dell'Arma dei Carabinieri

Rassegna

ISSN: 0485-3997

3

Anno LXIII -luglio/settembre 2015

dell'Arma dei Carabinieri
Rassegna

Direttore Responsabile
Gen. D. Vittorio Tomasone

Redattore Capo
Col. Giuseppe Arcidiacono

Redazione
Lgt. Remo Gonnella
M.A. s.UPS. Alessio Rumori
Brig. Mario Pasquale
App. Sc. Lorenzo Buono

Direzione e Amministrazione
Via Aurelia, 511 - 00165 Roma - tel. 06-66394680
fax 06-66394746; e-mail:scufrassegna@carabinieri.it

Grafica, Fotocomposizione e Impaginazione
a cura della Redazione

Fonti iconografiche
Ministero della difesa
Comando Generale dell'Arma dei Carabinieri
Scuola Ufficiali Carabinieri

Periodico trimestrale a carattere scientifico-professionale
a cura della Scuola Ufficiali Carabinieri
Proprietà editoriale del Ministero della Difesa
Iscritto nel Registro della Stampa del Tribunale di Roma
al n. 305/2011 in data 27-X-2011
Diffuso attraverso la rete internet sul sito www.carabinieri.it
dal Service Provider "BT Italia" S.p.A. Via Tucidide, 56 - 20134 Milano

EDITORIALE

Con il presente fascicolo assumo l'incarico di Direttore responsabile della "*Rassegna dell'Arma dei Carabinieri*". Rivista che nel settore editoriale della pubblicistica militare si presenta quale utile strumento di approfondimento di temi giuridici, scientifici e storici.

Un cordiale saluto ai nostri lettori, ai miei predecessori e a tutti coloro che collaborano alla redazione della Rassegna.

Nel rispetto di una oramai consolidata linea editoriale, verrà confermato un percorso logico-giuridico, teso a valorizzare - auspico sempre di più - il taglio specialistico di una pubblicazione che rimane eminentemente tecnica.

In questo numero presento, in apertura, un interessante studio nell'ambito dell'informatica forense, con una disamina, attraverso il sistema operativo "Linux", del recupero e dell'analisi dei dati informatizzati. Il fine è quello di ricavarne informazioni sensibili che, nel caso di specie, riguardano il campo delle indagini digitali.

Attraverso una trattazione approfondita del sistema, gli autori, un Ufficiale dell'Arma ed un Consulente tecnico, descrivono la struttura del *filesystem* utilizzato, fornendo una panoramica d'insieme delle potenzialità del sistema stesso, seguita da un caso pratico di applicazione con metodi e strumenti usati.

L'articolo che segue affronta il tema delle attività di *Peacekeeping* e, in particolare, il ruolo riservato alla componente di Polizia.

Gli organismi internazionali richiedono sovente assetti idonei a condurre operazioni in aree destabilizzate e, in tale ambito, l'Arma ha assunto un ruolo guida, con l'addestramento di oltre settemila "*peacekeepers*" presso il Centro di Eccellenza per Stability Police Units di Vicenza e con il diretto intervento in varie aree geografiche.

Il successivo articolo affronta un tema di grande attualità sul controllo del territorio e sull'attività informativa quali strumenti di contrasto al terrorismo di matrice religiosa. Fenomeno antico ed in costante evoluzione. L'analisi qui presentata individua i criteri, anche normativi, con i quali tale attività deve essere condotta, facilitata nella sua declinazione, per quanto riguarda il nostro Paese, dalla presenza capillare sul territorio dell'Arma dei Carabinieri.

Per la rubrica "*Materiali per una storia dell'Arma*", proponiamo un breve stralcio che ripercorre l'impegno profuso dai nostri militari nel corso della tormentata prima guerra mondiale, dal quale risaltano compiti e atti di valore che valsero, a fine conflitto, la prima Medaglia d'Oro al Valore Militare alla Bandiera dell'Arma.

Buona lettura.

Gen. D. Vittorio Tomasone

dell'Arma dei Carabinieri
Rassegna

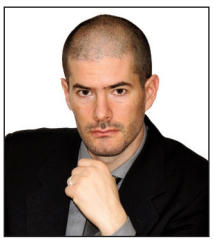
SOMMARIO n. 3
luglio - settembre 2015

Studi

Informazioni e Segnalazioni

Attualità e commenti

LINUX FORENSICS



Paolo DAL CHECCO

Consulente Tecnico in ambito Forense

Giuseppe SPECCHIO

Sottotenente,
Analista di laboratorio - Specialista in Informatica Forense
Raggruppamento Carabinieri Investigazioni Scientifiche

1. Introduzione

Con il termine "linux forensics" si possono intendere due cose ben distinte - ma non del tutto separate. La prima, quella per la quale si trova la maggior quantità di materiale in rete, consiste nell'eseguire analisi forensi tramite Sistema Operativo Linux e gli strumenti o i comandi che vengono forniti con esso. Ovviamente l'approccio ha i suoi vantaggi, gli strumenti presenti sono molteplici e spesso gratuiti, così da permettere a chi sa utilizzare un ambiente Linux di analizzare sistemi Windows, Mac OS ma persino iOS e Android oltre ovviamente a Linux stesso.

Noi però intendiamo procedere con una trattazione di come si può eseguire un'analisi forense di un sistema Linux, non con un sistema Linux. Vero che poi useremo - in particolare nel mock case - un ambiente Linux (il sistema DEFT, per essere precisi) per gli innumerevoli vantaggi che ciò comporta.

Ciò non toglie che quanto mostreremo può interamente o quasi essere riprodotto utilizzando per l'analisi un sistema Windows o persino Mac OS, ovviamente acquisendo, anche talvolta a pagamento, gli strumenti necessari allo scopo. Cosa che soprattutto nel caso del Mac OS non sempre è facile da farsi se non ci si avvale di soluzioni a pagamento oppure quali MacPorts od HomeBrew, package manager che permettono di utilizzare numerosi strumenti Linux anche sul Mac.

La linea conduttrice di questo breve saggio sarà quella di guidare il lettore negli aspetti di Linux che maggiormente riguardano il campo delle indagini digitali, partendo da una descrizione mirata del sistema. Lungi quindi dal proporre una sorta di "manuale" d'uso, verranno presentati i comandi e le locazioni di rilevanza che l'investigatore dovrà conoscere quando si troverà di fronte all'analisi forense di un sistema Linux. Dopo aver mostrato la struttura del sistema così come deve essere nota a un analista forense, verranno illustrati alcuni strumenti e comandi indispensabili per chi si occupa di indagini digitali di sistemi Linux.

In conclusione, un case study, o mock case, guiderà il lettore in un esempio pratico di indagine su un sistema Linux che egli potrà ripetere sul proprio ambiente di lavoro, grazie alla possibilità di scaricare dalla rete il disco virtuale su cui saranno eseguite le indagini e il sistema DEFT Linux, tramite il quale verranno eseguite le operazioni illustrate.

2. Struttura del sistema

Poiché la maggior parte dei lettori è probabilmente abitutata ad avere a che fare con sistemi Windows, utilizzeremo la linea del confronto evidenziando similitudini e differenze per sfruttare i riferimenti già noti come guida nell'esplorazione delle indagini forensi su sistemi Linux.

2.1 Il File system

La prima differenza risiede nella struttura del file system[1] utilizzato e in

(1) - È una gerarchia di directory e file, ospitata su un dispositivo di memorizzazione secondaria.

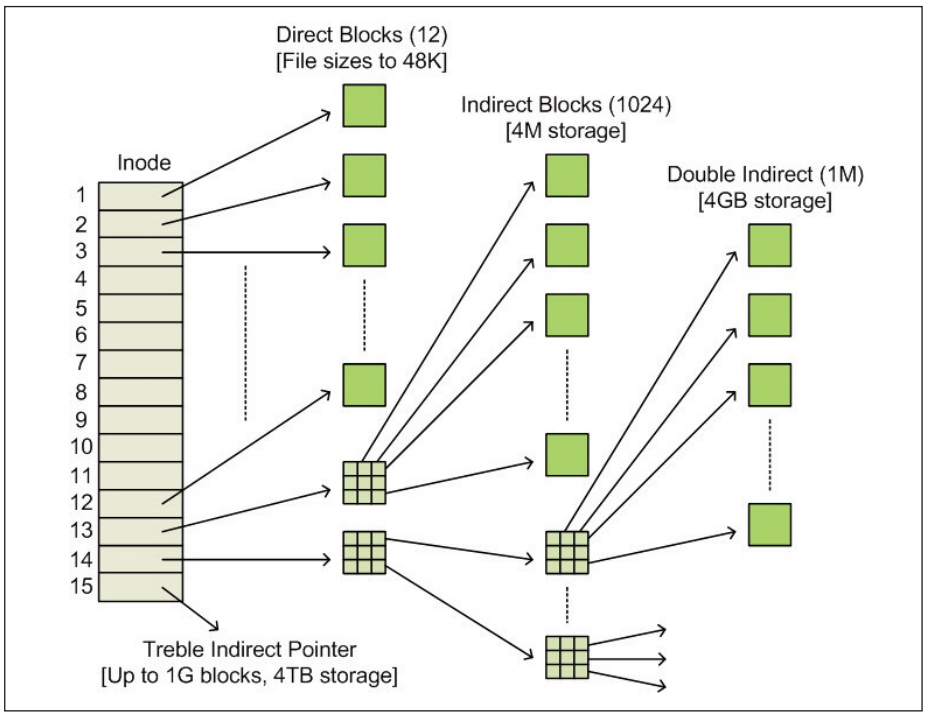
come viene mostrato all'utente. Windows utilizza principalmente file system NTFS, oppure FAT o ultimamente exFAT, mostrando in genere all'utente il dispositivo collegato assegnandovi una lettera dell'alfabeto (es. "C:\"). È anche possibile visualizzare i contenuti del dispositivo in una cartella o fare span di più dischi su un unico volume, ma la maggior parte degli utenti ignora queste possibilità e si limita ad utilizzare le lettere di volume.

Linux impiega invece come default e regola generale (ovviamente modificabile) il mounting dei dispositivi su directory, in genere "/mnt" o "/media". Questo significa che pendrive USB, hard disk e supporti di memorizzazione di massa si troveranno - su sistemi live - in una di quelle due cartelle. Il file system è gerarchico e tutto parte dalla cosiddetta "root" che si pone al livello superiore e viene identificata con il simbolo "slash" ("/"). Il disco principale - quello contenente il Sistema Operativo - è in genere montato su "/", talvolta (soprattutto sui server) singole partizioni vengono montate in percorsi diversi, avremo perciò la partizione "/home", "/var/www", "/boot" e altre di minore interesse. Il motivo della separazione delle partizioni è che, in questo modo, è possibile evitare che la saturazione di una comprometta la funzionalità del sistema e inotre è possibile impostare privilegi diversi per directory diverse. Ad esempio, su "/home" si potrebbe non volere che gli utenti eseguano applicativi, lo stesso anche su "/tmp" e così via.

Il file "/etc/fstab" conterrà indicazioni su eventuali mapping statici e sulle modalità di mount (es. l'hardi disk contenente i backup sarà in "/mnt/backup" e non avrà privilegi di esecuzione dei file). Altro aspetto da tenere in considerazione è che, mentre in Windows l'utente raramente si dovrà immischiare con gli identificativi dei dispositivi, in Linux file come "sda" o "hda1" all'interno della directory "/dev" sono all'ordine del giorno e indicano la tipologia e il numero di partizione dei dispositivi connessi al sistema. Ai vecchi drive IDE infatti vengono automaticamente assegnati i nominativi "/dev/hda" per il primary master, "/dev/hdb" per il primary slave e così via, mentre le partizioni dei drive vengono identificate con i numeri ordinali hda1, hda2 e successivi. I dispositivi SATA e USB vengono invece riconosciuti come i vecchi SCSI, tramite SCSI emulation, con la notazione "/dev/sda", "/dev/sdb" e così via, mentre per le partizioni vale lo stesso principio visto per i dischi IDE.

Parlando di file system, invece, Linux utilizza principalmente EXT3 ed EXT4, basati sul Berkeley FFS impiegato nei sistemi BSD. Una differenza non da poco perché la compatibilità del file system EXT è ridotta rispetto a quella dei tradizionali NTFS e FAT e così anche le nozioni e gli strumenti a riguardo.

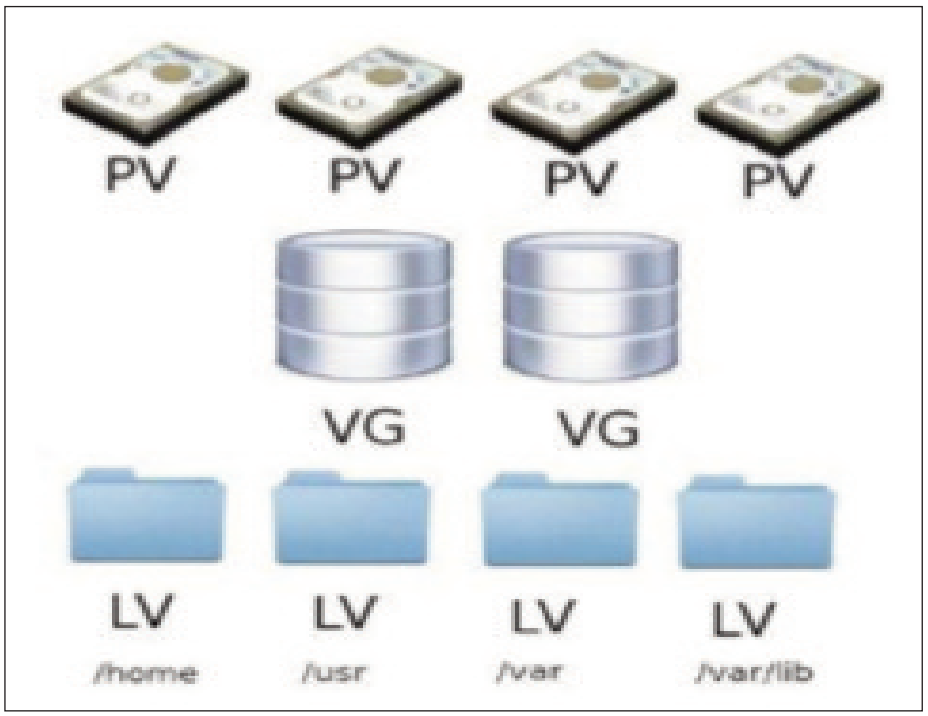
EXT3 è compatibile all'indietro con il file system EXT2 da cui deriva, aggiungendovi il journaling che permette di eseguire modifiche ai file in maniera transazionale preservando il più possibile l'integrità dei dati. EXT3 supporta file di dimensione fino a 4TB e file system fino a 16TB. Vi è un'ulteriore enorme differenza rispetto al file system EXT2, cioè il fatto che su EXT3 il recupero dei dati cancellati è decisamente arduo, spesso impossibile. EXT2 (così come NTFS e FAT) marcava semplicemente l'inode come inutilizzato e i blocchi come liberi, lasciandone i puntatori intatti. EXT3 - che supporta un meccanismo di mapping di blocchi indiretto - per poter garntire integrità anche dopo un crash azzera i puntatori e rende così particolarmente complesso capire dove e come erano organizzati i dati prima di essere cancellati. Osserviamo infatti il sistema di indirizzamento a blocchi indiretti del file system EXT3 nella seguente immagine.



