesse sia uguale o inferiore ad un certo livello x , si calcola andando a sostituire i parametri stimati precedentemente nella seguente espressione:

$$H(x) = P(X \leq x) = e^{-([1+\xi\left(\frac{x-\mu}{\sigma}\right)]^{-\frac{1}{\xi}}}$$

Invece, la probabilità di superamento del livello x è definita nel modo seguente:

$$P(Superamento) = (X > x) = 1 - P(X \leq x)$$

La frequenza di accadimento di questo superamento è detta periodo di ritorno ed è espresso in questo modo:

$$T = \frac{1}{P(Superamento)}$$

Quindi in media, una quantità pari a x per la grandezza di interesse si verifica una volta ogni T.

Il metodo dei blocchi massimi risulta poco efficiente in quanto cogliendo solo i valori massimi si riduce la base dati nel processo di stima del modello.

2.1.2 Metodo Peak Over Threshold (POT)

Il secondo metodo dei picchi oltre una soglia o delle eccedenze di una soglia, Peak Over Threshold, modellizza tutti i dati che eccedono una soglia detta threshold e di conseguenza permette di considerare maggiori informazioni, a seconda della soglia scelta, rispetto al metodo Block Maxima.
Centrale in questo metodo è il teorema limite di Pickands (1975), secondo cui data una variabile casuale X con funzione di ripartizione F appartenente al dominio di attrazione dei massimi, gli eccessi di X rispetto ad una soglia u, cioè $(X-u)|(X>u)$, al crescere di u tendono a distribuirsi come una distribuzione di Pareto generalizzata che presenta la seguente funzione di ripartizione:

$$H(x,\mu,\sigma,\xi) = 1-(1-\xi\left(\frac{x-\mu}{\sigma_u}\right)^{\frac{1}{\xi}} per\ \xi \neq 0$$

Quindi, per modellizzare le eccedenze $[X_1-u]$ si può utilizzare la distribuzione di Pareto Generalizzata.
Il parametro ξ è il parametro di forma che definisce lunghezza e spessore delle code della GPD, tale parametro è positivo per le distribuzioni con code pesanti e negativo per distribuzioni superiormente limitate. σ è il parametro di scala, mentre μ è il parametro di location che rappresenta la soglia di rifermento u per il calcolo delle eccedenze o eccessi delle osservazioni nel campione, $\mu = u$.
In questo metodo si estrae il campione delle eccedenze o eccessi rispetto alla soglia u,
un approccio di stima di tale threshold è basato su un approccio grafico detto *Mean Excess Function* che sfrutta il fatto che la GPD è una funzione lineare.
Costruendo questa funzione empirica o campionaria, $ex(u) = E(X-u|X>u)$, si ricava come stima della soglia il più piccolo valore a partire dal quale i punti della funzione mean excess empirica iniziano a disporsi lungo una linea retta, che ad esempio è crescente quando il parametro di forma è positivo e quindi la distribuzione è a code pesanti.
Se invece questo metodo non permette di individuare la stima della soglia u, si può scegliere a priori un certo percentile campionario che diventa la soglia di riferimento.

Il teorema di Pickands, in definitiva, fornisce una distribuzione limite per la variabile casuale e quindi permette la conoscenza della forma della coda della distribuzione di X dal valore di soglia u.

Quindi, se si vuole stimare il VaR ad un livello di confidenza α maggiore di u e quindi si vuole ottenere una metrica di rischio che riguarda la parte della distribuzione più a destra della soglia, è possibile stimare la misura di rischio senza conoscere l'intera distribuzione di X, basta avere un campione abbastanza numeroso di osservazioni iid, poi una volta scelta una soglia u elevata, si vanno a calcolare le eccedenze delle osservazioni X_i rispetto ad u, $[X_i - u]$, così si ottiene un nuovo campione i cui valori hanno una distribuzione che è ben approssimata dalla GPD e infine si vanno a stimare i parametri di questa distribuzione.

2.2 Applicazione empirica del metodo Block Maxima

Al fine di esemplificare l'applicazione delle metodologie descritte si è scelto di farne un'applicazione a dati relativi ad un evento naturale a cui possono essere associati dei rischi catastrofali.

Di seguito è applicato il metodo Block Maxima sulla serie storica riferita alle precipitazioni giornaliere, in termini di intensità o quantità di pioggia caduta al suolo, registrate nel Colorado[18] tra il 1900 e il 1999.

La quantità di pioggia caduta in una determinata area è una variabile utilizzata, ad esempio, nelle valutazioni dei temporali e consente l'individuazione ogni anno di periodi di siccità o di piogge abbondanti, quindi di valori estremi assunti da questa variabile.

Ad esempio, grandi quantità di pioggia concentrate in un breve tempo su un territorio che ha perso la capacità di assorbirla, possono generare una alluvione, infatti possono provocare l'esondazione o straripamento di un fiume che a sua volta si trasforma in una inondazione con conseguenze catastrofiche.

L'altezza pluviometrica cioè la quantità di pioggia caduta è misurata in pollici[19].

Da questa misura si ricava il volume caduto al suolo.

Ad esempio, una misura pari ad un millimetro di accumulo è pari ad 1 litro caduto su una superficie di un metro quadrato.

Nel 1966 sono bastati circa 180 mm di pioggia in 24 ore per causare l'alluvione a Firenze.

[18] Weather data from Fort Collins, Colorado, U.S.

[19] Nei paesi anglosassoni si utilizzano i pollici come unità di misura mentre, ad esempio, in Italia si utilizzano i millimetri.
1 pollice=25,4 mm quindi 100 pollici corrispondono a 2540 millimetri.

All'incirca 80-100 mm corrispondono alla media di quantità di pioggia caduta in un mese[20].
I dati corrispondono a precipitazioni giornaliere: $X_{1_m}, X_{2m} \dots, X_{nm}$, con n=365 giorni, si sono costruiti blocchi annuali di valori massimi delle precipitazioni giornaliere, da cui risultano m=(1,2……100 anni/blocchi).
Si assume che la serie dei massimi $M_1, \dots, M_m$ segua una distribuzione Generalizsed extreme distribution, $GEV(\mu, \sigma, \xi)$ e si procede con la stima dei parametri attraverso il metodo della Massima Verosimiglianza.
Una volta che è stato effettuato il fit della GEV sui massimi annuali, si calcola il periodo di ritorno T calcolando il quantile. Ad esempio, un evento T-ennale, è quel valore la cui probabilità di superamento, in un dato anno, è pari a p=$\frac{1}{T}$.
In figura 7 è presentata la serie storica dei valori massimi annuali, raffigurati come punti rossi. Ogni anno è un blocco e in ogni blocco è stato identificato il valore massimo tra le precipitazioni giornaliere.

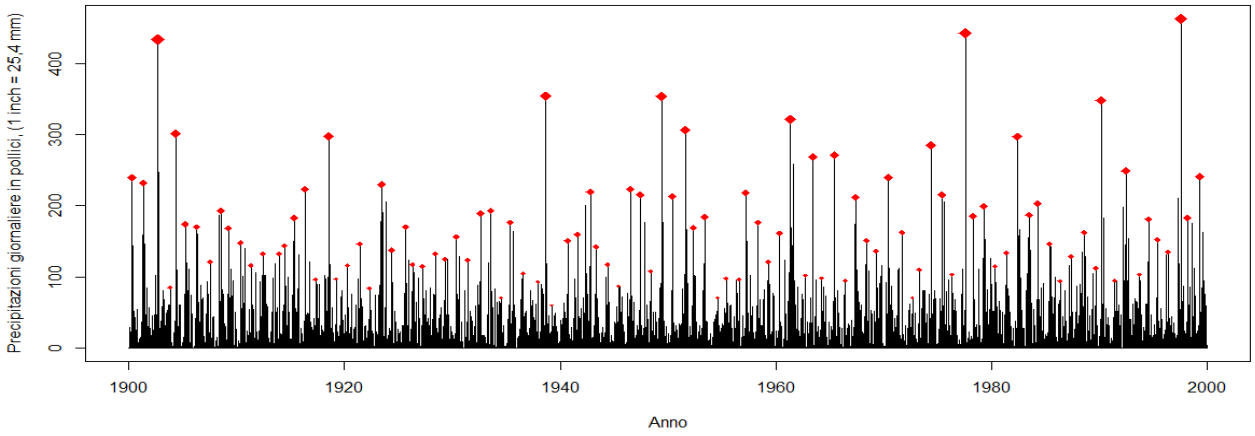

Figura 7: Massimi annuali tra le precipitazioni giornaliere riferite al periodo 1900-1999 (elaborazione personale mediante RStudio)

Successivamente, ricavata la serie dei massimi, si procede all'adattamento della GEV ai dati per osservare soprattutto il comportamento del parametro shape, in modo tale da poter individuare quale tra i tre tipi di distribuzioni estreme descrive meglio i dati. Per ottenere questo risultato, si utilizza la funzione *fevd,* contenuta nel pacchetto *extRemes*, per effettuare il fitting della GEV sui dati. I risultati sono mostrati in figura 8a e in figura 8b.

[20] http://www.arpa.veneto.it/arpavinforma/indicatori-ambientali/indicatori_ambientali/clima-e-rischi-naturali/clima/precipitazione-annua/view

[1] **"Estimation Method used: MLE"**

Negative Log-Likelihood Value: 565.4816

Estimated parameters:

location	**scale**	**shape**
134.66520	53.28089	0.17363

Standard Error Estimates:

location	scale	shape
6.16877130	4.87901653	0.09195688

AIC = 1136.963

BIC = 1144.779

Figura 8a: Stime metodo MLE

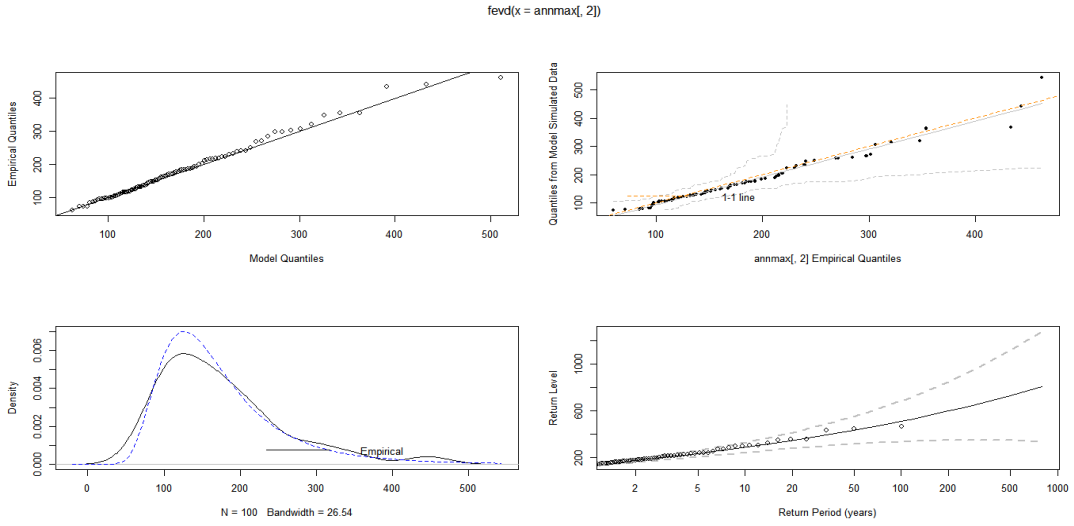

Figura 8b: Grafici per i blocchi annuali utilizzando il metodo MLE

Dalle stime dei parametri, $\xi > 0$, quindi la distribuzione di Fréchet descrive molto bene i dati. La GEV si adatta abbastanza bene ai dati empirici, linea tratteggiata in nero, la validità del modello GEV è confermata anche dal grafico dei quantili, QQ-plot, in quanto quasi tutti punti

sono ravvicinati alla linea. Sono stati effettuati anche i test di bontà di adattamento come prova usando KS, Chi-Squared e AD che portano all'accettazione dell'ipotesi nulla.

Test Method: Kolmogorov-Smirnov GOF Hypothesized Distribution: Generalized Extreme Value Estimated Parameter(s): location = 132.8549464 scale = 55.9377932 shape = 0.1850477 Estimation Method: mle Data: y Sample Size: 500 Test Statistic: ks = 0.02574446 Test Statistic Parameter: n = 500 P-value: **0.8947746** Alternative Hypothesis: True cdf does not equal the Generalized Extreme Value Distribution.	Test Method: Anderson-Darling GOF Based on Chen & Balakrishnan (1995) Hypothesized Distribution: Generalized Extreme Value Estimated Parameter(s): location = 132.8549464 scale = 55.9377932 shape = 0.1850477 Estimation Method: mle Data: y Sample Size: 500 Test Statistic: A = 0.2293169 Test Statistic Parameter: n = 500 P-value: **0.8080996** Alternative Hypothesis: True cdf does not equal the Generalized Extreme Value Distribution.	Test Method: Chi-square GOF Hypothesized Distribution: Generalized Extreme Value Estimated Parameter(s): location = 132.8549464 scale = 55.9377932 shape = 0.1850477 Estimation Method: mle Data: y Sample Size: 500 Test Statistic: Chi-square = 19.1 Test Statistic Parameter: df = 21 P-value: **0.5787252** Alternative Hypothesis: True cdf does not equal the Generalized Extreme Value Distribution.

Figura 9: Stima dei parametri MLE e test di bontà di adattamento

2.2 Modelli per il rischio catastrofale (Cat models)

Gli eventi catastrofali sono caratterizzati da bassa frequenza ed elevata severità, per questo motivo sono chiamati rischi di coda.
La probabilità che si verifichi un certo evento aleatorio è intesa come un numero che esprime la sua frequenza annuale su un gran numero di prove.
A questa misura di frequenza di occorrenza, considerata su base annuale, con cui un evento si verifica, viene associata la misura di periodo di ritorno che, in base ad un prefissato livello di severity dell'evento, indica in media l'intervallo di tempo entro il quale si può verificare un evento di eguale o superiore intensità.
La severity dell'evento è misurata secondo metriche fisiche ampiamente riconosciute che danno indicazione sulla potenziale conseguenza dell'evento, il danno, come ad esempio la magnitudo per un terremoto.
Tuttavia, la base storica per gli eventi catastrofali naturali è generalmente insufficiente e anche in funzione dei mutamenti climatici e dei loro impatti non rispecchia tutti i possibili stati del mondo futuri. Di conseguenza il settore assicurativo supporta il processo attuariale con modelli catastrofali (catastrophe models), sviluppati da diverse società specializzate nella modellizzazione di tali rischi. Di seguito sono presentati gli elementi fondamentali di tali modelli, per ulteriori approfondimenti si rinvia a Mitchell-Wallace et al.(2017), Banks (2005), Air Worldwide (2016), Lloyd's(2014), RMS(2008), Derris(2016).
Questi catastrophe models utilizzano cataloghi di eventi stocastici sulla base dei quali giungono in condizioni di incertezza ad una quantificazione prospettica degli effetti finanziari sui portafogli delle compagnie assicurative.
L'output di questi modelli è utile, oltre che alle imprese di assicurazione, anche agli investitori e agli organismi di vigilanza.
L'affidabilità di tali output dipende dall'efficace comprensione scientifica dei meccanismi sottostanti l'insorgenza e lo sviluppo degli eventi naturali.
Dal punto di vista di una compagnia assicurativa operante nel ramo danni, il rischio di una catastrofe naturale è concepito come una funzione della pericolosità dell'evento e del suo potenziale impatto economico in termini di perdite:

$$Risk = f(pericolosità, perdite)^{21}$$

[21] Banks (2005), European Commision, Derris (2016), sito Protezione Civile

Dove f rappresenta una funzione della pericolosità che corrisponde alla probabilità dell'evento e dalle perdite che dipendono dal grado di esposizione e dalla vulnerabilità.
L'impatto economico a sua volta è determinato dal valore dei beni esposti a questo rischio e dal loro grado di vulnerabilità in termini di danni potenziali subiti come conseguenza dell'occorrenza dell'evento.
In termini statistici il concetto di pericolosità esprime la probabilità di accadimento di un evento di una certa intensità assoluta, in una specifica zona geografica, in cui sono ubicati i beni oggetto di polizze, e in un determinato intervallo di tempo.
La componente vulnerabilità dipende dalle caratteristiche del bene considerato a rischio e dall'intensità dell'evento, di solito ha un range tra 0 (nessun danno) e 1 (distruzione).
Dunque, nella misurazione del rischio nat-cat è necessario valutare ogni singola dimensione e poi procedere successivamente all'integrazione delle diverse componenti in una misura di rischio.
Alcune società all'avanguardia nello sviluppo di questi strumenti di misurazione dei rischi di coda sono la Risk Management Solutions (RMS), l'Applied Insurance Research (AIR) e CoreLogic[22].
Il processo, come indicato da AIR(2016) ed RMS(2008), si basa su un approccio probabilistico e simulativo che cerca di ipotizzare i possibili stati del mondo futuri, utilizzando algoritmi con elevata capacità di calcolo che generano un gran numero di scenari di eventi stocastici con l'obiettivo di stimare la potenziale distribuzione di perdita associata ad un portafoglio di esposizioni.
Questa distribuzione di perdita aggregata supporta i processi decisionali di pricing, di ottimizzazione del portafoglio-rischi e di finanziamento del rischio mediante il trasferimento di questo tramite riassicurazione e cartolarizzazione.
I modelli richiedono innumerevoli quantità di dati ed incorporano le conoscenze di scienziati, ingegneri, statistici ed attuari.
Inoltre, sono supportati da enormi capacità di calcolo per effettuare le simulazioni.

22
- https://www.rms.com/
- https://www.air-worldwide.com/
- https://www.corelogic.com/solutions/catastrophe-risk-management.aspx

Ogni evento è concepito come una realizzazione di un processo stocastico, quindi sono intesi come una successione di variabili aleatorie che si manifestano nel tempo in modo casuale. E sono aleatori sia gli istanti in cui si presentano gli eventi sia la tipologia di evento che si verifica in ogni istante sia il numero di eventi che potrebbero occorrere in un determinato intervallo di tempo equivalente ad un anno.

Di conseguenza sono necessarie alcune ipotesi che permettono la caratterizzazione del processo stocastico secondo il quale evolve il fenomeno naturale.

Sulle ipotesi alla base del modello, come riportato da Albertini e Bareue (2009), vengono effettuati degli stress test per verificare la loro robustezza che ovviamente si ripercuote sulla bontà delle stime finali.

Ad esempio, si può supporre che gli eventi provengano da un processo stocastico di Poisson, un processo di punti-evento, dove gli eventi si presentano singolarmente e si manifestano in intervalli di tempo disgiunti e quindi sono indipendenti tra loro.

Risulta evidente come il processo che porta alla quantificazione finale del rischio in termini di perdite provocate da un determinato evento catastrofale, oltre ad essere molto complesso, essendo basato su diverse ipotesi, sulle quali si vanno poi a costruire gli scenari via simulazione, è governato da un certo livello di incertezza aleatoria ed incertezza epistemica (Mitchell-Wallace et al., 2017).

Incertezza che in realtà aumenta sempre di più a causa dei cambiamenti climatici in atto che influenzano i fenomeni naturali oggetto di misurazione.

Ad esempio, se consideriamo le analisi prodotte da EQECAT (Lloyd's, 2014) le previsioni sono che il global warming provocherà uno spostamento verso nord delle traiettorie delle tempeste europee e un'intensificazione degli eventi di maggiore intensità che, a sua volta, farà aumentare quasi del triplo il numero degli immobili soggetti a rischio se non saranno adottate adeguate misure di prevenzione.

La società è giunta a tale conclusione, attraverso la costruzione, via simulazione, dei cataloghi (*ensemble*) di eventi artificiali, andando a creare scenari che risultato dall'incrocio di valori storici, oltre 50 anni di dati di parametri fisici dell'evento tempesta come velocità del vento, durata ,pressione atmosferica, perturbazioni, temperatura e percentuale di umidità, forniti dalle varie stazioni meteorologiche di tutta Europa, con valori ipotizzati di questi parametri ed inoltre incrociati con diversi valori di CO_2.

Per cui, ad esempio, ogni simulazione prevede variazioni nei parametri fisici dell'evento come la variazione del comportamento storico del vento che quindi va a modificare la traiettoria della tempesta artificiale rispetto a quella storica osservata.

Servono migliaia e migliaia di simulazioni per comporre il catalogo stocastico che restituisce il più ampio spettro dei rischi possibili, intesi in questo caso come tempeste artificiali o sintetiche stocastiche (AIR, 2016).
Attraverso questo catalogo storico-artificiale, il modello catastrofale fornisce la distribuzione frequenza-severity e la distribuzione spaziale dei potenziali eventi naturali futuri T-ennali ossia a seconda del numero di scenari simulati. Questo è solo uno degli output del catastrophe model.
Infatti, i modelli catastrofali, restituiscono come output finale la perdita finanziaria potenziale derivante dall'evento catastrofale modellato e questo output è il risultato di un processo composto da diverse fasi a cui corrispondono diversi risultati che sequenzialmente diventano input di fasi successive.
Sempre secondo la Lloyd's Market Association di Londra, ogni modello catastrofale è un sistema computerizzato che genera un robusto set di eventi simulati e stima la frequenza, l'intensità e la localizzazione dell'evento catastrofale per determinare l'ammontare di danno e per calcolare le perdite assicurate, provocate dalla calamità naturale, combinando conoscenze scientifiche, riguardanti i fenomeni naturali, con conoscenze ingegneristiche e finanziarie.
Hanno il pregio di ampliare l'urna di eventi che potrebbero verificarsi in futuro, nel senso che integrano gli insufficienti dati storici restituendo misure di probabilità più veritiere.
I dati storici, e quindi l'approccio attuariale che si basa su questi dati per stimare le perdite future, non sono adatti, in quanto si tratta di rischi di coda che si verificano meno frequentemente, di conseguenza ci sono pochi dati a disposizione che non sono rappresentativi degli eventi a più alta severità.
Invece, nel catastrophe model la probabilità e la severità sono valutate sulla base sia di dati storici sia di realizzazioni simulate che riflettono le ipotesi di accadimento futuro degli eventi.
Per ogni fenomeno naturale, come riportato da RMS (2008), esistono diversi modelli, ogni modello si concentra sulle caratteristiche specifiche che definiscono l'evento naturale, quindi la frequenza, l'intensità, la posizione geografica e su come queste caratteristiche, che rappresentano la pericolosità dell'evento, interagiscono con le vulnerabilità delle esposizioni a rischio in termini di predisposizione a danni e quindi a perdite in portafoglio assicurativo.
Il processo di quantificazione del rischio è effettuato in condizioni di incertezza, quindi è governato da soggettività, input quantitativi ma anche qualitativi e opinioni tratte dall'esperienza di esperti.

L'impatto finanziario finale dell'evento è una funzione sia della pericolosità sia della vulnerabilità dell'area esposta al rischio. Quindi la probabilità di perdita dovuta al verificarsi di una catastrofe è una funzione della probabilità di accadimento dell'evento e della distribuzione di severity delle perdite dato l'accadimento dell'evento.

Il risk management può minimizzare il rischio agendo sulla gestione della vulnerabilità, facendo ad esempio valere l'obbligo di salvataggio della cosa ai sensi dell'articolo 1914 del cc, oppure può agire sia sulla riduzione del rischio in termini di diversificazione sia può utilizzare, come strategia alternativa o complementare alle altre, il trasferimento del rischio al mercato dei capitali.

Il processo di modellizzazione[23], come mostra la figura 10, si compone di diverse fasi di valutazione, ricomprese in moduli sequenziali:

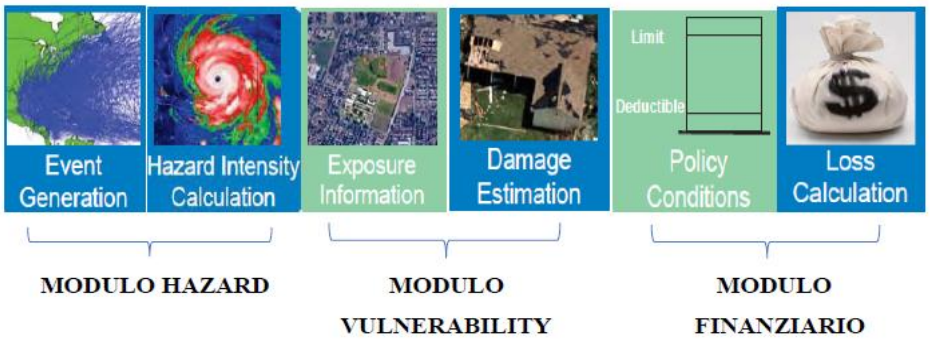

Figura10: Rielaborazione propria su AIR(2016)

- la valutazione della pericolosità, compresa nel primo modulo, prevede la stima della frequenza con la quale un evento di una certa intensità si verifica attraverso la stima dei parametri naturali dell'evento stesso. La stima è basata sia su dati storici, dati scientifici e simulazioni di diversi scenari che prevedono anche i mutamenti climatici come indicato da Lloyd's(2014).
- Nella modulo della vulnerabilità, intesa come grado di predisposizione del portafoglio di assets assicurati al rischio in esame, si valutano i danni provocati dall'evento e le conseguenti perdite lorde.
- Infine, nel modulo finanziario si calcola l'ammontare delle perdite assicurate al netto delle condizioni contrattuali applicate.

