Cosimo Comella

Alcune considerazioni sugli aspetti tecnologici della sorveglianza di massa, a margine della sentenza Safe Harbor *della Corte di giustizia dell'Unione Europea*

Sommario: Introduzione. – 1. Sorveglianza di massa e 'adeguata protezione'. – 2. Notizie dal *Datagate* e da altri *leaks*. – 3. La crittografia e la (in)sicurezza delle comunicazioni elettroniche. – Affrettate conclusioni.

Introduzione

La recente sentenza della Corte di giustizia dell'Unione Europea nel caso *Schrems vs Data Protection Commissioner*[1], sottoposto dalla *High Court* della Repubblica d'Irlanda, lascia sullo sfondo il tema della *mass surveillance*, soprattutto nella sua articolazione tecnologica, ancorché esso emerga in più punti della decisione.

Tuttavia l'argomento che sostiene l'azione iniziale di Maximilian Schrems nei confronti di Facebook e, successivamente, del *Data Protection Commissioner* irlandese è proprio l'esistenza di programmi di sorveglianza di massa su scala globale condotti da autorità federali statunitensi, portati a conoscenza del pubblico nel corso del 2013 a seguito delle dichiarazioni di Edward Snowden e alla pubblicazione di resoconti giornalistici e documenti riservati da parte del quotidiano britannico *The Guardian* e di quello statunitense *The Washington Post*, con la diffusione di ulteriori documenti a mezzo Internet da parte dell'organizzazione *Wikileaks*: azioni informative che hanno dato vita al clamoroso caso mediatico internazionale noto come *Datagate*.

In questo articolo, dopo una generale introduzione al tema della sor-

[1] Causa C-362/14 avente ad oggetto la domanda di pronuncia pregiudiziale proposta alla Corte di giustizia dell'Unione Europea, ai sensi dell'articolo 267 TFUE, dalla High Court (Corte d'appello, Irlanda), con decisione del 17 luglio 2014, pervenuta in cancelleria il 25 luglio 2014, nel procedimento *Maximillian Schrems contro Data Protection Commissioner*, con l'intervento di: Digital Rights Ireland Ltd.

veglianza di massa alla luce delle informazioni sulle attività di *intelligence* diventate di pubblico dominio, ci si concentra su alcuni aspetti tecnologici della *mass surveillance* contemporanea, presentando alcune delle principali metodologie di infiltrazione di reti e sistemi informatici e di telecomunicazione per attività di SIGINT condotte nell'ambito di programmi di spionaggio o di altre attività investigative.

Viene poi fatto cenno all'utilizzo delle tecnologie crittografiche e ai loro limiti rispetto alla protezione dei dati e della riservatezza delle comunicazioni, fornendo infine alcuni dettagli su due interessanti casi che hanno suscitato particolare allarme nella comunità di sicurezza informatica internazionale e che, interpretati alla luce delle rivelazioni del *Datagate*, costituiscono un monito riguardo all'affidamento acritico o inconsapevole a strumenti tecnologici per la protezione di informazioni e comunicazioni dalla cui *disclosure* può derivare un severo pregiudizio per i diritti e le libertà di un individuo.

1. Sorveglianza di massa e 'adeguata protezione'

La sentenza della Corte di giustizia UE del 6 ottobre 2015 non affronta direttamente il tema della sorveglianza di massa, tantomeno nella sua dimensione tecnologica, quantunque sia intuibile il peso che il caso *Datagate* ha esercitato sulla valutazione dei giudici, che nella ricostruzione fornita in narrativa e nella trattazione delle questioni pregiudiziali presentate dalla *High Court* fanno emergere chiaramente riferimenti al 'diritto e la prassi in vigore' nello Stato terzo (si veda il paragrafo 66 della decisione) che «non garantiscono un livello di protezione adeguato».

È invece nel procedimento principale intentato da Schrems innanzi al *Data Protection Commissioner*, e nel successivo giudizio d'appello innanzi alla *High Court*[2], che vengono fatti più espliciti ed estesi riferimenti alle rivelazioni di Edward Snowden sulle diverse campagne di raccolta di dati svolte da agenzie governative degli Stati Uniti (con la collaborazione di analoghi organismi di altri Paesi, anche europei).

In particolare, i giudici d'appello irlandesi hanno concluso che le rivelazioni di Edward Snowden dimostrano come le autorità americane abbiano commesso «eccessi considerevoli» nelle attività condotte, ancor-

[2] Schrems -v- Data Protection Commissioner [2014] IEHC 310 (18 June 2014) – http://www.bailii.org/ie/cases/IEHC/2014/H310.html [ultimo accesso 12.7.2016].

ché volte a tutelare un interesse pubblico, aggiungendo che «la NSA e altri organi federali, come il *Federal Bureau of Investigation* (FBI), potrebbero accedere a tali dati nell'ambito della sorveglianza e delle intercettazioni indifferenziate da essi praticate su larga scala».

D'altra parte, l'esistenza di programmi di spionaggio telematico (identificati con nomi in codice e acronimi ormai divenuti di pubblica notorietà come PRISM, XKeyscore, Tempora, Bullrun e altri), oltre a non essere contestata, veniva corroborata dalla divulgazione di ordini giudiziari emessi da corti americane in base al Chapter 36 del Title 50 dello U.S. Code[3], che forniva in questo modo conferme inaspettate alle rivelazioni a mezzo stampa. Conferme che non tardarono a venire direttamente dalle stesse autorità americane, seppur riferite alle attività di spionaggio estero (*foreign intelligence*)[4].

La stessa Facebook Inc., nel rispondere alle istanze iniziali di Schrems, aveva ammesso di sottostare a «significant constraints under US law» possibile eufemismo a fronte del ricorso da parte di autorità statunitensi (anche governative e non necessariamente giudiziarie) ai c.d. *gag orders* che vincolano chi vi è sottoposto a non divulgare nulla riguardo a determinati fatti e circostanze che formino oggetto di determinati ordini dell'autorità rispetto ai quali l'interessato è parte.

Si può sostenere, quindi, che almeno a partire dal 2013 l'esistenza di attività di *mass surveillance* sulle reti di comunicazione elettronica svolte dagli Stati Uniti e da altri Paesi per finalità dichiarate di lotta al terrorismo sia una realtà incontestata, tenendo ben presente che analoghe attività sono comunque praticabili e praticate ormai in ogni parte del mondo da chi ne abbia la capacità tecnica allorquando se ne determini la possibilità e la opportunità di trarne vantaggi economici, politici, militari.

«Yet only the foolish would deny that the United States has, by virtue of its superpower status, either assumed - or, if you prefer, has had cast upon it - far-reaching global security responsibilities. It is probably the only the world power with a global reach which can effectively monitor the activities of rogue states, advanced terrorist groups and major organised crime, even if the support of allied states such as the United Kingdom is also of great assistance in the discharge of these tasks and responsibilities. The monitoring of global communications

[3] http://uscode.house.gov/browse/prelim@title50/chapter36&edition=prelim [ultimo accesso 12.7.2016]

[4] C. Savage – E. Wyatt – P. Baker, *U.S. Confirms That It Gathers Online Data Overseas*, *The New York Times,* 6 giugno 2013, http://www.nytimes.com/2013/06/07/us/nsa-verizon-calls.html?_r=0 [ultimo accesso 12.7.2016].

- subject, of course, to key safeguards - is accordingly regarded essential if the US is to discharge the mandate which it has thus assumed. These surveillance programmes have undoubtedly saved many lives and have helped to ensure a high level of security, both throughout the Western world and elsewhere. But there may also be a suspicion in some quarters that

this type of surveillance has had collateral objects and effects, including the preservation and re-inforcing of American global political and economic power».