È proprio il journal, in realtà, che permette di recuperare file cancellati se questi sono stati acceduti di recente e il journal è abbastanza capiente da mantenere i dati dei puntatori ai blocchi del file cancellato.

EXT4 è l'evoluzione di EXT3, che ne aumenta le possibilità permettendo di supportare file fino a 16 TB e file system fino a 1 EB. EXT4 usa gli extent, cioè un gruppo di blocchi contigui, invece del mapping dei blocchi indiretto utilizzato da EXT4 ma anche i puntatori agli extent vengono azzerati dopo la cancellazione di un file, quindi il recupero dei file cancellati risulta anche in questo caso particolarmente difficile. EXT4 è compatibile all'indietro con EXT3 e EXT2, che si possono montare come EXT4 migliorando le prestazioni. Al contrario, EXT3 è compatibile in avanti con EXT4, che si può montare come EXT3 ma solo se non sono utilizzati gli extent.

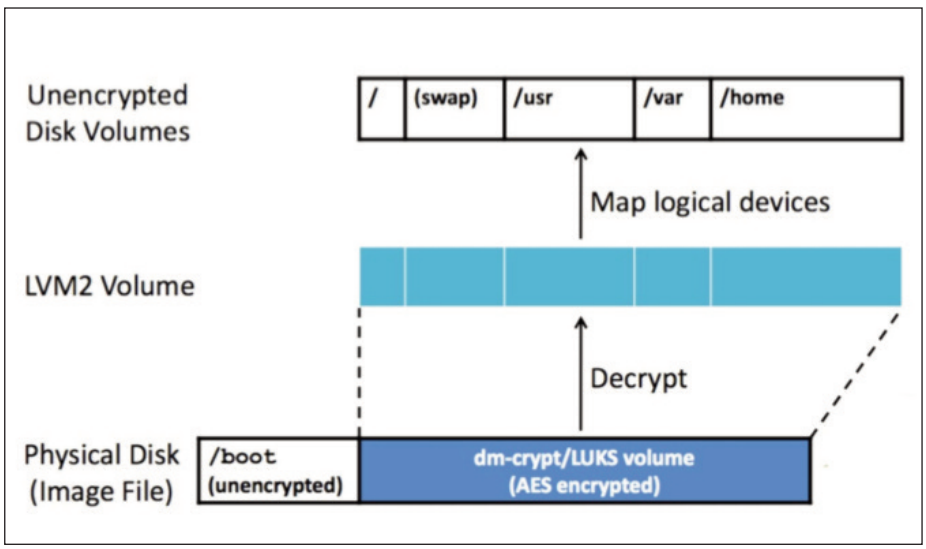
Per complicare ulteriormente le cose, i file system in Linux ormai tendono a essere organizzati in Volumi Logici tramite meccanismo di LVM2. Il sistema LVM2 consiste in un partizionamento logico che astrae l'hardware sottostante, con ovvi vantaggi di dinamicità, velocità e possibilità di eseguire napshot.



I livelli del sistema LVM2 mostrati in figura sono i seguenti, partendo dal volume fisico fino a giungere a quello logico:

- "Phisical Volume" (PV) corrispondono agli hard disk;
- "Volume Group" (VG) contiene volumi fisici e logici;
- "Logical Volume" (LV) sono l'equivalente delle partizioni.

Il meccanismo di LVM2 può essere utilizzato in concomitanza con la cifratura del file system tramite LUKS o dm-crypt, creando quindi due annidamenti che, in fase di analisi dei dati, complicano ulteriormente la vita all'investigatore.



Come si osserva in figura, sarà infatti necessario ricavare il volume logico da quello fisico tramite decifratura e, successivamente, assemblare i vari file system astraendo dal volume logico.

2.2 Il Registro di Sistema

Smarcato il problema del file system, concentriamoci sull'equivalente del "Registro di Sistema" che in Linux non esiste e in Windows contiene dati di configurazione del sistema, delle applicazioni e degli utenti. Windows fornisce appositi comandi (API) destinati alla modifica del Registro di Sistema, che non può essere acceduto direttamente perché è codificato e i file sono bloccati dal Sistema Operativo.

In Linux non c'è nulla di simile, la soluzione per mantenere le informazioni che in Windows sono nel registro di sistema è la cartella "/etc". All'interno di tale cartella risiedono diversi file di testo - alcuni direttamente sotto "/etc" altri in sottocartelle specifiche per le applicazioni - che contengono diverse configurazioni: dalle impostazioni di rete agli utenti, dai gruppi alle configurazioni delle applicazioni. Da tenere presente che alcune applicazioni - soprattutto quelle a linea di comando o le shell script che in Linux sono ancora frequenti - contengono file di configurazione nella propria cartella di esecuzione, altri invece vengono lanciati indicando la configurazione come parametro.

2.3 Il Registro degli Eventi

Anche il registro degli eventi, ben noto in Windows, ha un'alternativa in Linux che è bene conoscere. La directory "/var/log" contiene, infatti, i log delle attività di sistema ma non solo. Le applicazioni che mantengono storico sono in genere configurate per utilizzare tale locazione per il salvataggio dei propri archivi storici: avremo così i log del web browser Apache e di eventuali altri software installati sul sistema, spesso in sottocartelle dedicates. Uno dei file più importanti della directory è "/var/log/wtmp", che contiene l'elenco degli accessi riusciti al sistema, con il suo opposto "/var/log/btmp" che ne contiene invece quelli non riusciti. Utile integrare questi file con quanto contenuto in "/var/log/auth", "/var/log/secure" e talvolta "/var/logaudit/audit.log" che riportano informazioni più precise sugli accessi, anche remoti, come indirizzo IP di provenienza, utilizzo di password o certificati e così via. Vedremo nel mock case presentato qui di seguito quale è quanta ricchezza di informazione viene fornita, in ambito d'indagini digitali, dai file contenuti nella directory "/var/log". In genere - a meno che non sia stato deciso diversamente dal sistemista - i log vengono mantenuti per 4-5 settimane tramite il sistema di logrotate. Da ricordare che i file di log sono quasi tutti (ad eccezione ad esempio di "wtmp" e "btmp") in formato testo, quindi la loro validità e integrità non è garantita da strumenti checksum, codifica o strumenti di controllo. Chiunque potrebbe aggiungere o togliere righe, facendo eventualmente attenzione a ripristinare le date di creazione/modifica/accesso al file.

2.4 Lo Storico dei Comandi

Particolare attenzione - come vedremo in seguito nel mock case - merita lo storico dei comandi digitati dagli utenti sulla linea di comando, reperibile nel file "bash_history" nelle directory degli utenti.

Giova ricordare che tale file viene salvato e aggiornato al termine della sessione con i comandi mantenuti in memoria, quindi le istruzioni ivi contenute fanno parte di una sessione conclusa. Questo significa che - segnatevelo perché può tornare utile - semplicemente concludere un'attività su shell con il comando "kill -9 0" implica che la sessione verrà terminata bruscamente e il file bash_history non aggiornato.

I comandi digitati compaiono nell'ordine in cui vengono eseguiti, da tenere presente però che più sessioni diverse vengono mescolate nello stesso file creando quindi non poca difficoltà di comprensione.

2.5 Gli utenti

Parlando di utenti, ricordiamo che le cartelle degli utenti sono in genere contenute nella directory "/home" a parte l'utente root - equivalente all'Administrator di Windows - la cui directory è direttamente in "/root".

I privilegi degli utenti in genere sono assegnati tramite gruppi, quindi è importante per ogni utente valutare i file "/etc/passwd" (dal quale si evince la shell assegnata all'utente e il gruppo principale) e il file "/etc/group" che indica, appunto, i gruppi di appartenenza dell'utente. Anche il file "/etc/sudoers" va tenuto in considerazione in quanto contiene informazioni su quali utenti hanno autorizzazione a scalare i privilegi e in quale contesto, diventando ad esempio virtualmente "root" per particolari applicazioni.

All'interno della cartella "home" ogni utente possiede anche i propri documenti, oltre a diversi file nascosti che iniziano con il punto (".") e che contengono configurazioni specifiche di alcune applicazioni.

Tale cartella è da tenere sotto particolare controllo perché eventuali applicazioni di startup (buone o cattive) vengono inserite proprio nella "home" degli utenti, oltre che negli script di avvio sotto la cartella "/etc".

2.6 I programmi di avvio

Proprio gli script o i programmi di avvio possono contenere software malevoli, motivo per il quale oltre alla home degli utenti la directory "/etc" con le sue sottodirectory "init.d" e le varie "rcN.d" con N compreso tra S, 0 e 6 sono di interesse per l'investigatore che si trovi a valutare eventuali operazioni occorse su di una macchina Linux. In base al runlevel in cui si trova il sistema (non approfondiremo ma diremo che esistono 7 livelli con funzioni specifiche, in genere il sistema gira nei livelli da 2 a 5) possono essere avviati e interrotti servizi in base alla configurazione specifica. In Windows andremmo a cercare nel registro tra i servizi con avvio automatico o nella cartella "Startup".

3. Comandi e strumenti fondamentali per indagini forensi

Le indagini forensi partono o dovrebbero partire tutte da una copia forense del sistema, eseguita "adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione". Le distribuzioni forensi di Linux, quali ad esempio le italiane DEFT o CAINE o le straniere PALADIN o RAPTOR permettono di poter accedere a dispositivi senza alterare i dati in essi contenuti. Consigliamo quindi l'utilizzo di strumentazione di write blocking hardware oppure (o in aggiunta) l'impiego di distribuzioni live quali quelle sopra citate.

Poiché nel mock case verrà utilizzato il sistema DEFT, ne consigliamo l'utilizzo e in particolare, per eseguire copie forensi, suggeriamo le seguenti alternative:

- i tradizionali dd, dcfldd, ftkimager o cyClone, che tramite linea di comando permettono di esegure immagini di dispositivi senza alterarne il contenuto;
- il software Guymager che, da interfaccia grafica, permette l'acquisizione di dispositivi in modo agevole limitando se non eliminando la possibilità di errore;
- il software FTK imager, presente nel sistema DART accluso a DEFT, che viene in genere utilizzato su Windows in concomitanza con dispositivi di write blocking hardware (oppure software, ma consapevoli dei rischi).

Una volta eseguita una copia forense del sistema Linux, è necessario poterne visionare il contenuto. Per fare questo si possono utilizzare software quali FTK Imager che, su Windows oppure su Linux tramite emulazione mediante il software Wine, permettono di "aprire" l'immagine forense per esplorarne i file in essa contenuti e lo spazio non allocato. Alternativamente, si possono utilizzare software di mounting (vedremo nel mock case il funzionamento) atti a "montare" l'immagine su lettera di volume (in Windows) o su una directory (in Linux). Su Windows, consigliamo l'ottimo FTK Imager o il software Arsenal Image Mounter, entrambi gratuiti. Su Linux possiamo utilizzare FTK Imager tramite emulazione Wine oppure gli strumenti affuse, ewf_mount, xmount e i comandi mount integrato con losetup che permette di utilizzare file statici mostrandoli al sistema come dispositivi dinamici.

Per lo studio di ciò che è avvenuto sul sistema, essenziali e indispensabili i due strumenti tsk (The Sleuth Kit) e log2timeline, ora PLASO.

Il primo - The Sleuth Kit con la sua estensione grafica Autopsy - è ormai consolidato da anni e permette di eseguire una timeline del sistema basata sui metadati temporali del file system. Sostanzialmente, genera un diario temporale di tutte le attività di creazione, scrittura e lettura eseguite sui file presenti sul sistema. L'opzione di daily summary è vitale perché permette di ottenere un istogramma della quantità di attività rilevata sul sistema durante ogni giorno e, volendo, anche ogni ora del periodo selezionato. Spesso le attività anomale (es. copia massiva di file) vengono rilevate proprio grazie alle analisi statistiche sulla quantità di attività rilevata nel sistema.

Il secondo - log2timeline con la nuova versione PLASO - è uno strumento che permette di estendere la timeline generata tramite tsk aggiungendo al "diario" anche attività ricavate da metadati o da informazioni interne ai file, quali ad esempio dati exif, di registro, eventi di sistema, log di antivirus, journaling NTFS, storia della navigazione Internet e via dicendo. Ovviamente tale ricchezza di particolari permette un'analisi molto più approfondita, mostrando in modo quasi trasparente ciò che è avvenuto sul sistema in ogni ora o minuto in cui è stato acceso.

Ulteriore strumento che riteniamo essenziale durante le indagini su sistemi Linux (ma anche Windows e Mac) è il software Bulk extractor. Probabilmente

molti conoscono il software di analisi forense Internet Evidence Finder (IEF) rilasciato nel marzo 2009 dall'ex poliziotto canadese Jad Saliba, tramite la società Jad Software ora diventata Magnet Forensics. IEF, applicazione inizialmente gratuita che estrae svariati artefatti da un disco o immagine forense anche procedendo a livello di settore, è cresciuta nelle funzionalità e nel prezzo diventando, in alcuni contesti, inaccessibile. Forse non tutti sanno, però, che esiste un prodotto open source gratuito che, in qualche modo, si avvicina al tipo di analisi eseguite dal fratello maggiore IEF, permettendo di estrarre email, artefatti Facebook, indirizzi e domini web, numeri di telefono, carte di credito, prefetch, indirizzi IP, etc.

Bulk Extractor è un software open source e gratuito sviluppato da Simson L. Garfinkel, professore e ricercatore Californiano, autore tra l'altro delle librerie AFFLIB e di altri utili progetti relativi alla Computer Forensics. Tramite accesso sequenziale a livello di settore, BE è in grado di estrarre da dischi, immagini forensi o directory di file informazioni utili per gli investigatori, senza la necessità di dover accedere al file system sottostante.