[23] Mitchell-Wallace, Jones, Hillier and Foote (2017) e Banks (2016)

Il catastrophe model è composto da un insieme di sotto-modelli interconnessi che caratterizzano i diversi moduli sequenziali e sono in genere integrati in una piattaforma.
Ogni modulo prevede diverse analisi e si differenzia in base all'oggetto di valutazione, alle strumentazioni utilizzate, agli input in ingresso e alle conoscenze a supporto.
L'integrazione di conoscenze geofisiche, ingegneristiche e finanziarie permette di considerare i contributi di ciascuna componente alla misurazione del rischio complessivo.
L'output restituito dal modello attraverso l'analisi storica e le simulazioni di scenari è la curva frequency-severity delle perdite assicurate nette che può essere presentata in diverse forme come loss distribution aggregata oppure come curva di probabilità di superamento, che sono appunto due curve frequency-severity che evidenziano l'ammontare delle perdite attese e la frequenza associata.
Gli ouput generati in ogni fase modulare di una piattaforma di un cat model sono sintetizzati in figura 11 che presenta sulla sinistra le fasi di modellazione e sulla destra il corrispondente output:

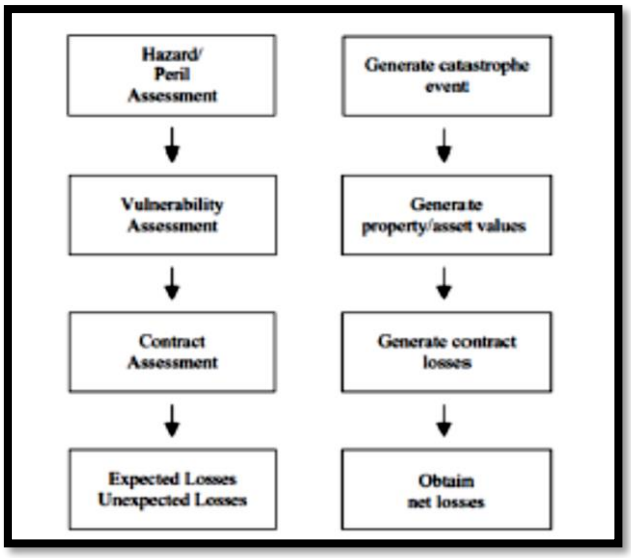

Figura11: *A sinistra le fasi del modello con rispettivo output sulla destra* (Banks, 2005)

2.2 I tre moduli di analisi

Il modulo pericolosità consiste in una quantificazione della pericolosità, in base ai dati storici che caratterizzano quel dato fenomeno e alle realizzazioni ricavate dalle simulazioni.
Ciò permette l'ottenimento della frequenza dell'evento naturale e la sua intensità su determinate coordinate in termini di longitudine e latitudine su un orizzonte temporale di un anno.

Il grado di pericolosità della zona, come indicato dal sito della Protezione Civile, dipende proprio dai valori diversi di intensità del fenomeno e di frequenza dell'evento.
La compagnia assicurativa deve definire il dominio geografico su cui è necessario valutare la pericolosità.
Per ogni zona geografica e per ogni fenomeno naturale ci sono appositi framework basati su modelli fisici e geolocici che permettono la comprensione della pericolosità in quella specifica zona territoriale relativa a quello specifico evento naturale.
L'analisi non è rivolta solo alla zona individuata dalla compagnia ma si estende anche allo spazio esterno limitrofo contenente le possibili fonti di generazione dell'evento che potrebbero agire sulla zona di interesse.
Una volta che è stata definita la zona geografica, assumendo l'indipendenza stocastica tra diversi eventi e quindi tra le diverse perdite attese nell'orizzonte temporale definito, si procede con l'analisi di pericolosità.
La pericolosità è il pericolo potenziale cioè esprime la probabilità che in una zona possa verificarsi, a causa di caratteristiche predisponenti, un evento catastrofale entro un determinato intervallo di tempo chiamato tempo di ritorno. E' descritta in termini di frequenza temporale dell'evento cioè frequenza dell'impatto di ogni evento sullo spazio.
Molti fenomeni naturali di regola mostrano una "memoria storica" ovvero sulla base delle loro manifestazioni verificatesi nel tempo è possibile determinare ogni quanto ci si può aspettare che un fenomeno di una certa entità possa ripetersi.
Inoltre, la pericolosità è descritta anche in termini di intensità del fenomeno come energia o potenza sprigionata nell' estensione geografica e anche in termini di variazione dell'intensità nella zona[24].
Ad esempio, come riportato da Ania, Guy Carpenter, Consap (2011), l'intensità di un uragano è classificata in base alla massima velocità del vento mentre la magnitudo di un terremoto (si parla di magnitudo in questo caso perché è una misura assoluta della severity mentre l'intensità è solo una misura relativa dell'evento sismico) è data dalla massima accelerazione del suolo indotta dal terremoto stesso.
Invece per l'evento alluvionale l'intensità è misurata dal tirante idrico cioè l'altezza o profondità raggiunta dall'acqua.
La valutazione è basata su un approccio probabilistico che prevede l'utilizzo di un catalogo contenente un elevato numero di eventi sintetici a cui sono associate le probabilità in termini di intensità, in modo tale da riflettere tutti i possibili eventi che potrebbero accadere in futuro.

[24] Mitchell-Wallace K., Jones M., Hillier J., Foote M.(2017)

Come indicato da AIR (2016), si creano spesso campioni contenenti un ampio numero di scenari anche superiori a 10,000.

Ogni evento sintetico è creato combinando dati storici con modelli fisici e statistici che estrapolano dai dati storici ciò che non è stato ancora osservato.

Viene prima individuato il dominio spaziale-temporale, cioè la regione e l'estensione geografica dell'area che potrebbe essere colpita dal fenomeno naturale sulla quale è presente l'area di interesse assicurativo. E si cerca di creare una mappa di pericolosità prospettica sulla base del catalogo stocastico del fenomeno naturale, creato da un gruppo di scienziati, statistici ed ingegneri utilizzando dati storici per dedurre cosa potrebbe accadere in futuro e facendo quindi delle ipotesi sulla probabilità di accadimento futuro di un certo evento in una determinata zona e sulla la loro severità-intensità.

In questa fase la stima dell'intensità dell'evento è fondamentale in quanto c'è correlazione tra intensità e livello di perdita.

La pericolosità viene valutata partendo da una valutazione dei rischi attuali su base storica cui si devono aggiungere scenari per rappresentare gli eventi di coda.

Quindi si parte dalle mappe di pericolosità storica, un esempio di mappa è mostrata in figura 10, che contengono le ricostruzioni storiche dei singoli eventi in quanto forniscono la base per sviluppare le ipotesi funzionali alla creazione di mappe di pericolosità stocastiche future.

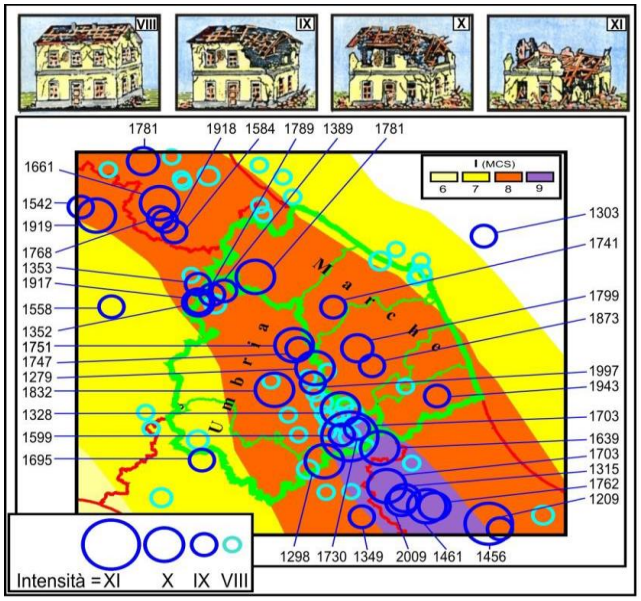

Figura 12: *Mappa di pericolosità per l'Italia (Meteoweb)*

Dalle mappe storiche si determinano le fonti da cui potrebbe scaturire l'evento catastrofale presenti su quel territorio, ad esempio le linee di faglia, bacini idrografici, reti fluviali o le zone di genesi di una tempesta[25].

Ogni area interessata dal fenomeno storicamente conterrà al suo interno la distribuzione spaziale dei diversi livelli di intensità che provocano il danno e questa diversa intensità del pericolo nell'area è rappresentata sulla mappa da diversi colori via via più scuri all'aumentare dell'intensità del fenomeno, vedi figura 12.

Si procede poi effettuando una vera e propria anatomia del fenomeno naturale andando ad identificare i parametri fisici legati all'evento.

In questa fase è centrale l'apporto di conoscenza da parte di geofisici, meteorologi, climatologi e fisici. Ad esempio, per valutare l'intensità del fenomeno alluvionale, è necessario prendere in considerazione, la velocità della corrente e l'altezza dell'acqua.

Una volta individuati i parametri fisici dell'evento specifico e le metriche di misurazione di questi, si decide l'orizzonte temporale di simulazione e, sulla base delle leggi fisiche che lo governano, si ipotizza una loro interazione nella generazione dell'evento futuro attraverso le simulazioni.

L'obiettivo è appunto catturare l'intero range degli eventi possibili e quindi descrivere lo spazio di probabilità degli eventi possibili.

Un processo di simulazione di un evento naturale può basarsi, per esempio, sull'ipotesi che una variabile casuale Poissoniana rappresenti i tempi di arrivo degli eventi e che quindi conteggi gli eventi, verificatisi nell'anno, assumendo che i tempi di arrivo siano distribuiti uniformemente[26].

Per cui da questa distribuzione di Poisson si genera un ampio numero di eventi indipendenti, ad ogni iterazione viene calcolato il numero degli eventi che si sono verificati nello scenario e il relativo impatto, infine si ordinano in base alla severity-intensità e si va a costruire la distribuzione di probabilità aggregata finale.

Il primo modulo restituisce l'output mostrato in figura 13 ovvero la probabilità di accadimento annuale dell'evento naturale con una determinata intensità, in una particolare regione ad esempio nella forma di exceedance probability.

Si ottiene quindi un diagramma basato su diversi livelli di intensità del fenomeno a cui è associata una frequenza in termini di periodo di ritorno o in termini di probabilità di occorrenza.

[25] Banks (2005)
[26] Banks E. (2005)

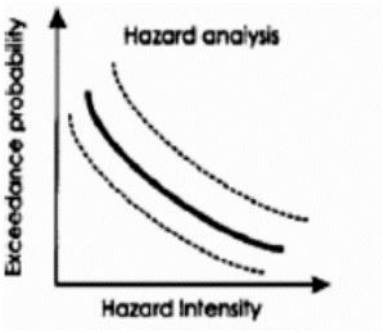

Figura 13: Hazard analysis, output del primo modulo (Banks, 2005)

Il diagramma definisce il grado di pericolosità nella zona che risulta quindi dalla combinazione di livelli di intensità con una scala di frequenza temporale.

Il secondo modulo[27] si concentra sul portafoglio di esposizioni a rischio e ne valuta la loro vulnerabilità che può essere interpretata come una stima dei danni che potrebbe subire un bene o un insieme di beni in conseguenza del verificarsi dell'evento avverso di una determinata intensità.

Questo modulo attraverso indici di danno quantifica la relazione tra la size in termini di severity della pericolosità nella zona e la risultante perdita lorda per ogni singola struttura o bene.

L'indice di danno, dato un evento di intensità j e un bene i, può essere calcolato, come indicato da Shane Latchman (2010), nel seguente modo:

$$DR(i,j) = \frac{Cost\ of\ repair\ (i,j)}{Total\ Replacement\ cost\ value(i)}$$

Gli output del primo modulo diventano quindi gli input di questo modulo che è caratterizzato dalle valutazioni tecniche di tipo ingegneristico sulla vulnerabilità del portafoglio di esposizioni a rischio.

I risultati di questa fase sono le stime dei danni ai potenziali immobili edificati nella zona geografica di interesse, che presenta una certa pericolosità, e rappresentano le stime delle potenziali perdite dirette lorde derivanti da un determinato evento naturale, dipendenti sia dall'intensità dell'evento sia dalle caratteristiche dei beni e del territorio.

[27] Dolce, Martinelli (2005), Latchman(2010)

Si procede andando a sovrapporre la mappa di pericolosità, e quindi l'evento avverso con una determinata intensità che sono stati modellizzati nella fase di pericolosità, sui dati legati alle caratteristiche delle infrastrutture e del territorio.
Successivamente si calcolano le funzioni di vulnerabilità che mettono in relazione diversi livelli di intensità con il grado di danni subiti per ogni classe di asset.
Per tenere in considerazione la variabilità del danno si costruiscono delle distribuzioni di danno relative alle diverse strutture che associano ad ogni grado di danneggiamento una probabilità di accadimento.
Da questa distribuzione poi si estrae il danno medio in termini di valore medio della distribuzione e si vanno a creare delle curve di vulnerabilità che mostrano la relazione tra diversi livelli di intensità con cui può verificarsi il fenomeno e valori possibili di danno medio.
Quindi il danno attraverso questa curva di vulnerabilità è espresso in funzione dell'intensità dell'evento naturale ossia per ogni livello di intensità si ha un determinato valore di danno atteso subito dalla struttura.
La figura 14 mostra una curva di vulnerabilità, all'aumentare dell'intensità (IE) aumenta il danno atteso (DM) subito dalla struttura A.

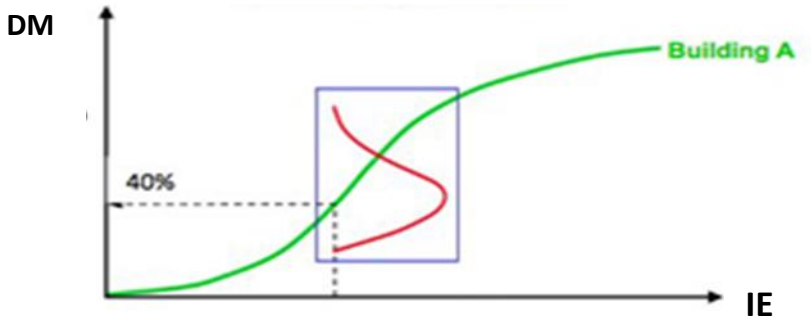

Figura 14: *Curva di vulnerabilità (Latchman, AIR)*

L'ubicazione del bene incide sulla valutazione della vulnerabilità e quindi sul danno, infatti si vanno a studiare i dati geologici come il tipo di suolo per l'analisi dei terremoti o la rugosità cioè l'irregolarità delle superfici in caso di uragani perché a seconda delle caratteristiche che presenta il territorio la vulnerabilità dei beni può aumentare o diminuire nel grado[28].
Per cui, per stimare la vulnerabilità e quindi il danno, si individuano prima i luoghi specifici su piccola scala che potrebbero essere colpiti, attraverso un processo di geocoding, poi se ne studiano le proprietà e si suddivide la zona in base al livello di vulnerabilità riscontrato.

[28] Ania, Guy Carpenter, Consap (2011)

A fronte di una potenziale copertura assicurativa, le zone ad alta vulnerabilità saranno associate ad alti valori di perdita e quindi l'assicurazione dei beni situati in quelle zone sarà associata a premi più elevati.

Per valutare il potenziale danno, si procede con la valutazione delle caratteristiche proprie degli edifici in termini di progettazione dell'edificio stesso.

Ad esempio, come riportano il sito della Protezione civile e Ania(2011), in caso di evento sismico, al verificarsi di un terremoto di eguale intensità, un edificio in muratura sarà caratterizzato da una maggiore vulnerabilità di quella presentata da un immobile in calcestruzzo.

Dal modulo di vulnerabilità, si ottengono per ogni zona soggetta a copertura assicurativa i danni subiti dagli assets per ogni evento stocastico simulato e questa base informativa costituisce l'input del modulo successivo, il modulo finanziario.

Nel modulo finanziario[29] si vanno a stimare le distribuzioni di perdita lorda e netta.

La perdita netta tiene conto dei contratti di assicurazione e quindi delle condizioni applicate, quindi si prendono in considerazione le delimitazioni del rischio cioè le limitazioni causali e spaziali del rischio e le clausole contrattuali, come le franchigie che lasciano a carico dell'assicurato una parte del danno.

In questa fase si traduce la stima dei danni ai beni in costi coperti dalle polizze assicurative per ogni assicurato e per ogni zona di interesse.

L'output finale del catastrophe model è quindi la stima delle perdite assicurate nette stand alone e di portafoglio.

La distribuzione di portafoglio supporta il processo decisionale di pricing e, per esempio, decisioni di trasferimento del rischio via securitization mediante emissione di catastrophe bonds.

La perdita lorda, come indicato da AIR, si ottiene andando a moltiplicare il danno atteso per il valore di sostituzione della struttura ottenendo così un ammontare monetario lordo perché non ancora al netto delle condizioni contrattuali.

Viene scelto un orizzonte temporale annuale e, assumendo che le perdite siano tra loro indipendenti, si vanno a generare diversi scenari catastrofali dove *n* sono le variabili casuali che rappresentano il numero di eventi causanti perdite, verificatisi nell'orizzonte temporale. Si considera l'impatto di ogni evento e la probabilità di ogni scenario.

[29] Banks (2005), Latchman- AIR (2010), Mitchell-Wallace et al. (2017)

Queste simulazioni permettono l'aggregazione dei danni stimati dalle funzioni di vulnerabilità per i diversi edifici in funzione di ogni evento stocastico simulato di una certa intensità, considerando le correlazioni tra gli assets localizzati nell'area di interesse.
Ad esempio, si considerino due distribuzioni di perdita f_{L_1} *e* f_{L_2} per un dato evento naturale relative gli immobili, 1 e 2, risultanti dall'accadimento dello stesso evento naturale.
Assumendo l'indipendenza delle singole perdite, la probabilità della perdita totale L, derivante dalle perdite sui due immobili, al verificarsi di quel dato evento, è data da:

$$P(L) = \sum_{L_1} f_{L_1}(L_1) \cdot f_{L_2}(L - L_1)$$

dove L rappresenta la perdita totale, mentre f_{L_1} *e* f_{L_2} sono le distribuzioni di probabilità per il primo ed il secondo immobile.
Quindi la convoluzione permette di calcolare la probabilità di ogni perdita totale.
Si ottiene così una distribuzione di perdita aggregata-totale che associa ai valori di perdita, derivanti dalla somma dei livelli di perdita relativi ai beni, le corrispondenti probabilità.
A titolo di esempio, in figura 15 sono mostrate le perdite relative a due immobili, a cui sono associate le relative probabilità.

$\boldsymbol{L_1}$	$\boldsymbol{P(L_1)}$		$\boldsymbol{L_2}$	$\boldsymbol{P(L_2)}$
0	0.2		0	0.35
5	0.15		5	0.25
10	0.3		10	0.2

Figura 15*: Perdite di due immobili (rielaborazione su Mitchell-Wallace et al.(2017))*

Una perdita totale pari a 10 sul dominio della distribuzione di perdita aggregata, output finale del catastrophe model, si ottiene convoluzionando in questo caso tre scenari di perdita: $(0{,}10), (5{,}5)$ *e* $(10{,}0)$ e per ottenere la probabilità di avere tale perdita totale si vanno a moltiplicare le probabilità individuali di perdita dei singoli immobili in ogni scenario e si sommano.

$$\begin{aligned} P(10) = {} & P_1(0) * P_2(10) + P_1(5) * P_2(5) + P_1(10) * P_2(0) \\ = {} & (0.2 * 0.2\,) + (0.15 * 0.25) + (0.3 * 0.35) \\ = {} & 0.1825 \end{aligned}$$

Quindi sulla distribuzione di perdita aggregata, la probabilità di ottenere una perdita pari a 10 è 0.1825.

Il dominio riferito ad un determinato livello di perdita sulla loss distribution aggregata, è ottenuto con riferimento alla somma dei livelli di perdita derivanti dalle singole loss distributions di ogni bene.

Ad esempio, per simulare scenari di perdita, l'algoritmo estrae dalla distribuzione dell'evento naturale in maniera casuale la realizzazione dell'evento con una certa intensità. Quel valore di intensità dell'evento spiega le realizzazioni congiunte di perdita dei beni.

Si può interpretare questa realizzazione X come la componente sistematica. Questo valore infatti va a condizionare le successive realizzazioni di perdita dei singoli beni, sulla base della loro sensitività in termini di vulnerabilità, β_i, a questo fattore sistematico X.

Poi ci sarà la componente di errore o idiosincratica che descrive la parte non spiegata dalla componente sistematica.

Quindi si può dare un'interpretazione basata su un semplice modello fattoriale del tipo:

$$y_i = \beta_i X + \varepsilon_i$$

In base a questo evento si vanno a calcolare le realizzazioni sulle singole distribuzioni di perdita dei singoli beni.

La distribuzione di perdita aggregata risultante dal processo simulativo, mostrata in figura 16, ha per dominio le possibili perdite nella zona di interesse che potrebbe essere affetta dall'evento catastrofale data la pericolosità del luogo e la vulnerabilità degli assets.

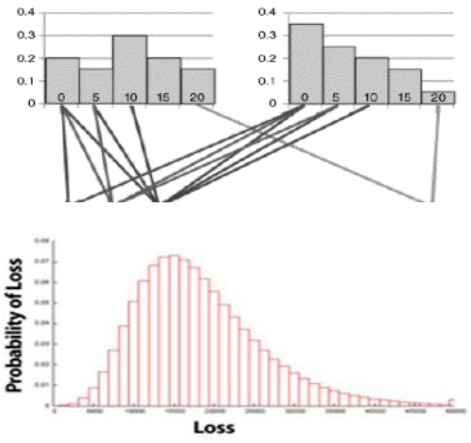

Figura 16: *Distribuzione di perdita aggregata risultante dal processo simulativo (Latchman-AIR e Mitchell-Wallace et al.(2017))*

Sull'asse delle x viene rappresentato il range delle possibili perdite riguardanti una singola zona assicurata, colpita dall'evento catastrofale di interesse, mentre l'asse y rappresenta la probabilità di perdita.
Per quanto riguarda il modulo finanziario, una volta che è stato creato il catalogo di eventi in base ai parametri fisici e quindi il modulo hazard abbia restituito come output la pericolosità per ogni evento ipotizzato nello spazio di interesse assicurativo sulla base di un insieme di assunzioni, la perdita totale netta finale, associata ad ogni singolo evento, è data dalla somma di tutte le perdite riscontrate nella zona analizzata colpita da quel particolare evento.
Le perdite totali di ogni evento stocastico sono raccolte nella tabella mostrata in figura 17:

Evento	Perdita totale	Tasso medio di accadimento nel tempo: λ
1°	L_1	λ_1
2°	L_2	λ_2
n°	L_n	λ_n

Figura 17: *Tabella delle perdite totali associate ad ogni singolo evento nel catalogo stocastico-artificiale (AIR)*

Una volta calcolata la perdita lorda si procede alla fase di valutazione dei contratti che prevede appunto l'applicazione delle condizioni di assicurazione specifiche di ogni polizza per determinare la perdita netta.
La distribuzione di perdita a livello di portafoglio consente di valutare, attraverso l'analisi di correlazione, il contributo delle posizioni stand alone al portafoglio per apprezzare il loro contributo al rischio complessivo.
Tale distribuzione supporta il processo decisionale di ottimizzazione del portafoglio, di pricing e di trasferimento del rischio via securitization cioè mediante emissione di titoli ILS.
Le perdite sono analizzate attraverso le distribuzioni di frequenza di perdita nella forma precedente oppure attraverso le curve di probabilità di eccedenza in base alle quali si calcolano diverse metriche di perdita come la massima perdita probabile, PML.
La distribuzione della frequenza di perdita e la curva di probabilità di eccedenza sono entrambe curve di frequenza-severità ma vengono raffigurate in modo diverso.

Le funzioni di distribuzione di perdita sono funzioni di distribuzioni cumulate, sull'asse orizzontale viene rappresentato il range delle perdite annuali in termini di percentuale di capitale eroso, mentre sull'asse verticale è rappresentata la probabilità che la perdita non superi un certo livello di danno[30].