(dalla decisione della High Court irlandese sul caso Schrems -v- Data Protection Commissioner - [2014] IEHC 310 – 18.06.2014)

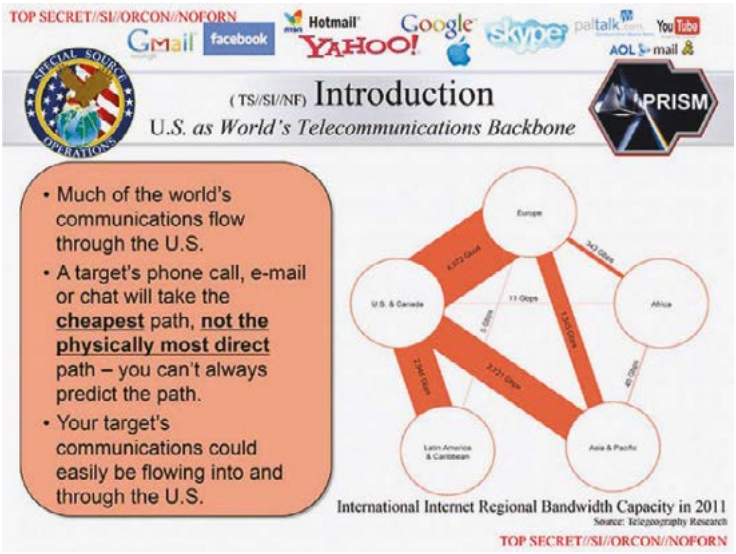
Ciò induce a qualche riflessione sullo scetticismo con cui furono accompagnate, a partire dal 1988, le notizie su un esteso *network* di SIGINT (*Signal Intelligence*) e COMINT (*Communications Intelligence*) realizzato con la cooperazione di Stati Uniti, Regno Unito, Canada, Australia e Nuova Zelanda (anche allora i *five eyes* della sorveglianza globale) per l'intercettazione globale di telefonia, posta elettronica e messaggi fax: si fa riferimento a quel *sistema Echelon* che, sollevando un enorme scalpore in Europa, suscitò anche l'interesse del Parlamento Europeo, con preoccupazioni per le possibili ricadute negative su imprese e sull'economia comunitaria, oltre che sui diritti civili dei cittadini europei[5].

La capacità tecnica di agire in determinati contesti tecnologici non è ovviamente esclusiva di organismi statunitensi o dell'area occidentale: altre potenze anche di rango regionale hanno dimostrato di possedere il *know-how* e le risorse per condurre operazioni di spionaggio informatico ed elettronico di altissimo livello, oltre che di essere protagoniste del mercato della sicurezza, anche informatica, a livello mondiale. Tuttavia le autorità statunitensi hanno goduto di una condizione di oggettivo privilegio, rispetto a quelle di altri Paesi, nel condurre operazioni di *intelligence* sulla rete Internet, per evidenti circostanze di fatto: i principali operatori della società dell'informazione sono infatti di origine americana e operano prevalentemente sul territorio degli Stati Uniti, su cui si concentra una mole di informazioni e di dati personali riferibili a una parte significativa della popolazione mondiale che non ha al momento analogie in nessun altro Paese. Basti pensare, in proposito, ai *social networks* quali *Facebook* e, in misura minore, *Google+* e

[5] *The ECHELON Affair – The EP and the global interception system 1998-2002* – http://www.europarl.europa.eu/EPRS/EPRS_STUDY_538877_AffaireEchelon-EN.pdf [ultimo accesso 12.7.2016]

LinkedIn, utilizzati ogni giorno da più di un miliardo di abitanti del pianeta[6] che consegnano ai *database* di queste imprese propri dati personali rivelatori di ogni aspetto della vita privata; e, soprattutto, ai grandi fornitori di piattaforme *cloud computing*, a cominciare da Amazon che con i suoi AWS – *Amazon Web Services* – ha creato il fenomeno *cloud* globale e fornisce servizi *IaaS* (*Infrastructure as a Service*) a una parte significativa di *sub-provider* o di *service provider*. Vi sono stime per cui fino al 70% del traffico Internet mondiale attraversi, grazie alla presenza dei *datacenter* Amazon, le reti della Virginia settentrionale, negli USA, in una zona geografica storicamente ricca di insediamenti industriali ICT e di agenzie governative operanti nei settori della difesa, della sicurezza e dell'intelligence[7].

A questo proposito è di particolare interesse un'altra delle famose *slides* di Snowden che qui si riporta e che mostra graficamente i volumi di dati scambiati tra le aree geografiche del mondo, e da cui si evidenzia il ruolo degli USA quale *hub* globale delle comunicazioni elettroniche, unitamente al dato della stretta connessione tra Europa e Stati Uniti, rilevabile dai flussi di comunicazione elettronica riportati graficamente in scala in base alla capacità trasmissiva.



[6] M. Zuckerberg, *Facebook*, 27 agosto 2015 – https://www.facebook.com/zuck/posts/10102329188394581 [ultimo accesso 12.7.2016].

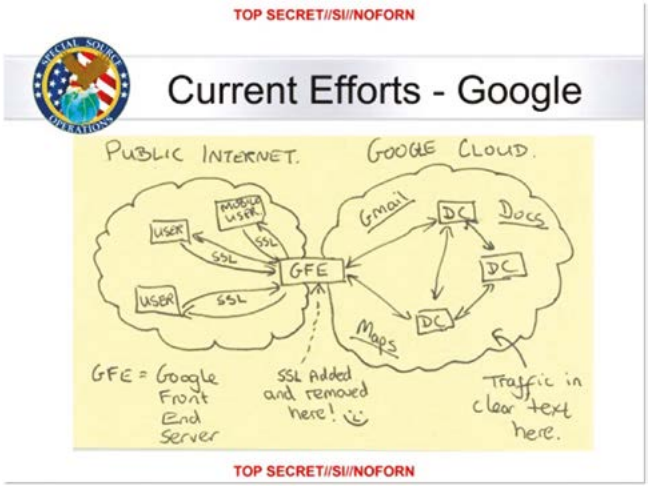
[7] *Up to 70 percent of global Internet traffic goes through Northern Virginia*, NextGov, January 8, 2016 – http://www.nextgov.com/big-data/2016/01/70-percent-global-internet-traffic-goes-through-northern-virginia/124976/ [ultimo accesso 12.7.2016]

2. Notizie dal Datagate e da altri leaks

Preso atto della realtà della *mass surveillance*, declinata in una pluralità di gradazioni che vanno dalla mera *data retention* normativamente prevista per i dati di traffico telefonico e telematico alla raccolta di informazioni frutto dell'applicazione di tecniche di *deep packet inspection* sui flussi di dati nella rete, all'acquisizione con tecniche invasive dei 'domicili digitali' praticate con l'ausilio di sofisticati sistemi *software*, è possibile analizzare, seppur sommariamente, le modalità con cui agenzie di *intelligence* e organismi investigativi possono concretamente ottenere accesso alle informazioni che quotidianamente vengono affidate al sempre più complesso e articolato ecosistema digitale.

Le tecniche di intrusione variano in base alla tipologia di comunicazione, alla selettività della ricerca che si intende svolgere, alla località geografica in cui avviene l'acquisizione del dato, alla minore o maggiore partecipazione di soggetti terzi: la casistica nota consente di individuarne alcune categorie, senza pretesa di esaustività, che qui sommariamente si discutono.