Oltre al rilevamento delle informazioni direttamente disponibili sul disco durante la passata di parsing, BE è in grado di rilevare, decomprimere e processare ricorsivamente i dati contenuti all'interno di archivi compressi con svariati algoritmi. Avremo quindi accesso alle analisi dei contenuti dei vari file ZIP, RAR e via dicendo presenti nelle aree allocate e non allocate del sistema. Anche per questo aspetto, se non opportunamente configurati, diversi tool commerciali rischiano di trascurare informazioni rilevanti non parsificando gli archivi. Bulk Extractor è stato uno dei primi strumenti che ha percepito la necessità di operare anche all'interno degli archivi compressi, soprattutto per il fatto che diversi software (es. Microsoft Office) adottano ormai un formato di file che utilizza la struttura ZIP per salvare le informazioni al loro interno.

Le informazioni estratte nel processo di parsing vengono, man mano, riportate in singoli file di report chiamati feature files, che possono essere successivamente all'elaborazione consultati dall'investigatore o parsificati tramite script e strumenti automatici.

Per la consultazione dei feature files, l'investigatore ha a disposizione una comoda interfaccia grafica che interpreta il contenuto del report mostrandone a video i dati, in maniera non dissimile da come IEF fa con il suo visualizzatore.

Durante l'esame dei risultati, il viewer mostra anche la parte del disco nel quale gli artefatti o i dati sono stati estratti, cosa che ovviamente con un editor di testo non è fattibile se non andando a interpretare l'offset tramite programma esterno. I feature file sono, inoltre, file di testo che, quando di grosse dimensioni, possono risultare scomodi da scorrere con i normali editor.

La stessa interfaccia grafica GUI può essere utilizzata per lanciare l'esecuzione del software bulk_extractor senza doverlo fare da linea di comando, avendo quindi a disposizione le diverse possibilità d'impostazione che altrimenti andrebbero configurate tramite parametri testuali.

Oltre all'estrazione dei dati, che viene eseguita durante la prima passata sul disco o sull'immagine sorgente, avviene successivamente un'elaborazione tramite creazione di semplici istogrammi che riportano la frequenza con la quale i dati sono stati rinvenuti sul supporto. I dati vengono quindi riportati in ordine decrescente in base alla quantità di volte in cui compaiono sul disco. Questa caratteristica è molto importante e funzionale perché permette di focalizzare l'attenzione sulle informazioni che si ripetono più frequentemente sul sistema (es. indirizzi email più utilizzati, siti più visitati, etc…).

Infine, per quanto riguarda il recupero di dati cancellati su sistemi Linux, i software più utilizzati sono Photorec/Testdisk, Scalpel e Foremost.

Testdisk è il software che permette di ricostruire partizioni danneggiate, utile quindi in caso di perdita dati a causa di corruzione delle strutture del sistema. L'applicazione si utilizza da linea di comando ma, una volta lanciata, mostra un'interfaccia a caratteri graficamente non piacevole ma comunque più comoda da utilizzare dei comandi diretti.

Insieme a Testdisk è possibile scaricare Photorec, applicazione che si presenta in modo simile ma serve per recuperare file cancellati dalle aree di memoria non allocate. Il recupero avviene tramite la tecnica cosiddetta di carving, basata sulle firme dei file. In pratica, ogni file ha un suo formato codificato secondo una struttura nota (es. i file PDF cominciano tutti con "%PDF") che permette di identificare diversi formati in base appunto alla struttura. L'inizio dei file, la fine o la dimensione sono fattori che permettono di individuare file anche quando il file system non indicizza più tali file che, quindi, risulterebbero dispersi nelle aree non più allocate.

Photorec, nata inizialmente come applicazione destinata al recupero di fotografie da macchine fotografiche digitali, si è evoluta fino a raggiungere se non superare gli storici Scalpel e Foremost. Tutte e tre le applicazioni permettono di scrivere le proprie regole (o signature) per individuare nuovi file o formati sconosciuti. Scalpel e Foremost producono un output più ordinato, suddividendo i file per estensione, mentre Photorec mantiene le cartelle quando rileva che i file facevano parte della stessa directory. Photorec riesce, talvolta, a recuperare anche i nomi dei file, prelevando le informazioni da metadati dei file o del file system.

4. Mock Case

Presentiamo ora un caso di studio contenente informazioni pratiche ed esercitazioni ripetibili anche dal lettore.

4.1 Introduzione

L'obiettivo di questo capitolo è spiegare in quali aree e come individuare le tracce salienti tipiche di un'indagine post mortem svolta su un sistema Linux. Per raggiungere tale obiettivo si è scelto un approccio hands on, cioè utilizzeremo un disco virtuale creato ad hoc contenente una distribuzione Linux da analizzare[2] insieme passo per passo.

L'ambiente operativo sarà una macchina virtuale[3] Deft v.8.1[4] con una cartella di rete condivisa con la macchina reale[5].

Una volta scaricata l'immagine ed avviata la vostra macchina virtuale, siamo pronti per partire con la nostra indagine.

(2) - Potete scaricare l'immagine da questo link https://app.box.com/s/87bngkjk0c2gw0z81o89.
(3) - In questo esempio si è proceduto tramite VMWare Player, ma potete usare anche VirtualBox.
(4) - Potete avvalervi di qualsiasi altra distribuzione Linux ad uso forense (esempio: Caine, Paladin, Raptor, Sift, etc.)
(5) - Si è scelto di utilizzare una cartella di rete condivisa con la macchina reale in quanto, generalmente le macchine virtuali non sono caratterizzate da grandi volumi di memorizzazione, inoltre è anche un buon metodo per condividere i dati con altri ambienti di analisi.

4.2 Attività preliminari

Una delle regole d'oro della digital forensics è documentare (ISO 27037:2012 al punto 6.6), quindi in sede di relazione tecnica dobbiamo aver cura di annotare dati relativi a:

- data, ora e luogo di inizio e fine operazioni;
- ambiente di analisi;
- versione dei software utilizzati;
- comandi e relativi parametri utilizzati;
- etc.

Oltre ai soliti rilievi tecnici caratterizzati da foto e video delle attività svolte, può ritornare utile una memorizzazione su scala temporale delle attività svolte dalla riga di comando.

```
script -ttiming.time file.script
```

Per rivedere cosa è stato digitato possiamo eseguire il seguente comando:

```
scriptreplay timing.time -sfile.script
```

Si noti come questo script genera questi due file:

- file.script, il quale contiene la lista dei comandi digitati (anche quelli errati!);

```
deft8vm ~ % cat file.script | head
Script started on Fri 27 Jun 2014 08:17:51 PM CEST
deft8vm ~ % pwd
/root
deft8vm ~ % apt-get update
Hit http://ppa.launchpad.net quantal Release.gpg
Hit http://extras.ubuntu.com precise Release.gpg
Hit http://deb.pinguin.lu ./ Release.gpg
Hit http://dl.google.com stable Release.gpg
Hit http://it.archive.ubuntu.com precise Release.gpg
Hit http://ppa.launchpad.net quantal Release.gpg
```

- timing.time, il quale memorizza la tempistica con cui sono stati memorizzati tali comandi;

```
% cat timing.time | head
0.271054 97
```

```
1.175371 1
5.961701 1
0.175916 1
1.055893 106
0.824311 3
4.256031 36
0.400126 53
0.688793 17
0.703140 17
```

Una volta avviato il processo di logging, procederemo con il mounting della cartella di rete condivisa dove andremo a memorizzare i dati ritenuti di pertinenza con il contesto investigativo.

```
% mount -t vmhgfs .host:/ /media/
```

In tale cartella creeremo delle sottocartelle secondo la seguente struttura:

```
/media % tree
.
 └─ evidence
 └─ HD01 —> è la sigla univoca del disco da acquisire
 ├─ data —> memorizza i dati ritenuti utili ai fini d'indagine
 ├─ raw —> contiene in forensc container in formato raw
 └─ reports —> contiene i report generati in sede di analisi
5 directories, 0 files
```

4.3 Identificazione del device

Una volta pronti con l'ambiente di analisi, il primo step da affrontare è la verifica dell'effettivo disco collegato al sistema di analisi.

```
% fdisk -l
Disk /dev/sda: 128.8 GB, 128849018880 bytes
255 heads, 63 sectors/track, 15665 cylinders, total 251658240 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
```

```
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0x0006334e

Device     Boot      Start       End      Blocks     Id         System
/dev/sda1 *         2048    249561087    124779520   83         Linux
/dev/sda2       249563134    251656191     1046529     5      Extended
/dev/sda5       249563136    251656191     1046528    82 Linux swap / Solaris
Disk /dev/sdb: 8589 MB, 8589934592 bytes
255 heads, 63 sectors/track, 1044 cylinders, total 16777216 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0x0009cad6

Device     Boot   Start         End      Blocks    Id         System
/dev/sdb1     *    2048     12810239     6404096    83         Linux
/dev/sdb2       12812286    16775167     1981441     5       Extended
/dev/sdb5       13651968    16775167     1561600    83         Linux
/dev/sdb6       12812288    13651967      419840    82   Linux swap / Solaris

Partition table entries are not in disk order
```

In alternativa avremmo potuto utilizzare il seguente comando:

```
% sfdisk -l -uS /dev/sdb
Disk /dev/sdb: 1044 cylinders, 255 heads, 63 sectors/track
Warning: extended partition does not start at a cylinder
boundary.
DOS and Linux will interpret the contents differently.
Units = sectors of 512 bytes, counting from 0

Device     Boot   Start         End    #sectors    Id         System
/dev/sdb1     *    2048     12810239    12808192    83         Linux
/dev/sdb2       12812286    16775167     3962882     5       Extended
/dev/sdb3              0           -           0     0         Empty
```

```
/dev/sdb4                      -          0      0          Empty
/dev/sdb5      13651968   16775167    3123200    83          Linux
/dev/sdb6      12812288   13651967     839680    82  Linux swap / Solaris
```

Il dispositivo d'interesse per l'indagine dovrebbe essere il dispositivo fisico /dev/sdb. Per avere conferma di ciò possiamo verificare accertando che non compare nella lista dei file system montati tramite il comando *mount*.

```
% mount
/dev/sda1 on / type ext4 (rw,errors=remount-ro)
proc on /proc type proc (rw,noexec,nosuid,nodev)
sysfs on /sys type sysfs (rw,noexec,nosuid,nodev)
none on /sys/fs/fuse/connections type fusectl (rw)
none on /sys/kernel/debug type debugfs (rw)
none on /sys/kernel/security type securityfs (rw)
udev on /dev type devtmpfs (rw,mode=0755)
devpts on /dev/pts type devpts (rw,noexec,nosuid,gid=5,mode=0620)
tmpfs on /run type tmpfs (rw,noexec,nosuid,size=10%,mode=0755)
none on /run/lock type tmpfs (rw,noexec,nosuid,nodev,size=5242880)
none on /run/shm type tmpfs (rw,nosuid,nodev)
none on /run/user type tmpfs (rw,noexec,nosuid,nodev,size=104857600,mode=0755)
binfmt_misc on /proc/sys/fs/binfmt_misc type binfmt_misc
(rw,noexec,nosuid,nodev)
vmware-vmblock on /run/vmblock-fuse type fuse.vmware-vmblock
(rw,nosuid,nodev,default_permissions,allow_other)
gvfsd-fuse on /run/user/root/gvfs type fuse.gvfsd-fuse (rw,nosuid,nodev)
```

Una volta appurato che il dispositivo fisico (nel nostro caso è "virtuale") non è connesso al sistema di analisi, procediamo con il ricavare informazioni relative sia all'hardware messo a disposizione per l'indagine, che la rispettiva integrità del contenuto informativo.

```
% hdparm -I /dev/sdb
/dev/sdb:
SG_IO: bad/missing sense data, sb[]: 70 00 05 00 00 00 00
0a 00 00 00 00 20 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00
```

```
ATA device, with non-removable media
  Model Number:         ..'@*n
  Serial Number:
  Firmware Revision:        PP
  Media Manufacturer:      @;&
Standards:
  Likely used:               4
Configuration:
  Logical       max              current
  cylinders       0                34816
  heads           0                65535
  sectors/track  34816             20560
  —
  bytes/track: 29648          bytes/sector: 14093
  CHS current addressable sectors:    4294934809
  Logical/Physical Sector size:       512 bytes
  device size with M = 1024*1024:     2097136 MBytes
  device size with M = 1000*1000:     2199006 MBytes (2199 GB)
  cache/buffer size = unknown
  Nominal Media Rotation Rate: 33049
Capabilities:
  IORDY(may be)(cannot be disabled)
  Buffer size: 5418.5kB  bytes avail on r/w long: 34816
  Standby timer values: spec'd by Vendor
  R/W multiple sector transfer: Max = 0  Current = 255
  DMA: not supported
  PIO: unknown
  Removable Media Status Notification feature set supported
Security:
  Master password revision code = 256
  not        supported
  not        enabled
  not        locked
```

```
  not         frozen
  not        expired: security count
  not        supported: enhanced erase
```

Si noti che su dispositivi virtuali il risultato della dimensione del device non è attendibile.

```
% md5sum /dev/sdb | tee /media/evidence/HD01/reports/sdb-md5.txt
119d8a142ad01524c8b3856b05f7e35f /dev/sdb
% cat /media/evidence/HD01/reports/sdb-md5.txt
119d8a142ad01524c8b3856b05f7e35f /dev/sdb
% sha1sum /dev/sdb | tee /media/evidence/HD01/reports/sdb-sha1.txt
f31db1a5605175c71122903d6f23c7d0bbdaa420 /dev/sdb
% cat /media/evidence/HD01/reports/sdb-sha1.txt
f31db1a5605175c71122903d6f23c7d0bbdaa420 /dev/sdb
```

4.4 Acquisizione e preservazione

Per realizzare tali attività sulla base delle raccomandazioni dall' ISO 27037:2012 ai punti 7.1.3.5 e 7.1.4 si è scelto di acquisire il contenuto informativo in un forensic container di tipo raw suddiviso in blocchi (split) da 4GB. L'integrità del rispettivo contenuto informativo viene garantita mediante due codici hash generati con gli algoritmi MD5 e SHA1.

```
/media/evidence/HD01/raw % dcfldd if=/dev/sdb
hash=md5,sha1 hashwindow=4G md5log=sdb-md5-2.txt
sha1log=sdb-sha1-2.txt hashconv=after bs=512 conv=noer-
ror,sync split=4G splitformat=nnn of=sdb.dd
16777216 blocks (8192Mb) written.
16777216+0 records in
16777216+0 records out
/media/evidence/HD01/raw % ls
sdb.dd.aa sdb.dd.ab sdb-md5-2.txt sdb-sha1-2.txt
/media/evidence/HD01/raw % cat sdb-md5-2.txt
0 - 4294967296: bdafc34eca0023b4f212cdb2bf02edd2
4294967296 - 8589934592: 1fba9e61d8a21fe02d5ef1b2e741585d
Total (md5): 119d8a142ad01524c8b3856b05f7e35f
```

```
/media/evidence/HD01/raw % cat sdb-sha1-2.txt
0 - 4294967296: 186cede87d585afaa5ba55916108cd4f6467c379
4294967296 - 8589934592:
c6ab54cf4f00824544d7b1c74114d7386de58372
Total (sha1): f31db1a5605175c71122903d6f23c7d0bbdaa420
```

L'opzione "splitformat=nnn" comporta la creazione di diversi split con estensione "000", "001", "002" e così via. Alternativamente, è possibile utilizzare anche "splitformat=aa" che impone invece l'utilizzo di caratteri "aa", "ab", "ac" e così via. Da tenere a mente che - come vedremo successivamente - lo strumento "affuse" supporta soltanto estensioni "000", "001", "002"… mentre lo strumento xmount supporta entrambe le estensioni. Questi strumenti saranno necessari per poter accedere all'immagine forense mostrando un'immagine compatta e non divisa in frammenti.