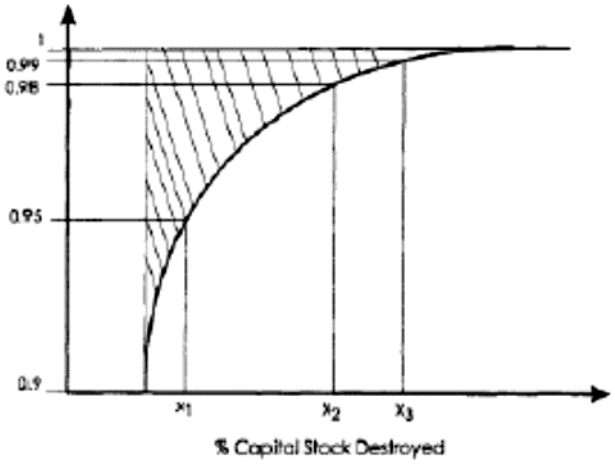

Figura 18: *Distribuzione della frequenza di perdita* (Banks (2005))

Quindi, ad esempio, nella distribuzione di perdita cumulata, mostrata in figura 18, il valore 0.98 sull'asse verticale indica che con una probabilità del 98% le perdite non supereranno il valore di danno pari a x_2 mentre con una probabilità complementare, quindi del 2%, le perdite invece supereranno tale ammontare.

Questa funzione di distribuzione di perdita rappresenta le perdite annuali e quindi la probabilità pari al 2% può essere interpretata anche come un evento 50-ennale cioè con un periodo di ritorno della perdita di 50 anni: 1/0.02=50.

Una misura importante di questa distribuzione è la perdita annua attesa cioè la perdita prevista mediamente ogni anno. La perdita annuale attesa è la somma di tutte le perdite ponderate in base alla loro probabilità di occorrenza.

In figura 17, la perdita attesa è rappresentata dall'area al di sopra della curva di distribuzione cumulata.

Un altro output finale del modello catastrofale in termini di perdita netta è la curva di probabilità di superamento, mostrata in figura 19, che rappresenta la probabilità che un determinato livello di perdita venga superato in un dato periodo di tempo.

La curva di probabilità di superamento è calcolata ordinando le perdite annuali dalla più grande alla più piccola e poi dividendo la perdita ordinata per la lunghezza del catalogo artificiale che spesso è pari a 10,000 come indicato da AIR.

[30] Banks (2005)

Quindi la prima perdita annuale rappresenterà la perdita più severa in assoluto e la la sua probabilità di superamento o di raggiungimento sarà pari a 1/ 10,000=0,01%.
Se quindi viene scelto un periodo annuale, la curva di probabilità di superamento contiene le stesse informazioni della funzione di frequenza della perdita cumulata con la differenza che l'asse verticale, nella distribuzione di perdita cumulata, rappresenta $P(X \leq x_1) = p_1$ mentre nella curva di probabilità di superamento l'asse verticale rappresenta $P(X > x_1) = 1 - p_1$.

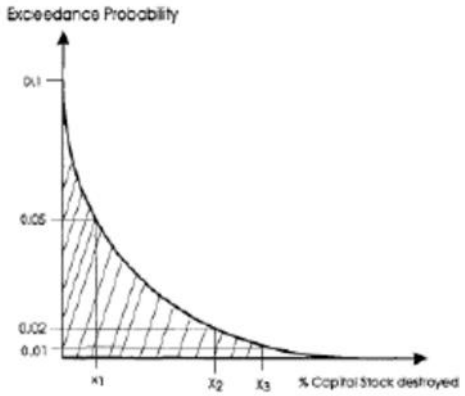

Figura 19: *Distribuzione di probabilità di superamento (Banks (2005))*

Ad esempio, la probabilità che l'ammontare di perdita x_2 sia superato è pari a 0.02.
Su questa curva di probabilità di superamento, ad una certa probabilità di eccedenza può essere associata la misura di perdita massima probabile (PML) in termini di periodo di ritorno.
Quindi, se la compagnia assicurativa decide di determinare la sua perdita massima probabile per un evento 100-ennale, poiché un evento 100-ennale ha una probabilità di accadimento annuale pari allo 0.01, allora la PML è x_3 che corrisponde al quantile 0.01 cioè all'evento 100-ennale. Si tratta dello stesso concetto della misura di rischio Value at Risk.
Come si può vedere la curva di probabilità di superamento è un'estensione della curva frequenza-severità della perdita aggregata netta e rappresenta la modalità più comune con cui il modello catastrofale restituisce l'informazione sulla perdita raffigurando la probabilità di perdere più di un determinato ammontare sull'asse verticale rispetto alla quantità di perdita sull'asse orizzontale. E' una curva utile sia per le compagnie assicurative che devono stabilire dei limiti di soglia in base ai quali prendono decisioni di copertura riassicurativa o di cartolarizzazione sia per gli investitori del mercato dei capitali per valutare il potenziale rischio di un titolo ILS, ad esempio un catastrophe bond.

E’ possibile costruire anche la curva di ritorno della perdita, mostrata in figura 20, che è un’altra versione della curva frequenza-severità, raffigurante la dimensione della perdita sull’asse verticale e la stima del periodo di ritorno sull’asse orizzontale.
Il periodo di ritorno è l’inverso della probabilità annuale di superamento.

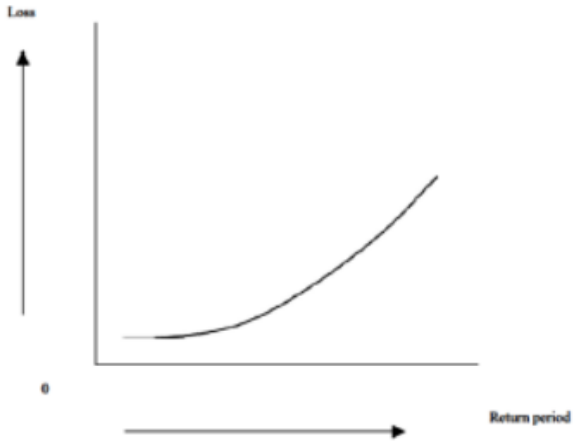

Figura 20: Curva di ritorno della perdita annuale (Banks (2005))

Questa funzione rivela come gli eventi che producono perdite più elevate abbiano periodi di ritorno più lunghi cioè sono caratterizzate da una bassa probabilità di accadimento.
Come si può vedere dalla figura 20, la curva è crescente e concava, bassi periodi di ritorno sono associati ad un’alta frequenza delle piccole perdite.
In figura 21 è mostrato l’effetto che deriva dal trasferimento del rischio.

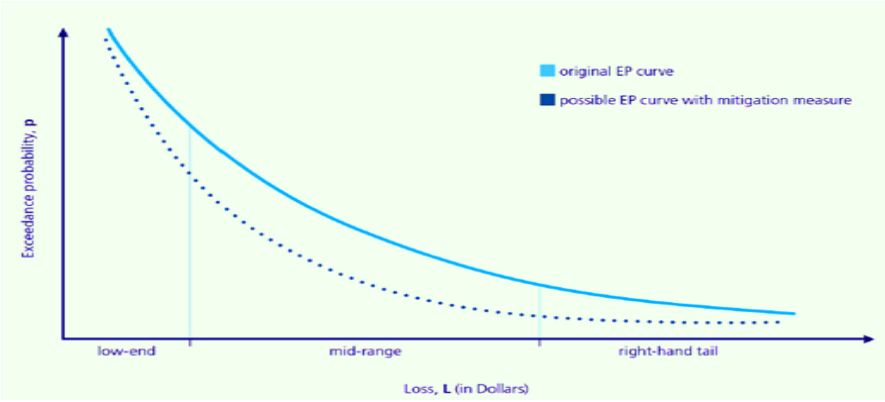

Figura 21: *Effetti del trasferimento del rischio sulla curva di PS annuale* (Schaefer (2017))

Nella coda a destra della curva di superamento sono mostrati livelli di perdita a bassa frequenza ma di elevata entità, tali livelli di perdita sono generati da eventi di elevato impatto in termini di danni.

Questi rischi di coda possono essere gestiti utilizzando ad esempio la strategia di trasferimento del rischio che permette una riduzione dell'esposizione alle perdite più estreme.

L'effetto del trasferimento del rischio produce un abbassamento nella curva che equivale ad una riduzione del rischio e quindi ad una conseguente riduzione del capitale economico immobilizzato, a fini normativi, a copertura del rischio.

Le obbligazioni catastrofali rappresentano proprio una modalità di trasferimento del rischio al mercato dei capitali.

Capitolo 3

Le obbligazioni catastrofali

3.1 La configurazione del titolo

L'obbligazione catastrofale rappresenta la strategia di trasferimento del rischio più utilizzata tra le ILS. Tali titoli di debito sono utilizzati per trasferire il rischio catastrofale, detto rischio di coda, da istituzioni finanziarie, società non finanziarie e governi, al mercato dei capitali.
A seconda del meccanismo di determinazione del trigger su cui si basa il titolo, il prezzo di questo strumento può dipendere dalle perdite assicurative, di conseguenza, è considerato una tipologia di derivato proprio perché il suo payoff dipende da un indice sottostante collegato alle perdite assicurative. Tale titolo è emesso, tramite una società veicolo, da un'entità detta cedente che è alla ricerca di capacità assicurativa o comunque di fonti alternative di capitale (Albertini e Bareaue (2009))
In figura 22 si propone la struttura del processo di cartolarizzazione del rischio catastrofale tramite l'emissione del cat bond.

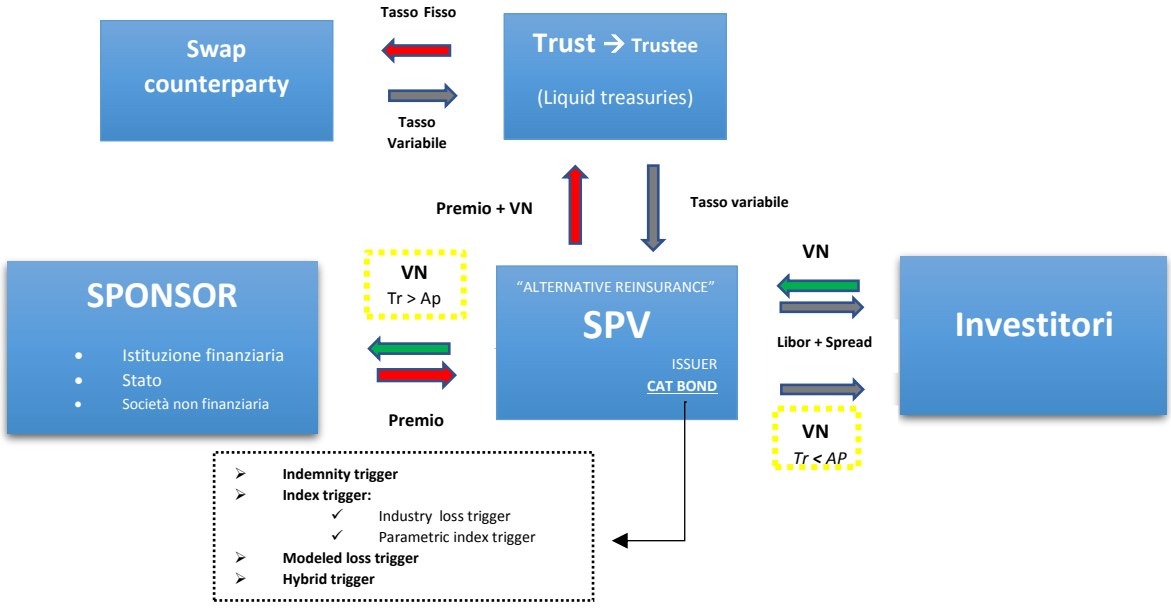

Figura 22: Configurazione del cat bond (Elaborazione personale)

La prima emissione di un catastrophe bond si è verificat nel 1994[31] e da quel momento è iniziata la sua rapida ascesa nel settore assicurativo e nel mercato dei capitali

[31] https://www.bermudareinsurancemagazine.com/article/a-short-history-of-insurance-linked-indices

Sulla base del meccanismo di determinazione del threshold, da cui dipende il payoff dell'investitore, si possono distinguere 4 categorie di cat bond:

1) Indemnity trigger
2) Index trigger
3) Modeled loss trigger
4) Hybrid

Per i cat bond indemnity trigger, il funzionamento della copertura è uguale a quello di un contratto di riassicurazione non proporzionale in quanto il payoff è strettamente legato alle perdite effettive sostenute dallo sponsor della transazione nel processo di indennizzo.
Il rischio base insito in questa tipologia è minore per lo sponsor ma al tempo stesso è maggiore il rischio di moral hazard affrontato dagli investitori. Tale trigger permette altresì una minore disclosure da parte della compagnia riassicurativa sul sottostante portafoglio.
La seconda macrocategoria è quella dei cat bond basati su index trigger, in questo caso la copertura è direttamente legata ad un indice, la cui composizione determina all'interno di questa macrocategoria un' ulteriore distinzione tra industry loss trigger, parametric index e modeled loss trigger.
I cat bond index trigger rispetto a quelli di tipo indemnity, presentano un minore rischio di azzardo morale, una maggiore trasparenza, la conseguenza di queste prime due caratteristiche li rende anche più liquidi in quanto gli investitori sono più propensi ad acquistarli rispetto a quelli di tipo indemnity per le ragioni espresse precedentemente. Presentano però un più alto rischio base per il protection buyer.
Negli industry loss index ciò che rileva è la perdita registrata dalle società del settore che mettono a disposizione i loro dati di perdita, ad esempio alla società Verisk Analytic[32]s che produce l'indice PCS Catastrophe loss index. Ciò che viene coperto e recuperato dallo sponsor è la parte di perdita, registrata a livello di settore, in eccesso rispetto ad una soglia predeterminata.
Nel cat bond di tipo parametrico, invece, il pagamento scatta quando il fenomeno naturale si verifica assumendo una certa dimensione pretederminata, in particolare ciò che rileva è il valore assunto dai parametri fisici dell'evento verificatosi, come la velocità del vento per un uragano o i millimetri o pollici di pioggia caduti al suolo per una alluvione o ancora la

[32] https://www.verisk.com/insurance/products/property-claim-services/pcs-catastrophe-loss-index/

magnitudo di un terremoto. Un vantaggio per lo sponsor è il fatto di mantenere confidenziali le caratteristiche del proprio portafoglio.

Per il cat bond modeled-loss trigger, terza macrocategoria, dopo l'occorrenza dell'evento, sulla base dei valori effettivi assunti dai parametri fisici del fenomeno, si stimano le perdite attese subite dal portafoglio dello sponsor, che non sono quelle effettive, attraverso un modello catastrofale che utilizza come input questi parametri fisici reali: la copertura scatta se le perdite stimate sono superiori ad una certa soglia.

I cat bond hybrid presentano un trigger che è la combinazione dei precedenti.

La maggior parte delle transazioni è di tipo indemnity, come indicato da Swiss RE (2018), per cui strutturano come una copertura da riassicurazione non proporzionale di tipo excess of loss.

Questo peculiare bond è un titolo a reddito fisso che, come un bond tradizionale, offre all'investitore, il fornitore di capitale che si assume il rischio catastrofale, la possibilità di ricevere una remunerazione di entità predefinita, in epoche predeterminate al momento dell'emissione. Tale provento è una remunerazione non dipendente dal livello di redditività del soggetto emittente in quanto è garantito dalla gestione di un patrimonio separato da parte di un trustee esterno.

Il contratto obbligazionario può essere annuale o pluriennale e, a determinate condizioni, rimborsa il valore nominale cioè il capitale investito a scadenza.

A differenza di un bond tradizionale, gli investitori sono soggetti ad un fenomeno stocastico naturale o tecnico che, una volta verificatosi, li espone al rischio di perdita totale o parziale del valore nominale e/o dei coupons. Di conseguenza le obbligazioni catastrofali si caratterizzano per avere pagamenti condizionati ad un evento che presenta certe caratteristiche fisiche oppure che causa determinati livelli di perdite economiche, detto trigger, stabilito all'emissione. Inoltre, tale aleatorietà non dipende dalla situazione finanziaria in cui versano emittente e cedente.

Nel periodo a rischio, la copertura può essere attivata non solo dall'avverarsi di un singolo evento ma può essere prevista l'occorrenza congiunta di più eventi, in quest'ultimo caso si parla di cat bond multi-pericolo (Albertini e Bareue(2009)).

Nel processo di cartolarizzazione, le perdite, a cui è associata una probabilità di accadimento o di superamento, cioè in base ai quantili della loss distribution, sono suddivise in più layer più o meno rischiosi.

Le perdite effettive registrate dalla cedente o quelle stimate devono eccedere un predeterminato ammontare detto attachment point, cioè un livello superato il quale scatta il

pagamento e l'investitore subirà la perdita totale del capitale investito nel caso in cui le perdite della cedente eccedano oltre che l'attachment point anche il punto di copertura totale detto exit point. Questa parte eccedente che va dall'attachment point fino alla copertura totale nel punto di exit point è proprio il layer.

Nel paragrafo successivo si descriverà il premio al rischio del cat bond secondo questa impostazione.

Per quanto riguarda la transazione, la cui architettura è mostrata in figura 23, la compagnia cedente il rischio utilizza uno special purpose vehicle che è una società giuridicamente autonoma costituita appositamente per questa transazione e situata generalmente in un paradiso fiscale, a cui la compagnia assicurativa o riassicurativa, detta cedente o sponsor dell'emissione, cede il rischio contro il versamento di un premio.

Questo veicolo speciale trasferisce il rischio mediante l'emissione di questi titoli sul mercato ed in caso di insolvenza di questa società gli investitori non possono rivalersi sulla compagnia sponsor. Quindi è la società veicolo che emette in questo caso il prestito obbligazionario, i cui pagamenti cedolari ed il rimborso del capitale, per la durata del titolo, sono condizionati dalla pericolosità di una predeterminata zona geografica, in termini di esposizione al rischio catastrofale, dalla dinamica stagionale degli eventi naturali, dal valore che assumerà un certo indice predefinito rappresentante il rischio o dalle perdite effettive affrontate dalla compagnia per i danni subiti dagli asset a rischio in quella zona geografica.

Il veicolo, emettendo il prestito e quindi trasferendo agli investitori il rischio o i rischi connessi alla copertura pattuita, svolge una sorta di ruolo di un riassicuratore verso la compagnia cedente. La durata di questo contratto di cessione non può essere superiore a quella del prestito obbligazionario.

Inoltre, il veicolo accantona il valore nominale e i proventi in un patrimonio separato mediante il ricorso ad un trust attraverso il quale tali beni sono gestiti da un trustee che investe il capitale raccolto con l'emissione del titolo in asset liquidi, ad esempio può investire in un money market fund.

Questi asset liquidi separati dal patrimonio della SPV assumono la funzione di collateral sia dal punto di vista degli investitori-protection seller sia dal punto di vista della cedente perché garantisce la copertura delle sue perdite.

I flussi in entrata di questa società appositamente costituita comprendono i premi pagati dalla cedente nella stipula del contratto, il capitale raccolto mediante il prestito obbligazionario e i rendimenti derivanti dalle attività-collateral.

I flussi in uscita invece prevedono i pagamenti cedolari, il rimborso del capitale a scadenza del titolo e, in caso di accadimento del trigger event oggetto del contratto, i risarcimenti dovuti alla compagnia assicurativa che ha cartolarizzato il rischio mediante questo meccanismo.
L'ammontare dei risarcimenti che il veicolo erogherà al cedente-protection buyer coincideranno in toto o per una percentuale con la somma che ha ricevuto in prestito.
Il trustee oltre ad investire i proventi in investimenti con orizzonte temporale breve può garantire la copertura alla cedente con una operazione swap ma dopo la crisi finanziaria del 2008 con il fallimento di diverse controparti, questa modalità di copertura è andata riducendosi nel tempo[33].

3.2 Lo spread del cat bond

Il premio è simile a quello ricevuto da un bond che comporta un elevato rischio di credito ma con la differenza che la perdita del capitale deriva non dal default ma dall'occorrenza della catastrofe naturale.
Questo premio al rischio o spread rispetto al risk free rate, Libor, del catastrophe bond, secondo la letteratura è determinato da diversi fattori (Andrego Pinto and Zilberman (2014), Papachristou (2011), Mitchell-Wallace et al. (2017),Braun (2012),Lei et al(2008), Lane (2001), Bodoff(2009)).
E' stata condotta un'analisi di regressione lineare OLS mediante Excel verificando empiricamente se esiste o meno una relazione tra spread e perdita attesa del cat bond.
L'analisi è stata effettuata su un campione di 94 cat bonds, tale dataset contiene dati su diverse emissioni di cat bonds, intercorse tra il 2015 e il 2019, estrapolati da diversi reports forniti da compagnie di riassicurazione, tra cui Swiss RE e Willis Re, dalla società veicolo Bermuda e dalla banca dati Artemis, ed includono cat bonds indemnity, loss industry index e parametric index trigger.
La scelta delle specifiche transazioni è stata effettuata sulla base delle informazioni disponibili, in particolare, informazioni sullo spread e sulla perdita attesa associata ai titoli.
Il risultato della regressione lineare è mostrato in figura 23.

[33] RMS (2012)

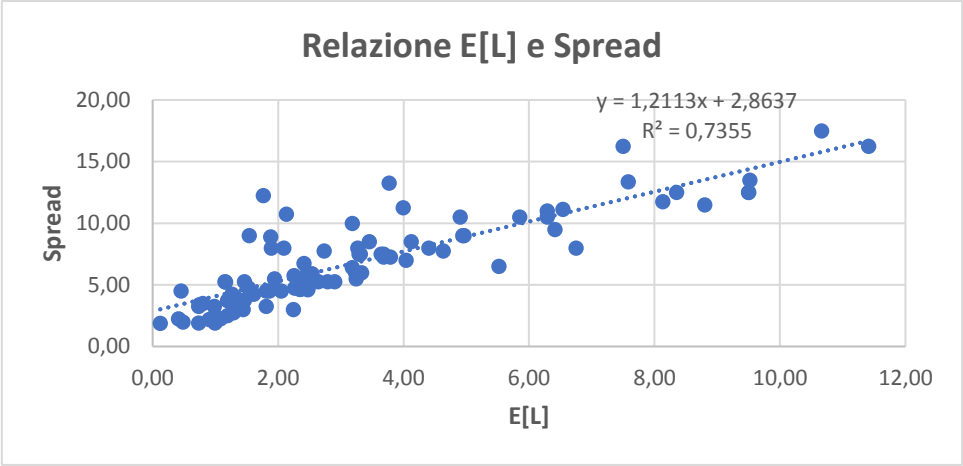

Figura 23: Spread funzione lineare della perdita attesa (Elaborazione personale)

Dal grafico si evince il fatto che lo spread è una funzione lineare della perdita attesa.
Un elevato numero di cat bonds presenta una perdita attesa tra l' 1% ed il 4%.
Si rilevano anche pochi cat bonds con valori estremi di perdita attesa maggiori del 8%.
Nel campione tali valori sono rappresentati da cat bonds ti tipo indemnity trigger
con sottostante l'evento uragano negli U.S.
In linea con la letteratura il rendimento derivante da un cat bond è mostrato in figura 24.

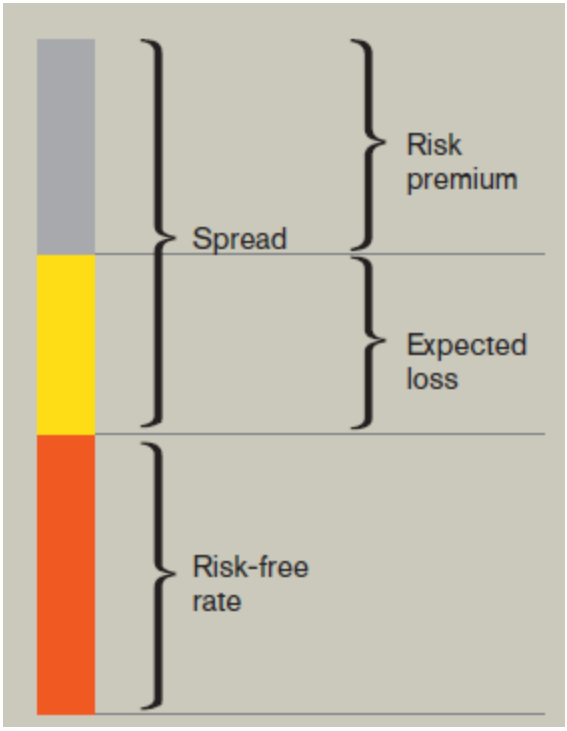

Figura 24: *Rendimento del cat bond* (Partner Re(2015))

Il coupon rate percepito dagli investitori è la risultante di due componenti: il risk free rate e lo spread, quest'ultimo remunera gli investitori per il rischio assuntosi, quindi può essere visto come il premio cioè il prezzo di emissione pagato dalla compagnia agli investitori per fare hedging del rischio catastrofale:

$$\%\ COUPON\ RATE = \%\ EURIBOR + \%\ SPREAD$$

Lo spread, cioè il rendimento differenziale, a sua volta remunera la componente di expected loss e offre un rendimento aggiuntivo detto expected excess return (EER):

$$\%\ SPREAD = \%\ E(L) + \%\ EER \text{ o risk premium}$$

Lo sponsor, infatti, si attende una certa perdita a fronte del verificarsi dell'evento catastrofale, che rappresenta l'output del cat model. Questa quantità è misurata dalla perdita attesa E(L) o annual average loss AAL.
Per l'investitore questa quantità misura la perdita mediamente associata all'investimento e rappresenta l'area sotto la curva di probabilità di superamento, mostrata in figura 25.

