La sicurezza nell'impero delle comunicazioni

Marco Baldi – Michele Elia – Massimiliano Sala

Globalizzazione è un termine molto controverso, al centro di dibattiti su cosa e come si deve intendere. È incontrovertibile, che le telecomunicazioni siano divenute una rete avviluppante il cui impatto sui sistemi economici, sociali, industriali e di governo è ben visibile. Il funzionamento e la vita degli Stati dipendono sempre più dalla loro affidabilità, per il cui conseguimento la crittografia è uno degli strumenti principali. Nello sviluppare l'idea di pubblicare una versione elaborata degli interventi tenuti in un convegno, dedicato alla crittografia, svoltosi a Roma nel 2014, ne è nato un progetto che si ripromette di ripercorrerne le tappe, dagli incerti inizi fino ai giorni nostri, ed esporre le tematiche alle frontiere della protezione e della sicurezza che, oggi, questa intrigante disciplina può o dovrebbe assicurare.

Il piano si compone di sette articoli di cui questo, introduttivo, descrive il composito stato del pervasivo sistema mondiale delle telecomunicazioni e le relative problematiche. I due successivi tracceranno una sintetica storia della crittografia, i passi rilevanti susseguitisi in due millenni e la sua evoluzione, da occulto strumento del potere a indispensabile ausilio della vita quotidiana. Ne seguiranno altri tre focalizzati sulla crittografia moderna e sulle applicazioni che si stanno dispiegando nell'impero delle comunicazioni, simboleggiato da internet, moderno Moloch che, pur sovrastandoci, ci aiuta a costruire una società forse più equa. Infine, chiuderà la rassegna un testo in cui saranno delineati i possibili sviluppi delle applicazioni, delle tecnologie e delle teorie matematiche che si dovranno impiegare o inventare. L'auspicio è che una meditata rivisitazione del passato permetta di comprendere meglio il presente al fine di affrontare con maggior consapevolezza un futuro tanto incerto quanto appassionante.

Chi non applicherà nuovi rimedi
deve aspettarsi nuovi mali, perché
il tempo è il più grande innovatore
Francis Bacon

È storia, seppur recente, che negli ultimi due decenni del XX secolo una rivoluzione scientifica, tecnologica e culturale ha interessato i sistemi di comunicazione dei paesi ad alta tecnologia. Telecomunicazioni satellitari, telefonia mobile, televisione digitale, personal computer e internet sono testimonianza visibile che la convergenza delle telecomunicazioni (sorte alla fine del XIX secolo col contributo determinante di Guglielmo Marconi) e della tecnologia dei computer (avviata durante la Seconda guerra mondiale dagli apporti teorici fondamentali di Alan Turing e John von Neumann nonché tecnologici di Presper Eckert e John Mauchly) ha determinato il nuovo assetto delle 'tecnologie dell'informazione'.

Quest'atipica rivoluzione ha avuto imprevedibili ripercussioni anche sui tradizionali metodi di produzione, di trasmissione e di 'utilizzo' del sapere. Tuttavia, anche se gli effetti su uno strategico e vitale bene quale il sapere si potranno osservare solo nei prossimi decenni, molto probabilmente saranno più dirompenti delle modifiche, oggi ben visibili e con cui ci dobbiamo invece confrontare, che hanno coinvolto la finanza, l'industria, l'intera economia e le varie forme di governo mondiali.

I commerci si stanno sempre più affermando su internet con effetti spesso stravolgenti per i consolidati sistemi di contrattazione e di movimentazione delle merci.

Il tradizionale sportello nel mondo bancario tende a spostarsi presso ciascun cliente: nelle case grazie alla rete e in ogni luogo raggiunto dai sistemi radiomobili di ultima generazione, modificando sia il modo di rapportarsi dell'utenza ai servizi bancari, sia l'organizzazione interna degli stessi istituti di credito.