4.5 Informazioni su partizioni e file system presenti

L'operazione c.d. di *splitting* del *forensic container* risulta comoda per la portatilità dei suoi componenti su *file system* diversi tra loro, di converso però ha degli effetti collaterali per quanto concerne l'attività di *mounting*.

Per risolvere questo problema abbiamo tre opzioni:

1) concateniamo tutti i blocchi mediante il comando cat:

```
/media/evidence/HD01/raw % cat sdb.dd.0* > sdb.dd
/media/evidence/HD01/raw % chmod 444 *.*
/media/evidence/HD01/raw % ls -l
total 16777216
-r--r--r-- 1 501 dialout 8589934592 Jun 29 09:51 sdb.dd
-r--r--r-- 1 501 dialout 4294967296 Jun 29 08:55 sdb.dd.000
-r--r--r-- 1 501 dialout 4294967296 Jun 29 08:55 sdb.dd.001
```

2) emuliamo un unico file attraverso *affuse* (utilizzabile con formato "001", "002", "003", etc…):

```
/media/evidence/HD01/raw % affuse sdb.dd.000 /mnt/raw/
/media/evidence/HD01/raw % ls -l /mnt/raw/
total 0
-r--r--r-- 1 root root 8589934592 Jan 1 1970 sdb.dd.000.raw
```

Si noti che come parametro è stato inserito il primo frammento.

3) utilizziamo il tool xmount (utilizzabile con entrambi i formati, numerici e con caratteri):

```
/media/evidence/HD01/raw % xmount —in dd —out dd sdb.dd.0* /mnt/raw
/media/evidence/HD01/raw % ls -l /mnt/raw/
total 0
-r—r—r— 1 root root 8589934592 Jan  1  1970   sdb.dd.dd
-r—r—r— 1 root root         71 Jan  1  1970  sdb.dd.info
```

Si noti che in questo caso, per indicare il parametro, sono state utilizzate le wildcards "*" (che sostituisce qualsiasi numero di caratteri/numeri) e "?"(che sostituisce un solo carattere/numero): avremmo quindi potuto mettere in modo equivalente "sdb.dd.0*" oppure "sdb.dd.0??".

Utilizziamo ora alcuni comandi delle suite SleuthKit per analizzare la morfologia interna del *forensic container*.

4.6 Informazioni sulla tipologia del forensic container

Verifichiamo il tipo di contenitore nel quale è stata salvata la copia forense tramite il comando img_stat:

```
% img_stat sdb.dd
IMAGE FILE INFORMATION
--------------------------------------------

Image Type: raw
Size in bytes: 8589934592
```

4.7 Informazioni sulle partizioni

Otteniamo informazioni sulle partizioni del device tramite un apposito comando fornito dalla suite Sleuthkit.

```
% mmls -M sdb.dd
DOS Partition Table
Offset Sector: 0
Units are in 512-byte sectors
```

```
   Slot      Start         End         Length    Description
01: ---    0000000000  0000002047  0000002048  Unallocated
02: 00:00  0000002048  0012810239  0012808192  Linux (0x83)
03: ---    0012810240  0012812287  0000002048  Unallocated
08: 02:00 0       012812288  0013651967  0000839680  Linux
Swap / Solaris x86 (0x82)
09: 01:00  0013651968  0016775167  0003123200  Linux (0x83)
10: ---    0016775168  0016777215  0000002048  Unallocated
```

Si noti come è possibile ottenere lo stesso risultato con il comando nativo sfdisk illustrato al precedente par. 6.3

4.8 Informazioni sul file system

Per ogni partizione di interesse, possiamo approfondire la tipologia di file system con la quale è stata creata. Come si evince dall'attività precedente, all'interno del forensic container sono definite tre partizioni identificate dai numeri 02, 08 e 09. Andiamo ora a verificare i dettagli dei file system presenti in tali aree, escludendo per questa esercitazione l'area di swap.

```
% fsstat -o 2048 sdb.dd
FILE SYSTEM INFORMATION
--------------------------------------------
File System Type: Ext4
Volume Name:
Volume ID: c9461d489008dbb4f74ab71b2fa44e18
Last Written at: 2014-01-22 15:24:24 (CET)
Last Checked at: 2014-01-21 09:35:25 (CET)
Last Mounted at: 2014-01-22 15:24:24 (CET)
Unmounted properly
Last mounted on: /
Source OS: Linux
Dynamic Structure
Compat Features: Journal, Ext Attributes, Resize Inode, Dir Index
InCompat Features: Filetype, Extents, Flexible Block Groups,
Read Only Compat Features: Sparse Super, Large File, Huge File, Extra Inode Size
```

```
Journal ID: 00
Journal Inode: 8
METADATA INFORMATION
————————————————————

Inode Range: 1 - 400625
Root Directory: 2
Free Inodes: 234502
Inode Size: 256
CONTENT INFORMATION
————————————————————

Block Groups Per Flex Group: 16
Block Range: 0 - 1601023
Block Size: 4096
Free Blocks: 528766
BLOCK GROUP INFORMATION
————————————————————

Number of Block Groups: 49
Inodes per group: 8176
Blocks per group: 32768

Group: 0:
 Block Group Flags: [INODE_ZEROED]
 Inode Range: 1 - 8176
 Block Range: 0 - 32767
 Layout:
  Super Block: 0 - 0
  Group Descriptor Table: 1 - 1
  Group Descriptor Growth Blocks: 2 - 391
  Data bitmap: 392 - 392
  Inode bitmap: 408 - 408
  Inode Table: 424 - 934
  Data Blocks: 8600 - 32767
 Free Inodes: 3 (0%)
```

```
 Free Blocks: 19799 (60%)
 Total Directories: 1084
 Stored Checksum: 0x8998

Group: 1:
<snip>
% fsstat -o 13651968 sdb.dd
FILE SYSTEM INFORMATION
--------------------------
File System Type: Ext4
Volume Name:
Volume ID: 3acd86331a12b2b1844048df905cdfcd
Last Written at: 2014-01-22 15:54:08 (CET)
Last Checked at: 2014-01-21 09:35:26 (CET)
Last Mounted at: 2014-01-22 15:24:24 (CET)
Unmounted properly
Last mounted on: /home
Source OS: Linux
Dynamic Structure
Compat Features: Journal, Ext Attributes, Resize Inode,
Dir Index
InCompat Features: Filetype, Extents, Flexible Block
Groups,
Read Only Compat Features: Sparse Super, Large File, Huge
File, Extra Inode Size
Journal ID: 00
Journal Inode: 8
METADATA INFORMATION
--------------------------
Inode Range: 1 - 97729
Root Directory: 2
Free Inodes: 96036
Inode Size: 256
```

```
CONTENT INFORMATION
--------------------------
Block Groups Per Flex Group: 16
Block Range: 0 - 390399
Block Size: 4096
Free Blocks: 321452
BLOCK GROUP INFORMATION
--------------------------
Number of Block Groups: 12
Inodes per group: 8144
Blocks per group: 32768

Group: 0:
 Block Group Flags: [INODE_ZEROED]
 Inode Range: 1 - 8144
 Block Range: 0 - 32767
 Layout:
  Super Block: 0 - 0
  Group Descriptor Table: 1 - 1
  Group Descriptor Growth Blocks: 2 - 96
  Data bitmap: 97 - 97
  Inode bitmap: 113 - 113
  Inode Table: 129 - 637
  Uninit Data Bitmaps: 109 - 112
  Uninit Inode Bitmaps: 125 - 128
  Uninit Inode Table: 6237 - 8272
  Data Blocks: 8273 - 32767
 Free Inodes: 6452 (79%)
 Free Blocks: 25981 (79%)
 Total Directories: 548
 Stored Checksum: 0xE925

Group: 1:
```

Si faccia presente che il gruppo data - orario potrebbe essere oggetto di attività di anti forensics da parte di un utente esperto, pertanto esso dovrà essere opportunamente contestualizzato da parte dell'analista con altri elementi temporali che caratterizzano il dispositivo oggetto di analisi

4.9 Mounting

Una volta ottenuti i dettagli tecnici siamo pronti per realizzare il mount delle due partizioni identificate nell'attività precedente. A tal proposito si noti come la partizione 02 è da intendersi come quella principale (Last mounted on: /), mentre la 09 contiene l'area dati degli utenti (Last mounted on: /home). Per tale motivo procederemo nell'attività di mounting nel seguente ordine:

```
/media/evidence/HD01/raw % mount -o ro,loop,offset=$((2048*512)) sdb.dd /mnt/HD01/
/mnt/HD01 % ls
bin  etc         lib           mnt    root  selinux  tmp vmlinuz
boot home        lost+found    opt     run   srv      usr
dev  initrd.img media         proc   sbin   sys      var
/mnt/HD01 % ls -lath home/
total 8.0K
drwxr-xr-x 23 root root 4.0K Jan 21 10:17 ..
drwxr-xr-x 2 root root 4.0K Jan 21 09:35 .
/media/evidence/HD01/raw % mount -o ro,loop,offset=$((13651968*512))
sdb.dd /mnt/HD01/home/
/mnt/HD01 % ls -lath home/
total 52K
drwxr-xr-x   23  1001   1001  4.0K  Jan  22  15:51  mirco
drwxr-xr-x   23  1002   1002  4.0K  Jan  22  14:58  alessandro
drwxr-xr-x   24  1000   1000  4.0K  Jan  22  14:57  mario
drwxr-xr-x   19  1003   1003  4.0K  Jan  22  14:08  mauro
drwxr-xr-x   10  root   root  4.0K  Jan  21  11:29 .
drwxr-xr-x    2  1006   1006  4.0K  Jan  21  11:29  andrea
drwxr-xr-x    2  1005   1005  4.0K  Jan  21  11:19  guest
drwxr-xr-x    2  1004   1004  4.0K  Jan  21  11:18  luca
```

```
drwxr-xr-x   23  root   root  4.0K  Jan  21  10:17 ..
drwx——       2   root   root   16K  Jan  21  09:35  lost+found
```

Un'altra soluzione per il mouting è il comando losetup, che crea dei device "virtuali", i quali corrispondono a posizioni specifiche all'interno dell'immagine.

```
losetup /dev/loop0 -o 6989807616 sdb.dd
```

4.10 Informazioni relative al sistema operativo

Vediamo ora quali informazioni possiamo reperire sul Sistema Operativo installato sul disco di cui abbiamo eseguito copia forense.

4.10.1 Tipo e versione del Sistema Operativo

Vediamo quale tipo di Sistema Operativo è installato sul disco e la relativa versione.

```
% ls etc/*-release
etc/os-release
% cat etc/os-release
PRETTY_NAME="Debian GNU/Linux 7 (wheezy)"
NAME="Debian GNU/Linux"
VERSION_ID="7"
VERSION="7 (wheezy)"
ID=debian
ANSI_COLOR="1;31"
HOME_URL="http://www.debian.org/"
SUPPORT_URL="http://www.debian.org/support/"
BUG_REPORT_URL="http://bugs.debian.org/"
```

In alternativa analizziamo il boot loader.

```
% cat boot/grub/grub.cfg | grep linux
### BEGIN /etc/grub.d/10_linux ###
menuentry 'Debian GNU/Linux, con Linux 3.2.0-4-486' —class
debian —class gnu-linux —class gnu —class os {
linux   /boot/vmlinuz-3.2.0-4-486 root=UUID=184ea42f-1bb7-
4af7-b4db-0890481d46c9 ro quiet
```

```
menuentry 'Debian GNU/Linux, con Linux 3.2.0-4-486 (modalità ripri-
stino)' –class debian –class gnu-linux –class gnu –class os {
linux   /boot/vmlinuz-3.2.0-4-486 root=UUID=184ea42f-1bb7-
4af7-b4db-0890481d46c9 ro single
### END /etc/grub.d/10_linux ###
### BEGIN /etc/grub.d/20_linux_xen ###
### END /etc/grub.d/20_linux_xen ###
```

Oppure ci serviamo dei file "issue" e "issue.net" che contengono le informazioni con le quali il sistema si presenta all'utente e in rete.

```
% cat etc/issue
Debian GNU/Linux 7 \n \l
% cat etc/issue.net
Debian GNU/Linux 7
```

4.10.2 Versione del Kernel

La versione del Kernel l'abbiamo ricavata involontarmente al punto precedente quando abbiamo consultato il GRUB, ossia è la v.3.2.0-4-486.