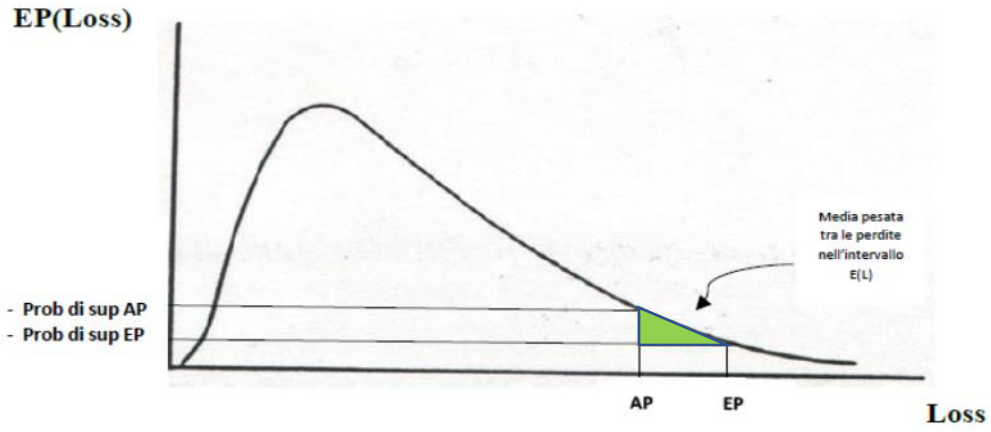

Figura 25: Curva di PS nella prospettiva del protection seller (rielaborazione su Arpa)

La componente di rendimento atteso in eccesso, EER o premio per il rischio, può essere intesa come funzione del downside risk che quantifica l'entità degli scarti rispetto al valore medio cioè il rischio di perdere non la media delle perdite relative all'intervallo tra l'attachment point (AP) e l'exaustion point (EP) ma tutto il capitale a rischio.

Questo contribuisce a spiegare il risultato della regressione con variabile esplicativa E[L]. Tale regressione infatti spiega solo lo 0.73 della variabilità dello spread.

Infatti, la figura 25, mostra la curva di probabilità di superamento, dove sulla y è riportata la probabilità di superare un determinato livello di perdita e quindi vi sono riportate le probabilità di superamento dell'AP ed dell'EP mentre sulla x sono rappresentate le perdite aggregate. La perdita che in media si subisce il protection seller è pari alla media delle perdite nell'intervallo [AP,EP], tale valore rappresenta appunto per il protection seller la perdita media associata all'investimento. Il livello exit point rappresenta la copertura massima e coincide con il valore nominale del titolo cioè rappresenta la perdita massima subita dall'investitore.

L'evento catastrofale, infatti, attiva la perdita prevista dal layer che rappresenta la perdita coperta dagli investitori. A questa perdita è associata una probabilità di superare un determinato livello, che può essere l'output del catastrophe model. Tale probabilità coincide con la probabilità di attachment point per gli investitori.

Al verificarsi di tale perdita, il layer può essere completamente esaurito, quindi si verificherà la completa copertura e la conseguente perdita di tutto il capitale investito perché l'impegno del protection seller consiste nel risarcimento dei sinistri che eccedono un determinato ammontare fino ad una misura massima cioè la parte di layer. Mentre fino al di sotto dell'AP il danno è a carico della cedente. E questo approccio è utilizzato anche nella formula stop loss nella riassicurazione non proporzionale, secondo la quale, l'intervento del protection seller avviene quando le perdite subite dalla cedente superano una soglia prefissata ex-ante detta attachment point.

Quindi la perdita attesa è solo una porzione dello spread in quanto gli investitori essendo avversi al rischio richiedono un premio aggiuntivo dovuto principalmente all'incertezza sulla perdita attesa e quindi sulla distribuzione di probabilità delle perdite associate al rischio catastrofale.

Una parte della letteratura[34] ha proposto modelli di regressione multipla per spiegare come varia la componente di premio al rischio aggiuntivo o EER, e quindi il rendimento atteso, proponendo diversi fattori di rischio. Ad esempio, il tipo di trigger su cui si basa il cat bond ha un certa influenza, in quanto, esiste un trade off tra rischio base in capo allo sponsor e opacità in termini di trasparenza in capo all'investitore che influisce sulla percezione dell'incertezza rispetto alla perdita attesa. Tale trade off è mostrato in figura 26.

[34] Bodoff, Gan (2012), Lane, Mahul(2008)

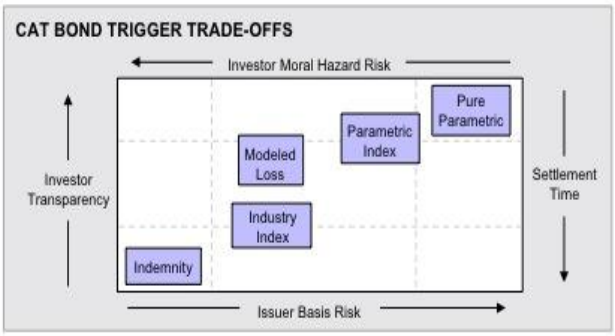

Figura 26: *Trade off tra sponsor ed investitore nelle varie tipologie di trigger (Swiss Re)*

Se ad esempio il bond ha come trigger un parametro fisico legato al rischio, tipo parametric index, ciò riduce sensibilmente il rischio in capo all'investitore ma per la compagnia il rischio effettivo rispetto a quello stimato dai modelli catastrofali potrebbe risultare più elevato e di conseguenza il premio pagato agli investitori sarà molto basso.
Mentre un cat bond indemnity based pagherà un premio molto più alto, in quanto gli investitori sono esposti ad una maggiore incertezza.
In questo caso l'incertezza deriva dalla qualità del portafoglio di esposizioni della cedente, dalla modalità di svolgimento del processo di liquidazione delle perdite e dallo svantaggio informativo in merito alla vera esposizione sottostante il bond.
Inoltre, dal lato dell'offerta, c'è da considerare anche la componente liquidity risk premium in quanto i cat bonds sono titoli illiquidi. E' prevista comunque in futuro una maggiore liquidità nel mercato secondario[35] e quindi una conseguente riduzione del premio per la liquidità

3.3 Processo di Poisson

I processi di Poisson rivestono un ruolo centrale sia a fini di modellizzazione del fenomeno catastrofale sia a fini di pricing.
Per la trattazione dei processi di Poisson si è fatto riferimento in particolare a Ibe (2009) e Ross (2007)
Gli eventi catastrofali possono essere interpretati come degli arrivi casuali indipendenti e ad istanti di tempo casuali.
Nel processo di Poisson il numero degli eventi-salti in ogni intervallo di tempo segue una distribuzione di Poisson con media pari a λ volte la lunghezza dell'intervallo, quindi $\lambda\Delta$, ed il numero di eventi in intervalli disgiunti sono tra loro stocasticamente indipendenti.

[35] Aon(2018), Swiss Re(2018)

Un processo di Poisson è utilizzato per descrivere un fenomeno che presenta arrivi nel tempo. Ad esempio, uno sportello di una banca dove un numero di clienti sono in coda, in attesa di essere ricevuti, e supponiamo che solo un cliente alla volta potrà essere servito allo sportello, allora in ogni istante di tempo t ci sarà un cliente che sta usufruendo del servizio ed un numero di clienti che sta attendendo in coda.

T_m è l'istante di arrivo dell'm-simo cliente in coda o tempo di arrivo, tali variabili sono iid in modo esponenziale. Mentre $A(t)\ con\ t > 0$ è il numero totale di clienti che sono arrivati alla coda nell'intervallo $(0, t]$. Il valore $A(t)$ incrementa di una unità ad ogni istante di arrivo di un nuovo cliente cioè in corrispondenza di ciascun istante di arrivo T_m, quindi $A(t)$ è detto processo contatore o di conteggio. L'andamento tipico di una realizzazione del processo di conteggio è mostrato dalla figura 27, dove T_m è appunto l'istante o tempo di arrivo dell'm-simo cliente alla coda, con m=1,2,3,4.

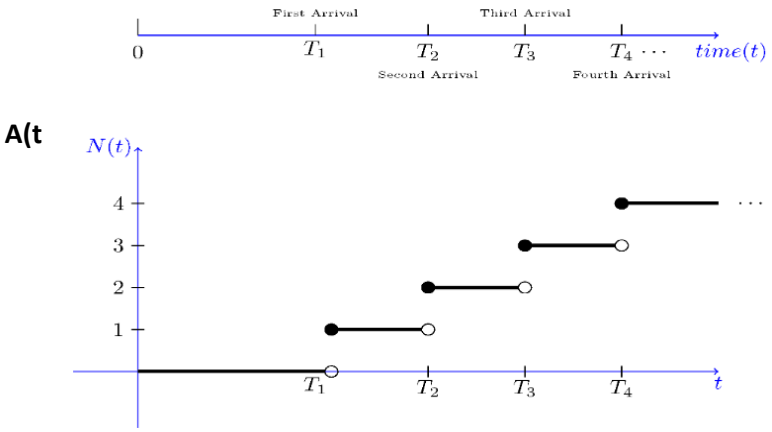

Figura 27*: Realizzazione di un processo di conteggio (Pishro-Nik, Kappa Research LLC (2014))*

L'istante di arrivo T_m alla coda dell'm-esimo cliente non è noto a priori quindi è la determinazione di una variabile casuale a valori reali e definita su uno spazio di probabilità (Ω, B, P).

La sequenza degli istanti di arrivo $\{\ T_m(\omega) \in R,\ m = 0,1,2,3, \ldots\ldots;\ \omega \in \Omega\}$ è modellata come una sequenza casuale di tempi o istanti di arrivo.

Il corrispondente numero totale di arrivi $A(t)$ che si sono verificati nell'intervallo di tempo (0,t] è una determinazione di una variabile aleatoria, per ogni valore di t ≥0.

$A(t; \omega) \in \{0,1,2 \ldots\}$; $\omega \in \Omega\}$ è la realizzazione di un processo stocastico a valori interi, non negativi e a tempo continuo. Questo processo è un processo di conteggio di Poisson con tasso λ, arrivi per unità di tempo, se soddisfa le seguenti proprietà:

a) A(0)=0 , A(t) assume solo valori interi non negativi
b) La differenza $A(t_1) - A(t_0)$, per ogni coppia di istanti $t_1 > t_0 \geq 0$, rappresenta il numero di arrivi nell'orizzonte temporale o intervallo $(t_0, t_1]$
c) Per ogni M-pla di istanti, ad esempio per ogni 4-pla di istanti $t_3 > t_2 > t_1 > t_0 \geq 0$ le due variabili casuali "differenza" sono tra di loro stocasticamente indipendenti: $A(t_2) - A(t_1)$, $A(t_3) - A(t_2)$

Quindi un processo contatore di Poisson è un processo stocastico ad incrementi indipendenti.

d) Il numero di arrivi nell'intervallo di tempo Δ>0 è una variabile aleatoria di Poisson con valore medio pari a λΔ:

$$\mathrm{P}(\mathrm{A}(\mathrm{t}+\Delta) - A(t) = k) = e^{-\lambda\Delta}\frac{(\lambda\Delta)^k}{k!} \; con\; k = 0,1,2,3, \ldots\ldots$$

Dove il tasso λ del processo contatore di Poisson indica il numero medio di arrivi per unità di tempo. Ed inoltre il numero di arrivi in intervalli di tempo disgiunti sono determinazioni di variabili aleatorie stocasticamente indipendenti cioè vale il punto c) della precedente definizione.

Quindi, in conclusione se S è un insieme in uno spazio unidimensionale, la semiretta positiva, ed *A* è una σ-algebra cioè una famiglia di sottoinsiemi di S, che è una collezione di intervalli della forma A=(s,t], allora il processo puntuale in S è un processo stocastico N(A) con A ∈ *A* che ha come valori possibili la collezione di elementi dell'insieme {0,1,2,…} che conta i punti in A che si trovano dispersi in maniera aleatoria in S. E questo processo è un processo puntuale di Poisson di intensità λ se N(A) ha una distribuzione di Poisson con parametro λA ed il numero di punti in intervalli disgiunti sono tra loro stocasticamente indipendenti.

3.4 Metodologia di pricing

In letteratura sono diversi i metodi per il pricing dell'obbligazione catastrofale proposti che sono accomunati dal fatto di considerare la componente spread come funzione della perdita attesa. Si veda Ma and Ma (2013), Burnecki, Kukla (2003), Mayo, Taylor (2001).

Briys (1997), Baryshnikov et al. (2001) sviluppano un modello di pricing in un contesto arbitrage-free e sotto l'ipotesi di mercato completo.

Si fa, inoltre, ricorso anche alla teoria dei valori estremi per modellare sulla base dei dati storici la dinamica dell'intensità del fenomeno naturale sottostante il titolo, per poi combinare tale modello con un modello stocastico per la dinamica del tasso di interesse (Zimbidis et al.(2007)).

Un filone della letteratura, invece, si concentra sull'individuazione dei fattori che influenzano lo spread del titolo, ad esempio Lane e Maku (2008) e Nowak (2013) identificano come fattori rilevanti il ciclo del mercato riassicurativo, la perdita attesa e la dinamica dell'evento sottostante.

Embrechts (1997) e Loubergé et al. (1999) sviluppano un approccio stocastico secondo il quale nel modello di valutazione le perdite sono rappresentate da un processo composto di Poisson.

Cox e Pedersen (2000) mettono in luce l'incompletezza del mercato in quanto non esiste un portafoglio di asset che possa replicare il cat bond.

Yu e Lee (2002) utilizzano un tasso di interesse stocastico e tengono conto del rischio base, del rischio di credito e del moral hazard nella valutazione dell'obbligazione.

Un altro filone della letteratura, adopera misure di rischio basate su delle funzioni di probabilità distorte, in particolare, la funzione crescente detta funzione di distorsione g: $[0,1] \rightarrow [0,1], per\ cui\ g(0) = 0\ e\ g(1) = 1$, trasforma la funzione di distribuzione F(x) in una distribuzione di probabilità distorta $F^*(x)$.

Se ad esempio il titolo ha una determinata distribuzione di probabilità $F(x)$, la funzione di ripartizione corretta per il rischio sarà pari a $F^*(x) = g(u)F(x)$ ed il valore di tale titolo si ottiene scontando al tasso free risk la distribuzione corretta per il rischio.

Wang(2000) propone una trasformata di questo tipo: $g(u) = \varphi(\varphi^{-1}(u) - \lambda)$.

Sia X una variabile casuale con funzione di ripartizione F, applicando la trasformata di Wang si ha

$$F^*(X) = \varphi(\varphi^{-1}\big(F(X)\big) - \lambda)$$

da cui si può poi calcolare il valore atteso $E^*(X)$ utilizzando la distribuzione distorta $F^*(X)$.

Ad esempio, consideriamo la loss exceedance probability curve o curva di superamento del livello di perdita:

$$S(x) = 1 - F(X), dove\ F(X) = P(X < x)$$

che rappresenta le perdite derivanti dal fenomeno catastrofale con $F(X)$ che rappresenta la distribuzione cumulata della variabile casuale perdita X. Non ci sono restrizioni sul tipo di distribuzione di F(X).
Il modello di pricing basato sulla trasformata di Wang risulta il seguente:

$$S^*(X) = \varphi\left(\varphi^{-1}(S(X)\right) - \lambda)$$

La distribuzione originaria $S(X)$ viene sostituita da $S^*(X)$ che dà più peso alla coda shiftando il percentile della loss distribution originaria.
La trasformata di Wang consente quindi il pricing di un'obbligazione mediante probabilità aggiustate per il rischio in base a questo operatore di distorsione che corregge la funzione di ripartizione da cui derivano valori attesi ponderati per il rischio con il tasso privo di rischio. Il modello dipende dalla scelta del parametro λ.
Se F(X) è normale o log-normale, è stato dimostrato che $E(X)^* = E(X) + \lambda\sigma$ mentre $\sigma^* = \sigma$.
Wang inoltre propone anche un modello in cui sostituisce alla normale la distribuzione t di Student per tenere conto dell'asimmetria della distribuzione di perdita.
L'evento catastrofale, sottostante al catatastrophe bond, è simile all'evento default di un'obbligazione ordinaria. Di conseguenza per comprendere i meccanismi che regolano gli eventi estremi di insolvenza e catastrofali naturali si possono utilizzare i modelli basati sull'intensità, detti modelli a forma ridotta relativi al rischio di credito.
Questi modelli adottano un approccio che si focalizza sulla probabilità di accadimento dell'evento estremo e cercano di descrivere le proprietà statistiche del processo che porta all'avveramento di tale evento in modo tale da poter effettuare la valutazione del titolo.
Nel rischio catastrofale, si può ipotizzare che il momento in cui si verifica l'evento trigger è quello in cui la perdita aggregata L_t supera una certa soglia S_t.
L'evento è modellato come un tempo o momento d'arresto C ovvero una variabile casuale non negativa per cui la filtrazione $\mathbb{F}_T$ porta informazioni sul fatto che C si sia verificato o meno nell'intervallo. C rappresenta il tempo d'arresto in cui avviene l'evento catastrofale che determina il superamento del threshold level S: $C = \min[t \geq 0: A(t) > 0]$. Ed in linea con il processo stocastico di Markov C descrive proprio il passaggio tra lo stato in cui non si sono ancora verificati degli eventi allo stato in cui invece il processo inizia a conteggiare gli eventi avveratisi.

I processi di Poisson puntuali a tempo continuo sono adatti per l'analisi di questi eventi estremi in quanto il momento d'arresto C può farsi coincidere con il salto iniziale ossia con la catastrofe, come individuato dalla figura 28:

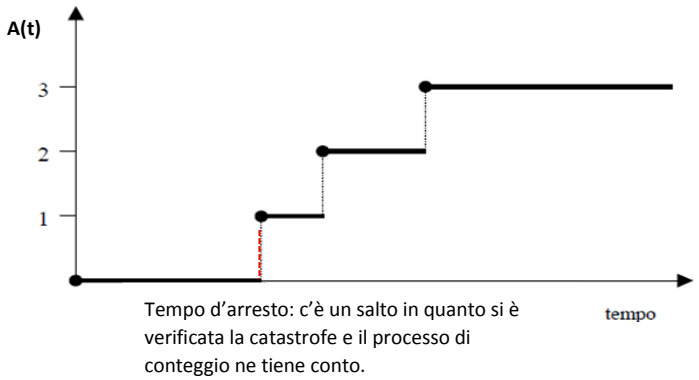

Figura 28: Processo di conteggio A(t) con i salti-istanti in cui avvengono gli eventi catastrofali (rielaborazione su Matta)

Tale processo di conteggio A(t) è il processo di Poisson e C_i sono i passaggi da uno stato all'altro disgiunti in cui avvengono i salti del processo.
Se il λ dell'evento-salto è costante nel tempo allora il processo poissoniano si dice omogeneo ed è caratterizzato dal fatto di essere un processo puntuale A(t) governato dalla distribuzione di Poisson, ossia il numero di accadimenti dell'evento in un intervallo di tempo ha distribuzione di Poisson di parametro λ, mentre gli intervalli di tempo intercorsi tra due eventi sono indipendenti si considerano iid in modo esponenziale.
Se invece tale parametro non è indipendente dal tempo ma rappresentabile come λ_t , il processo prende il nome di processo di Poisson non omogeneo.
La differenza tra processo di Poisson omogeneo e non omogeneo sta nel fatto che nel primo processo λ_t è una costante.
Se invece il parametro λ è descritto da una relazione di tipo stocastico, il p.s. si dice Processo di Poisson doppiamente stocastico, definito come un processo di Poisson N(t) condizionale al processo stocastico dell'intensità Λ_t.
La differenza tra questo processo e il non omogeneo è che nel secondo caso Λ_t è deterministica.
In linea quindi, con le similarità tra l'evento naturale catastrofico sottostante al cat bond e l'evento estremo default del corporate bond è possibile sviluppare il seguente modello di pricing.

Per quanto riguarda la compagnia assicurativa la perdita aggregata, output del modello catastrofale, presentando una distribuzione composta attraverso convoluzioni dalla frequenza degli eventi catastrofali e dalla severity cioè l'ammontare di perdita derivante dal realizzarsi dell'evento avverso, si assume che il processo delle perdite accumulate segua un processo di Poisson composto (Compound Poisson process).

Questo processo è una generalizzazione del processo di Poisson che consente salti di grandezza non necessariamente unitaria, la cui definizione è la seguente:

Un processo stocastico $\{X(t), t \geq 0\}$ è un processo di Poisson composto se può essere rappresentato da $L(t) = \sum_{i=1}^{A(t)} L_i \ , t \geq 0$, dove $\{A(t), t \geq 0\}$ è un processo di Poisson di conteggio con tasso di arrivo degli eventi λ e $L_1, L_2, \ldots$ sono variabili casuali non negative iid che sono indipendenti dal processo A(t) e rappresentano i livelli di perdita singoli. E quindi i sinistri sopraggiungono secondo un processo di Poisson le cui quantità L_i sono variabili casuali identicamente e indipendentemente distribuite.

L'ammontare cumulato di perdita L_t derivante dai sinistri sopraggiunti al tempo t è appunto una realizzazione di un p.s. Poisson composto.

La media e la varianza sono dati da:

$$E[X(t)] = \lambda t \, E(L_1) \ \ e \ \ \sigma^2[X(t)] = \lambda t \, E\left[\left(L_1{}^2\right)\right], \ \ t \geq 0$$

Questo è dovuto al fatto che sia media che varianza del processo di Poisson $A(t)$ sono uguali a λt.

La relazione tra perdita aggregata, cat bond ed evento catastrofale risulta quindi la seguente: si assume l'esistenza di un processo puntuale di Poisson $A(t) \ con \ (t \ \epsilon \ [0, T])$ che descrive la dinamica o afflusso dei potenziali eventi catastrofali di un certo tipo, in una determinata zona. Informazioni specificate al momento dell'emissione e quindi predeterminate.

L'intensità di questo processo non è costante cioè il tasso è una funzione del tempo, λ_t ,in quanto sembra più rappresentare la realtà rispetto ad un'intensità costante.

La probabilità di ottenere n eventi per unità di tempo è: $Pr\{n\} = \frac{(\lambda t)^n}{n!} e^{-\lambda t}$ ed il numero di eventi dal tempo 0 al tempo t ha una distribuzione di Poisson.

C è il momento d'arresto su un orizzonte temporale finito T cioè l'istante, o passaggio di stato, in cui la perdita aggregata L_t eccede il threshold level S cioè $C = inf\{L_t > S\}$, dove:

$$C > T = \ L_t \leq S \rightarrow \ non \, supera \ \text{ mentre } \ C \leq \ T \ = \ L_t > S \rightarrow supera.$$

Il momento di trigger è quindi l'istante in cui la perdita aggregata L_t eccede il livello S cioè $L_t > S$.

Le singole perdite assicurate derivanti da ogni evento lungo il periodo di istanti in cui accadono gli eventi, come detto precedentemente, sono variabili casuali indipendentemente e identicamente distribuite L_i con funzione di distribuzione:

$$F(x) = P\{L_i < x\}$$

Pertanto, date queste assunzioni il processo di perdita aggregata continuo descritto da un processo Compound Poissonè definito come:

$$L_t = \sum_{t_j<C} L_i = \sum_{j=1}^{A(t)} L_i$$

Con t_j indicante gli istanti degli eventi avversi mentre $A_t\, e\, L_i$ sono assunti essere indipendenti.

Considerando uno zero coupon cat bond[36] con un payoff pari a $P_{cat}(T)$ di un ammontare pari a VN alla scadenza T, la struttura di questo payoff è data da:

$$P_{cat}(T) = \begin{cases} VN\ se\ L_T \leq S \\ 0\ se\ L_T > S \end{cases}$$

dove S è il valore di soglia predeterminata nel contratto e L_T è la perdita aggregata alla scadenza T.

Nel caso in cui la perdita aggregata superi il trigger al tempo T l'investitore perde VN. Quindi il prezzo dello zero-coupon bond al tempo t che paga VN alla scadenza è legato alle variabili: threshold level S, dinamica catastrofale $A(t)$ e funzione di distribuzione di perdita $F(x)$.

Queste sono anche le variabili che sono state indicate come determinanti,nel precedente paragrafo dello spread.

Di seguito si riassumono le ipotesi da cui il modello di pricing è ricavato:

- Le perdite assicurate derivanti da ogni evento catastrofale sono $L_i \geq 0$ e considerate iid con funzione di distribuzione F(x)= P{L_j<x}

[36] Ma e Ma(2013), Burnecki e Kukla(2003)

- L'arrivo dei sinistri-eventi osservati fino al tempo t segua un processo di Poisson non omogeneo $A(t)$ e con intensità λ_t
- Si assume inoltre, assenza di arbitraggio e completezza del mercato
- con un tasso r free risk tale che al tempo t di 1 dollaro pagato al tempo T sia $e^{-R(t,T)} = e^{-\int_t^T r_s\, ds}$ (in questo caso si fa riferimento al money market account[37] cioè il conto di mercato monetario che è una sorta di titolo che vale 1 dollaro al tempo zero e frutta continuamente il tasso r istantaneo).