Collegamenti diretti ai datacenter delle Internet companies. Questa modalità di accesso è particolarmente rilevante nel contesto Internet, perché è quella cui risulta siano state sottoposte le maggiore aziende di comunicazione elettronica e *over the top* (OTT) che, basate negli USA, offrono servizi su scala geografica globale. In base ai documenti svelati da Snowden, le autorità statunitensi hanno potuto avere accesso diretto,



con propria connettività, alle reti interne dei maggiori operatori Internet, dei *social networks*, dei fornitori di *search engines*, dei *cloud providers* e di altri servizi di rete, considerati come veri e propri *provider* nell'ambito dei programmi PRISM, Xkeyscore, MUSCULAR.

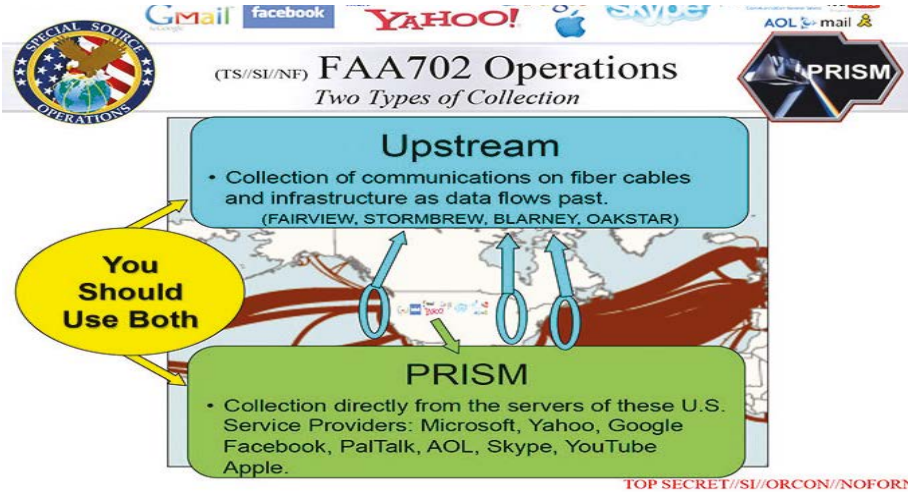
Ciò ha come immediata implicazione il fatto che la gestione da parte di un utente di propri dati tramite servizi resi, nel loro strato di presentazione, in forma di *web application* assistita da protezione crittografica (quindi con ricorso a connessioni basate su protocolli HTTPS/SSL – *Secure Socket Layer*, ingenerando nell'utente una percezione di riservatezza delle comunicazioni tra i propri dispositivi e il *service provider*) non abbia dato, e non dia attualmente, alcuna garanzia sul fatto che i medesimi dati, una volta registrati sui sistemi di *storage* nei *datacenter*, rimangano nella esclusiva sfera di conoscibilità e disponibilità dell'utente del servizio.

La protezione crittografica, infatti, pur correttamente predisposta e nei limiti della sua robustezza, è efficace solo nella fase di transito delle informazioni, mentre non è utilizzata, normalmente, quando il dato perviene alla sua destinazione presso i *server* che erogano tecnicamente il servizio, che lo elaborano per lo più 'in chiaro', per motivi di efficienza e a volte di praticabilità (essendo l'elaborazione di dati in forma crittografica ancora, in generale, argomento di ricerca e, per quel che è possibile già osservare, comunque gravata da pesanti limitazioni e penalizzazioni in *performance*).

È eloquente, a questo proposito, una delle più note *slide* fornite da Snowden, relativa allo schema delle connessioni alle reti *cloud* private di Google e Yahoo da parte degli utenti Internet, e allo 'spacchettamento' del protocollo SSL, sopra riportata.

Mentre questa modalità di accesso 'diretto', a cui fanno riferimento diversi documenti divulgati nel *Datagate*, appare tecnicamente priva di sofisticazioni, essendo basata sulla materiale accessibilità ai dati ottenuta tramite la collaborazione (spontanea o forzosa) del *service provider*, essa è quella quantitativamente più rilevante, poiché consente l'accesso indiscriminato a tutta la *customer base* delle *Internet companies* e a tutti i dati a essa collegati. In alcuni casi risultano allestiti veri e propri sistemi di interrogazione e ricerca che consentono agli analisti e agli investigatori di operare autonomamente le *query* sui *database* di interesse, siano essi costituiti dalle *spool directory* dei messaggi di posta elettronica o dai *repository* documentali dei servizi *cloud* pubblici con cui si realizzano servizi di *storage* in rete.

Nel contesto del *Datagate*, è documentata la raccolta di dati effettuata dalla NSA con questa modalità sfruttando connessioni dirette ai sistemi centrali di Microsoft, Yahoo, Google, Facebook, PalTalk, AOL, Skype,



YouTube, Apple[8].

Compromissione dei grandi nodi di smistamento delle comunicazioni elettroniche. In questo scenario, l'acquisizione dei dati avviene agendo sui flussi di comunicazione che attraversano le reti transcontinentali e le grandi centrali di smistamento costituite dai *router* di frontiera tra gli *autonomous systems* della rete Internet, dagli apparati di *switching* dei grandi *carrier* internazionali, dalle infrastrutture di *peering* del traffico come quelle dei c.d. *Internet eXchange Providers* (IXP) o *neutral access point* per l'interscambio 'paritario' di traffico IP, dalle reti e dagli apparati dei *transit operators*, dalle infrastrutture fisiche costitute dalle reti di cavi sottomarini in fibra ottica.

Al di là delle peculiarità di ciascuna di queste diverse infrastrutture, ciò che le accomuna è la distanza dall'utente finale, normalmente non in rapporto diretto con l'organizzazione che le gestisce, e il fungere esclusivamente da intermediatrici della comunicazione.Va da sé che reti e apparati di questa classe siano attraversati da flussi di enorme portata il cui filtraggio per la ricerca di contenuti o di dati esteriori di interesse investigativo richiede enormi capacità di elaborazione dei dati, ragionevolmente disponibili solo in strutture *ad hoc*, esterne alla rete o infrastruttura vigilata.

Il caso estremo di sfruttamento dei *landing sites* dei grandi cavi sotto-

[8] *U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program*, *The Washington Post*, 6 giugno 2013 – https://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html [ultimo accesso 12.7.2016]

marini, che pure risulta tra le azioni svolte da potenze occidentali nell'ambito dei programmi di *mass surveillance* (anche in danno, parrebbe, di Paesi alleati) e che ha suscitato preoccupazione e interesse tra le autorità di protezione dati europee, è un'attività che può essere quasi esclusivamente appannaggio di apparati statali e avvenire, salvi i pur ipotizzati scenari di alto spionaggio tra potenze nemiche con le intercettazione di cavi *in the middle* sui fondali oceanici, solo grazie a forme di collaborazione da parte degli operatori responsabili delle infrastrutture o da parte di organismi di sicurezza.

Nell'ambito del *Datagate*, tale modalità di spionaggio delle comunicazioni pare sia stata adottata da organismi di sicurezza del Regno Unito, nell'ambito del programma TEMPORA condotto dal *Government Communications Headquarters* (GCHQ), ritenuto da Edward Snowden più insidioso degli analoghi programmi americani[9].

Le intercettazioni dei cavi sottomarini plausibilmente possono svolgersi attaccando le componenti elettroniche dei 'punti di rigenerazione' delle linee di comunicazione in fibra ottica, in cui i segnali vengono amplificati per compensare le attenuazioni prodotte dalla distanza. Oltretutto negli stessi punti i fasci di cavi non sono accorpati e intrecciati, e sono più facilmente manipolabili singolarmente.