Un'alternativa è

```
/mnt % ls boot/vmlinuz-*
boot/vmlinuz-3.2.0-4-486
```

altrimenti nei log di sistema

```
% cat var/log/syslog | grep -i "linux version"
Jan 22 13:00:04 Server1 kernel: [  0.000000] Linux version
3.2.0-4-486 (debian-kernel@lists.debian.org) (gcc version
4.6.3 (Debian 4.6.3-14) ) #1 Debian 3.2.51-1
Jan 22 15:24:25 Server1 kernel: [  0.000000] Linux version
3.2.0-4-486 (debian-kernel@lists.debian.org) (gcc version
4.6.3 (Debian 4.6.3-14) ) #1 Debian 3.2.51-1
```

che sono gli stessi che vengono consultati da dmesg su una macchina live

```
% dmesg | grep -i "linux version"
[   0.000000] Linux version 3.5.0-30-generic (buildd@pan-
long) (gcc version 4.7.2 (Ubuntu/Linaro 4.7.2-2ubuntu1) )
```

```
#51-Ubuntu SMP Tue May 14 18:47:48 UTC 2013 (Ubuntu 3.5.0-
30.51-generic 3.5.7.9)
% dmesg | grep -i "command line"
[  0.000000] Command line: BOOT_IMAGE=/boot/vmlinuz-3.5.0-
30-generic  root=UUID=69bd4ffc-58de-411a-9b0f-d192923321d7
ro quiet splash
[  0.000000] Kernel command line: BOOT_IMAGE=/boot/vmli-
nuz-3.5.0-30-generic  root=UUID=69bd4ffc-58de-411a-9b0f-
d192923321d7 ro quiet splash
```

sempre in un contesto live si può usare il comando uname

```
% uname -a
Linux deft8vm 3.5.0-30-generic #51-Ubuntu SMP Tue May 14
18:47:48 UTC 2013 x86_64 x86_64 x86_64 GNU/Linux
```

Dato che ci possono essere più moduli kernel, per conoscere quale è quello che parte di default, dobbiamo leggere sempre il GRUB cercando le voci menuentry

```
% cat /boot/grub/grub.cfg | grep -i "set default"
set default="0" –> il primo menuentry
/mnt % cat boot/grub/grub.cfg | grep -in "^menuentry"
71:menuentry 'Debian GNU/Linux, con Linux 3.2.0-4-486' –
class debian –class gnu-linux –class gnu –class os {
83:menuentry 'Debian GNU/Linux, con Linux 3.2.0-4-486
(modalità ripristino)' –class debian –class gnu-linux –
class gnu –class os {
```

4.10.3 Impostazione del fuso orario

Quello della macchina usata per l'analisi è

```
% date
Sun Jun 29 10:33:25 CEST 2014
```

mentre quello della macchina oggetto di analisi e montata in /mnt è

```
/mnt/HD01 % zdump etc/localtime
etc/localtime Sun Jun 29 08:34:48 2014 etc
```

oppure per sapere quello scelto in sede di installazione

```
% find * -type f -exec sh -c "diff -q /etc/localtime '{}'
> /dev/null && echo {}" \;
posix/Europe/San_Marino
```

In alternativa possiamo lavorare sfruttando i codici hash

```
/mnt/HD01 % md5sum etc/localtime
9828f4466350e4529d97c04e85554430 etc/localtime
/mnt % find usr/share/zoneinfo/ -type f -exec md5sum '{}'
\+ | grep 9828f4466350e4529d97c04e85554430
9 8 2 8 f 4 4 6 6 3 5 0 e 4 5 2 9 d 9 7 c 0 4 e 8 5 5 5 4 4 3 0
usr/share/zoneinfo/posix/Europe/San_Marino
```

Possiamo riassumere tutto in unico comando

```
/mnt/HD01 % find usr/share/zoneinfo/ -type f -exec md5sum
'{}' \+ | grep $(md5sum etc/localtime | awk '{print $1}')
9 8 2 8 f 4 4 6 6 3 5 0 e 4 5 2 9 d 9 7 c 0 4 e 8 5 5 5 4 4 3 0
usr/share/zoneinfo/posix/Europe/San_Marino
```

4.10.4 Data di installazione

Per ricavare la data di installazione del sistema operativo dobbiamo consultare la data di creazione del file system di root, cioè il mount point "/".

```
% cat etc/fstab
# /etc/fstab: static file system information.
#
# Use 'blkid' to print the universally unique identifier for a
# device; this may be used with UUID= as a more robust way to name devices
# that works even if disks are added and removed. See fstab(5).
#
# <file system> <mount point>  <type> <options>    <dump> <pass>
# / was on /dev/sda1 during installation
UUID=184ea42f-1bb7-4af7-b4db-0890481d46c9 /       ext4  errors=remount-ro 0    1
# /home was on /dev/sda5 during installation
UUID=cddf5c90-df48-4084-b1b2-121a3386cd3a /home     ext4  defaults    0    2
```

```
# swap was on /dev/sda6 during installation
UUID=02209d20-f362-4095-bbdb-9b8b5ca9ab23 none      swap  sw      0    0
/dev/sr0    /media/cdrom0  udf,iso9660 user,noauto   0    0
```

Ricaviamo ora gli UUID dei file system montati sulla macchina reale.

```
/mnt % blkid
/dev/sda1: UUID="69bd4ffc-58de-411a-9b0f-d192923321d7" TYPE="ext4"
/dev/loop0: UUID="184ea42f-1bb7-4af7-b4db-0890481d46c9" TYPE="ext4"
/dev/loop1: UUID="cddf5c90-df48-4084-b1b2-121a3386cd3a" TYPE="ext4"
/dev/sda5: UUID="c948e457-851a-4b29-80fa-fe11136b067a" TYPE="swap"
/dev/sdb1: UUID="184ea42f-1bb7-4af7-b4db-0890481d46c9" TYPE="ext4"
/dev/sdb5: UUID="cddf5c90-df48-4084-b1b2-121a3386cd3a" TYPE="ext4"
/dev/sdb6: UUID="02209d20-f362-4095-bbdb-9b8b5ca9ab23" TYPE="swap"
```

un'alternativa a blkid è il seguente modo

```
ls /dev/disk/by-uuid/
02209d20-f362-4095-bbdb-9b8b5ca9ab23   c948e457-851a-4b29-
80fa-fe11136b067a
184ea42f-1bb7-4af7-b4db-0890481d46c9   cddf5c90-df48-4084-
b1b2-121a3386cd3a
69bd4ffc-58de-411a-9b0f-d192923321d7
```

Una volta ricavato l'UUID lo diamo in pasto a dumpe2fs

```
% dumpe2fs /dev/disk/by-uuid/184ea42f-1bb7-4af7-b4db-
0890481d46c9 | grep -i "file system created"
dumpe2fs 1.42.5 (29-Jul-2012)
File system created:      Tue Jan 21 09:35:25 2014
```

Quindi il giorno 21 gennaio 2014 alle ore 09:35:25.

In un sistema live, se già conosciamo con certezza qual'è la partizione d'interesse, possiamo usare il comando tune2fs con il parametro -l

```
/mnt % tune2fs -l /dev/sdb1
tune2fs 1.42.5 (29-Jul-2012)
File system volume name:  <none>
Last mounted on:             /
File system UUID:         184ea42f-1bb7-4af7-b4db-0890481d46c9
File system magic number:  0xEF53
```

```
File system revision #:  1 (dynamic)
File system features:   has_journal ext_attr resize_inode
dir_index filetype extent flex_bg sparse_super large_file
huge_file uninit_bg dir_nlink extra_isize
File system flags:              signed_directory_hash
Default mount options:          user_xattr acl
File system state:                   clean
Errors behavior:                  Continue
File system OS type:                 Linux
Inode count:                        400624
Block count:                       1601024
Reserved block count:                80051
Free blocks:                        528766
Free inodes:                        234502
First block:                             0
Block size:                           4096
Fragment size:                        4096
Reserved GDT blocks:                   390
Blocks per group:                    32768
Fragments per group:                 32768
Inodes per group:                     8176
Inode blocks per group:                511
Flex block group size:                  16
File system created:            Tue Jan 21 09:35:25 2014
Last mount time:                Wed Jan 22 15:24:24 2014
Last write time:                Wed Jan 22 15:24:24 2014
Mount count:                             9
Maximum mount count:                    -1
Last checked:                   Tue Jan 21 09:35:25 2014
Check interval:                 0 (<none>)
Lifetime writes:                   8031 MB
Reserved blocks uid:            0 (user root)
Reserved blocks gid:            0 (group root)
```

```
First inode:          11
Inode size:          256
Required extra isize: 28
Desired extra isize:  28
Journal inode:        8
Default directory hash:  half_md4
Directory Hash Seed:  50ea6610-846c-447c-b97c-2975411fabc9
Journal backup:     inode blocks
```

In un sistema Debian, un'altra fonte è il percorso /var/log/installer

```
% ls -ial var/log/installer/
total 1400
261645 drwxr-xr-x 3 root root  4096 Jan 21 10:17 .
261781 drwxr-xr-x 15 root root  4096 Jan 22 15:54 ..
261647 drwxr-xr-x 2 root root  4096 Jan 21 10:17 cdebconf
261651 -rw-r--r-- 1 root root 14294 Jan 21 10:17 hardware-summary
261653 -rw-r--r-- 1 root root  161 Jan 21 10:17 lsb-release
261649 -rw------- 1 root root 424211 Jan 21 10:17 partman
261652 -rw-r--r-- 1 root root 69140 Jan 21 10:17 status
261650 -rw------- 1 root root 865400 Jan 21 10:17 syslog
261648 -rw------- 1 root root 36392 Jan 21 10:17 Xorg.0.log
% ls -ial etc/ssh/ssh_host*
215614 -rw-------  1 root root 668 Jan 21 10:02 etc/ssh/ssh_host_dsa_key
215615 -rw-r--r-- 1 root root 602 Jan 21 10:02 etc/ssh/ssh_host_dsa_key.pub
215616 -rw------- 1 root root 227 Jan 21 10:02 etc/ssh/ssh_host_ecdsa_key
215617 -rw-r--r-- 1 root root 174 Jan 21 10:02 etc/ssh/ssh_host_ecdsa_key.pub
215612 -rw------- 1 root root 1679 Jan 21 10:02 etc/ssh/ssh_host_rsa_key
215613 -rw-r--r-- 1 root root 394 Jan 21 10:02 etc/ssh/ssh_host_rsa_key.pub
```

4.10.5 Date di accensione e spegnimento della macchina

Ricerchiamo le date in cui la macchina è stata accesa e spenta, in maniera "pulita" ovviamente, cioè senza distacco di corrente ma tramite procedura di "shutdown".

```
% who -b     var/log/wtmp
             system boot 2014-01-21 10:17
             system boot 2014-01-21 10:33
             system boot 2014-01-21 11:11
             system boot 2014-01-21 11:14
             system boot 2014-01-21 18:25
             system boot 2014-01-22 10:05
             system boot 2014-01-22 13:00
             system boot 2014-01-22 15:24
```

oppure

```
% last reboot -f var/log/wtmp
reboot  system boot 3.2.0-4-486   Wed Jan 22 15:24 - 15:53 (00:29)
reboot  system boot 3.2.0-4-486   Wed Jan 22 13:00 - 15:13 (02:13)
reboot  system boot 3.2.0-4-486   Wed Jan 22 10:05 - 12:42 (02:37)
reboot  system boot 3.2.0-4-486   Tue Jan 21 18:25 - 12:42 (18:16)
reboot  system boot 3.2.0-4-486   Tue Jan 21 11:14 - 12:38 (01:23)
reboot  system boot 3.2.0-4-486   Tue Jan 21 11:11 - 11:14 (00:03)
reboot  system boot 3.2.0-4-486   Tue Jan 21 10:33 - 11:10 (00:37)
reboot  system boot 3.2.0-4-486   Tue Jan 21 10:17 - 10:22 (00:04)
```

Se vogliamo un quadro completo consultiamo i messaggi di sistema tramite un'espressione regolare

```
/mnt/HD01 % cat var/log/messages | grep 'shutting\|started'
Jan 21 10:17:55 Server1 kernel: imklog 5.8.11, log source = /proc/kmsg started.
Jan 21 10:22:20 Server1 shutdown[3595]: shutting down for system halt
Jan 21 10:33:14 Server1 kernel: imklog 5.8.11, log source = /proc/kmsg started.
Jan 21 11:10:54 Server1 shutdown[4392]: shutting down for system reboot
Jan 21 11:11:11 Server1 kernel: imklog 5.8.11, log source = /proc/kmsg started.
Jan 21 11:14:14 Server1 shutdown[4393]: shutting down for system reboot
Jan 21 11:14:35 Server1 kernel: imklog 5.8.11, log source = /proc/kmsg started.
Jan 21 12:38:25 Server1 shutdown[5164]: shutting down for system halt
Jan 21 18:25:47 Server1 kernel: imklog 5.8.11, log source = /proc/kmsg started.
Jan 22 10:05:10 Server1 kernel: imklog 5.8.11, log source = /proc/kmsg started.
Jan 22 12:42:19 Server1 shutdown[4709]: shutting down for system halt
```

```
Jan 22 13:00:04 Server1 kernel: imklog 5.8.11, log source = /proc/kmsg started.
Jan 22 15:13:25 Server1 shutdown[6556]: shutting down for system halt
Jan 22 15:24:25 Server1 kernel: imklog 5.8.11, log source = /proc/kmsg started.
Jan 22 15:53:59 Server1 shutdown[3809]: shutting down for system halt
```

4.11 Impostazioni di rete

Verifichiamo quali impostazioni di rete sono configurate sulla macchina della quale è stata eseguita copia forense.