L'assunzione di assenza di opportunità di arbitraggio in un mercato completo implica l'esistenza di una misura di probabilità neutrale al rischio Q in base alla quale il valore del bond è pari al valore attuale atteso del prezzo a scadenza sotto la misura di probabilità neutrale al rischio Q condizionale alla filtrazione e al fattore di sconto risk free:

$$V_t = E^Q\left(P_{CAT}(T)e^{-\int_t^T r_s\, ds}\middle|\mathbb{F}_T\right)$$
$$= E^Q\left(e^{-\int_t^T r_s\, ds}\cdot(Z\cdot P(L_T \le S) + 0\cdot P(L_T > S)\right)$$
$$= E^Q\left(e^{-\int_t^T r_s\, ds}\cdot(Z\cdot P(L_T \le S) + 0\cdot(1 - P(L_T \le S))\right)$$
$$= E^Q\left(e^{-\int_t^T r_s\, ds}\cdot(Z\cdot P(L_T \le S)\right)$$

In questo modello di pricing il cat bond è quindi dato dal valore attuale atteso dei flussi di cassa futuri sotto una misura di probabilità neutrale al rischio Q. Il problema principale, come mostrato da Cox e Pedersen, è che il mercato dei cat bonds non è completo. Quindi è necessario un diverso framework per il pricing come l'approccio basato sulla trasformata di Wang che distorce la distribuzione di probabilità per generare valori attesi aggiustati per il rischio che possono essere scontati al tasso risk free.

[37] J.C. Hull (2015)

Capitolo 4

Nuove frontiere: la securitization del rischio informatico

4.1 Opportunità e problematiche del mercato assicurativo cyber

Secondo l'EIOPA (2018) la domanda di copertura assicurativa è in costante aumento e gli analisti di Morgan Stanley prevedono che il mercato cyber varrà tra gli 8 e i 10 miliardi di dollari entro il 2020[38].

Tali aspettative sono avvalorate dal processo di digitalizzazione dell'economia in atto e dalla conseguente pervasività delle tecnologie dell'informazione e delle telecomunicazioni nella vita quotidiana che determinano una maggiore esposizione al rischio informatico.

Nel settore non prevale né una definizione di cyber risk nè una tassonomia per categorizzare i diversi tipi di incidenti informatici.

La Geneva Association (2016), think thank internazionale, ha avanzato la seguente definizione di rischio informatico: "qualsiasi rischio derivante dall'uso di tecnologie dell'informazione e della comunicazione (ICT) che comprometta la riservatezza, la disponibilità o l'integrità dei dati o dei servizi".

Attualmente il mercato assicurativo per il cyber risk è ancora poco sviluppato, l'offerta di prodotti assicurativi cyber è limitata e relativamente costosa rispetto ad altri tipi di copertura assicurativa.

Tra il 2015 e il 2016 il mercato mondiale delle polizze informatiche stand alone cioè specificatamente dedicate ai cyber rischi è arrivato a 3,5 miliardi di dollari (OECD, 2017) di cui 3 miliardi sottoscritti negli Stati Uniti e 300 milioni in Europa (PWC, 2015).

Invece secondo stime riferite all'anno 2017, il mercato statunitense rappresenta circa l'80% - 90% del mercato cyber totale, l'assicurazione cyber rappresenta comunque una piccola quota del totale dei 555 miliardi di dollari in premi per quanto riguarda il ramo property e casualty (EU-U.S. Insurance Dialogue Project), mentre l'Unione Europea detiene una quota del mercato tra il 5% e il 9%.

In media il livello di copertura disponibile è stimato tra i 25 milioni di dollari e i 100 milioni di dollari ma per le grandi imprese e per i service provider può arrivare fino ai 500 milioni di dollari.

[38] https://www.morganstanley.com/ideas/Cyber-security-risks-and-opportunities

I premi per le coperture informatiche invece sono tre volte più alti rispetto alle tradizionali coperture (Swiss Re, OECD; 2017).

In Europa le tipologie più comuni di cyber insurance sono le polizze che indennizzano per l'interruzione dell'attività (BI[39]) e per spese di ripristino dei dati perduti mentre sono diffuse in misura minore rispetto agli Stati Uniti la copertura da estorsione cibernetica, le coperture delle spese legali da responsabilità verso terzi e la polizza che indennizza da danni d'immagine e di reputazione.

Gli incidenti informatici dolosi e accidentali possono causare danni per centinaia di milioni di dollari, il costo totale medio di un data breach si attesta intorno ai 3,62 milioni di dollari (Ponemon Institute, 2017).

L'entità delle perdite conseguenti a questi eventi variano ovviamente in base al settore industriale di appartenenza della società indennizzata, ad esempio i settori più regolamentati e i settori il cui core business è il trattamento di dati sensibili sopportano maggiori costi. Le perdite variano anche per dimensione dell'organizzazione e per tipologia di incidente informatico.

Secondo il report di Accenture Security (2018) i danni massimi dovuti a divulgazione di dati personali involontaria o dolosa si attestano tra i 486 e i 638 milioni di dollari mentre l'interruzione del sistema informatico, eccetto per il settore retail, può provocare danni per 85 milioni di dollari.

Nel 2017 in Italia il 30%-50% delle aziende ha subito cyber crime, i settori più colpiti sono stati quello finanziario e farmaceutico. E i danni totali da incidenti informatici sono stati pari circa a 10 miliardi di euro, per un danno medio di 2 milioni di euro (Ania, 2017).

La domanda di copertura per il cyber risk dipende in parte dalla divulgazione della frequenza di incidenti informatici di alta severità, dall'innovazione tecnologica e dall'evoluzione del contesto legislativo ad esempio in materia di tutela della Privacy. Infatti il numero crescente di incidenti informatici su larga scala, la continua trasformazione digitale e le nuove iniziative normative nell'Unione Europea con l'attuazione del regolamento UE, GDPR, stanno favorendo una maggiore consapevolezza del rischio cyber e un aumento della domanda di assicurazione in Europa.

L'industria assicurativa italiana sta offrendo una vasta gamma di prodotti che coprono perdite derivanti da incidenti informatici, verificatisi per dolo o per causa accidentale. Quindi viene offerta copertura sia per eventi dolosi-malevoli sia per eventi non dolosi-accidentali.

[39] Business Interruption

Premesso il fatto che non esistono attualmente prodotti standard generalmente utilizzati, nella maggior parte dei casi i prodotti cyber assicurativi si configurano come polizze all risk che offrono copertura per danni diretti e danni a terzi. Ad esempio, attivano la copertura assicurativa i seguenti incidenti informatici[40]:

- Violazione dei dati sensibili propri e di terzi che comportano costi da risarcimento danni e spese legali. Tale incidente genera responsabilità civile per le alte cariche societarie e danni reputazionali in capo alla società da cui scaturiscono che si vanno ad aggiungere ai costi suddetti.

  L'articolo 4 del GDPR[41] definisce una violazione dei dati come "la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi e conservati".

  L'introduzione della nuova normativa ha incrementato la dimensione del mercato delle polizze informatiche in quanto il regolamento europeo introduce l'obbligo di notifica di violazioni dei dati da parte dei gestori ai diretti interessati.

  Per dati sensibili e confidenziali si intendono dati finanziari, segreti commerciali o proprietà intellettuale e altri dati sui clienti tipo dati medici, per quest'ultimi esiste un florido mercato nero[42].
- Compromissione accidentale di dati riservati che si traducono nella cancellazione dei dati sensibili in seguito ad un virus che porta appunto all'alterazione dei dati oppure ad un'erronea conservazione che può portare accidentalmente al deterioramento dei dati stessi.
- Furto di dati e perdita di dati dolosa o accidentale
- Attacchi crypto-ransomware o malware, software malevoli che crittografano i dati richiedendo un riscatto per permettere nuovamente l'accesso al database oppure che danneggiano la reputazione dell'azienda mostrando pubblicità fuorviante ed indesiderata
- Attacchi detti Phishing che consistono in truffe che si tramutano ad esempio in furto di dati sensibili.
- Malfunzionamento dei sistemi informatici a causa di guasti agli hardware, manipolazione o attacco doloso ai software, ad esempio un attacco DoS[43] che

[40] Ania (2017), Swiss Re (2017), CRO Forum (2016)
[41] General Data Protection Regulation, (GDPR), EU 2016/679
[42] https://www.ey.com/en_gl/digital/why-health-care-is-a-favored-target-for-cybercriminals
[43] DoS: Denial of service

bombarda un server web con del traffico per interrompere le sue funzionalità. Tale incidente può causare interruzione dell'esercizio dell'attività e quindi provocare mancati guadagni, danni fisici al sistema ma anche infortuni ai dipendenti se si pensa ad un attacco hacker che agendo su un hardware, la componente fisica dell'infrastruttura di rete, provoca un incendio che determina a sua volta danni a persone e a cose

Sul mercato prevale la copertura corporate piuttosto che l'assicurazione cyber retail anche se con lo sviluppo e la diffusione della tecnologia dell'internet of things (IoT) si prevede un'espansione di questo segmento in quanto i consumatori stanno diventando sempre più consapevoli della loro esposizione a questo tipo di rischio con l'avvicendamento di notizie sugli attacchi informatici.

Sul mercato US, ad esempio, sono presenti prodotti assicurativi specifici per la clientela retail che coprono ad esempio il furto di identità digitale, furto di dati finanziari, spese per recupero di dati e anche il cyberbullismo. Invece tale segmento in Europa rimane ancora una nicchia.

Attualmente il rischio informatico è sotto assicurato, questo è dovuto a diverse problematiche associate alle caratteristiche di questo settore.

Il mercato assicurativo cyber è infatti estremamente complesso, la sottoscrizione della copertura cyber è una vera e propria sfida in quanto il rischio informatico per sua natura è in costante mutamento, in quanto condizionato dall'evoluzione della tecnologia, ed i dati storici disponibili sui sinistri sono insufficienti ai fini di un'accurata valutazione del rischio.

Questo è in parte dovuto al breve periodo di sottoscrizione di questo rischio, è infatti un rischio piuttosto recente, e in parte dovuto al fatto che le stesse vittime di cyber attack non diffondono questo tipo di notizie per ragioni d'immagine e reputazione. Si pensi ad esempio all' impatto sul prezzo di un titolo dopo l'annuncio di un attacco informatico.

Biener et al. (2015) hanno individuato come principali ostacoli al decollo del mercato assicurativo cyber, la forte correlazione delle perdite dovute ad uno stesso incidente informatico, la mancanza di dati che inficia sul livello di copertura offerto, in quanto dati esigui determinano volatilità nelle stime e quindi gli assicuratori tendono a fissare alti deducibili congiuntamente ad un basso livello di massima copertura, ed incide ovviamente sul prezzo finale del prodotto. E' comunque prevista dagli autori col tempo un'attenuazione di questi problemi.

Sempre l'insufficiente base dati e anche la loro scarsa qualità, che li rende di conseguenza biased, è fonte di un pericolo di sottovalutazione del rischio stesso ed inoltre rappresenta una barriera allo sviluppo di metodologie robuste e affidabili di modellizzazione probabilistica del rischio.

Le compagnie assicurative per sopperire a queste difficoltà di mancanza di dati e di skills ICT potrebbero stipulare partnership con società specializzate nella sicurezza tecnologica dell'informazione per avere accesso ad una più ampia mole di dati sugli incidenti informatici. Poi in realtà c'è anche il problema che, anche se questi dati fossero disponibili, potrebbero risultare comunque inadeguati a cogliere le minacce future o anche strettamente attuali perché il rischio informatico si caratterizza per una rapida evoluzione in termini di nuove tecnologie a sostegno delle frodi, ad esempio con l'evoluzione della tecnologia si prevede una maggiore efficacia degli attacchi DoS, l'avvento di nuovi virus, nuovi metodi di estorsione e di appropriazione dei dati (RMS 2016).

Per quanto riguarda la modellizzazione del rischio cyber, il processo di sottoscrizione di tale rischio prevede un'analisi probabilistica basata sull'esperienza storica in termini di frequenza e gravità degli incidenti supportata dalla costruzione di potenziali scenari in base al giudizio di esperti in campo ICT e sicurezza informatica.

I dati sulle violazioni passate forniscono alla compagnia un primo input per valutare il livello di rischio in base alle diverse caratteristiche aziendali come settore in cui opera il potenziale contraente e la sua dimensione che sono utili per stimare il valore del dato compromesso.

Tale processo di valutazione richiede una profonda comprensione del business in termini di architettura dei processi aziendali che portano alla creazione del valore, l'identificazione del numero e del tipo di dati sensibili detenuti e gestiti dalla società.

Gran parte dei dati disponibili sugli incidenti informatici deriva dall'esperienza registrata negli Stati Uniti in quanto lì la base dati è più ampia essendo previsto già dal 2003 l'obbligo di notifica delle violazioni della privacy.

La letteratura ha proposto distribuzioni asimmetriche e a code pesanti per la severità e per la frequenza, ad esempio distribuzioni Log-normale e Binomiale negativa[44], nel paragrafo 4.3 sarà presentata un'analisi empirica su dati di frequenza e size riguardanti data braches per verificare l'adattamento dei dati a tali distribuzioni di probabilità.

Wheatley et al. (2016) hanno mostrato empiricamente il fatto che le leggi che governano frequenza e severità del rischio informatico sono altamente dinamiche, di conseguenza questo richiede un aggiornamento continuo della modellizzazione.

[44] Elling e Loperfido (2017), Carfora et al. (2019), The Geneva Association (2016)

Per quanto invece riguarda l'aggregazione del rischio informatico, Böhme and Kataria (2006) mettono in luce l'elevata correlazione non lineare tra i rischi informatici. Secondo gli autori il rischio informatico presenta correlazione intra-società e tra società diverse. Infatti, un incidente informatico potrebbe interessare diversi sistemi informativi di una stessa società e in secondo luogo potrebbe provocare danni a diverse entità. Quest'ultima correlazione considerata "globale" è quella più dannosa per la compagnia assicurativa e al tempo stesso per l'esistenza stessa del mercato perché ne limita lo sviluppo.

Data questa caratteristica, nella modellizzazione è necessario tenere in considerazione una struttura di dipendenza non lineare trovandovi quindi applicazione la metodologia delle funzioni copula che sono strumenti che permettono l'aggregazione di diversi profili di rischio asimmetrici, ad esempio, le funzioni di perdita di diverse polizze, rappresentandone la struttura di dipendenza, e sono considerati flessibili, in quanto consentono l'utilizzo di qualsiasi distribuzione marginale.

Più forte è la correlazione tra le variabili casuali e più la loss distribution di portafoglio assume una forma leptocurtica, in linea con la teoria classica di portafoglio di Markowitz, in quanto aumenta la massa di probabilità nella coda essendo maggiore la frequenza dei valori estremi ma anche dei valori modali. Per contro ovviamente si riduce la massa nella parte centrale della distribuzione perché ovviamente la probabilità somma a 1.

Il risultato è un portafoglio più rischioso perché meno diversificato, caratterizzato appunto dall'aumento della probabilità di avere perdite molto elevate dovute a sinistri congiunti. Ciò implica che la compagnia assicurativa, a parità di altri fattori, richiederà premi più alti per proteggersi dalla maggiore probabilità di incorrere in perdite catastrofali dovute appunto all'elevata correlazione. Anche Mukhopadhyay et al. (2006) mettono in evidenza questa caratteristica dei rischi informatici.

Herath e Herath (2011) inoltre suggeriscono, essendo le distribuzioni non normali-ellittiche, quindi i rischi informatici sono correlati non linearmente, di utilizzare le copule di Archimede o Archimedee come la copula Gumble e la copula Clayton.

Sempre in tema di modellizzazione, un altro filone della letteratura, invece, ha messo in luce il fatto che le infezioni dolose come i virus, gli attacchi malware e i DoS si propaghino allo stesso modo della diffusione di una pandemia, adottando di conseguenza, per la modellizzazione di tali rischi, approcci derivanti dalla epidemiologia come ad esempio modelli epidemici SIS, SIR ed ε-SIS basati su processi markoviani cioè su catene di Markov a tempo continuo (Piet Van Mieghemy et al.; 2014).

Data la difficoltà nel modellare tale rischio dal punto di vista probabilistico per via della sua continua evoluzione e per via degli esigui dati disponibili che generano volatilità nelle stime, è diffusa nel settore la scenario analysis di tipo deterministico per valutare il rischio complessivo di portafoglio.

La società inglese Lloyd's (2017), ad esempio, ha reso pubblico uno scenario di sabotaggio da parte di un attacco malevolo dei sistemi di controllo industriale di una centrale elettrica da cui consegue un blackout elettrico che interessa 15 stati US del nord-est tra cui Washington, D.C. e New York City.

Lo scenario è basato su un'infezione da malware che causa il sovraccarico e la conseguente interruzione dell'attività dei generatori di elettricità, con conseguenti diffusi blackout con ripristino dell'operatività solo dopo settimane. Tale scenario è ritenuto improbabile ma tecnicamente e soprattutto tecnologicamente fattibile.

Le stime degli impatti economici in questo scenario vanno dai 243 miliardi USD a più di 1 trilione di dollari nello scenario peggiore, con perdite assicurate tra i 21.4 miliardi a 71.1 miliardi di dollari a seconda della gravità dello scenario. Questi scenari comportano quindi perdite assicurate catastrofali, infatti le richieste di indennizzo si verificano in un certo numero di polizze assicurative riferite a diversi soggetti per danni alla proprietà, danni da interruzione del business nelle società di produzione di energia elettrica, danni alla proprietà e perdite di interruzione del business presso le aziende nella zona di blackout e anche perdite di guadagni da parte delle aziende con fornitori in quella zona soggetta a blackout.

Come risulta da questi scenari, il rischio informatico può assumere una dimensione catastrofale proprio come il rischio nat-cat (natural catastrophe), infatti in caso di occorrenza, i disastri naturali e gli incidenti informatici su larga scala possono provocare perdite concentrate che coinvolgono contemporaneamente più linee di business e che possono addirittura risultare superiori ai premi totali accumulati.

Altra fonte di problemi ma anche di opportunità è rappresentata dal rischio informatico silente, il cosiddetto silent cyber risk.

L'autorità di vigilanza del settore finanziario del Regno Unito, ha messo in luce in un suo report (Swedney;2019) i rischi di sottoscrizione derivanti dalle polizze che coprono il cyber risk sia di tipo affermativo ma soprattutto di tipo silent.

Sul mercato infatti sono diffuse polizze che prevedono una copertura del rischio informatico in modo esplicito, dette affermative che possono essere stand alone o configurarsi come coperture accessorie in altre polizze tradizionali, caratterizzate dal fatto che sottostante al processo di sottoscrizione vi è una valutazione e tariffazione di tale rischio assunto.

Le polizze stand alone vanno proprio a coprire quei rischi cyber esclusi mediante clausola nelle polizze tradizionali. Ma al tempo stesso sono presenti anche polizze in cui l'esposizione al rischio informatico non è né espressamente esclusa né inclusa nella copertura offerta dalla polizza, per cui contengono in modo silente la copertura del rischio informatico e per questo motivo sono dette non affermative o silenti.

Il business casualty tradizionale, ad esempio, è molto esposto ad un rischio silente, dovuto allo scarso utilizzo di esclusioni ad hoc che circoscrivono il rischio in sede di sottoscrizione delle polizze, all'impossibilità di stimare, e quindi di escludere ragionevolmente, perdite dovute al rischio informatico ed inoltre le clausole di esclusione potrebbero persino essere presenti nel contratto ma risultare inefficaci nella delimitazione del rischio. Ciò può quindi prefigurare scenari catastrofici se non vengono adottati presidi idonei ad arginare tale eventualità.

Si pensi ad esempio all' assicurazione all risk property che copre danni diretti ai beni e danni indiretti derivanti dall'attività aziendale.

Da questa copertura assicurativa sono esclusi, oltre a ciò che è espressamente indicato come escluso nel contratto, anche i danni causati da eventi eccezionali ai sensi dell'articolo 1912 del cc o da azioni dolose e colpose messe in atto dal contraente.

Per eventi eccezionali si intendono le guerre o le catastrofi naturali.

In questo caso non essendo indicato esplicitamente che gli incidenti informatici sono eventi eccezionali oppure che sono esclusi, spesso l'efficacia della copertura dei sinistri scaturenti da eventi di quel tipo potrebbe sussistere ed è per questo motivo dibattuta in sede legale.

Non escludendo la polizza property gli incidenti informatici è possibile quindi che l'assicuratore debba pagare sinistri derivanti dal rischio cyber pur essendo una polizza tradizionalmente non cyber.

Queste esposizioni silenziose al rischio informatico costituirebbero ben il 90%[45] delle polizze sul mercato cyber mondiale.

Negli Stati Uniti le polizze cyber stand alone rappresentano il 52% del mercato, (OECD; 2017) di conseguenza la componente silente si può presumere abbia un certo peso nel mercato. Ovviamente non ci sono stime attendibili sulla percentuale di coperture informatiche silenti che sono presenti sul mercato.

Le compagnie di assicurazione si possono quindi considerare potenzialmente soggette a esposizioni sconosciute e silenti in quanto riferite a polizze che non contengono clausole che esplicitamente escludono i danni dovuti ad incidenti informatici.

[45] Capsicum Reinsurance Brokers LLP (2017)

Le autorità di vigilanza stanno spingendo verso la quantificazione di queste esposizioni involontarie al rischio informatico in tutte le linee di business tradizionali attraverso stress test che permettano valutazioni dettagliate sulle potenziali esposizioni nelle linee di business property e casualty tradizionali.
Queste spinte esterne, inoltre, creano opportunità non indifferenti in quanto una volta che le esposizioni sono identificate e quantificate diventa necessario trasferire questi rischi o attraverso i canali tradizionali di riassicurazione e di retrocessione, anche se plausibilmente le compagnie riassicurative riscontrano lo stesso pericolo di accumulo di cyber rischi silenti e quindi non assumeranno o assumeranno in misura insufficiente tali rischi per non incorrere in sinistri congiunti che a loro volta portano alla potenziale insolvenza. Di conseguenza il cyber risk silente, oltre a quello stand alone, rappresenta una fonte di opportunità per lo sviluppo di un mercato cyber-ILS, in particolare cyber-cat bonds, che offra quella capacità assicurativa mancante sul mercato.

4.2 Funzioni copula e dipendenza

Le funzioni copula sono utilizzate dal settore assicurativo nei processi di pricing e di ottimizzazione del portafoglio in quanto permettono di modellare la struttura di dipendenza non lineare tra le variabili.
Le copule sono utilizzate per modellare la distribuzione di perdita che nel caso del rischio informatico presenta asimmetria e correlazione con altri rischi. Tali funzioni permettono di determinare i premi assicurativi in modo non distorto quando i rischi analizzati sono ad esempio associati ad uno stesso evento o fenomeno catastrofico. Ad esempio, se consideriamo nell'ambito delle catastrofi naturali il rischio associato ad un evento tempesta, il fattore di rischio, può causare danni sia alle polizze incendio sia alle polizze RCA (Levi 2001) ed è necessario quindi tenere conto della struttura di dipendenza tra queste grandezze. Di seguito sono brevemente introdotte le funzioni copula e le loro proprietà, per ulteriori approfondimenti si rinvia a Cherubini et al. (2004) e Mazzoleni (2005).
Alla base della funzione copula c'è il principio della trasformazione integrale di probabilità, si considerino i seguenti teoremi (Piazza, 2002).

Teorema 1. $Se\ X$ è $una\ variabile\ aleatoria\ la\ cui\ funzione\ di\ ripartizione\ F_X$ è $strettamente\ crescente\ allora\ U = F_X(X)\ ha\ distribuzione\ uniforme\ in\ [0,1]$.