Tuttavia si deve ritenere che tale tecnica rappresenti una soluzione estrema, ben potendosi raggiungere lo stesso risultato operando senza le scomodità, la complessità tecnica e i costi dell'ambiente sottomarino: i cavi oceanici hanno pur sempre un «safe harbor» a cui approdare, e sono proprio le stazioni costiere le sedi in cui più agevolmente intercettare le comunicazioni, grazie a sonde ottiche che riflettono i segnali per captare le comunicazioni senza interferirvi in modo rilevabile.

I volumi di dati in transito sui cavi transcontinentali sono enormi, e per favorirne l'analisi con il sistema TEMPORA si è predisposta una capacità tecnica di *bufferizzazione* del traffico che consente il *full dump* delle comunicazioni per 72 ore e la registrazione dei *metadati*, ovvero dei dati di traffico esteriori alla comunicazione, per 30 giorni.

Sull'onda delle polemiche seguite al *Datagate*, il Parlamento britannico ha nominato il 5 novembre 2015 (la *House of Commons*) e il 25 novembre 2015 (la *House of Lords*) una speciale *Joint Committee* per la valutazione del *Draft Investigatory Powers Bill* che regolerà, una volta approvato, le intercettazioni delle comunicazioni, la raccolta, la conservazione e l'uso

[9] *GCHQ taps fibre-optic cables for secret access to world's communications, The Guardian*, 21 giugno 2013 – http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa [ultimo accesso 12.7.2016]

dei dati, definendo le modalità della vigilanza su tali delicate attività.[10]

Tra le più significative critiche rivolte al programma TEMPORA e agli analoghi programmi di raccolta di massa di informazioni è degna di nota quella dell'ex direttore tecnico del servizio di analisi della NSA, William Binney, secondo cui le raccolte di enormi volumi di dati omnicomprensivi rischiano di avere effetti controproducenti ai fini dell'analisi, assorbendo enormi risorse per la loro interpretazione e mimetizzando nei grandi volumi di dati le informazioni di rilievo investigativo[11]. Analoga preoccupazione è stata più volte espressa, anche recentemente, dal Garante per la protezione dei dati personali in riferimento al problema generale della raccolta di dati personali a fini di sicurezza nel contesto nazionale italiano[12].

Compromissione dei nodi locali di una rete. Questa attività richiede una capacità di penetrazione su componenti minori e più capillari di una rete di comunicazioni elettroniche, ma consente, a differenza del caso precedente, una maggiore selettività dei *target* che vengono discriminati a monte, rendendo nel contempo necessaria una minore capacità di elaborazione e filtraggio, operando sugli stadi di linea e sugli apparati più prossimi al soggetto o ai soggetti di interesse investigativo. In contesti non ostili, sia dal punto di vista normativo che di fatto, o in cui non ci siano esigenze di segretezza assoluta dell'attività, l'azione è realizzata con la collaborazione dell'operatore della rete, sia esso un *carrier* telefonico, un operatore di trasmissione dati o i reparti ICT di un'organizzazione, e può comportare l'installazione di apparati *ad hoc* oppure l'utilizzo di dispositivi già in possesso dell'operatore, per acquisire dati di traffico o flussi di comunicazione. L'esfiltrazione dei dati può avvenire tramite memorizzazione su dispositivi di *storage* o tramite la disponibilità di risorse di comunicazione *out-of-the-band* che garantiscano la consegna delle informazioni digitali a un 'punto di ascolto' predisposto.

Nel caso di centrali telefoniche per telefonia fissa o mobile e in quello

[10] *Joint Committee on the Draft Investigatory Powers Bill* – http://www.parliament.uk/business/committees/committees-a-z/joint-select/draft-investigatory-powers-bill/ [ultimo accesso 12.7.2016].

[11] *GCHQ mass spying will 'cost lives in Britain,' warns ex-NSA tech chief, The Register,* 6 gennaio 2016 – http://www.theregister.co.uk/2016/01/06/gchq_mass_spying_will_cost_lives_in_britain/ [ultimo accesso 12.7.2016].

[12] *La vera minaccia è quella cibernetica, un attacco alle grandi strutture del Paese. È lì che serve più protezione.* Intervista ad Antonello Soro di Liana Milella, *La Repubblica*, 27 novembre 2015.

di nodi di smistamento di traffico Internet (con dispositivi di *routing* o di *switching* per i protocolli di rete in uso) sono di ausilio, nello scenario collaborativo, le funzionalità di *lawful interception* insite negli stessi apparati, che consentono la duplicazione della comunicazione vocale oppure, nel caso del traffico dati, il c.d. *port mirroring*.

In via teorica, le stesse funzionalità di *lawful interception* o *port mirroring* possono essere sfruttate anche in contesti non collaborativi od ostili, sfruttando una qualche capacità di accesso nascosto alla rete dell'operatore (*backdoor*), ma è ragionevole pensare che la maggior parte delle attività di acquisizione di dati e di traffico avvenga e sia avvenuta in contesti che non richiedano l'applicazione di ulteriori tecniche informatiche invasive, e ciò appare rispondere al vero soprattutto nello scenario europeo che vede la presenza di Paesi che, a diverso livello di coinvolgimento, hanno dato sostegno alle attività di *intelligence* statunitensi svelate dal *Datagate*.

Occorre osservare come le misure di sicurezza degli apparati di commutazione telefonica e degli altri sistemi che compongono una rete nazionale di telecomunicazione siano esposti a rischi di accesso abusivo al pari di ogni altro sistema informatico, ragion per cui il settore telefonico è stato destinatario, in Italia, di una serie di provvedimenti prescrittivi dell'Autorità Garante per la protezione dei dati personali che, a partire dal 2006, ha dedicato una particolare attenzione agli aspetti di sicurezza nel settore TLC nazionale, a tutela della riservatezza delle comunicazioni e dei dati a esse riferiti.

Dirottamento e attrazione del traffico. L'accesso ai flussi di comunicazione elettronica attuato tramite compromissione di canali di comunicazione o di apparati è un'attività costosa e impegnativa e, in determinati scenari, tecnicamente impraticabile o non opportuna. Ci sono infatti metodi alternativi, ben più economici e quasi altrettanto efficaci con cui ottenere il controllo di flussi di comunicazione, agendo sui protocolli di rete che governano l'instradamento dei dati sulle 'reti a pacchetto'.

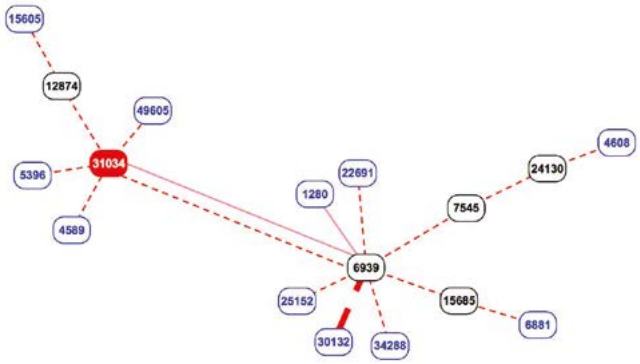
Sulla la rete Internet è noto che il protocollo utilizzato per lo scambio di informazioni sull'instradamento degli *IP datagram*, il *Border Gateway Protocol* (BGP), basa il proprio funzionamento sulla buona fede dei gestori nel trasmettere solo e soltanto *announcements* genuini, ovvero che rispecchino la reale situazione e le esigenza di instradamento delle reti appartenenti a un determinato *autonomous system* (AS).

E' stato più volte ipotizzato lo sfruttamento del meccanismo di annun-

cio e di aggiornamento delle rotte IP al fine di realizzare una sorta di 'sifonaggio' del traffico, ovvero per dirottare flussi destinati a una determinata rete verso un'altra rete o sistema autonomo senza che vi sia una seria motivazione tecnica, ma al solo fine di rendere il traffico dirottato ispezionabile o per sottrarlo al controllo del legittimo operatore[13].