4.11.1 Hostname

Il nome della macchina si ottiene osservando il contenuto del file "/etc/hostname".

```
/mnt/HD01 % cat etc/hostname
Server1
```

4.11.2 Configurazione delle interfacce di rete

Verifichiamo come sono state configurate le interfacce di rete installate sulla macchina.

```
% cat etc/network/interfaces
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).
# The loopback network interface
auto lo
iface lo inet loopback
% cat var/log/daemon.log | grep NetworkManager | less
...
Jan 21 10:17:55 Server1 NetworkManager[2257]: <info>  address 10.0.2.15
Jan 21 10:17:55 Server1 NetworkManager[2257]: <info>  prefix 24 (255.255.255.0)
Jan 21 10:17:55 Server1 NetworkManager[2257]: <info>  gateway 10.0.2.2
Jan 21 10:17:55 Server1 NetworkManager[2257]: <info>  nameserver '155.185.1.2'
```

```
Jan 21 10:17:55 Server1 NetworkManager[2257]: <info>  nameserver '155.185.1.5'
Jan 21 10:17:55 Server1 NetworkManager[2257]: <info>  domain name 'ing.unimo.it'
Jan 21 10:17:55 Server1 NetworkManager[2257]: <info> Activation (eth0) Stage 5 o:
...
```

4.11.3 Ultimi lease DHCP

Verifichiamo quali sono gli ultimi indirizzi DHCP acquisiti dalla macchina dal server DHCP eventualmente presente nella sua rete.

```
/mnt % cat var/lib/dhcp/dhclient*
lease {
 interface "eth0";
 fixed-address 10.0.2.15;
 filename "forensics.pxe";
 option subnet-mask 255.255.255.0;
 option routers 10.0.2.2;
 option dhcp-lease-time 86400;
 option dhcp-message-type 5;
 option domain-name-servers 155.185.1.2,155.185.1.5;
 option dhcp-server-identifier 10.0.2.2;
 option domain-name "ing.unimo.it";
 renew 3 2014/01/22 22:44:51;
 rebind 4 2014/01/23 09:00:04;
 expire 4 2014/01/23 12:00:04;
}
lease {
 interface "eth0";
 fixed-address 10.0.2.15;
 filename "forensics.pxe";
 option subnet-mask 255.255.255.0;
 option dhcp-lease-time 86400;
 option routers 10.0.2.2;
 option dhcp-message-type 5;
```

```
 option dhcp-server-identifier 10.0.2.2;
 option domain-name-servers 155.185.1.2,155.185.1.5;
 option domain-name "ing.unimo.it";
 renew 3 2014/01/22 23:43:04;
 rebind 4 2014/01/23 11:24:25;
 expire 4 2014/01/23 14:24:25;
}
```

4.11.4 Assegnazioni statiche

Se sul sistema sono state inserite assegnazioni statiche di indirizzi IP e nomi DNS, saranno visionabili nel file "/etc/hosts".

```
% cat etc/hosts
127.0.0.1  localhost
127.0.1.1  Server1
# The following lines are desirable for IPv6 capable hosts
::1   localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

4.12 Informazioni su utenti e gruppi

Come già visto nella parte teorica, nei sistemi Linux gli account e le password di accesso sono memorizzati nella cartella /etc. Vediamo in particolare in quali locazioni e con quale notazione.

4.12.1 Utenti

Gli account degli utenti si trovano in /etc/passwd.

```
% cat etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
[...]
```

```
Debian-gdm:x:114:122:Gnome Display Manager:/var/lib/gdm3:/bin/false
mario:x:1000:1000:Mario Rossi,,,:/home/mario:/bin/bash
vboxadd:x:999:1::/var/run/vboxadd:/bin/false
mirco:x:1001:1001:Mirco Marchetti,,,:/home/mirco:/bin/bash
alessandro:x:1002:1002:Alessandro Guido,,,:/home/alessandro:/bin/bash
mauro:x:1003:1003:Mauro Andreolini,,,:/home/mauro:/bin/bash
luca:x:1004:1004:Luca Ferretti,,,:/home/luca:/bin/bash
guest:x:1005:1005:Utente Ospite,,,:/home/guest:/bin/bash
andrea:x:1006:1006:Andrea Balboni,,,:/home/andrea:/bin/bash
```

Vediamo come interpretare una stringa generica

```
mauro:x:1003:1003:Mauro Andreolini,,,:/home/mauro:/bin/bash
```

1. Nome utente, utilizzato per il login —> mauro;

2. UID, identificativo numerico dell'account utente —> 1003;

3. GID, identificativo numerico del gruppo principale dell'utente —> 1003;

4. Informazioni addizionali, quali nome completo, ma anche altre informazioni di contatto separate da virgola (Chiamto GECOS) —> Mauro Andreolini;

5. Directory home, quando un utente effettua il login —> /home/mauro

6. Default shell, path dell'eseguibile del processo da avviare dopo aver eseguito il login —> /bin/bash

Le password sono memorizzate in forma di hash nel file /etc/shadow

```
% cat etc/shadow
root:$6$F07aG0cy$xOR.bkHAYrIlxNxHhJY89/Ryma3zb4XixCRKWiVXhJDf1U
3n2BQeUTQEEhN.M8qBr3ZdXmFWZkAMUwr6yYNYY1:16091:0:99999:7:::
daemon:*:16091:0:99999:7:::
[...]
Debian-gdm:*:16091:0:99999:7:::
mario:$6$ZxH.0pY2$I0GNJ6L9HBLF45kUYbnK9HqvWpxBDAMevuLLZAlyhFl3f
Vp/mkpeiiE6/l2tzQHoZz1aTcHyYLhCqCL93d7Kr.:16091:0:99999:7:::
vboxadd:!:16091::::::
mirco:$6$MiHSDS3Z$tAXEZ7ZN7Wk.k08h88xMxgzutb.Qmokmg9YvkST2T2FvZ
IOz6cSAbyNegfnVUNJu.zXTkQidMjg5nB9/rq7WL.:16091:0:99999:7:::
alessandro:$6$xG7FxGoN$CBD7bDUeS6pyzUDEyzxO3tLXzNnDVfJXVKDmIrR2D
```

```
JI.OZ/r7IrFZtmf2snllhX6quPknJwMtIbmludkYLprx0:16091:0:99999:7:::
mauro:$6$nb63AjNh$MLHUSbZQPDqKnTzuTZZaZigmZRjZLUVOhe7QLL4mE9bIu
SoeW/.vgnKAGZ8B0tz7ArwRKLcgK/sCLEYzmuJrH1:16091:0:99999:7:::
luca:$6$.hknq2KP$k7jX1KxHR8vZ2X1LCjgI1xiGo/dEV4r1EjO9oFohqmfP2s
0PLHjsrsWGuba1ZDnru1QSaR.ty8HnO6Aj9qjVK1:16091:0:99999:7:::
guest:$6$9NJk9.ZJ$gL2ywGt13FQ9Kuoaq9zEfMEDYDvUTqJpK9a2xmLtboqFl
W2DDcW60xw4xSwvEy05FvHQ9seot86EBCJ6rL7XF.:16091:0:99999:7:::
andrea:$6$bnTGo7ug$nIhlZBjR98WMRtRYzk3n5md0BPwU3drpCr0gM1w/z8m7
VxiDS3tYqsCcu0uh8ElwoD5jkcPZsgNJyNKI5br73.:16091:0:99999:7:::
```

Vediamo come interpretare una stringa generica

```
mauro:$6$nb63AjNh$MLHUSbZQPDqKnTzuTZZaZigmZRjZLUVOhe7QLL4mE9bI
uSoeW/.vgnKAGZ8B0tz7ArwRKLcgK/sCLEYzmuJrH1:16091:0:99999:7:::
```

1. Nome utente —> mauro

2. Hash della password (con algoritmo di cifratura e SALT) —> 6nb63AjNh$MLHUSbZQPDqKnTzuTZZaZigmZRjZLUVOhe7QLL4mE9bIuSoeW/.vgnKAGZ8B0tz7ArwRKLcgK/sCLEYzmuJrH1

In un sistema tradizionale Unix based, la password ha una lunghezza fissa di 11 caratteri, di cui primi 2 caratteri rappresentano il salt gli altri 9 caratteri rappresentano la codifica del salt utilizzando la password dell'utente come chiave dell'algoritmo DES.In quelli moderni la password viene memorizzata con la seguente regola: `$[algoritmo]$[salt]$[hash]`

In particolare:

- Se vuota non c'è alcuna password

- Se "*" significa che l'account è disabilitato, esempio `daemon:*:16091:0:99999:7:::`

- Algoritmo: 1 md5 - 2 blowfish - 5 sha256 - 6 sha512, esempio `mauro:$6$nb63AjNh$MLHU[...]`

- Se non specificato significa DES.

- Il tool John the Ripper utilizzato per fare il cracking delle password[6].

3. Data di ultima modifica (in giorni dal 01/01/1970) —> 16091

```
/mnt/HD01 % utime=$((16091*60*60*24))
/mnt/HD01 % echo $utime
```

(6)- Tale attività esula dall'obiettivo del presente articolo.

```
1390262400
/mnt/HD01 % date -d @1390262400 +"%d-%m-%Y %T %z"
21-01-2014 01:00:00 +0100
```

4. Numero minimo di giorni tra modifiche —> 0

5. Durata massima in giorni della password —> 9999

6. Numero di giorni di preavviso —> 7

7. Numero di giorni dopo il quale un account con password scaduta viene considerato disabilitato

8. Data di scadenza in giorni dal 01/01/1970;

9. Riservato per possibili usi futuri.

Si noti come il file /etc/passwd è leggibile da tutti gli utenti, mentre il file /etc/shadow è leggibile solo da root.

4.12.2 Gruppi

I gruppi invece sono in /etc/group

```
% cat etc/group
root:      x:     0:
daemon:    x:     1:
bin:       x:     2:
sys:       x:     3:
adm:       x:     4:
tty:       x:     5:
disk:      x:     6:
lp:        x:     7:
mail:      x:     8:
news:      x:     9:
uucp:      x:    10:
man:       x:    12:
proxy:     x:    13:
kmem:      x:    15:
dialout:   x:    20:
fax:       x:    21:
```

```
voice:     x:    22:
cdrom:     x:    24:      mario
floppy:    x:    25:      mario
tape:      x:    26:
sudo:      x:    27:      mario
audio:     x:    29:      pulse,mario
dip:       x:    30:      mario
www-data:  x:    33:
backup:    x:    34:
operator:  x:    37:
list:      x:    38:
irc:       x:    39:
src:       x:    40:
gnats:     x:    41:
shadow:    x:    42:
utmp:      x:    43:
video:     x:    44:      mario
sasl:      x:    45:
plugdev:   x:    46:      mario
staff:     x:    50:
games:     x:    60:
users:     x:   100:
nogroup:   x:   65534:
libuuid:   x:   101:
crontab:   x:   102:
vboxsf:    x:   103:
fuse:      x:   104:
avahi-autoipd: x:  105:
scanner:   x:   106:      saned,mario
messagebus:x:   107:
colord:    x:   108:
lpadmin:   x:   109:
ssl-cert:  x:   110:
```

```
bluetooth: x:   111:      mario
utempter:  x:   112:
netdev:    x:   113:      mario
Debian-exim:  x:1    14:
mlocate:   x:   115:
ssh:       x:   116:
avahi:     x:   117:
pulse:     x:   118:
pulse-access:  x:    119:
rtkit:     x:   120:
saned:     x:   121:
Debian-gdm:  x:   122:
mario:     x:  1000:
mirco:     x:  1001:
alessandro: x:  1002:
mauro:     x:  1003:
luca:      x:  1004:
guest:     x:  1005:
andrea:    x:  1006:
webmasters:x:   123:      mirco,alessandro,mauro
```

Vediamo come interpretare una stringa generica

```
webmasters:x:123:mirco,alessandro,mauro
```

Nome del gruppo —> webmaster

GID - id numerico del gruppo —> 123

Elenco degli utenti del gruppo —> mirco, alessandro, mauro

Per individuare tutti i gruppi di uno specifico utente

```
/mnt/HD01 % grep mauro etc/group
mauro:x:1003:
webmasters:x:123:mirco,alessandro,mauro
```

oppure

```
/mnt/HD01 % egrep -i "root|sirfrancis|mony" etc/group
root:      x:     0:       root
bin:       x:     1:       root,bin,daemon
```

```
daemon:     x:     2:    root,bin,daemon
sys:        x:     3:    root,bin
adm:        x:     4:    root,daemon
disk:       x:     6:       root
wheel:      x:    10:    root,sirfrancis,mony
log:        x:    19:       root
video:      x:    91:    sirfrancis,mony
audio:      x:    92:    sirfrancis,mony
scanner:  x:9     6:    sirfrancis,mony
```

Per individuare tutti gli utenti di uno specifico gruppo

```
/mnt/HD01 % grep '^webmasters:' etc/group
webmasters:x:123:mirco,alessandro,mauro
```

4.12.3 Utenti amministratori

In Linux di default l'utente ha un account non privilegiato e acquisisce privilegi di super-utente quando necessario con i comandi su o sudo.

Sono utenti amministratori tutti gli utenti:

- con UID 0 in /etc/passwd

```
/mnt/HD01 % cat etc/passwd | grep ":0:"
root:x:0:0:root:/root:/bin/bash
```

- che hanno come gruppo sudo o wheel

```
/mnt/HD01 % cat etc/group | egrep -i "sudo|wheel"sudo:x:27:mario
```

- elencati in /etc/sudoers

```
/mnt/HD01 % cat etc/sudoers
#
# This file MUST be edited with the 'visudo' command as root.
#
# Please consider adding local content in /etc/sudoers.d/ instead of
# directly modifying this file.
#
# See the man page for details on how to write a sudoers file.
#Defaults    env_reset  Defaults    mail_badpass  Defaults
```

```
secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/us
r/bin:/sbin:/bin"
# Host alias specification
# User alias specification
# Cmnd alias specification
# User privilege specificatio
root  ALL=(ALL:ALL) ALL
# Allow members of group sudo to execute any command
%sudo  ALL=(ALL:ALL) ALL
# Consenti ad Alessandro Guido di utilizzare il packet manager
alessandro  ALL = /usr/bin/apt-get
# See sudoers(5) for more information on "#include" directives:
#includedir /etc/sudoers.d
```

4.12.4 Storico degli accessi degli utenti

Gli accessi riusciti sono contenuti nel file "/var/log/wtmp", codificato in binario e perciò non direttamente leggibile come gli altri file di testo presenti nella directory. Utilizziamo il comando "last" con opportuni parametri per visualizzarne il contenuto.