Analogamente,

Teorema 2. $Se\ U\ ha\ distribuzione\ uniforme\ in\ [0,1]\ allora\ X = F^{-1}(U)$
$ha\ funzione\ di\ distribuzione\ F_X\colon\ F^{-1}(U) = F_X$

La trasformazione $U = F_X(X)$ si chiama trasformazione integrale di probabilità.
Questo teorema è utilizzato dai software statistici per generare numeri pseudo casuali perché basta simulare un valore di u, estratto da una variabile uniforme, per ottenerne uno di X dato che $X = F_X^{-1}(u)$ cioè è uguale all'inversa della funzione di ripartizione.
Con le copule si vuole proprio ottenere la "correlazione" tra due variabili X_1 e X_2 andando a "correlare" le rispettive u_1 e u_2 cioè variabili con distribuzione uniforme.
Il teorema di Sklar (1959)[46] fornisce la base per l'utilizzo delle funzioni copula in diversi ambiti.
Sia C una copula multivariata, n-variata, e siano $F_1, F_2, \dots F_n$ funzioni di distribuzione univariate, allora la funzione

$$F(x) = \mathrm{C}\ (F_1(x_1), \dots\ , F_n(x_n))$$

è una funzione di ripartizione multivariata con marginali $F_1, F_2, \dots F_n$.
Ogni funzione di ripartizione multivariata ha una copula. Se F è una funzione di ripartizione multivariata con funzioni di ripartizione univariate continue $F_1, F_2, \dots F_n$ allora esiste una copula C tale che:

$$C(u) = H(F^{-1}(u_1), \dots, F^{-1}(u_n))$$

Se le funzioni di distribuzioni marginali $F_i, i = 1, \dots\ , n$ sono continue allora C è unica, altrimenti C è determinata in modo univoco da $RanF_1\ x \dots . x\ RanF_n$, dove $RanF_i$ denota il range di F_i per ogni $i = 1, \dots, n$, cioè C è unica solo sui possibili valori di F_i.
Al contrario se C è una copula e $F_1, F_2, \dots, F_n$ sono funzioni di distribuzione univariate allora la funzione $F(x)$, come definita precedentemente, è una funzione di distribuzione multivariata con marginali $F_1, F_2, \dots, F_n$.
Applicando quindi determinate copule multivariate a funzioni di distribuzioni univariate di qualsiasi tipo è possibile ricavare tutte le funzioni di distribuzione multivariate. Ed n funzioni

[46] Per approfondimenti si veda Sklar (1959; 1996)

di distribuzioni univariate arbitrarie possono sempre essere combinate in funzioni di distribuzione multivariate.

Ad esempio, per il caso bivariato, ogni funzione di distribuzione bivariata si ricava applicando una determinata copula alle sue marginali arbitrarie e, viceversa, applicando una copula a due funzioni di distribuzioni univariate si ottiene sempre una funzione di distribuzione bivariata: se $H(x,y)$ è una funzione di ripartizione bivariata con marginali $F(x)\ e\ F(y)$, allora esiste una copula bivariata $C\colon [0,1]^2 \rightarrow [0,1]$ tale che

$H(x,y) = \mathrm{C}\big(\mathrm{F(x)},\mathrm{F(y)}\big)$ ed è unica se le due marginali sono continue.

Se C è una copula bivariata mentre $F(x)\ e\ F(y)$ sono funzioni di ripartizione univariate continue allora $H(x,y) = \mathrm{C}\big(\mathrm{F(x)},\mathrm{F(y)}\big)$ è una funzione di probabilità congiunta con marginali proprio $F(x)\ e\ F(y)$

Si consideri il corollario del teorema di Sklar.

Corollario. $Siano\ H, F_1, F_2\ , dove\ H$ è $una\ distribuzione\ congiunta\ con\ marginali\ F_1, F_2,\ e\ siano\ {F_1}^{-1}\ e\ {F_2}^{-1}\ le\ pseudo\ inverse\ di\ F_1, F_2,\ allora\ per\ ogni\ (u_1, u_2) \in DomC'\colon C(u_1 u_2) = H(F^{-1}(u_1), F^{-1}(u_2))$

dove C' è una subcopula unica e $Dom\ C' = RanF_1 x RanF_2$.

Il corollario al teorema di Sklar fornisce il metodo per la costruzione della copula cioè la congiunta a partire dalle funzioni di ripartizione marginali se queste sono continue e strettamente crescenti, quindi, la probabilità congiunta può essere rappresentata come funzione delle marginali e viceversa:

$$C(u,v) = H(F^{-1}(u), F^{-1}(v))$$

la copula C, assumendo che le due variabili siano continue, è proprio la distribuzione congiunta delle variabili aleatorie trasformate uniformi $U = F(X)\ e\ V = F(Y)$, quindi, passando dalle marginali uniformi a marginali arbitrarie qualsiasi, la copula rappresenta la struttura di dipendenza per una distribuzione bivariata di qualsiasi tipo. Devono essere però note la funzione di ripartizione e la sua inversa.

Le copule permettono quindi la modellizzazione della struttura di dipendenza tra diverse variabili casuali che possono essere di qualunque tipo, dal teorema di Sklar si deduce infatti che le funzioni di distribuzione marginali hanno una struttura separata dalla struttura della copula.

La relazione di dipendenza tra le variabili analizzate viene determinata dalle relazioni che si trovano tra le distribuzioni uniformi simulate.

La copula soddisfa le seguenti proprietà[47]:

- E' pari a zero se uno qualsiasi dei suoi argomenti è zero:
  $C(u_1, \dots., u_{i-1,}, 0, u_{i+1}, \dots. u_n) = 0$ per ogni $1 \leq i \leq n \; e \; 0 \leq u_k \leq 1$,
  $k = 1, \dots, n$

- La copula è uguale a u se un argomento è u e tutti gli altri sono uguali a 1:
  $$C(1, \dots..1, u, 1, \dots \dots, 1) = u \; per \; 0 < u < 1$$

- $E' \; n - crescente$, quindi se $n = 2$, $la \; funzione \; G: A_1 \; x \; A_2 \rightarrow \mathbb{R}$
  è $chiamata \; 2 - crescente$ se per ogni rettangolo $[u_1, u_2]x[z_1, z_2]$
  i cui vertici giacciono in $A_1 \; x \; A_2$, tale che $u_1 \leq u_2, z_1 \leq z_2$,
  $$G(u_2, z_2) - G(u_2, z_1) - G(u_1, z_2) + G(u_1, z_1) \geq 0$$

La densità f di una funzione di distribuzione F bivariata , se esiste, è definita da

$$f(x, y) = \frac{\partial F(x, y)}{\partial x \partial y}$$

allora la densità associata alla copula è la seguente:

$$c(u, v) = \frac{\partial C(u, v).}{\partial u \partial v}$$

La densità della copula $c(u,v)$ è legata alla densità f della funzione di distribuzione F dalla seguente relazione: $f(x, y) = c(F_x(x), F_y(y)) \cdot f_x(x) f_y(y)$, dove $f_x(x) f_y(y)$ sono le densità delle distribuzioni marginali.
Se $(x, y) \; e \; (x', y')$ sono due osservazioni di un vettore aleatorio bivariato continuo (X, Y), le due osservazioni si dicono concordanti cioè la probabilità di avere grandi o piccoli valori delle due variabili è molto elevata mentre la probabilità di valori grandi/piccoli per una e piccoli/grandi per l'altra è bassa.

[47]Cherubini et al. (2004);

La misura di tale concordanza di senso o di segno che misura appunto il grado di dipendenza è la $\tau\ di\ Kendall$, una misura di correlazione analoga ma più generale rispetto al coefficiente di correlazione di Pearson.
Tale misura di concordanza non dipende dalla copula di (X,Y), è detta correlazione di rango in quanto il suo stimatore empirico può essere calcolato osservando l'ordinamento del campione di dati senza conoscere il valore numerico.
Restituisce un valore compreso tra -1 e 1 ed è definita come la differenza tra le probabilità di concordanza e di discordanza di due osservazioni distinte della coppia aleatoria:

$$\tau(X,Y) = P[(X - X')(Y - Y') > 0] - P[(X - X')(Y - Y') < 0]$$

Un altro coefficiente di correlazione di rango è il ρ di Spearman:

$$\rho_S = 3(P[(X - X')(Y - Y') > 0] - P[(X - X')(Y - Y') < 0]$$

Le variabili aleatorie indipendenti presentano un valore τ e ρ pari a zero ma non vale il contrario cioè la relazione inversa e quindi una correlazione che assume il valore nullo non implica necessariamente indipendenza tra le variabili aleatorie.
I due coefficienti sono delle funzioni crescenti del valore della copula.
Dal teorema di Sklar deriva il fatto che le variabili sono indipendenti solo se la congiunta è pari al prodotto delle marginali e quindi se la loro copula è una copula prodotto.
Ci sono diverse famiglie di copule a loro volta divise in diverse classi in base alla funzione generatrice, come ad esempio la famiglia di copule ellittiche di cui fa parte la copula Gaussiana ma le più usate nel settore assicurativo sono quelle Archimedee come la copula Gumbel.

4.2.1 Copule Archimedee[48]

Le copule Archimedee permettono di ridurre lo studio della copula multivariata ad un'unica funzione univariata, la funzione φ, detta funzione generatrice archimedea della copula C.

[48]
- Embrechts et al. (1999)
- Cherubini et al (2004)

Tali copule sono infatti costruite a partire dalla seguente funzione generatrice continua, convessa e strettamente decrescente:

$$\varphi(u): [0,1] \rightarrow [0,\infty] \; e \; tale \; che \; \varphi(1) = 0$$

La sua funzione pseudo-inversa è definita come:

$$\varphi^{-1}(u) = \begin{cases} \varphi^{-1}(u) & 0 \leq u \leq \varphi(0) \\ 0 & \varphi(0) \leq u \leq \infty \end{cases}$$

Nel caso bivariato le copule archimedee presentano la seguente forma:

$$C(u,v) = \varphi^{-1}(\varphi(u) + \varphi(v))$$

Tra le copule Archimedee le più utilizzate sono la Clayton, la Frank e la Gumbel.
Il tau di Kendall per una copula Archimedea C con generatore φ e con variabili aleatorie continue X e Y diventa funzione del generatore nel seguente modo:

$$\tau = 1 + 4 \int_0^1 \frac{\varphi(t)}{\varphi'(t)} dt$$

La copula Archimedea può essere costruita usando l'inverso della trasformazione di Laplace come generatore, di seguito consideriamo la copula di Gumbel.
Il generatore per la copula di Gumbel è dato da:
$\varphi_\vartheta(u) = [-\ln(u)]^\vartheta$
La copula bivariata diventa quindi:
$C_\vartheta^{Gumbel}(u,v) = \exp\{-([-\ln(u)]^\vartheta + [-\ln(v)]^\vartheta)^{\frac{1}{\vartheta}}\}$
La copula Gumbel è molto usata perché ha la proprietà di dipendenza nella coda superiore.
Il coefficiente di correlazione tau di Kendall in funzione del parametro ϑ della copula è definito come:

$$\tau_{GC\vartheta} = 1 - \frac{1}{\vartheta}$$

4.2.2 Modello di pricing

Di seguito presentiamo la procedura per la stima del modello di copula per i dati.
Per quanto riguarda il modello, si costruisce la distribuzione delle perdite annue, per ogni posizione, con la convoluzione tra la frequenza e la severità mediante simulazione Monte Carlo.
Il primo passo è la stima del numero di sinistri, se consideriamo, ad esempio, una distribuzione di Poisson, utilizzando la serie storica annuale del numero di incidenti informatici, stimato il parametro $\lambda = \frac{n° \, incidenti}{totale \, anni}$, si ottiene la distirbuzioone di probabilità del numero di sinistri per ogni polizza.
Il secondo passo è la stima della distribuzione in termini di impatto dei singoli sinistri e successivamente tramite simulazione Monte Carlo, si determina la distribuzione delle perdite annue associata agli incidenti informatici per ogni polizza.
Si ottiene così per ogni singola esposizione la distribuzione empirica dei danni annui o perdite aggregate annue.
Di seguito in figura 29 si riporta lo schema del processo di calcolo.

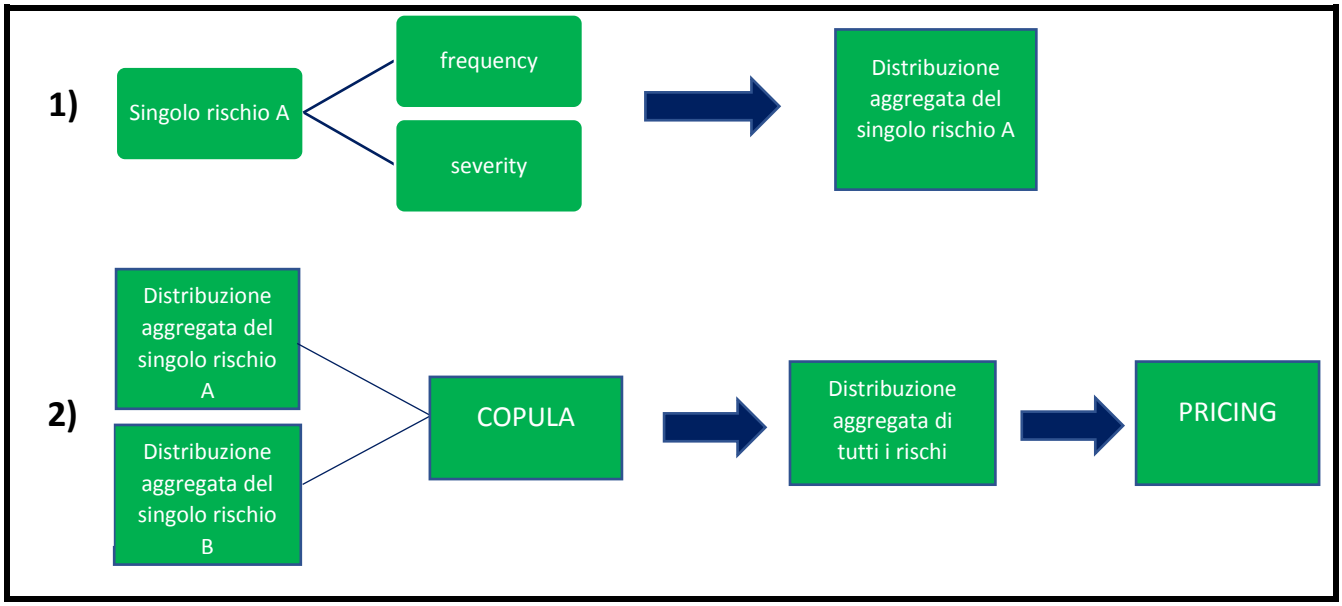

Figura 29: Processo di calcolo

Tramite la copula si aggregano le diverse distribuzioni di perdita per determinare la struttura di dipendenza.

Prima si determina la struttura di correlazione tra i rischi, poi si procede alla scelta della copula ottimale per rappresentare la distribuzione multivariata di questi rischi mediante il fitting dei dati dei danni aggregati con diverse copule.
Per le copule bivariate Archimedee il parametro ϑ si può ricavare dal Tau di Kendall, che per la copula Gumbel diventa:

$$\tau_{GC\vartheta} = 1 - \frac{1}{\vartheta}$$

Da questa espressione, a partire da $\tau_{GC\vartheta}$ stimato dai dati si ricava il ϑ per la copula legato alla correlazione tra le variabili.
Successivamente si effettua un test di goodness of fit, ad esempio, il test Cramer-von Mises, per valutare se la copula è adatta a rappresentare la struttura bivariata dei dati di danni aggregati con livello di significatività pari al 5%.
In linea con il lavoro di Herath e Herath (2006), se consideriamo due polizze A,B e i danni associati X,Y rispettivamente, la copula, come suddetto, rappresenta la distribuzione di perdita bivariata asimmetrica tenendo in considerazione la struttura di dipendenza tra le variabili casuali X=danni polizza A e Y= danni polizza B.
I danni sono in entrambi i casi associati al rischio di un incidente informatico che affetta entrambe le polizze.
L è la funzione di distribuzione congiunta bivariata di perdita delle due polizze:
$L = f(X,Y)$, il valore della distribuzione aggregata di perdita si ottiene simulando osservazioni bivariate $u = (u_{k_1}, u_{k_2})$ dalla copula ottima selezionata, andando a determinare i quantili sulla distribuzione di perdita empirica di ogni rischio X e Y.
Si effettuano in totale N iterazioni andando appunto a simulare i dati bivariati per ogni n-esima iterazione (X_n, Y_n) con la copula ottima e si computa la distribuzione totale congiunta $L^n = f(X_n, Y_n)$.
E' necessario poi considerare la determinazione del premio.
Il premio assicurativo per un rischio cyber P è definito come:

$$E[P] = \overline{c}E(e^{-rt_1})E(S)$$

dove c è il valore assunto dalla variabile dicotomica Bernoulliana che assume per semplicità solo un valore di probabilità pari a 1 se si verifica l'incidente informatico oppure zero in caso

di nessun sinistro, r è il tasso di sconto, S è l'indennizzo, t_1è il tempo che trascorre tra la stipulazione della polizza e l'occorrenza del sinistro che si assume coincida con l'epoca di indennizzo: T_n= $t_1 - t_{i-1}$.

Tale variabile t_1 si stima simulando un processo di Poisson discreto a tempo continuo di parametro λ, $Po(\lambda)$. I tempi di interarrivo T_n sono distribuiti in modo esponenziale con media $\frac{1}{\lambda}$.

Partendo dalla variabile casuale u con distribuzione uniforme,

$$f(x) = \begin{cases} 1 & 0 < x < 1 \\ 0 & altrove \end{cases}$$

si simula l'osservazione dalla distribuzione esponenziale nel seguente modo:

$u = F(X) = 1 - e^{-\lambda x}$, dove F(X)=fdp esponenziale e $x = t_1 - t_{i-1} = T_n$, $t_0 = 0$

e risolvendo rispetto a x si ottiene:

$$x = \frac{[-ln(1-u)]}{\lambda}$$

$$t_1 = t_{i-1} - \frac{1}{\lambda}\ln u$$

Riassumendo, si procede quindi simulando u uniforme e si sostituisce nell'espressione, poi si determina la copula che meglio si adatta ai dati (X,Y) con il procedimento suddetto.

Si effettuano in totale N iterazioni andando a simulare i dati bivariati per ogni n-esima iterazione (X_n, Y_n) con la copula ottima, si computa la distribuzione congiunta

$L^n = f(X_n, Y_n)$, si simula il processo di Poisson per ottenere t_1^n, si calcola

$P^n = c \cdot e^{-rt_1^n} \cdot S^n$ e infine si calcolano il valore atteso e la deviazione standard del premio assicurativo:

$$E[P] = \frac{1}{N}\sum_{n=1}^{N} P^n$$

$$\sigma(P) = \sqrt{\frac{1}{N}\sum_{n=1}^{N}(P^n)^2 - [E(P)]^2}$$

4.3 Il rischio informatico come rischio catastrofale

La crescente dipendenza di enti ed individui dallo spazio cibernetico, inteso come l'insieme delle infrastrutture informatiche tra loro interconnesse e caratterizzato da software, hardware, utenti e dati[49], influenza il trend crescente della frequenza e della severità degli attacchi informatici, come mostrato dai dati in figura 30, nonostante l'applicazione di diversi protocolli di sicurezza che permettono l'uso di crittografia nel traffico dei dati sensibili.

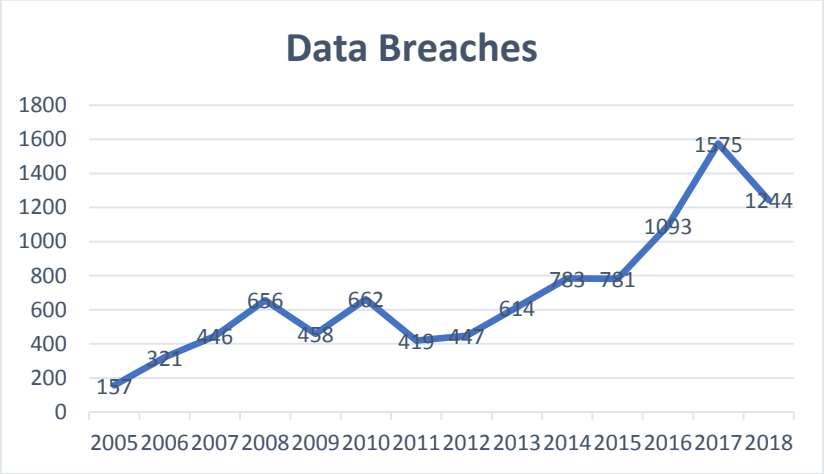

Figura 30: numero di data breaches registrati negli Stati Uniti tra il 2005-2018 (elaborazione propria su dati PCR)

Il rischio informatico è stato classificato tra i dieci principali rischi globali dal World Economic Forum (2018) e può essere concepito, sotto determinate condizioni, come un rischio catastrofale man-made.

Di seguito viene analizzato il caso delle smart grids[50], sistemi di reti intelligenti e digitalizzate, che percorrono un intero territorio permettendo, attraverso un continuo flusso di informazioni tra i providers e gli utenti, una gestione innovativa ed efficiente del servizio di erogazione dell'energia elettrica, tramite il collegamento diretto tra offerta e domanda mediante contatori intelligenti interconnessi tramite sensori alla rete, risulta evidente come questo grande network intelligente sia vulnerabile a cyber attack che producono danni su larga scala, si pensi allo scenario di Lloyd's, ad esempio, illustrato nel paragrafo 4.1.

[49] Direttiva DPCM, 17/2/2017, articolo 2

[50] https://www.e-distribuzione.it/it/progetti-e-innovazioni/smart-grids.html

Il flusso di informazioni nella rete se alterato o arrestato può portare ad un'interruzione della corrente elettrica.
Una smart grid oltre a rendere più vulnerabile la centrale elettrica crea anche un rischio a cascata perché se tale sistema interconnesso viene attaccato, in questo caso oggetto di attacco diretto è la centrale ma, al tempo stesso, anche tutti gli altri "satelliti" interconnessi a questa rete diventano vulnerabili e subiscono l'attacco.
Dipendono dalla smart grid, tutte le infrastrutture più critiche, quindi le conseguenze di un arresto del fabbisogno energetico al settore sanitario o ai mercati finanziari prefigurano scenari ancora più drammatici rispetto a quelli previsti dagli scenari dei Lloyd's.
Inoltre, a sua volta ogni device connesso alla smart grid diventa una potenziale fonte di pericolo per la rete stessa perché diventa un nodo di trasmissione dell'attacco.
L'attacco informatico infatti può essere lanciato direttamente alla rete attraverso la quale si diffonde verso i suoi nodi rappresentati da devices interconnessi di qualunque tipo che hanno bisogno di energia e dai contatori intelligenti domestici, provocando danni molteplici, oppure l'attacco informatico può essere diretto ad un contatore digitale, ad esempio, cioè ad uno dei tanti nodi della rete, e, attraverso questo, giunge al cuore della rete stessa cioè la centrale provocando un blackout generale perché il contatore digitale di un utente domestico, interconnesso alla rete tramite sensori, oltre a rendere vulnerabile la singola rete domestica diventa una porta d'ingresso verso l'intera rete e quindi verso anche tutti gli altri nodi del network.
Come mostrato, le vulnerabilità sono molteplici, è facile pensare quindi a scenari di attacchi informatici su larga scala che possono arrivare a colpire ad esempio tutta la catena energetica dal sito di produzione ai nodi finali degli utenti: attacchi DoS[51] finalizzati al rallentamento o alla interruzione del flusso informativo nella rete, trasmissione di virus nella smart grid via internet per ottenere il controllo della stessa per causare un black out su larga scala, oppure ancora, l'inserimento di flussi informativi errati per alterare il reale fabbisogno di corrente elettrica, furto di proprietà intellettuale ma anche violazione della privacy. I modi per sabotare le infrastrutture critiche diventano molteplici.
Questa rete intelligente offre diversi vantaggi come efficienza nel funzionamento della rete elettrica, il collegamento delle fonti rinnovabili ma al tempo stesso l'integrazione di un sistema fisico come la rete energetica con la rete informatica espone la smart grid stessa e tutto ciò ad essa connesso, come suddetto, a minacce informatiche inevitabilmente catastrofali.

[51] DoS: denial of service

Data la concretezza di questi scenari, si pone il tema della modellizzazione di questo rischio nel consueto framework catastrofale. Tale rischio sarà la risultante dei fattori pericolosità della minaccia informatica in termini di frequenza, vulnerabilità del sistema ed effetti in termini di gravità dei danni attesi.

Il rischio si può interpretare, in questo caso, come la probabilità che un attacco informatico sfruttando le vulnerabilità del sistema generi delle perdite.

Per valutare l'esposizione ad attacchi informatici è possibile adottare, con qualche adattamento, il framework del modello catastrofale per i rischi nat-cat. Anche per il rischio informatico man-made è necessario partire dai dati storici per determinare le distribuzioni in termini di frequenza di occorrenza degli eventi e in termini di severità.

Qui si incontra la prima difficoltà, già messa in luce nei precedenti paragrafi, della mancanza di una sufficientemente ampia base dati sui passati eventi.

Diventa necessario, quindi, integrare tale base con un catalogo di potenziali eventi sintetici stocastici, tenendo in considerazione le tipologie possibili di incidente informatico che possono concretarsi in quella determinata realtà, poi sarà necessario individuare i possibili asset, in base al loro valore economico, che potrebbero essere colpiti.

Restringendo il caso ad un'azienda che gestisce dati, l'evento informatico di interesse potrebbe essere quell'evento che, se si verifica, può inficiare l'integrità, la confidenzialità in termini di protezione del dato, la disponibilità dello stesso nell'azienda e il suo normale svolgimento dell'attività.

Si partirà quindi dalla creazione del catalogo di eventi stocastici sintetici costruito in base a quelle tipologie di incidente informatico che hanno per oggetto i dati sensibili.

Tale catalogo è costruito tenendo conto degli incidenti accaduti storicamente in quello specifico settore, in settori simili e ad aziende che presentano stessa dimensione per fatturato di quella oggetto di valutazione.