Sedi preferenziali di svolgimento di questa attività sono i grandi nodi di interscambio gestiti dagli *Internet eXchange Provider* o da singole organizzazioni che gestiscono direttamente i propri router di frontiera.

Proprio la consapevolezza di queste criticità e il timore che gli IXP nazionali venissero utilizzati per realizzare operazioni di *traffic hijacking*



portarono l'Autorità Garante per la protezione dei dati personali a svolgere nel 2014 un'attività ispettiva specifica sugli IXP italiani, le cui risultanze furono condivise con le autorità nazionali di sicurezza e stimolarono, da una parte, un'azione di adeguamento tecnico da parte degli operatori interessati, dall'altra, il rafforzamento delle misure di protezione esterna da parte delle autorità di pubblica sicurezza[14].

Una inattesa conferma delle preoccupazioni dell'Autorità venne successivamente, a distanza di pochi mesi dalle attività ispettive, a seguito della

[13] *Revealed: The Internet's Biggest Security Hole, Wired.com*, August 2008 – http://www.wired.com/2008/08/revealed-the-in/ [ultimo accesso 12.7.2016].

[14] *Internet: adottate dagli Ixp le misure di sicurezza richieste dal Garante*, Newsletter n. 398 del 9 febbraio 2015 – http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3710265 [ultimo accesso 12.7.2016].

violazione dei sistemi della società milanese Hacking Team da parte di ignoti e della sottrazione in copia massiva di dati, documenti, codici programmativi e posta elettronica poi diffusi da WikiLeaks (luglio 2015)[15,16].

Si poté constatare in quella circostanza come i timori sulla corretta gestione dei flussi IP fossero stati più che giustificati: emergeva infatti come almeno una operazione di *traffic hijacking* fosse stata messa in atto nell'agosto 2013 nei confronti dell'operatore britannico Santrex, fornitore di servizi *cloud* e VPS (*Virtual Private Server*), con finalità riconducibili ad attività investigative svolte da un reparto specializzato di un corpo di polizia italiano (secondo quanto riportato, si trattava del ROS dell'Arma dei Carabinieri)[17].

A conferma delle informazioni divulgate da Wikileaks, l'analisi degli *announcements* BGP disponibile in forma storicizzata in rete tramite appositi siti, ha permesso di verificare l'accaduto nella sua evidenza tecnica e di precisarne i riferimenti temporali e i soggetti (operatori Internet) attivamente coinvolti.

Nello specifico, è risultato che il gestore dell'Autonomous System AS31034 (assegnato ad Aruba S.p.A.) a partire dalle ore 7,32 UTC del 16 agosto 2013 ha iniziato ad annunciare il prefisso IP 46.166.163.0/24. Conseguentemente, gli Autonomous Systems AS12874 (Fastweb), AS6939 (Hurricane Electric), AS49605 (Reteivo), AS4589 (Easynet) e AS5396 (MC-link) hanno iniziato ad accettare gli annunci e hanno messo in comunicazione le proprie reti, inconsapevolmente, con una rete IP appositamente configurata presso un operatore italiano per impersonare la rete dell'operatore britannico. La figura precedente, elaborata tramite BGplay, mostra schematicamente il *routing* risultante a seguito dell'annuncio surrettiziamente propagato.

L'azione di dirottamento è durata fino alle ore 13,53 UTC del 22 agosto 2013, dopodiché è stato ripristinato il normale *routing* verso la rete Sentrex. L'episodio, al di là di ogni valutazione di merito, conferma la delicatezza dell'infrastruttura Internet concepita negli anni '70 – '80 e ampiamente basata, in alcuni suoi snodi cruciali, sulla fiducia riposta nel corretto operare di alcuni soggetti che svolgono peculiari funzioni tecniche.

[15] www.wikileaks.org/hackingteam/emails/ [ultimo accesso 12.7.2016].
[16] Alex Hern, *Hacking Team hack casts spotlight on murky world of state surveillance, The Guardian*, 11 luglio 2015 – http://www.theguardian.com/technology/2015/jul/11/hacking-team-hack-state-surveillance-human-rights [ultimo accesso 12.7.2016].
[17] A. Toonk – D. Mahjoub, *How Hacking Team helped Italian Special Operations Group with BGP routing hijack* – http://www.bgpmon.net/how-hacking-team-helped-italian-special-operations-group-with-bgp-routing-hijack/ [ultimo accesso 12.7.2016].

Compromissione del terminale. Quando l'azione invasiva volta all'acquisizione di dati e informazioni si sposta dai grandi nodi delle reti verso i suoi elementi terminali, più prossimi all'utilizzatore finale, abbassandosi considerevolmente la complessità tecnologica (senza nulla togliere alla sofisticazione degli attacchi) e quindi, contestualmente, le barriere all'accesso a questo tipo di attività, lo scenario si arricchisce di nuovi attori, con la partecipazione di una più ampia platea di soggetti che producono e forniscono *software*, apparati e, soprattutto, servizi . È questo il caso delle *software house* specializzate nella produzione di strumenti intrusivi per il controllo a distanza e la 'colonizzazione' degli apparati terminali, siano essi *personal computer* o *smartphone*, in genere volti all'uso individuale. In alcuni scenari d'uso è possibile poi che il '*software* spia' venga inoculato sul terminale agendo da una sede remota rispetto all'ubicazione del *target*, mentre nella maggior parte dei casi l'inoculazione avverrà sfruttando meccanismi di *social engineering*, mediante *phishing* e *spoofing* di indirizzi di posta elettronica, oppure disponendo del materiale possesso del dispositivo da infettare. Qualora il terminale venga compromesso, comunque si giunga al risultato, verranno vanificate tutte le precauzioni eventualmente adottate, comprese quelle crittografiche, poiché lo *spyware*, agendo in modo silente e non venendo rilevato dai sistemi di protezione, avrà accesso a tutte le risorse del dispositivo, con possibilità di acquisire l'*input* da tastiera o da interfacce audio e video, e di osservare il traffico 'in chiaro' anche nel corso di sessioni assistite da protocolli di cifratura (SSL/TLS). Ciò è possibile perché, agendo sul terminale, lo *spyware* non opererà quale *man in the middle* tra le parti comunicanti, ma il suo punto di osservazione coinciderà con uno degli estremi della comunicazione in corso.

Questo genere di attacco ai sistemi terminali è sempre più diffuso per indagini giudiziarie e di polizia, e anche in Italia, pur con qualche incertezza sulla compatibilità dell'uso di tali strumenti con l'ordinamento giuridico, sembra che le possibilità di svolgimento per via tecnologica e senza la necessaria intermediazione tecnica di terzi (come i fornitori telefonici, nel caso della *lawful interception*) stia attraendo sempre più l'interesse delle forze di polizia, della magistratura inquirente e delle agenzie di sicurezza, inducendo lo sviluppo dell'offerta di servizi da parte di società specializzate che ottengono anche riconoscimenti all'estero ma godono di un significativo mercato interno fornendo supporto alle indagini giudiziarie.

3. La crittografia e la (in)sicurezza delle comunicazioni elettroniche

Del ricorso a tecniche di occultamento delle comunicazioni, soprattutto in ambito politico-militare, fornisce una straordinaria testimonianza lo storico Svetonio, nelle *Vite dei Cesari*, riferendo dello stratagemma usato da Giulio Cesare per comunicare con Marco Tullio Cicerone.