```
/mnt/HD01 % last -f var/log/wtmp -F
mirco  tty7     :0       Wed Jan 22 15:24:39 2014 - Wed Jan 22 15:53:59 2014  (00:29)
(unknown tty7   :0       Wed Jan 22 15:24:27 2014 - Wed Jan 22 15:24:38 2014  (00:00)
reboot  system boot 3.2.0-4-486  Wed Jan 22 15:24:25 2014 - Wed Jan 22 15:53:59 2014  (00:29)
(unknown tty8   :0       Wed Jan 22 14:58:14 2014 - down                      (00:15)
<snip>
10:22:20 2014 (00:00)
(unknown tty7     :0       Tue Jan 21 10:17:57 2014 - Tue Jan 21 10:21:59 2014  (00:04)
reboot  system boot 3.2.0-4-486  Tue Jan 21 10:17:55 2014 - Tue Jan 21 10:22:21 2014  (00:04)
wtmp begins Tue Jan 21 10:17:55 2014
```

Se vogliamo filtrare in base ad una data scritta nel formato YYYYMMA-AHHMMSS

```
% last -f /var/log/wtmp.1 -t 20131216170000
```

```
root   pts/3    :0        Mon Dec 16 16:46  gone - no logout
root   pts/2    :0        Mon Dec 16 15:52  gone - no logout
root    pts/2   :0        Mon Dec 16 15:05 - 15:42 (00:36)
root   pts/1    :0        Mon Dec 16 14:33  gone - no logout
reboot  system boot 3.5.0-30-generic Mon Dec 16 14:21 - 14:20 (36+23:58)
root   pts/0    :0        Fri Dec 13 12:03 - crash (3+02:18)
reboot  system boot 3.5.0-30-generic Fri Dec 13 11:32 - 14:20 (40+02:48)
reboot  system boot 3.5.0-30-generic Fri Dec 13 11:26 - 11:31 (00:05)
```

Oppure ricaviamo ulteriori informazioni interessanti dall'analisi del file auth.log

```
/mnt % cat var/log/auth.log | head
Jan 21 10:17:57 Server1 gdm-welcome][2963]: pam_unix(gdm-wel-
come:session): session opened for user Debian-gdm by (uid=0)
Jan 21 10:17:57 Server1 gdm-welcome][2963]: pam_ck_connec-
tor(gdm-welcome:session): nox11 mode, ignoring PAM_TTY :0
Jan 21 10:17:57 Server1 sshd[3114]: Server listening on 0.0.0.0 port 22.
Jan 21 10:17:57 Server1 sshd[3114]: Server listening on :: port 22.
Jan 21 10:17:58 Server1 polkitd(authority=local): Registered
Authentication Agent for unix-
session:/org/freedesktop/ConsoleKit/Session1 (system bus name
:1.33 [/usr/lib/policykit-1-gnome/polkit-gnome-authentication-
agent-1], object path
/org/gnome/PolicyKit1/AuthenticationAgent, locale it_IT.UTF-8)
Jan 21 10:17:59 Server1 dbus[2195]: [system] Rejected send mes-
sage, 2 matched rules; type="method_call", sender=":1.34"
(uid=114 pid=3340 comm="/usr/lib/gdm3/gdm-simple-greeter ")
interface="org.freedesktop.DBus.Properties" member="GetAll"
error name="(unset)" requested_reply="0" destination=":1.16"
(uid=0 pid=2978 comm="/usr/sbin/console-kit-daemon —no-daemon ")
Jan 21 10:17:59 Server1 dbus[2195]: [system] Rejected send
message, 2 matched rules; type="method_call", sen-
der=":1.34" (uid=114 pid=3340 comm="/usr/lib/gdm3/gdm-sim-
ple-greeter ") interface="org.freedesktop.DBus.Properties"
```

```
member="GetAll" error name="(unset)" requested_reply="0"
destination=":1.16" (uid=0 pid=2978 comm="/usr/sbin/conso-
le-kit-daemon —no-daemon ")
Jan 21 10:17:59 Server1 dbus[2195]: [system] Rejected send
message, 2 matched rules; type="method_call", sen-
der=":1.34" (uid=114 pid=3340 comm="/usr/lib/gdm3/gdm-sim-
ple-greeter ") interface="org.freedesktop.DBus.Properties"
member="GetAll" error name="(unset)" requested_reply="0"
destination=":1.16" (uid=0 pid=2978 comm="/usr/sbin/conso-
le-kit-daemon —no-daemon ")
Jan 21 10:17:59 Server1 dbus[2195]: [system] Rejected send
message, 2 matched rules; type="method_call", sen-
der=":1.34" (uid=114 pid=3340 comm="/usr/lib/gdm3/gdm-sim-
ple-greeter ") interface="org.freedesktop.DBus.Properties"
member="GetAll" error name="(unset)" requested_reply="0"
destination=":1.16" (uid=0 pid=2978 comm="/usr/sbin/conso-
le-kit-daemon —no-daemon ")
Jan 21 10:17:59 Server1 dbus[2195]: [system] Rejected send
message, 2 matched rules; type="method_call", sen-
der=":1.34" (uid=114 pid=3340 comm="/usr/lib/gdm3/gdm-sim-
ple-greeter ") interface="org.freedesktop.DBus.Properties"
member="GetAll" error name="(unset)" requested_reply="0"
destination=":1.16" (uid=0 pid=2978 comm="/usr/sbin/conso-
le-kit-daemon —no-daemon ")
```

Gli accessi falliti, invece, sono contenuti nel file "/var/log/btmp", anch'esso binario e interpretabile tramite lo strumento "last" o "lastb".

```
% lastb -f var/log/btmp
mario  tty7     :0        Tue Jan 21 18:30 - 18:30 (00:00)
btmp begins Tue Jan 21 18:30:01 2014
```

Anche in questo caso, ulteriori informazioni sugli accessi non riusciti (es. Password errata, certificate errato, utente inesistente, etc…) possono essere trovati in auth.log.

4.13 Attività degli utenti

Vediamo dove andare a cercare informazioni sulle attività degli utenti.

4.13.1 History dei comandi bash

La storia dei comandi digitati dagli utenti è contenuta nella loro home directory, nel file ".bash_history".

```
/mnt/HD01 % cat home/alessandro/.bash_history
cd Scaricati
ls
unzip -e python_examples.zip
ls
ls *zip
ls
ls *zip
mv python_examples.zip ../
ls
[...]
```

Si faccia attenzione che in un sistema live, tale file può risultare non completo, in quanto i comandi digitali durante la sessione vengono memorizzati temporanemanete in RAM e solo al logout vengono storicizzati. Si noti infine come non compaiono timestamp dei comandi ne viene fatta una distinzione in caso di più shell aperte.

4.13.2 File usati di recente

Vediamo quali file hanno visionato di recente gli utenti.

```
/mnt/HD01 % cat home/alessandro/.local/share/recently-used.xbel
<?xml version="1.0" encoding="UTF-8"?>
<xbel version="1.0"
   xmlns:bookmark="http://www.freedesktop.org/standards/desktop-
bookmarks"
```

```
    xmlns:mime="http://www.freedesktop.org/standards/sha-
red-mime-info"
>
    <bookmark    href="file:///tmp/python_examples.zip"
added="2014-01-22T12:22:55Z"          modified="2014-01-
22T12:22:55Z" visited="2014-01-22T12:22:55Z">
  <info>
   <metadata owner="http://freedesktop.org">
    <mime:mime-type type="application/zip"/>
    <bookmark:applications>
               <bookmark:application   name="Iceweasel"
exec="&apos;iceweasel    %u&apos;"    modified="2014-01-
22T12:22:55Z" count="1"/>
    </bookmark:applications>
   </metadata>
  </info>
 </bookmark>
 <bookmark href="file:///home/alessandro/Scaricati/python_exam-
ples.zip"   added="2014-01-22T12:24:01Z"   modified="2014-01-
22T12:24:01Z" visited="2014-01-22T12:24:01Z">
  <info>
   <metadata owner="http://freedesktop.org">
    <mime:mime-type type="application/zip"/>
    <bookmark:applications>
               <bookmark:application   name="Iceweasel"
exec="&apos;iceweasel    %u&apos;"    modified="2014-01-
22T12:24:01Z" count="1"/>
    </bookmark:applications>
   </metadata>
  </info>
 </bookmark>
</xbel>
```

4.14 Chiavi SSH

Per effettuare un accesso senza inserire password SSH permette un'autenticazione a chiave asimmetrica generate con ssh-keygen.

Le chiavi vengono memorizzate con nomi arbitrari in una directory nascosta, come ad esempio:

- $HOME/.ssh/id_rsa, che è la chiave privata e può essere o meno cifrata;

```
/mnt/HD01 % cat home/mario/.ssh/id_rsa
——-BEGIN RSA PRIVATE KEY——-
Proc-Type:         4,ENCRYPTEDDEK-Info:         AES-128-
CBC,514955678994D3A6594B10E423BAFF8AzaV6neGJEDJb/Bma/NSwj
Un/emzjrkkW1l3zK8+XqatAsNIpHHlBAbsZzfVtmULeXOziZhwfrr09kW
lk6L/giO+hrboBe+Qkk3aYMOlnbBMap9YriN+H3CyUO/XK1IQY[...]6B
Img+j0rcCR8ssku4v7tDJLbq94RclerHoRc/0Ri+8HWLJr2DoQfoHIIIG
+5OkME9/FSTBmCcskB09dPewjQbVaJxqWv3+79boa0OxOOpsK4+lIQopt
keBACIPumTUPwf5u509/j/5JPXM9Hejr2azhM6q+csF2hHODycpsODIKa
YW2nuv6WtfFO6yrXAU0——-END RSA PRIVATE KEY——-
```

- $HOME/.ssh/id_rsa.pub, che è la chiave pubblica;

```
/mnt/HD01   %   cat   home/mario/.ssh/id_rsa.pubssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQDP9ovyg7f12qITAz0SZnFxlYtRy
BYhAmTgAYeKW6apUPR5J/JUWVOlSwMO7f5t04cK60KTgKhUD/wVm+ovPD
ON8hkv/QxbgzqAEt6BRiMda6HwpRGF9LzXpsrnxIFYqT3A3+IAUEwRXCt
ISoBZlW71J/Fe/CbohcL5rOeN4DhNIkA3wUjH0/f/6sIiQd7UcRAHzR/N
xAFMw7GHujS9+WmxRAMyle0XDjpfREM120bp1b8DuZ2oY5O6rwPZgKX0W
VMAcDAYTULfF86qdaMx2TvvPUQEjwqllJ37Lgenf/IoD3ydEVsVfRPXE1
CJY054JbgQHoQDLbkLld7+b7B10O3d mario@Server1
```

4.15 Attività del browser Firefox

Vediamo ora dove reperire informazioni sulle attività del browser Firefox. Firefox è il browser di default di molte distribuzioni Linux e salva nella directory del profilo /home/$USER/.mozilla/firefox/profiles/$ID.$NAME/.

4.15.1 Profili in uso

Per conoscere quali sono i profili in uso ad un determinato account bisogna consultare il file profiles.ini

```
/mnt/HD01 % cat home/mario/.mozilla/firefox/profiles.ini
[General]
StartWithLastProfile=1
[Profile0]
Name=default
IsRelative=1
Path=22asgspj.default
```

Così facendo ricaviamo la directory di lavoro

```
/mnt/HD01 % cd home/mario/.mozilla/firefox/22asgspj.default/
deft8vm ../firefox/22asgspj.default % ls
addons.sqlite         downloads.sqlite       search.json
blocklist.xml         extensions.ini         secmod.db
bookmarkbackups       extensions.sqlite      sessionstore.bak
bookmarks.html        formhistory.sqlite     sessionstore.js
Cache                     key3.db            signons.sqlite
_CACHE_CLEAN_         localstore.rdf         startupCache
cert8.db              mimeTypes.rdf          thumbnails
chrome                permissions.sqlite     urlclassifierkey3.txt
chromeappsstore.sqlite places.sqlite         webapps
compatibility.ini     pluginreg.dat          webappsstore.sqlite
content-prefs.sqlite prefs.js
cookies.sqlite        safebrowsing
```

Poiché il file system è in sola lettura, il motore SQLite considererà gli archivi come in uso, quindi necessita salvare il contenuto della cartella in un'area con permessi di lettura e scrittura.

```
../mario/.mozilla/firefox % cp -R 22asgspj.default/
/media/evidence/HD01/data/
```

4.15.2 Siti visitati

I siti visitati durante la navigazione vengono memorizzati all'interno della tabella moz_places.

```
../22asgspj.default % sqlite3 places.sqlite
SQLite version 3.7.13 2012-06-11 02:05:22
Enter ".help" for instructions
Enter SQL statements terminated with a ";"
```

Con il comando .tables ricaviamo l'elenco della tabelle che caratterizzano il database.

```
sqlite> .tables
moz_anno_attributes     moz_favicons        moz_items_annos
moz_annos               moz_historyvisits   moz_keywords
moz_bookmarks           moz_hosts           moz_places
moz_bookmarks_roots     moz_inputhistory
```

Con il comando .schema ricaviamo invece la struttura della tabella.

```
sqlite> .schema moz_places
CREATE TABLE moz_places (  id INTEGER PRIMARY KEY, url LON-
GVARCHAR,  title  LONGVARCHAR,  rev_host  LONGVARCHAR,
visit_count INTEGER DEFAULT 0, hidden INTEGER DEFAULT 0
NOT NULL, typed INTEGER DEFAULT 0 NOT NULL, favicon_id
INTEGER,  frecency  INTEGER  DEFAULT  -1  NOT  NULL,
last_visit_date INTEGER , guid TEXT);
CREATE INDEX moz_places_faviconindex ON moz_places (favicon_id);
CREATE INDEX moz_places_frecencyindex ON moz_places (frecency);
CREATE UNIQUE INDEX moz_places_guid_uniqueindex ON moz_places (guid);
CREATE INDEX moz_places_hostindex ON moz_places (rev_host);
CREATE INDEX moz_places_lastvisitdateindex ON moz_places (last_visit_date);
CREATE UNIQUE INDEX moz_places_url_uniqueindex ON moz_places (url);
CREATE INDEX moz_places_visitcount ON moz_places (visit_count);
```

Visualiziamo ora il contenuto della tabella.

```
sqlite> select * from moz_places;
1|http://www.mozilla.com/en-US/firefox/central/||moc.alli-
zom.www.|0|0|0||140||ZI3pXAKmEkgN
2|http://www.mozilla.com/en-US/firefox/help/||moc.alli-
zom.www.|0|0|0|1|140||ZSpKS5kpsX1c
<snip>
19|http://code.google.com/p/firefox-cache-
forensics/downloads/list|Downloads - firefox-cache-forensics - Tools
for forensic analysis of Firefox Cache - Google Project
Hosting|moc.elgoog.edoc.|1|0|0|14|100|1390386372830240|Rm_BiLWA0-UE
20|http://code.google.com/p/firefox-cache-forensics/downlo-
ads/detail?name=ff_cache_find_0.3.pl&can=2&q=|ff_cache_find_
0.3.pl - firefox-cache-forensics - ff_cache_find_0.3.pl -
search and recover firefox cache entries - Tools for forensic
analysis of Firefox Cache - Google Project Hosting|moc.elgo-
og.edoc.|1|0|0|14|100|1390386374744411|qaQnmcNpdPFf
21|http://firefox-cache-
forensics.googlecode.com/files/ff_cache_find_0.3.pl|ff_ca
che_find_0.3.pl|moc.edocelgoog.scisnerof-ehcac-
xoferif.|0|0|0||0|1390386376725322|TfAqZauNQ7LX
```

Vediamo che il generico record assume la seguente forma:

id|*url*|*titolo*|*hostname rovesciato*|*numero visite*|*nascosto*|*scritto*|*id icona*|*frecency*|*data ultima visita*|*GUID*

- id = 21
- URL = http://firefox-cache-forensics.googlecode.com/files/ff_cache_find_0.3.pl
- Titolo = ff_cache_find_0.3.pl
- Hostname rovesciato = moc.edocelgoog.scisnerof-ehcac-xoferif.
- Numero di visite = 0
- Nascosto = 0 (impostato se il link visitato automaticamente senza alcuna selezione diretta da parte dell'utente)

- Scritto = 0 (impostato se il link è stato scritto direttamente a mano dall'utente)

- Id icona =

- Frecency = 0

- Ultima visita = 13903863767253221390386376725322 / 1000000 = 1390386376

```
% date -d @1390386376
Wed Jan 22 11:26:16 CET 2014
```

- Guid = TfAqZauNQ7LX

Formuliamo ora una query che ci fornisca le URL ed il rispettivo orario di ultima visita.