Anche gli eserciti tendono sempre più a utilizzare le infrastrutture di rete civili, sia per motivi di economicità sia per ragioni di disponibilità di dati e informazioni contro catastrofi naturali o deliberati atti offensivi su vasta scala.
Infine, le diplomazie devono confrontarsi con sistemi di comunicazione che hanno azzerato i tempi delle decisioni e de localizzato le sedi dei contatti interpersonali.
Tutti questi fenomeni, al momento non strettamente controllabili, se per un verso hanno migliorato la qualità della vita, per contro, hanno reso il sistema globale più fragile, più sensibile a eventuali, pericolosi e drammatici regressi, più facilmente attaccabile da ogni sorta di avversari. Il mondo della comunicazione è divenuto un impero senza frontiere, ma debole all'interno per la vulnerabilità delle strutture portanti: le reti di telecomunicazione.
Mentre l'uso dei supporti elettronici digitali può avere un effetto favorevole anche nei piccoli business, il problema di mantenere la sicurezza delle comunicazioni va considerato in tutta la sua ampiezza e globalità.
I messaggi digitali sono relativamente facili da intercettare. La situazione è resa agevole ai predatori dal fatto che i testi in arrivo e in partenza, normalmente, devono essere reindirizzati attraverso un numero relativamente piccolo di stazioni, mentre i segnali nell'etere possono essere intercettati senza difficoltà ed effrazioni.
Avversari di ogni tipo, connazionali o stranieri, governativi o privati, possono ordinare e scandire testi in chiaro intercettati e selezionati secondo particolari indirizzi, oppure convenienti parole chiave presenti nel messaggio. Questo è accaduto per decenni, ovviamente anche prima che i calcolatori rendessero il lavoro ancor più facile. L'aspetto nuovo è dato dalla proporzione e dal numero di utenti che affidano i loro affari e segreti personali a segnali digitali che corrono su fibre ottiche, cavi o nell'etere.
Più un Paese è tecnologicamente avanzato, più usualmente è suscettibile all'intercettazione del traffico digitale. Pertanto, la protezione dell'informazione sta diventando una necessità inderogabile per assicurare il buon funzionamento della società.
Le tecnologie sviluppate per proteggere l'informazione sono molteplici, ma molte possono essere viste come generate nell'alveo della disciplina, genericamente nota come crittografia. Per millenni essa ha avuto come principale obiettivo la riservatezza dell'informazione ma, in tempi recenti, l'evoluzione tecnologica, unitamente al formarsi di una società mondiale con servizi integrati e sistemi di comunicazione globali, le ha delegato obiettivi molto più ampi, compositi e articolati.
Specificamente, il numero di servizi che hanno bisogno di una protezione dell'informazione cresce continuamente. In una lista, peraltro incompleta, si trovano, come sistemi, telefoni fissi e mobili, reti di calcolatori, o di grandi spazi e di ambienti domestici oppure di luoghi riservati. E come servizi si possono includere: e-mail, commercio elettronico, operazioni bancarie a distanza, telemedicina e ogni sorta di pubblico servizio che tende a spostarsi dagli uffici alle case e alle persone.

Lo scenario globale delle comunicazioni e la sua esigenza di sicurezza sono la proiezione moderna di una situazione antica. Rivisitare la storia della crittografia, rimarcandone i punti salienti, è un modo per imparare le lezioni del passato al fine di non ripeterne gli errori e di meglio penetrarne le idee per applicarle con profitto alle nuove imprevedibili e appassionanti sfide. È un modo per prepararsi al futuro, per comprendere, padroneggiare e prevedere le nuove tecnologie che sono e saranno indispensabili all'operatività in questo villaggio globale, come nelle preveggenti descrizioni di McLuhan.
Si è scelto di raccontare questo viaggio nel tempo e nell'ingegno diviso in due grandi periodi storici che hanno visto differenti evoluzioni della crittografia. Il primo periodo è stato caratterizzato dalla convinzione, forse ingenua o forse romantica, di poter nascondere al nemico l'algoritmo usato per cifrare i messaggi, mentre nel secondo si è iniziato a comprendere il ruolo della chiave e l'importanza sia della sua distribuzione, sia della sua difesa e segretezza.
Si è invece scelto di ripartire la descrizione dello stato moderno della crittografia in quattro diverse parti per tracciare il passaggio da arte delle scritture segrete a disciplina scientifica, per descrivere la grande novità della crittografia a chiave pubblica, frutto della matematica, per disegnare le intriganti e profittevoli applicazioni al riconoscimento personale e alla medicina e, infine, chiudere con le operazioni distribuite (cloud computing) e la crittografia quantistica. L'auspicio è che la lettura consenta di avere una visione articolata, ma completa, dello stato dell'arte della scienza crittografica. Le conclusioni sono state tratte cercando di estendere lo sguardo 'oltre la siepe' che ci separa dal futuro, arrischiando una fantasiosa ma plausibile descrizione degli sviluppi a venire. La realtà supererà la fantasia perché – come direbbe Mark Twain – non è costretta dalla logica.