Dagli eventi storici e sulla base di giudizi ed opinioni di esperti del settore ICT e degli specifici settori industriali che sono coinvolti, si sviluppano, mediante simulazione, diversi scenari che portano alla creazione degli eventi sintetici stocastici.

Una variabile di interesse nella creazione del catalogo, potrebbe essere il numero di records gestiti da quelle aziende con quella size appartenenti a quei settori.

Tale catalogo generale, applicabile ad ogni azienda simile a quelle su cui è stato fondato, conterrà migliaia eventi informatici che potrebbero occorrere durante un anno.

Per ogni potenziale incidente informatico viene quindi stimata la frequenza e l'impatto economico in termini di perdite, in base al valore del dato gestito, che potrebbero prodursi al verificarsi della minaccia.
Successivamente confrontando questo catalogo con la specifica realtà aziendale, oggetto di valutazione, si valutano le specifiche vulnerabilità tenendo conto ad esempio del numero totale di records gestiti, delle modalità di svolgimento del business, dei software, degli hardware, delle modalità di accesso a questi dati, della loro conservazione e dei sistemi di sicurezza utilizzati come i firewall per tenere conto dei presidi che l'azienda mette in atto per mitigare gli incidenti informatici. Ed infine si determina l'impatto monetario potenziale in un anno subito da questa azienda conseguente ad un incidente informatico.

4.4 Analisi statistica su data breaches

Di seguito si presenta un'analisi della serie storica di data breaches, violazioni di sicurezza che comportano in modo accidentale o in modo illecito "la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati".
I dati derivano dalla Privacy Rights Clearinghouse[52], un'organizzazione non profit.
La serie di dati giornalieri iniziale è riferita ad attacchi informatici intercorsi tra il 2017 e il 2019 negli Stati Uniti.
In particolare i dati riguardano i seguenti eventi:

- Attacchi malevoli provenienti dall'esterno, ad esempio intrusioni ed infezioni da Malware, Ramsomware, DoS (HACK)
- Frodi interne, l'utilizzo indebito di dati e manipolazioni dei dati stessi dall'interno cioè qualcuno con accesso legittimo che viola intenzionalmente la confidenzialità delle informazioni (INSD)
- Danneggiamenti accidentali ad hardware (PHYS)
- Perdita, alterazione di dati sensibili non intenzionale dovuta a erronea conservazione (DISC)

I settori presi in considerazione che sono stati oggetto di attacchi durante il periodo sono i seguenti:

- Financial Institutions (FIN_SER)

[52] https://www.privacyrights.org/data-breaches

- Educational Institutions (EDU)
- Healthcare (MED)
- Government & Military (GOV)

Nelle figure 31 e 32 è riportata l'analisi descrittiva e grafica dei tipi di attacco.

Tipologia	***Frequenza***	***Percentuale***
HACK	651	54%
INSD	15	1%
PHYS	168	14%
DISC	363	31%
tot	1197	100%

Figura 31: Tipologia e numero di attacchi (elaborazione propria su dati PCR)

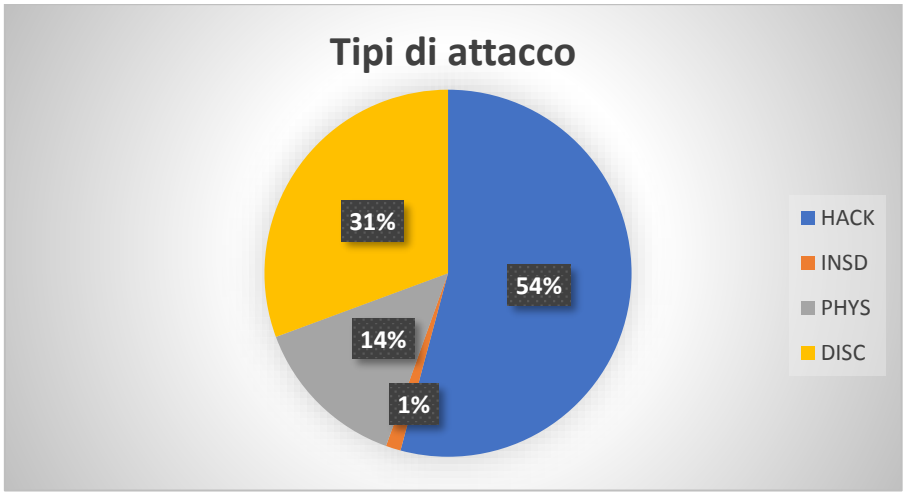

Figura 32: Frequenza di attacchi per tipologia (elaborazione propria su dati PCR)

Il diagramma in figura 32 mostra gli attacchi informatici verificatisi nel periodo tra il 2017 e il 2019, il 54% degli attacchi informatici proviene da attacchi malevoli di tipo hacking e infezioni da Malware, segue con il 31% la perdita e alterazione di dati sensibili non intenzionale, poi i danneggiamenti a dispositivi informatici che causano distruzione di dati hanno rappresentato il 14% del campione e infine solo l'1% è attribuibile a frodi interne come uso improprio e appropriazione indebita di dati sensibili nel periodo considerato. In figura 33 e 34 sono riportati i dati rielaborati relativi ai diversi settori oggetto degli attacchi informatici.

Settore	*Frequenza*	*Percentuale*
EDU	47	4%
GOV	42	4%
MED	816	68%
FIN_SER	292	24%
tot	1197	100%

Figura 33: Settori (elaborazione propria su dati PCR)

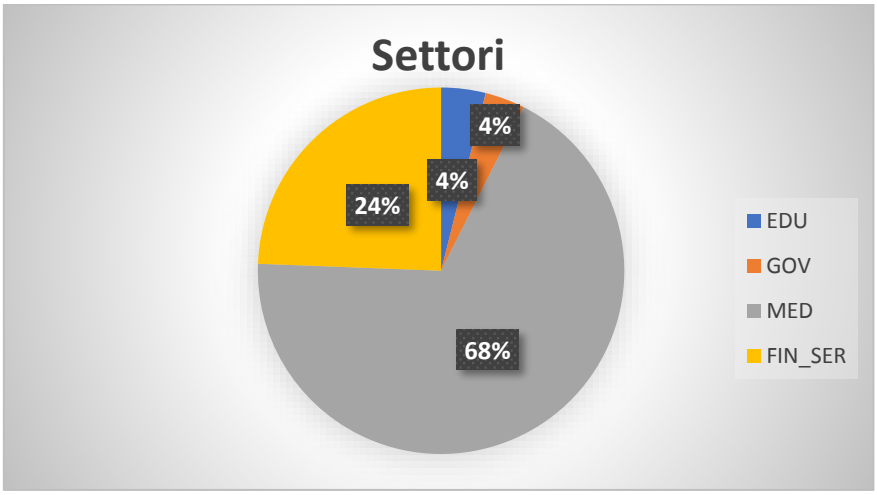

Figura 34: Frequenza degli attacchi nei diversi settori (elaborazione propria su dati PRC)

Il settore Healtcare è stato quello che ha riportato la maggiore quantità di attacchi informatici, rappresenta infatti ben il 68% del campione, segue il settore delle Istituzioni finanziarie con un 24%.

Il settore governativo-militare ed il settore educational sono stati oggetto di attacchi solo nel 4% dei casi, questo può indicare un efficace sistema di presidi per quanto riguarda il settore GOV e uno scarso interesse da parte delle organizzazioni criminali per il settore educativo.

Visto il maggior peso della tipologia attacchi informatici malevoli, HACK, e del settore Healthcare, MED, si prosegue con un'analisi della frequenza e della severità, quest'ultima intesa come quantità di dati compromessi in ogni attacco a sistemi informatici in quanto le informazioni sui dati di perdita non sono disponibili.

L’analisi è stata condotta attraverso il software RStudio.

Per quanto riguarda la frequenza i dati sono giornalieri e fanno riferimento al periodo 03/01/2017 - 20/12/2017 per un totale di 352 osservazioni.

In figura 35 sono riassunti i dati relativi al numero di sinistri verificatisi giornalmente, 0 sta ad indicare nessun attacco in quel determinato giorno, in totale i giorni senza attacco sono stati 225 mentre nell’8,5% dei casi si sono verificati 2 sinistri al giorno.

Hack	Freq	Freq.rel
0	225	0,639205
1	84	0,238636
2	30	0,085227
3	8	0,022727
4	4	0,011364
5	1	0,002841

Figura 35: Numero di sinistri giornalieri (elaborazione propria su dati PCR)

In figura 36 i dati sono rappresentati mediante bar plot.

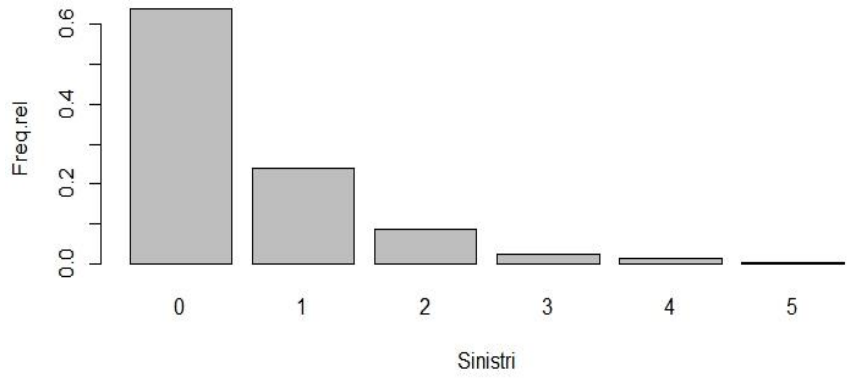

Figura 36: Frequenza del numero di sinistri (elaborazione propria su dati PCR)

E’ stato quindi condotto un test Chi-square dal quale si ottiene che la distribuzione che meglio si adatta ai dati è la binomiale negativa di parametri 1.2966074 e 0.5368914, con

una significatività del 10% non si rifiuta l'ipotesi nulla, si accetta quindi l'ipotesi nulla che i dati seguano una distribuzione binomiale negativa (p-value 0.7583253).

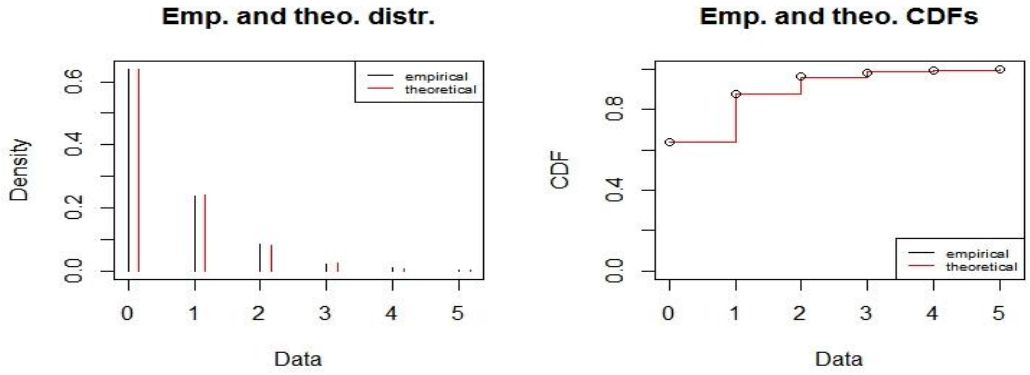

Figura 37: Distribuzione binomiale negativa (elaborazione propria su dati PCR)

I dati non sono descritti da una distribuzione di Poisson, dal test di bontà di adattamento ai dati di questa distribuzione si ottiene infatti un p-value pari a 0.0003462035 che porta a rifiutare l'ipotesi nulla. Nel caso della distribuzione di Poisson il valore atteso e la varianza coincidono e sono pari λ, quindi la varianza è ben approssimata dalla media ma nella realtà è facile trovare che i dati abbiano una varianza maggiore.
Nel caso della distribuzione binomiale negativa si ha:

$$X \sim (r, p)$$
$$E(Y) = \frac{rp}{1-p}$$
$$Var(Y) = \frac{rp}{(1-p)^2}$$

questo permette quindi di cogliere la caratteristica dei dati di avere una varianza maggiore della media.
Per quanto riguarda la severità, il numero di dati compromessi nel campione, nel periodo 3/01/2017-20/12/2017, è N=189.
Alcune statistiche descrittive riguardanti la distribuzione della severità che aiutano nella scelta della distribuzione sono la kurtosi e la skewness.
Se il valore di skewness è differente da zero ciò indica una distribuzione empirica non simmetrica, mentre la kurtosi quantifica il peso dei dati estremi. Il valore base per la curtosi è 3 cioè la kurtosi della distribuzione normale. In figura 38 sono mostrate queste statistiche,

mentre in figura 39 si mostra l'istogramma dei dati che evidenzia la forte asimmetria positiva della distribuzione empirica.

Summary statistics	
min:	0
max:	971
median:	12.806
mean:	129.2699
estimated sd:	248.9045
estimated skewness:	2.033716
estimated kurtosis:	5.796855

Figura 38: Statistiche descrittive sui records campionari (elaborazione propria su dati PCR)

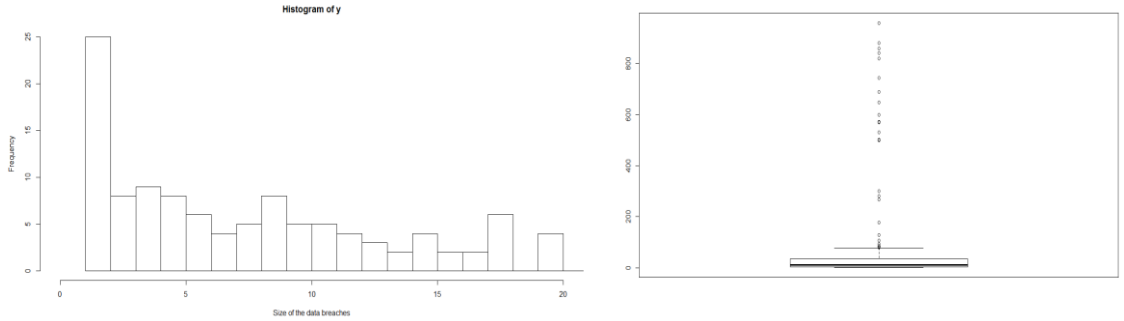

Figura 39: Istogramma e boxplot dei records compromessi (elaborazione propria su dati PCR)

L'istogramma in figura 39, suggerisce una trasformazione logaritmica, vista la lunga coda e l'elevata deviazione standard che indica un alto livello di dispersione nei dati.
Inoltre, il boxplot mostra la presenza di numerosi outliers.
Si procede quindi alla trasformazione logaritmica e successivamente si effettuano i test di bontà per la scelta della funzione di distribuzione continua con cui modellare la severità. Nella figure 40 sono presentati i risultati per tre diverse ipotesi distributive.

Weibull	Log-normale	Gamma
Fitting of the distribution 'weibull' by maximum likelihood Parameters : estimate Std. Error shape 1.751901 0.10619706 scale 1.398548 0.06726153 Loglikelihood: -159.1735 AIC: 322.347 BIC: 328.4722	Fitting of the distribution 'lnorm ' by maximum likelihood Parameters : estimate Std. Error meanlog 0.02599786 0.04983818 sdlog 0.62645622 0.03524051 Loglikelihood: **-154.4071** AIC: **312.8142** BIC: 318.9394	Fitting of the distribution 'gamma ' by maximum likelihood Parameters : estimate Std. Error shape 2.823942 0.3008464 rate 2.281280 0.2659503 Loglikelihood: -155.5481 AIC: 315.0962 BIC: 321.2213
Kolmogorov-Smirnov test p-value = 0.07012	Kolmogorov-Smirnov test p-value = **0.7366**	Kolmogorov-Smirnov test p-value = 0.306

Figura 40: Stime parametri MLE e Test KM non parametrico per goodness of fit

La distribuzione Lognormale presenta un p-value pari allo 0.7366, per cui con un livello di significatività del 10% si accetta l'ipotesi che i dati siano descritti dalla distribuzione Log-normale.

4.5 Cyber-cat bond

Negli ultimi anni si è spesso discusso sull'espansione del mercato ILS verso l'emergente cyber risk (Capsicum Re(2017), OECD(2017), Milliman(2017)), Carter S.(2018).
Il mercato dei capitali rappresenta il naturale sbocco per la copertura delle perdite da incidenti informatici di tipo catastrofale secondo Artemis (2017).
Diversi fattori conducono verso questa evoluzione, ad esempio, generalmente per stimare la probabilità di un potenziale sinistro è necessario avere dati storici, ma in questo mercato si genera il seguente paradosso: senza dati l'assicuratore non è in grado di offrire copertura ma al tempo stesso senza l'offerta di coperture un settore non cresce e tanto meno genera dati da elaborare per il futuro. Se i riassicuratori, quindi, si ritirano dal mercato per le diverse problematiche che lo affliggono, evidenziate nei paragrafi precedenti, gli assicurati avranno una copertura costosissima oppure all'estremo non sarà presente sul mercato un'offerta di coperture rispondenti al reale fabbisogno di mitigazione del rischio informatico.
Di conseguenza una cartolarizzazione assicurativa di questa tipologia di rischi, contribuirebbe allo sviluppo di un mercato assicurativo cibernetico, apportando benefici sia dal lato settore assicurativo, in termini di capacità aggiuntiva per gestire le perdite catastrofali da polizze cyber affermative e non affermative che si traduce in maggiori profitti, sia dal lato società in generale in quanto permetterebbe di colmare il divario attuale tra esposizioni assicurate ed effettivo fabbisogno di copertura cibernetica. Infatti, come sottolineato, il rischio informatico attualmente è sotto assicurato.
Inoltre, col passare del tempo, il rischio di catastrofe cibernetica assumerà sempre maggior rilievo per via dell'incremento della domanda di copertura che determina a sua volta l'entrata nel mercato di nuovi competitor che non sempre possiedono quella specializzazione, e quindi quella comprensione del business, necessaria per una valutazione accurata del rischio informatico sottostante. In aggiunta tale aumento della domanda di copertura da parte del mercato determina un potenziale incremento in termini di peso del cyber silenzioso, il quale presenta una maggiore propensione ad assumere dimensione catastrofale rispetto a quello affermativo. Dunque, gli strumenti ILS, in particolare i cat bonds, possono risultare idonei a trasferire anche il rischio informatico catastrofale al mercato dei capitali.
Seppur diffusisi negli anni 90' a supporto delle perdite da disastri naturali, col tempo, a partire dalla fine del 2016, gli strumenti ILS sono stati utilizzati, data la loro flessibilità, anche

per trasferire altre tipologie di rischio, ad esempio, hanno permesso la cartolarizzazione dei crediti assicurativi ed il trasferimento del rischio di terrorismo, come mostrano le figure 41 e figura 42.

Questo comprova la loro flessibilità ed idoneità a trasferire rischi non nat-cat cioè rischi derivanti da cause non naturali.

ISSUER / TRANCHE	SPONSOR	PERILS	SIZE ($M)	DATE
Oak Leaf Re Ltd. (Series 2018-1)	Southern Oak Insurance Co.	Florida named storms	45.26	Jun
Frontline Re Ltd. (Series 2018-1)	Frontline Insurance	U.S. named storm	350	Jun
Eclipse Re Ltd. (Series 2018-02A)	Unknown	Unknown property catastrophe risks	97.6	Jun
Dodeka XV	Unknown	U.S. property catastrophe risks	9.269	Jun
Resilience Re Ltd. (Series 1861A)	Unknown	Unknown property catastrophe risks	37	Jun
Market Re Ltd. (Series 2018-1)	Unknown	Florida named storms	84	Jun
Operational Re II Ltd.	Zurich Insurance Co. Ltd.	Operational risks	148	Jun
Eclipse Re Ltd. (Series 2018-01A)	U.S. Coastal Insurance Co.	U.S. property catastrophe risks	53.3	May
Atlas Capital UK 2018 PLC (Series 2018 ISPV 1)	SCOR Global P&C SE	International multi-peril	300	May
Alamo Re Ltd. (Series 2018-1)	Texas Windstorm Insurance Association	Texas multi-peril	400	May
Long Point Re III Ltd. (Series 2018-1)	Travelers	U.S. multi-peril	500	May
Dodeka XIII	Unknown	U.S. property catastrophe risks	23.567	May
Bowline Re Ltd. (Series 2018-1)	Transatlantic Re	International multi-peril	250	May
Everglades Re II Ltd. (Series 2018-1)	Citizens Property Insurance	Florida named storms	250	May
Residential Reinsurance 2018 Limited (Series 2018-1)	USAA	U.S. multi-peril	300	May
Caelus Re V Ltd. (Series 2018-1)	Nationwide Mutual	U.S. multi-peril	450	May
Kilimanjaro Re Ltd. (Series 2018-1)	Everest Re	International multi-peril	262.5	Apr
Kilimanjaro Re Ltd. (Series 2018-2)	Everest Re	International multi-peril	262.5	Apr
Resilience Re Ltd. (Series 1841A)	Unknown	Unknown property catastrophe risks	150	Apr
Pelican IV Re Ltd. (Series 2018-1)	Louisiana Citizens	Louisiana multi-peril	100	Apr
Kendall Re Ltd. (Series 2018-1)	Aspen Bermuda Limited	International multi-peril	225	Apr
Integrity Re Ltd. (Series 2018-1)	American Integrity	Florida multi-peril	79	Apr
Bellemeade Re Ltd. (Series 2018-1)	Arch Capital Group Ltd.	Mortgage insurance risks	374.46	Apr
Fidus Re Ltd. (Series 2018-1)	Build America Mutual	Financial guarantee risks	100	Apr
Armor Re II Ltd. (Series 2018-1)	United P&C Insurance	U.S. multi-peril	100	Apr
Manatee Re II Ltd. (Series 2018-1)	Safepoint Insurance Co.	U.S. multi-peril	200	Apr

Figura 41: Report transazioni CAT BOND del secondo trimestre del 2018 (Artemis)

ISSUER / TRANCHE	SPONSOR	PERILS	SIZE ($M)	DATE
Merna Re II Ltd. (Series 2019-1)	State Farm	U.S. earthquake	300	Mar
Sanders Re II Ltd. (Series 2019-1)	Allstate	U.S. multi-peril	300	Mar
Bellemeade Re 2019-1 Ltd.	Arch Capital Group Ltd.	Mortgage insurance risks	341.79	Mar
Bowline Re Ltd. (Series 2019-1)	Transatlantic Reinsurance Co.	International multi-peril	250	Mar
Dodeka XXII	Unknown	U.S. property catastrophe risks	18.67	Mar
Dodeka XXI	Unknown	U.S. property catastrophe risks	17.96	Mar
Radnor Re 2019-1 Ltd.	Essent Guaranty	Mortgage insurance risks	473.184	Feb
Orchard ILS Pte Ltd	Insurance Australia Group (IAG)	Australia and New Zealand catastrophe risks	54	Feb
Baltic PCC Limited (Series 2019)	Pool Re	Terrorism risk	97	Feb
Cape Lookout Re Ltd. (Series 2019-1)	North Carolina Insurance Underwriting Association	North Carolina named storm & severe thunderstorm	450	Feb
Atmos Re DAC	UnipolSai Assicurazioni S.p.A.	Italian multi-peril	51.03	Feb
Jungfrau IC Limited 2019	Unknown	Unknown property catastrophe risks	12	Jan
Alpha Terra Validus III	Terra Brasis Re	Latin American property catastrophe risks	5	Jan
Dodeka XX	Unknown	U.S. property catastrophe risks	23.936	Jan
Dodeka XIX	Unknown	U.S. property catastrophe risks	27.609	Jan
Dodeka XVIII	Unknown	U.S. property catastrophe risks	25.181	Jan
Vitality Re X Ltd. (Series 2019)	Aetna	Medical benefit claims levels	200	Jan
Seaside Re (Series 2019-22)	Unknown	U.S. property catastrophe risks	10	Jan
Seaside Re (Series 2019-21)	Unknown	U.S. property catastrophe risks	30	Jan
Resilience Re Ltd. (Series 1912A)	Unknown	Unknown property catastrophe risks	88	Jan

Figura 42: Report transazioni in CAT BOND del primo trimestre del 2019 (Artemis)

Tra queste transazioni riepilogate nelle tabelle di figg. 41 e 42 in particolare rileva, a sostegno della tesi di una potenziale futura emissione di un cyber catastrophe bond, la transazione Operational Re.Ltd nel mese di giugno del 2018 con sponsor Zurich Insurance Co. Lts.

Tale emissione di cat bond, con taglia pari a 148 milioni di CHF, ha avuto ad oggetto la cartolarizzazione del rischio operativo al cui interno era compreso anche il rischio informatico del gruppo bancario Credit Suisse.

Credit Suisse ha cartolarizzato infatti parte della sua esposizione a rischi operativi estremi incluse perdite catastrofali legate ad incidenti informatici come guasto al sistema informatico che causa business interruption, nonché guasti operativi ad hardware dovuti ad attacchi informatici[53].