«Extant et ad Ciceronem, item ad familiares, id est sic structo litterarum ordine, ut nullum verbum effici posset: quae si qui investigare et persequi velit, quartam elementorum, id est D pro A et perinde reliquas commutet».

Vite dei Cesari (56, I), Svetonio

Come si rileva dal testo latino, il *cifrario cesariano* consisteva in una sostituzione monoalfabetica a passo ternario (lettere A sostituita da D, B da E…) oggi di facilissima decifrazione con una elementare criptoanalisi (anche in assenza di strumenti informatici), ma molto efficace nel I secolo a.C. in cui era già un'eccezione trovare persone in grado di leggere un testo in chiaro, figurarsi quindi un testo cifrato, seppure in un modo che oggi consideriamo banale.

Le tecniche di cifratura si sono evolute dall'antichità fino al XX secolo, ma sono state accomunate dalla necessità di condivisione della conoscenza sul metodo di cifratura adottato da parte degli interlocutori, ponendo sempre il problema della scelta del canale sicuro su cui veicolare informazioni come le chiavi di cifratura condivise (cifratura simmetrica) tramite cui provvedere alla ricostruzione del testo in chiaro.

Negli anni '70 la pubblicazione dei primi risultati di ricerca su tecniche alternative 'a chiave pubblica' apriva la strada a nuovi modi di protezione delle informazioni sensibili, abilitando la comunicazione sicura su canali insicuri che è oggi alla base del funzionamento dei protocolli SSL (*Secure Socket Layer*) e TLS (*Transport Layer Security*) senza i quali non esisterebbero oggi, per esempio, il commercio elettronico o l'*home banking*.

I lavori di Rivest, Adleman e Shamir e altri[18,19], e le tecnologie che ne sono derivate, hanno aperto un'era di ottimismo riguardo alla possibilità di comunicare in modo sicuro, al riparo da orecchie e occhi indiscreti.

Oggi occorre esercitare molta attenzione perché, pur non essendo finora stati messi in discussione i principi di base della moderna crittografia a

[18] R.L. Rivest - A. Shamir – L. Adleman, *A method for obtaining digital signatures and public-key cryptosystems,* Comm. ACM 21, 2 (Feb. 1978), 120-126.

[19] R.C. Merkle, *Secure communications over insecure channels.* Comm. ACM 21, 4 (Apr. 1978), 294-299.

chiave pubblica, esistono accorgimenti e tecniche che possono significativamente ridurre il livello di protezione o vanificarlo del tutto, esponendo le parti comunicanti allo svelamento delle proprie comunicazioni.

Si è già fatto cenno a come la contaminazione dei terminali della comunicazione eluda all'origine quasi ogni forma di protezione: la comunicazione avverrebbe in modo tecnicamente sicuro rispetto all'ascolto sul canale da parte del c.d. *man in the middle*, mentre un altro intruso potrebbe ascoltare il traffico collocandosi comodamente a uno degli estremi del cavo (in senso figurato). Un attacco di questo tipo non richiede alcuna competenza di criptoanalisi o di tecniche crittografiche, poiché l'abilità richiesta è soltanto quella necessaria a conquistare il controllo di un terminale utilizzato da una delle parti comunicanti, e una volta ottenuto questo risultato il resto verrà da sé.

Affrontiamo invece nel seguito due differenti e ben più sofisticati casi di compromissione di sistemi *software* e *hardware* in cui una più complessa linea d'azione è stata individuata, suscitando dubbi e incertezze che hanno scosso la fiducia fin qui ottimisticamente nutrita riguardo alle correnti tecniche di cifratura a chiave pubblica.

Si tratta di due casi piuttosto recenti che hanno interessato l'uno lo sviluppo degli standard crittografici adottati dall'industria informatica mondiale e l'altro un grande produttore di apparati di rete e di sicurezza, rivelando singolari e inquietanti collegamenti.

Il caso NIST/Dual_EC_DRBG

Alla base di diversi sistemi crittografici è la capacità di generare efficientemente *numeri pseudo-casuali* e *sequenze random* con più che buone qualità statistiche, da usare per comporre coppie di chiavi robuste in sistemi a chiave pubblica. Qualora le sequenze *random* generate non siano di buona qualità, e siano quindi in qualche misura prevedibili, anche a costo di un certo impegno di risorse computazionali, gli algoritmi di cifratura che le utilizzano verranno significativamente indeboliti e le informazioni con essi cifrate esposte potenzialmente ad attacchi e alla decifrazione da parte di soggetti non legittimati.

I generatori pseudocasuali utilizzati in ambito crittografico vengono chiamati *Cryptographically Secure Pseudorandom Number Generator* (CSPRNG), e uno di questi, basato sulla c.d. crittografia ellittica (*Elliptic Curve Cryptography)*, è il Dual_EC_DRBG (*Dual Elliptic Curve Deterministic Random Bit Generator*), utilizzato a partire dal 2004 in diver-

si sistemi di cifratura.[20]

Già al momento della sua standardizzazione da parte del *National Institute of Standards and Technology* (NIST) negli Stati Uniti erano emerse nella comunità scientifica serie perplessità sull'algoritmo, perché in determinati suoi passaggi si celava la possibilità per un soggetto a conoscenza dei valori assunti da alcuni parametri matematici prefissati, utilizzati nella costruzione del generatore, di predire le sequenze *random* (che sono in effetti totalmente deterministiche, e appaiono *random* solo a un'analisi stocastica) con un limitato sforzo computazionale, potendo quindi calcolare le chiavi di decifratura per leggere in chiaro i messaggi (o analizzare in chiaro il flusso dei dati su un canale trasmissivo).

Grazie al *Datagate* seguito alle rivelazioni di Snowden si è potuto appurare, nel corso del 2013, come i dubbi sollevati da insigni matematici e criptoanalisti[21,22,23], basandosi sul dato scientificamente acquisito della potenziale vulnerabilità individuata e di cui era ignota la paternità, fossero più che fondati. Si è infatti appreso che, da una parte, la NSA aveva assicurato un cospicuo finanziamento alla società RSA perché rendesse l'algoritmo Dual_EC_DRBG come CSPRNG di *default* nei propri prodotti *software* e, nel contempo, che la stessa agenzia aveva agito affinché l'algoritmo fosse incluso nello standard ANSI X9.82 e, successivamente, in ISO/IEC 18031:2005 e in NIST SP 800-90 (dicembre 2005), assicurandone un'ampia diffusione e accettazione nell'industria informatica e negli utilizzatori.

Particolarmente interessante è il passaggio dalla standardizzazione ANSI del giugno 2004 alla pubblicazione dello standard NIST, perché nei lavori preparatori il problema della possibile vulnerabilità era stato discusso nel gruppo di lavoro, ma la formulazione artatamente adottata da NIST al momento della pubblicazione dello standard fece sì che gli implementatori fossero invogliati, rispettando la norma tecnica, ad adottare l'algoritmo Dual_EC_DRBG affinché i loro prodotti potessero conseguire la certificazione FIPS 140-2 *Security Requirements for Cryptographic Modules*

[20] *Recommendation for Random Number Generation Using Deterministic Random Bit Generators* - NIST Special Publication 800-90A – http://csrc.nist.gov/publications/nistpubs/800-90A/SP800-90A.pdf [ultimo accesso 12.7.2016].

[21] K. Gjøsteen, *Comments on Dual-EC-DRBG/NIST SP 800-90, Draft December 2005* – 16 Marzo 2006 – http://www.math.ntnu.no/~kristiag/drafts/dual-ec-drbg-comments.pdf [ultimo accesso 12.7.2016].