[53] Artemis (2018)

Di seguito si prendono in considerazione diversi vantaggi per protection buyer e protection seller che lo sviluppo di un mercato cyber-cat bond potrebbe apportare e le barriere che invece ad oggi non ne hanno permesso la realizzazione.

L'aspettativa è che ci possa essere comunque un superamento di questi limiti.

Come già sottolineato dal lato offerta il cyber cat bond offre una soluzione alternativa e complementare per il finanziamento del rischio con tutti i vantaggi esposti nel primo capitolo tra cui la possibilità di trasferire una grande quantità di rischio che molti riassicuratori attualmente non possono assorbire.

Per questo tipo di transazione ci sono diversi ostacoli come la mancanza di un modello robusto per quantificare il rischio e quindi l'impossibilità attuale di ottenere una stima della perdita attesa poco volatile, principalmente per mancanza di una base dati sulle perdite abbastanza ampia e non biased.

Altro ostacolo che ne mina lo sviluppo, è il fatto che cyber-cat bond non permetterebbe di ottenere benefici dalla diversificazione in quanto questo rischio emergente è considerato altamente correlato con equity e bond tradizionali rispetto alle classiche ILS natural catastrophe.

Le recenti transazioni, però, mostrano che comunque esiste una fascia di investitori con una maggiore propensione al rischio interessata ad aggiungere rischio, almeno in piccole quantità, al proprio portafoglio e quindi ad integrare asset più correlati con l'economia in generale rispetto alle classiche ILS considerate incorrelate.

Questo è dovuto sia al fatto che una maggiore incertezza e correlazione si accompagna a più elevati premi per il rischio assunto che si traducono in interessanti potenziali guadagni, che è proprio ciò che gli investitori più propensi al rischio richiedono, sia al fatto che in realtà l'aggiunta di un cyber cat bond ad un portafoglio ILS, si pensi ad un fondo comune di investimento specializzato in ILS, permette di conseguire maggiore diversificazione intra-mercato, cioè sempre restando all'interno del settore ILS, e quindi mantenendo anche tutti i vantaggi maturati nel tempo con la specializzazione come le economie di apprendimento o di esperienza.

Inoltre, anche se gli effetti di un attacco cibernetico su larga scala potrebbero avere il potenziale di influire negativamente sui prezzi azionari, la percezione di una maggiore correlazione del cyber-cat bond rispetto al nat-cat bond non è così sostenibile perché per entrambe le categorie solo determinati settori saranno più duramente colpiti rispetto ad altri. Quando, infatti, si verifica una catastrofe naturale in un determinato luogo i retailer on line

non sono significativamente colpiti da questo evento, invece i settori più colpiti saranno quello assicurativo, che copre questi eventi, ed il settore healthcare.
Lo stesso si può dire quando si verifica un attacco informatico: infatti solo determinati settori saranno più duramente colpiti, sicuramente le imprese più dipendenti dal web e i cloud service provider saranno quelli che affronteranno una maggiore volatilità in borsa ma ad esempio il settore edile non dovrebbe subire elevate fluttuazioni di prezzo.
Quindi non tutti i titoli azionari sono correlati ai disastri naturali e non tutti i titoli azionari sono correlati agli incidenti informatici.
A supporto inoltre della modellizzazione di questo rischio emergente subentra in questo caso il framework proprio dei fenomeni catastrofali naturali, infatti è possibile replicare il processo di modellizzazione con dovuti adattamenti al contesto cyber.
Ciò porta alla stima delle metriche che diventano input, familiari agli investitori, del pricing del cat bond. E questo sviluppo dal punto di vista della modellistica è possibile perché molte società specializzate in questo ambito stanno sviluppando questi cyber cat-model. Non c'è comunque disclosure sulla struttura di questi recenti modelli.
Nel paragrafo precedente si è delineato un possibile pattern logico che potrebbe caratterizzare tale modello nel contesto cyber.
Un ostacolo esistente allo sviluppo di questi modelli, e quindi al cyber-cat bond, è il fatto che mancano dei parametri di confronto reali perché concretamente un Uragano Andrew "cibernetico" non si è ancora verificato, fortunatamente, quindi non si hanno a disposizione valori reali di perdite catastrofali per sviluppare delle ipotesi robuste ma esistono solo degli scenari deterministici e quindi questo inficia ulteriormente sullo sviluppo di un set di modelli appropriati a supporto di questa cartolarizzazione.
L'ostacolo alla mancanza di dati, tra l'altro, si attenuerà col tempo, rendendo le stime stocastiche meno volatili e questo spingerà la modellistica a proporre modelli più robusti.
Tra l'altro, l'introduzione del regolamento UE GDPR, prevedendo un obbligo di segnalazione dei data braches, contribuirà a ridurre in gran parte il bias dei dati attuali e a rendere più prontamente disponibili per il settore i dati che vanno ad ampliare appunto il data base attuale.
Altro ostacolo a queste transazioni potrebbe essere dovuto alla mancanza di comprensione del rischio informatico da parte del mercato dovuto alla mancanza di conoscenza tecnica in ambito ICT ma un'architettura efficace dello strumento ILS da parte del settore assicurativo potrebbe risultare vincente (Artemis 2015).

Ad esempio, in linea con una parte della letteratura che adotta modelli epidemici in contesto cyber, il rischio cibernetico può essere considerato un rischio epidemico che si espande come un'epidemia su larga sala infettando un'elevata porzione della rete, per cui un trigger puramente parametrico o un indice parametrico sembrano costituire la migliore scelta per un cyber cat bond proprio per riflettere il livello di contagio[54].

Questo perché il trigger parametrico è quello che più si avvicina ad un indice di sinistro definito in maniera chiara ed inoltre permette una quantificazione celere e obiettiva al verificarsi dell'evento informatico.

Infatti, fornisce trasparenza e chiarezza agli investitori ed inoltre permette la personalizzazione ad hoc cioè può essere strutturato in modo tale da rappresentare i parametri rilevanti di ogni incidente informatico. E riunisce in sé un set di condizioni parametriche che rappresentano la natura e la portata ad esempio dell'interruzione della rete e quindi diventa idoneo a rappresentare il threshold che fa scattare la copertura informatica.

Ad esempio, potrebbe essere composto da diverse statistiche che, in linea con i fattori rilevanti per le pandemie, includono il numero di devices colpiti o la mole di dati compromessa, la velocità di diffusione del malware o del DoS ed il perimetro geografico o aziendale che deve essere colpito affinchè scatti la copertura.

Ad esempio, per una copertura da attacchi DoS, il trigger, per approssimare l'impatto fisico dell'attacco, potrebbe essere strutturato in modo tale da riflettere il volume di dati in entrata che arresta il servizio o sito web e la durata dei giorni di interruzione dell'attività.

Concretamente questo indice parametrico potrebbe incorporare il sistema Intrusion detection system (IDS) a livello però nazionale e non locale.

Attualmente infatti l'IDS è un software utilizzato per identificare gli accessi non autorizzati, o comunque anomalie nel traffico ordinario di dati, ad esempio, a computer o alle reti locali, quindi non ha un raggio a livello nazionale ma si presume la possibilità di sviluppare un sistema dotato di un più ampio raggio.

Una parte del settore invece ritiene che l'uso di un industry loss index tipo il PCS Global cyber potrebbe contribuire anch'esso allo sviluppo del mercato[55].

Questi due indici, per quanto riguarda gli investitori, evitano l'opacità e la necessità di comprendere lo specifico complesso portafoglio cyber sottostante il cat bond, mentre dal

[54] Van Mieghem et. al(2014), Carter et. al (2018)

[55] https://www.artemis.bm/news/pcs-aims-to-help-understanding-of-the-silent-side-of-cyber-risk-johansmeyer/

lato della cedente questi trigger permettono la confidenzialità delle proprie informazioni in quanto, ad esempio, nel caso di industry loss trigger è l'indice stesso a fornire un valore a livello di settore e quindi non rivela ad esempio le posizioni o strategie della compagnia e in più elimina tutti gli svantaggi che presenta l'indemnity trigger, anche se per la compagnia assicurativa o riassicurativa aumenta il rischio base.

Conclusioni

Il surriscaldamento globale è un dato di fatto come anche i suoi effetti nella trasformazione degli equilibri del pianeta. La frequenza dei disastri naturali è in aumento così come il loro impatto è diventato sempre più devastante. Parimenti ai rischi catastrofali naturali tradizionali si vanno ad aggiungere rischi antropici emergenti, in particolare il rischio informatico, un rischio che può assumere dimensioni catastrofali.

In questo scenario governato dall'incertezza, dalla mancanza di una robusta base dati storica e dall'inasprirsi della dipendenza tra i rischi a livello globale che mina la capacità (ri)assicurativa delle compagnie, i cat bonds si configurano come soluzioni flessibili ed efficaci per cogliere le opportunità collegate alla gestione dei rischi più estremi, per i quali, essendo rari e severi, la disponibilità di capitale, idoneo alla loro assunzione, risulta ridotta nel settore assicurativo.

Le società specializzate nella modellizzazione del rischio catastrofale naturale possono sviluppare modelli di misurazione del rischio informatico robusti all'interno del framework attuale dei modelli catastrofali rendendo possibile un efficace cartolarizzazione di tale rischio mediante i cat bonds, strumenti finanziari, che is configurano come canali aggiuntivi per l'approvvigionamento delle risorse necessarie per la gestione dei rischi catastrofali mediante il trasferimento del rischio al mercato dei capitali.

I cat bonds, oltre ad essere degli strumenti strategici a supporto della gestione del rischio residuo, sono degli strumenti etici, perché, ad esempio, uno stato attraverso il capitale raccolto dall'emissione di questi titoli, può provvedere alla ricostruzione delle rovine di un paese causate dall'occorrenza di calamità naturali senza dover aggravare il deficit pubblico. Le compagnie (ri)assicurative, con l'emissione di questi titoli, sono messe nelle condizioni di svolgere il business, nel rispetto dei principi di economicità e prudenziali, in quanto i cat bonds contribuiscono a ridurre problematiche di insolvibilità delle imprese di (ri)assicurazione, che potrebbero insorgere nell'offerta di coperture contro rischi catastrofali, una evenienza che avrebbe ripercussioni a livello sistemico.

Altresì, questi strumenti possono essere utilizzati per attenuare i rischi nella determinazione del requisito patrimoniale di solvibilità e quindi consentono la liberazione di capitale che altrimenti risulterebbe immobilizzato. Sono strumenti di diversificazione del rischio, in quanto titoli che presentano bassa correlazione con gli altri asset tradizionali in portafoglio. Sono dotati di elevata flessibilità, in quanto, applicando lo stesso meccanismo di cartolarizzazione,

possono inglobare e quindi trasferire rischi di diversa natura, come comprovato dalle recenti transazioni.

Per tutte queste ragioni i cat bonds si configurano come una valida strategia di gestione e controllo del rischio catastrofale complementare alla riassicurazione tradizionale. Inoltre, creano nell'attuale economia 4.0 e nel nuovo contesto normativo post regolamento europeo GDPR, un circolo virtuoso, in quanto, lo sviluppo di un mercato cyber-cat bonds offre quella capacità assicurativa, attualmente mancante sul mercato, che si traduce nella possibilità di colmare il divario tra dimensione della copertura informatica attuale e reale fabbisogno e, l'accesso da parte della clientela a coperture rispondenti alle loro necessità, ne determina l'espansione del mercato che a sua volta si traduce in un incremento del fatturato per il settore (ri)assicurativo.

Bibliografia

Accenture (2017), *Cost of Cyber Crime Study,* Ponemon Institute LLC

Accenture (2018), *Cyber Threatscape Report 2018*, Midyear Cybersecurity Risk Review

Adrego Pinto A., Zilberman D. (2014), *Modeling, Dynamic, Optimization and Bioeconomics I*: *Contributions from ICM0D 2010 and the 5th Bioeconomy conference*, Springer

Air Worldwide, Kazuya F., (2016), *Catastrophe model for the assessment of exposure to disaster risks*,

Albarello D. (2013), *La pericolosità sismica*, Auditorium Reiss Romoli- Coppito (AQ)

Albertini L., Bareue P. (2009), The *handbook of insurance-linked securities,* John Wiley Sons Inc

Andrego Pinto A., Zilberman D. (2012), *Modeling, Dynamics, Optimization and Bioeconomics: contributions from ICMOD 2010 and 5th Bioeconomy Conference,* Springer

Ania, Associazione Nazionale tra le imprese Assicuratrici (2019), *Il rischio cyber, conoscerlo di più per proteggersi meglio,* Paper

Ania, Guy Carpenter, CONSAP (2011)*, Danni da eventi sismici e alluvionali al patrimonio abitativo italiano: studio quantitativo e possibili schemi assicurativi,* Report

AON Benfield (2016), *Annual Global Climate and Catastrophe Report,* Report

Aon Benfield (2018), *Reinsurance Market Outlook,* Report

Artemis (2015), *Could the capital markets solve the $1B cyber insurance policy gap?,* Report

Artemis (2015), *Life insurers need to diversify assets, include alternatives like ILS: Study,* Conning, American Council of Life Insurers, Report

Artemis (2018), *Cyber is the new property: Niklaus Hilti,* Credit Suisse ILS, Report

Artemis (2018), *ILS' role in paying climate related catastrophe claims to increase:Moody's,* Report

Artemis(2018), *Climate change presents both P&C threat & opportunity: Moody's,* Report

Arthur J. Gallagher (2017), *Addressing Non-affermative Cyber*, Capsicum Reinsurance Brokers LLP

Banca d'Italia (2017), *Cyber-attacks: preliminary evidence from the Bank of Italy's business survey,* Questioni di Economia e Finanza

Banca d'Italia, Ivass (2018), *Sicurezza cibernetica: il contributo della Banca D'Italia e dell'Ivass,* Tematiche istituzionali, Gruppo di coordinamento sulla sicurezza cibernetica (GCSC)

Bank of England-Prudential Regulation Authority (2019), *Cyber Insurance risk-follow-up survey results*, letter, A. Sweeney

Banks E. (2005), *Catastrophic Risk,* John Wiley & Sons, Ltd

Baryshnikov Yu., Mayo A., Taylor D.R. (1998), *Pricing of Cat Bonds*, Preprint

Belguise O., Levi C. (2003), Tempêtes: Étude des dépendances entre les branches Automobile et Incendie a l'aide de la theorie des copules, ASTIN Colloquium

Biagio S. (2015), *La grande truffa da un miliardo di dollari*, Il Sole 24 Ore, 22/02/2015

Bodoff N.M., Gan Y.(2009), *An Analysis of the Market Price of Cat Bonds, Casualty Actuarial Society E-Forum*

Bohme,R., Kataria G. (2006), *Models and measures for correlation in cyber-insurance*, Worshop of Economics of information Security

Braun A.(2012), Determinants of the cat bond spread at issuance, Zeitschrift fur die gesamte Versicherungswissenschaft, Volume 101, Issue 5,pp 721-736, Springer

Braun A., Weber J. (2017), *Evolution or Revolution? How Solvency II will change the balance between Reinsurance and Ils*, Working Papers on Risk Management and Insurance, N. 190

Briys E.(1997), From Genoa to Kobe: Natural Hazards, Insurance Risks and the Pricing of insurance linked bonds, London, Lehman Brothers International

Burnecki K, Kukla G., (2003), *Pricing of zero-coupon and coupon cat bond*, Applicationes Mathematicae 30(3) p.315-324,

Carfora M.F., Martinelli F., Mercaldo F., Orlando A. (2019), *Cyber Risk Management: an actuarial point of view,* IAC pre-print submitted

Carter S., Mainelli M. (2018), *Cyber-Catastrophe Insurance-linked Securities On Smart Ledgers,* Cardano Foundation

Cherubini U., Luciano E., Vecchiano W.(2004), *Copula methods in finance*, Wiley Finance

Cizek P., Hardle W.K., Weron R.(2011), *Statistical tools for finance and insurance*, Springer

CRO Forum (2016), *Concept Paper on a proposed categorization methodology for cyber risk*, CRO Forum, Amsterdam, Paper

Cummins J.David (2007), *Cat Bonds and Other Risk-liked Securities: State of the Market and Recent Developments*, Risk Management & Insurance & Actuarial Science.

Decreto del Presidente del Consiglio dei ministri,,17/2/2017*, Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionali,* Gazzetta Ufficiale n.87 del 13 Aprile 2017

Doherty Neil A. (2000), *Integraterd risk management: techniques and strategies for managing corporate risk*, McGraw-Hill

Dolce M., Martinelli A. (2004), *Analisi di vulnerabilità e rischio sismico,* Progetto Save, INGV/GNDT , Report

Volpe Putzolu G., Donati A. (2015), *Manuale di diritto delle assicurazioni*, Giuffrè Editore

Edesess M.(2014), *Catastrophe bonds: An important new financial instrument,* Alternative investment Analyst Review, CAIA Association

EIOPA(2018), Understanding Cyber Insurance- a structuterd dialogue with insurance companies, Report

Eling M., Schnell W., Sommerrock F.(2016), *Ten Key Questions on Cyber Risk and Cyber Risk*, Geneva Association Newsletter

Elling, M., Loperfido N. (2017), *Data breaches:goodness of fit, pricing and risk measurement*, Insurance: Mathematics and Economics, 75, pp 126-136

Embrechts P., Kluppelberg C., Mikosch T. (1997), *Modelling Extremal Events for Insurance and Finance*, Springer-Verlag

Embrechts P., Meister S.(1997), *Pricing Insurance derivatives : the case of CAT futures*, Proc. 1995 Bowles Symposium on Securitization of Insurance Risk, Georgia State University Atlanta, pp.15-26

European Commision, (2016), *Il clima cambia riduciamo i rischi. Strumenti finanziari per l'adattamento*, Derris , Report

EU-U.S. insurance dialogue project : new iiziatives for 2017-2019, Report

Francescani C. (2016), *Ransomware hackers blackmail U.S. Police Departments*, nbcnews, 26/04/2016

Galeotti M., Gurtler M., Winkelvos C., (2009), Accuracy of premium calculation models for CAT bonds: an empirical analysis, Working paper series No IF29V4, Technische Universitat Braunschweig

General Data Protection Regulation (GDPR), Regulation EU 2016/679

Haag M., Niraj Cholokshi (2017), *Hurricane Irma, now a category 5 storm, threatens the Caribbean and Florida* , 09/04/2017

Hedberg M.(2018), *Climate change will drive ILS market growth*, Entropics Asset Management AB

Herath H.B.S., Herath T.C. (2011), Copula-based actuarial model for pricing cyber insurance policies, Analyses and Actuarial Computations

Hofmann A., Wheatley S.(2019), Heavy-Tailed Data Breaches in the Nat-Cat Framework & the Challenge of Insuring Cyber Risks, arXiv preprint

Holzheu T., Karl K., Helfenstein R.(2006), *Securitization-new opportunities for insurers and investors*, Sigma (7/2006)

Ibe O. C. (2009), Stochastic Modeling , Academic Press

Ispra, Sistema Nazionale per la protezione dell'Ambiente (2018): *Dissesto idrogeologico in Italia: pericolosità e indicatori di rischio*

John C. Hull (2015), *Opzioni, futures e altri derivati*, Pearson

Johnson L.(2014), *Geographies of securitized catastrophe risk and the implications of climate change,* Volume 90, Issue 2, Clark University

Koch A.C. (2017), *Non-NatCat insurance linked securities: identifying market opportunities for diversifying perils*, Milliman

Lane M., Mahul O. (2008) Catastrophe Risk Pricing : An Empirical Analysis. Policy Research Working Paper; No. 4765. World Bank

Lane M.N. (2000), *Pricing risk transfer transactions*, Astin Bulletin, vol. 30, pp 259-293

Latchman S.,(2010*), Quantifying the risk of natural catastrophes,* AIR Worldwide Limited, Report

Lei. D.T, Wang J.H., Tzeng L. Y.(2008), *Explaining the Spread Premiums on Catastrophe bonds*, NTU International Conference on Finance, Taiwan

Lloy's Market Association (2013), *Catastrophe modelling, guidance for non-catastrophe modellers ,* Report

Lloyd's(2015), *Business Blackout, The insurance implications of a cyber attack on the Us power grid*, Emerging risk report

Loubergè H., Kellezi E. (1999), *Using Catastrophe-linked securities to diversify insurance risk: a financial analysis of cat bonds*, Journal of Insurance Issues

M. Amann (2010), *Greenhouse gases and air pollutants in the European Union*, European Consortium for modelling air pollution and climate strategies, Report

Ma C.Q., Ma Z.G. (2013), *Pricing catastrophe risk bonds: a mixed approximation method*, Insurance: mathematics and Economics, pp. 243-254

MacMinn R. (2009*), Securitization of Catastrophe Risk: New Developments in Insurance-Linked securities and Derivatives*, Journal of Insurance Issues

Mazzoleni P. (2005), *Dalla matematica finanziaria alla finanza matematica*, Istituto di Econometria e Matematica per le Applicazioni economiche, finanziarie, attuariali-Università Cattolica, Milano

McNeil A.J.., Frey R., Embrechts P.(2005*), Quantitative Risk Management*, princeton University Press

Michel-Kerjan E., Morlaye F. (2008), *Extreme events, global warming, and insurance-linked securities: how to trigger the tipping point,* The Geneva Papers on Risk and Insurance - Issues and Practice. January 2008 Volume 33, Issue 1, pp 153–176

Mitchell-Wallace K., Jones M., Hilier J., Foote M. (2017*), Natural catastrophe risk management and modelling: a practitioner's guide,* Wiley Blackwell

Mukhopadhyay A, Saha D, Mahanti A., Chakrabarti B.B(2005), *Insurance for cyber risk: a utility model*, Decision, pp. 153-169

OECD Publishing, No. 8(2005), *Policy Issues in Insurance; Catastrophic risks and Insurance,* OECD Publishing , Report

OECD(2017), *Enhancing the Role of Insurance in Cyber Risk Management*, OECD Publishing, Paris, Report

OECD-ADBI Workshop on Disaster Risk Financing in Asia

P. Scandone, M. Strucchi (1999): *Note di commento sulla zonazione sismogenetica ZS4 e di introduzione agli obiettivi del progetto 5.1.1 ,* Report

Paci S. (2018): *Assicurazioni. Economia e gestione*, Egea

Papachirstou D. (2009), *Statistical analysis of the spreads of catastrophe bonds at the time of issue*, Aon Benfield Re, 39th ASTIN Colloquium

Partner Re(2015), *The drivers of catastrophe bond pricing,* Report

Ponemon Institute(2017), *2017 Cost of Data Breach Study: Global Analysis,* Ponemon Institute LLC, Traverse City, Report

PRA, Supervisory Statement SS4/17 (2017), *Cyber Insurance underwriting risk,* Report

PwC(2015), Turnaround and transformation in cybersecurity:key findings the glob al state of information security, Survey

Ralph O. (2018), *Catastrophe bond losses force investors to reassess risk,* Financial Times

Risk Management Solutions (2012), Cat bonds demystified, Rms Guide to the asset class, Report

Risk management solutions Inc, Cambridge Centre for *risk studiess((2016), Maging cyber insurance acccumlation risk*, RMS

Ross S.M. (2007), *Introduction to probability models*, Academic Press

Rzym A., Abou Zeid T. (2018): *Catastrophe bonds: investing with impact*, Man Group, AHL

Sigma 50 years (2018), *Preliminary sigma estimates for 2018: global insured losses of USD 79 billion are fourh highest on sigma records*, Swiss Re Institute

Sigma No 1 (2008), *Calamità naturali e catastrofi man-made nel 2007: danni elevati in Europa*, Swiss Re Institute

Sigma No 1 (2017), *Cyber: getting to grips with a complex risk,* Swiss Re Institute

Sigma No 2 *(2009), Natural catastrophes and man-made disasters in 2008,* Swiss Re Institute

Swiss Re (2018), *Insurance-Linked Securities market update*, volume XXIX

Swiss Re(2017, Cyber liability: data breach in Europe, Swiss Re, Zurich

Van Mieghem P., Cator E. (2012), *Epidemics in networks with nodal self-infections ans the epidemic threshold*, Physical Review E

Wang S. (2000), *A class of distorsion operators for pricing financial and insurance risks*, Journal of risk and ainsurance

Wheatley, S., Maillart T. Sornette D.(2015*), The Extreme risk of personal data breaches the erosion of privacy*, Cornell University Library

Willis Re (2019), *ILS Market Update,* Report

World Economic Forum Marsh & McLennan Companies and Zurich Insurance Group (2019), *The Global Risks Report 2019 14th Edition,* available at: http://www3.weforum.org/docs/WEF_Global_Risks_Report_2019.pdf

Zimbidis A.A., Frangos N., Pantelous A.A.(2007*), Modeling Eartquake risk via Extreme Value theory and the pricing the respective catastrophe bonds,* ASTIN Bull

Sitografia

www.protezionecivile.gov.it

climate.nasa.gov

www.artemis.bm

www.morganstanley.com

www.e-distribuzione.it

www.ey.com

www.privacyrights.org

www.bermudareinsurancemagazine.com

www.verisk.com