[22] *D.R. L. Brown , Conjectured Security of the ANSI-NIST Elliptic Curve RNG*, 29 Marzo 2006 – http://eprint.iacr.org/2006/117.pdf [ultimo accesso 12.7.2016]

[23] B. Schoenmakers – A. Sidorenko, *Cryptanalysis of the Dual Elliptic Curve Pseudorandom Generator*, 29 Maggio 2006 – http://eprint.iacr.org/2006/190.pdf [ultimo accesso 12.7.2016].

richiesta dalle amministrazioni USA. Questo specifico vincolo fu efficace anche tra gli sviluppatori del software *open source* OpenSSL, ampiamente usato in tutto il mondo grazie alla sua inclusione nei sistemi operativi Linux e Unix, nonostante la consapevolezza dei rischi insiti nell'algoritmo.

Dopo la pubblicazione dei retroscena dell'elaborazione dello standard NIST SP 800-90 per merito del *Datagate* il NIST ha pubblicato una sua versione aggiornata, introducendo delle misure correttive che impediscono di sfruttare la conoscenza occulta dei parametri per calcolare le chiavi di decifrazione delle comunicazioni protette.

Il caso Dual_EC_DRBG qui sinteticamente riassunto è di enorme gravità, perché dimostra come, a fronte di un interesse molto forte, agenzie dotate di particolare capacità tecnica, finanziaria e di persuasione politica possano condizionare in modo molto sottile l'evoluzione di *standard* basilari per la sicurezza delle comunicazioni in Internet, con impatto potenzialmente disastroso sulla fiducia degli utenti nella sicurezza della rete e, in caso di utilizzo distorto rispetto a quello pubblicamente dichiarato di contrasto al terrorismo, con gravissime conseguenze su diritti e libertà fondamentali degli individui, a cominciare dalla libertà di espressione.

Dal punto di vista informatico, gli studiosi di *computer science* non potranno che ricordare la frase con cui Donald E. Knuth, nel secondo volume della sua monumentale opera *The Art of Computer Programming,* ammoniva rispetto all'uso disinvolto dei generatori pseudo-casuali:

> «*Random numbers should not be generated with a method chosen at random*»[24].

L'attuale dibattito sul controllo delle reti crittograficamente protette, acuito dalle stragi di Parigi del novembre 2015, deve tenere in considerazione tutti i possibili effetti di un indebolimento programmato della sicurezza informatica delle reti, poiché gli stessi strumenti che nel mondo ritenuto libero e democratico proteggono la *privacy* delle comunicazioni e la correttezza delle transazioni finanziarie (valori considerabili possibilmente recessivi rispetto alla sicurezza e all'ordine pubblico), nei paesi non democratici o in cui non sono garantiti i fondamentali diritti umani la disponibilità di strumenti crittografici per comunicare è una delle poche forme di protezione dei cittadini e del dissenso contro lo strapotere dei regimi.

[24] D.E. Knuth, *The Art of Computer Programming – Volume 2 – Seminumerical Algorithms*, Reading, Massachusetts: Addison-Wesley, 1969.

Il caso Juniper Networks

Nel dicembre 2015 la nota azienda americana Juniper Networks, produttrice di apparati di *routing* e *switching* per reti locali e geografiche e di sistemi di sicurezza, ha segnalato tramite il proprio sito[25] l'esistenza di due vulnerabilità nei propri *firewall* dotati di sistema operativo NetScreenOS™. La notizia ha suscitato grande scalpore per via della diffusione dei sistemi Juniper e per le caratteristiche delle due differenti vulnerabilità.

Nel caso della prima vulnerabilità si trattava di una classica *backdoor* di relativamente facile scoperta: Ronald Prins di FoxIT ha per primo comunicato su Twitter di avere individuato la *password* nascosta in meno di sei ore di tempo[26] dall'annuncio di Juniper grazie a un confronto tra diverse versioni del *firmware* dell'apparato, e di averla trovata uguale alla stringa di caratteri *<<< %s(un='%s') = %u* , appositamente scelta per mimetizzarla e confonderla tra le diverse *format-string C++* presenti nel codice sorgente, nascondendola agli occhi di analisti e sviluppatori. Chi fosse stato a conoscenza della *password* avrebbe potuto accedere in modo interattivo (tramite protocolli SSH e Telnet) a uno qualsiasi dei circa 26.000 apparati NetScreen venduti da Juniper in tutto il mondo, con privilegi di amministratore di sistema, qualunque fosse la *username* utilizzata anche se non esistente nella configurazione del dispositivo.

Nel caso della seconda, ancora più grave, vulnerabilità si è trattato della possibilità di mettere in atto la temuta 'decifrazione passiva' del traffico da parte di un soggetto in grado di operare come *man-in-the-middle* sui flussi di dati trasmessi lungo circuiti VPN (*Virtual Private Network*) gestiti con apparati NetScreen.

Sono stati ipotizzati collegamenti tra la prima vulnerabilità e la seconda, nel senso che l'accesso abusivo a un sistema NetScreen consentiva la modifica di parametri crittografici delle connessioni VPN, ma è certamente la seconda vulnerabilità a destare maggiore preoccupazione e a rivestire maggiore interesse nel presente contesto.

[25] *Juniper Networks Security Incident Response – Important Announcement about ScreenOS®* - http://forums.juniper.net/t5/Security-Incident-Response/Important-Announcement-about-ScreenOS/ba-p/285554 [ultimo accesso 12.7.2016].

[26] R. Prins, *Hmmm. It took @foxit 6 hours to find the password for the ssh/telnet backdoor in the vulnerable Juniper firewalls. Patch now* – https://twitter.com/cryptoron/status/677900647560253442 [ultimo accesso 12.7.2016].

Essa, infatti, si è rivelata consistere in una *backdoor crittografica*[27,28] connessa all'algoritmo Dual_EC_DRBG per la crittografia ellittica delle cui caratteristiche si è già detto, e rappresenta quindi una delle possibili applicazioni della vulnerabilità artatamente introdotta da NSA nello standard crittografico NIST SP 800-90[29].

È interessante come Juniper Networks, secondo produttore mondiale di apparati di rete dopo Cisco Systems, abbia laconicamente dichiarato, da una parte, di «non avere alcuna prova di sfruttamento della vulnerabilità su sistemi» da essa venduti, dall'altra, che «non c'è alcun mezzo per scoprire se questa vulnerabilità è stata sfruttata».

Alla luce di altre rivelazioni del Datagate, come quelle pubblicate da *Der Spiegel* nel 2013[30] e relative al software FEEDTROUGH progettato dalla NSA per creare una differente *backdoor* persistente sui sistemi firewall della Juniper, si ritiene che diversi altri produttori di apparati possano aver subito analoghe attenzioni, a cominciare da Cisco e CheckPoint, aziende *leader* di mercato della sicurezza di rete che, al pari di ogni altra azienda informatica operante nel medesimo settore, dovranno applicare ogni possibile diligenza per una revisione straordinaria dei propri codici programmativi, alla ricerca di analoghe vulnerabilità suscettibili di sfruttamento.

Affrettate conclusioni

Il caso *Snowden/Datagate* ha consentito all'opinione pubblica di toccare con mano e di misurare l'esile distanza che protegge la sfera delle comunicazioni elettroniche e dell'esperienza digitale dall'invasività della *mass surveillance* praticata per finalità di lotta al terrorismo: il difficile equilibrio tra rispetto della vita privata e tutela della sicurezza, messo a dura prova dagli scenari apertisi dopo l'11 settembre 2001 e dalle differenti sensibilità presenti nelle diverse aree del mondo rispetto alla protezione degli indi-

[27] B. Schneier, *Back Door in Juniper Firewalls*, 21 December 2015, https://www.schneier.com/blog/archives/2015/12/back_door_in_ju.html [ultimo accesso 12.7.2016].

[28] A. Langley, https://www.imperialviolet.org/2015/12/19/juniper.html [ultimo accesso 12.7.2016].

[29] CVE-2015-7755: *Juniper ScreenOS Authentication Backdoor* – https://community.rapid7.com/community/infosec/blog/2015/12/20/cve-2015-7755-juniper-screenos-authentication-backdoor [ultimo accesso 12.7.2016].

[30] *Shopping for Spy Gear: Catalog Advertises NSA Toolbox, Der Spiegel*, 29 dicembre 2013, http://www.spiegel.de/international/world/catalog-reveals-nsa-has-back-doors-for-numerous-devices-a-940994.html [ultimo accesso 12.7.2016].

vidui dall'invasività e dai poteri degli Stati, costituisce oggi la sfida più importante della società dell'informazione, e richiede il coinvolgimento di competenze giuridiche, tecnologiche, di sicurezza oltre che di *intelligence*.

Nell'ambito delle azioni di monitoraggio generalizzato, le tecnologie crittografiche costituiscono un mezzo di difesa degli individui, nonché lo strumento abilitante lo sviluppo dell'economia digitale, ma sono anche armi efficaci a disposizione di organizzazioni terroristiche per comunicare eludendo l'interferenza delle legittime autorità. Al centro, il difficile ruolo di chi deve applicare le leggi, governare la complessità di fenomeni globali come il terrorismo, l'instabilità internazionale e le ondate migratorie, la criminalità organizzata, utilizzando gli strumenti che il progresso rende disponibili.

In questo senso, i recenti attacchi terroristici di Parigi e di San Bernardino negli USA hanno spinto tutte le società occidentali a interrogarsi ancora più emotivamente su cosa fare per impedire in futuro simili azioni, evocando in particolare il pericolo che il terrorismo sfrutti tecniche di cifratura delle comunicazioni, offerte anche da reti amatoriali, per operare al riparo dalle forze di polizia.

Sia in Europa che negli Stati Uniti si moltiplicano le richieste di assicurare 'entrate di emergenza' alle comunicazioni, garantendo la possibilità di accedere a informazioni e dispositivi protetti crittograficamente come i moderni *smartphone* e *tablet*.

Purtroppo la comprensibile aspirazione degli operatori e delle agenzie di *law enforcement* spesso non si traduce in una specificazione di ciò che dovrebbe essere fatto in concreto sul piano delle tecnologie, riproponendo la situazione che si creò negli USA negli anni '90 per iniziativa dell'amministrazione Clinton, sostenitrice della *key escrow* e dell'introduzione dei *Clipper Chip* sui dispositivi informatici. Ma in quell'occasione (novembre 1993) il Congresso americano ebbe la sensibilità di costituire una commissione *ad hoc* presso il *National Research Council* (NRC), ampiamente partecipata da esponenti della ricerca scientifica e della comunità di *intelligence* e di *law enforcement*, per studiare la politica nazionale riguardo alla crittografia, in quel momento vista come tecnologia abilitante il controllo delle comunicazioni e dei 'domicili digitali', per finalità di tutela della sicurezza nazionale.

Il ponderoso rapporto conclusivo[31] della commissione (di cui facevano parte, tra gli altri, Ann Caracristi, ex vice direttrice della NSA e compo-

[31] K. W. Dam – H.S. Lin, eds., Cryptography's role in securing the information society, – Committee to Study National Cryptography Policy – National Research Council NATIONAL ACADEMY PRESS, Washington, D.C. 1996.

nente del *Foreign Intelligence Advisory Board* del gabinetto Clinton, e Benjamin Civiletti, ex *U.S. Attorney General*) si tradusse in una presa d'atto della difficoltà di affrontare il problema nei termini proposti dall'amministrazione.

Infatti, relativamente alle soluzioni sul *key escrowing* la commissione osservò che qualunque regolamentazione fondata sulla disponibilità di 'chiavi di scorta' su base nazionale sarebbe stata naturalmente votata al fallimento, essendo impraticabile un accordo internazionale sui ruoli nella custodia delle chiavi e nella loro condivisione su scala planetaria, e avrebbe costituito un fattore di penalizzazione dell'industria ICT americana, poiché il mercato globale avrebbe presumibilmente rifiutato soluzioni tecnologiche caratterizzate da una capacità di controllo da parte di organismi di uno Stato estero. Inoltre, osservava come quel tipo di tecnologia si sarebbe prestato naturalmente al *dual use* a favore di regimi dittatoriali o comunque non rispettosi dei diritti umani, trasformandosi in uno strumento di ulteriore oppressione. Comunque, l'elevata complessità di un sistema articolato di *key escrow* avrebbe accresciuto il rischio di esposizione a vulnerabilità impreviste: l'esperienza dell'informatica mostra infatti come ogni sistema complesso non sia esente da difetti ed errori di programmazione (*bugs*) che sono causa di incidenti informatici che mettono a rischio la sicurezza delle banche dati nella quotidiana vita digitale.

Oggi il dibattito pubblico sulla sicurezza nella sfera digitale, condizionato dai tragici fatti di cronaca relativi al terrorismo, ci riporta a quel tempo, ma con un contesto tecnologico e sociale profondamente cambiato grazie alla pervasività della rete Internet, delle tecnologie ICT, dei *social network*, con i problemi già sul tappeto sostanzialmente irrisolti e una complessità notevolmente accresciuta, in presenza delle quali si produce una spinta verso soluzioni rapide, momentaneamente rassicuranti ma rischiose nel medio-lungo termine, che spaziano dalle già note limitazioni all'uso della crittografia alla diffusione di strumenti di controllo dei dispositivi ICT per scopi di indagine, alla raccolta massiva e duratura di dati di traffico, all'interconnessione di banche dati per finalità di sicurezza, all'analisi del traffico telematico da operare presso i grandi *Internet provider*, all'utilizzo delle funzionalità di localizzazione ormai insite in tutte le tecnologie che si interfacciano in vario modo alla rete globale.

Nell'attuale situazione sarebbe invero auspicabile una maggiore consapevolezza dei problemi e dei limiti delle tecnologie da parte di decisori politici, assemblee legislative, singoli legislatori e *opinion makers*, affinché la conciliazione delle libertà individuali e sociali con le esigenze di sicurez-

za rifugga dalle emotività e si basi esclusivamente su valutazioni razionali ponderate, rifuggendo semplificazioni e scorciatoie inefficaci che possono danneggiare e comprimere gli spazi di libertà che la nostra civiltà ha conquistato anche grazie anche ai progressi delle tecnologie dell'informazione.

Per far questo, è essenziale il coinvolgimento del mondo della ricerca scientifica e tecnologica e dell'industria ICT nazionale per consentire il necessario approfondimento dei problemi e delle possibili soluzioni; inoltre, occorre una parallela forte azione di raccordo internazionale senza la quale ogni iniziativa locale, anche da parte di Paesi tecnologicamente avanzati, rischia di sconfinare nel velleitarismo e di non produrre alcun beneficio.

Abstract

This paper addresses the mass surveillance activities revealed by Edward Snowden, emphasizing the role of the Datagate as background issue in the recent European Court of Justice decision against the EU-USA «Safe Harbor» agreement. Importance and limitations of cryptography as a self-defense weapon against the invasiveness of surveillance technologies are also briefly discussed.

The recent discovery of two different cases of vulnerability in network security equipment is described along with its relations to the Datagate, whilst readers are cautioned against placing blind confidence in cryptographic technology to protect sensitive data.