```
sqlite> SELECT moz_places.url,
datetime(moz_places.last_visit_date/1000000, 'unixepoch',
'localtime') FROM moz_places;
http://www.mozilla.com/en-US/firefox/central/|
http://www.mozilla.com/en-US/firefox/help/|
http://www.mozilla.com/en-US/firefox/customize/|
http://www.mozilla.com/en-US/firefox/community/|
http://www.mozilla.com/en-US/about/|
place:sort=8&maxResults=10|
place:folder=BOOKMARKS_MENU&folder=UNFILED_BOOKMARKS&folder=T
OOLBAR&queryType=1&sort=12&maxResults=10&excludeQueries=1|
place:type=6&sort=14&maxResults=10|
https://www.google.com/search?q=firefox+history&ie=utf-
8&oe=utf-8&aq=t&rls=org.mozilla:it:unofficial&client=ice-
weasel-a&channel=fflb|2014-01-22 10:25:01
http://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&
cd=1&ved=0CCoQFjAA&url=http%3A%2F%2Fkb.mozillazine.org%2FV
i e w i n g _ t h e _ b r o w s i n g _ h i s t o r y _ -
_Firefox&ei=f5zfUpyWD6SXyAO9jYGgAQ&usg=AFQjCNFlKLhRzmI1tyr
X0Z7MUf5rDJOHiA&bvm=bv.59568121,d.bGQ|2014-01-22 10:25:05
http://kb.mozillazine.org/Viewing_the_browsing_history_-
_Firefox|2014-01-22 10:25:06
```

```
https://www.google.com/search?q=firefox+cache&ie=utf-8&oe=utf-8&aq=t&rls=org.mozilla:it:unofficial&client=iceweasel-a&channel=fflb|2014-01-22 10:25:15
https://support.mozilla.org/questions/681194|2014-01-22 10:25:19
https://support.mozilla.org/it/questions/681194|2014-01-22 10:25:20
https://www.google.com/search?q=firefox+cache+ff_cache&ie=utf-8&oe=utf-8&aq=t&rls=org.mozilla:it:unofficial&client=iceweasel-a|2014-01-22 10:25:45
https://www.google.com/search?q=firefox+cache+ff_cache&ie=utf-8&oe=utf-8&aq=t&rls=org.mozilla:it:unofficial&client=iceweasel-a#q=ff_cache_find&rls=org.mozilla:it:unofficial|2014-01-22 10:26:05
http://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0CCgQFjAA&url=http%3A%2F%2Fcode.google.com%2Fp%2Ffirefox-cache-forensics%2Fwiki%2FFfCacheFind&ei=v5zfUsSwMOOXyAOL_oDgAQ&usg=AFQjCNEllSSMkIi50EbnqnIRJ-2-UaoC3A&bvm=bv.59568121,d.bGQ|2014-01-22 10:26:09
http://code.google.com/p/firefox-cache-forensics/wiki/FfCacheFind|2014-01-22 10:26:09
http://code.google.com/p/firefox-cache-forensics/downloads/list|2014-01-22 10:26:12
http://code.google.com/p/firefox-cache-forensics/downloads/detail?name=ff_cache_find_0.3.pl&can=2&q=|2014-01-22 10:26:14
http://firefox-cache-forensics.googlecode.com/files/ff_cache_find_0.3.pl|2014-01-22 10:26:16
```

Possiamo anche esportare i risultati in un file ad hoc.

```
sqlite> .show
    echo: off
 explain: off
 headers: off
    mode: list
nullvalue: ""
  output: stdout
```

```
separator: "|"
  stats: off
  width:
sqlite> .headers on
sqlite> .mode csv
sqlite> .output places.csv
sqlite>              SELECT              moz_places.url,
datetime(moz_places.last_visit_date/1000000,  'unixepoch')
FROM moz_places;
sqlite> .output stdout
sqlite> .show
   echo: off
 explain: off
 headers: on
   mode: csv
nullvalue: ""
  output: stdout
separator: ","
  stats: off
  width:
```

4.15.3 Bookmark

I siti preferiti (o c.d. bookmarks) sono indicizzati nella tabella moz_bookmarks.

```
sqlite> .schema moz_bookmarks
CREATE TABLE moz_bookmarks ( id INTEGER PRIMARY KEY, type
INTEGER, fk INTEGER DEFAULT NULL, parent INTEGER, position
INTEGER, title LONGVARCHAR, keyword_id INTEGER, folder_type
TEXT, dateAdded INTEGER, lastModified INTEGER, guid TEXT);
CREATE UNIQUE INDEX moz_bookmarks_guid_uniqueindex ON
moz_bookmarks (guid);
CREATE INDEX moz_bookmarks_itemindex ON moz_bookmarks (fk, type);
```

```
CREATE INDEX moz_bookmarks_itemlastmodifiedindex ON
moz_bookmarks (fk, lastModified);
CREATE INDEX moz_bookmarks_parentindex ON moz_bookmarks
(parent, position);
```

Per essere consultata agevolgemente necessita di essere messa in relazione con la tabella moz_places.

```
sqlite> SELECT moz_places.url,
datetime(moz_bookmarks.dateAdded/1000000, 'unixepoch', 'localtime')
FROM moz_bookmarks, moz_places where moz_bookmarks.fk = moz_places.id;
http://www.mozilla.com/en-US/firefox/central/|2014-01-21 17:37:20
http://www.mozilla.com/en-US/firefox/help/|2014-01-21 17:37:20
http://www.mozilla.com/en-US/firefox/customize/|2014-01-21 17:37:20
http://www.mozilla.com/en-US/firefox/community/|2014-01-21 17:37:20
http://www.mozilla.com/en-US/about/|2014-01-21 17:37:20
place:sort=8&maxResults=10|2014-01-21 17:37:20
place:folder=BOOKMARKS_MENU&folder=UNFILED_BOOKMARKS&folder=TOOLBAR&q
ueryType=1&sort=12&maxResults=10&excludeQueries=1|2014-01-21 17:37:20
place:type=6&sort=14&maxResults=10|2014-01-21 17:37:20
```

4.15.4 History

La tabella moz_historyvisits tiene il log delle visite dei siti visitati.

```
sqlite> .schema moz_historyvisits
CREATE TABLE moz_historyvisits ( id INTEGER PRIMARY KEY, from_visit INTEGER,
place_id INTEGER, visit_date INTEGER, visit_type INTEGER, session INTEGER);
CREATE INDEX moz_historyvisits_dateindex ON moz_historyvisits (visit_date);
CREATE INDEX moz_historyvisits_fromindex ON moz_historyvisits (from_visit);
CREATE INDEX moz_historyvisits_placedateindex ON moz_historyvisits
(place_id, visit_date);
```

Per essere consultata agevolmente necessita di essere messa in relazione con la tabella moz_places.

```
sqlite> SELECT datetime(moz_historyvisits.visit_date/1000000,'unixe-
poch', 'localtime'), moz_places.url FROM moz_places, moz_historyvisits
```

```
WHERE moz_places.id = moz_historyvisits.place_id;
2014-01-22 10:25:01|https://www.google.com/search?q=firefox+history&ie=utf-8&oe=utf-8&aq=t&rls=org.mozilla:it:unofficial&client=iceweasel-a&channel=fflb
2014-01-22 10:25:05|http://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0CCoQFjAA&url=http%3A%2F%2Fkb.mozillazine.org%2FViewing_the_browsing_history_-_Firefox&ei=f5zfUpyWD6SXyAO9jYGgAQ&usg=AFQjCNFlKLhRzmI1tyrX0Z7MUf5rDJOHiA&bvm=bv.59568121,d.bGQ
2014-01-22 10:25:06|http://kb.mozillazine.org/Viewing_the_browsing_history_-_Firefox
2014-01-22 10:25:15|https://www.google.com/search?q=firefox+cache&ie=utf-8&oe=utf-8&aq=t&rls=org.mozilla:it:unofficial&client=iceweasel-a&channel=fflb
2014-01-22 10:25:19|https://support.mozilla.org/questions/681194
2014-01-22 10:25:20|https://support.mozilla.org/it/questions/681194
2014-01-22 10:25:45|https://www.google.com/search?q=firefox+cache+ff_cache&ie=utf-8&oe=utf-8&aq=t&rls=org.mozilla:it:unofficial&client=iceweasel-a
2014-01-22 10:26:05|https://www.google.com/search?q=firefox+cache+ff_cache&ie=utf-8&oe=utf-8&aq=t&rls=org.mozilla:it:unofficial&client=iceweasel-a#q=ff_cache_find&rls=org.mozilla:it:unofficial
2014-01-22 10:26:05|https://www.google.com/search?q=firefox+cache+ff_cache&ie=utf-8&oe=utf-8&aq=t&rls=org.mozilla:it:unofficial&client=iceweasel-a#q=ff_cache_find&rls=org.mozilla:it:unofficial
2014-01-22 10:26:09|http://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0CCgQFjAA&url=http%3A%2F%2Fcode.google.com%2Fp%2Ffirefox-cache-forensics%2Fwiki%2FFfCacheFind&ei=v5zfUsSwMOOXyAOL_oDgAQ&usg=AFQjCNEllSSMkIi50EbnqnIRJ-2-UaoC3A&bvm=bv.59568121,d.bGQ
```

```
2014-01-22   10:26:09|http://code.google.com/p/firefox-
cache-forensics/wiki/FfCacheFind
2014-01-22   10:26:12|http://code.google.com/p/firefox-
cache-forensics/downloads/list
2014-01-22   10:26:14|http://code.google.com/p/firefox-cache-
forensics/downloads/detail?name=ff_cache_find_0.3.pl&can=2&q=
2014-01-22  10:26:16|http://firefox-cache-forensics.goo-
glecode.com/files/ff_cache_find_0.3.pl
```

4.15.5 Download

Per consultare la lista dei file scaricati dobbiamo cambiare database.

```
../22asgspj.default % sqlite3 downloads.sqlite
SQLite version 3.7.13 2012-06-11 02:05:22
Enter ".help" for instructions
Enter SQL statements terminated with a ";"
sqlite> .tables
moz_downloads
sqlite> .schema moz_downloads
CREATE TABLE moz_downloads (id INTEGER PRIMARY KEY, name
TEXT, source TEXT, target TEXT, tempPath TEXT, startTime
INTEGER, endTime INTEGER, state INTEGER, referrer TEXT,
entityID TEXT, currBytes INTEGER NOT NULL DEFAULT 0,
maxBytes INTEGER NOT NULL DEFAULT -1, mimeType TEXT,
preferredApplication TEXT, preferredAction INTEGER NOT
NULL DEFAULT 0, autoResume INTEGER NOT NULL DEFAULT 0);
```

Possiamo ricavare informazioni in merito a:

Nome file;

URL di origine;

Percorso di destinazione;

Tempo di inizio download;

Tempo di fine download;

Referer.

```
sqlite>                                                    SELECT
id,name,source,target,datetime(startTime/1000000,'unixe-
poch',  'localtime'),datetime(endTime/1000000,'unixepoch',
'localtime'),mimeType FROM moz_downloads
1|ff_cache_find_0.3.pl|http://firefox-cache-
forensics.googlecode.com/files/ff_cache_find_0.3.pl|file:
///home/mario/Scaricati/ff_cache_find_0.3.pl|2014-01-22
10:26:16|2014-01-22 10:26:19|text/plain
```

Si tenga presente che da questa lista mancano gli elementi acquisiti tramite addon (es. DownThemAll).

4.15.6 Credenziali salvate

Le credenziali salvate sono memorizzate nella tabella tabella moz_logins del database signons.sqlite.

```
../22asgspj.default % sqlite3 signons.sqlite
SQLite version 3.7.13 2012-06-11 02:05:22
Enter ".help" for instructions
Enter SQL statements terminated with a ";"
sqlite>.tables
moz_deleted_logins moz_disabledHosts  moz_logins
sqlite> .schema moz_logins
CREATE TABLE moz_logins (id INTEGER PRIMARY KEY,hostname TEXT
NOT  NULL,httpRealm  TEXT,formSubmitURL  TEXT,usernameField
TEXT NOT NULL,passwordField TEXT NOT NULL,encryptedUsername
TEXT  NOT  NULL,encryptedPassword  TEXT  NOT  NULL,guid
TEXT,encType INTEGER,timeCreated INTEGER,timeLastUsed INTE-
GER,timePasswordChanged INTEGER,timesUsed INTEGER);
CREATE      INDEX      moz_logins_encType_index      ON
moz_logins(encType);
CREATE INDEX moz_logins_guid_index ON moz_logins(guid);
CREATE  INDEX  moz_logins_hostname_formSubmitURL_index  ON
moz_logins(hostname, formSubmitURL);
```

```
CREATE INDEX moz_logins_hostname_httpRealm_index ON
moz_logins(hostname, httpRealm);CREATE INDEX
moz_logins_hostname_index ON moz_logins(hostname);
```

I valori di username e password non sono in chiaro, ma cifrati tramite l'algoritmo 3DES. La rispettiva chiave è nel file key3.db.Il modo più rapido per leggere le password in chiaro è creare un nuovo profilo e copiare i file signons.sqlite e key3.db

4.15.7 Cookies

Sono memorizzati all'interno della tabella moz_cookies del database cookies.sqlite,

```
% sqlite3 cookies.sqlite
SQLite version 3.7.13 2012-06-11 02:05:22
Enter ".help" for instructions
Enter SQL statements terminated with a ";"
sqlite> .tables
moz_cookies
sqlite> .schema moz_logins
sqlite> .schema moz_cookies
CREATE TABLE moz_cookies (id INTEGER PRIMARY KEY,
baseDomain TEXT, name TEXT, value TEXT, host TEXT, path
TEXT, expiry INTEGER, lastAccessed INTEGER, creationTime
INTEGER, isSecure INTEGER, isHttpOnly INTEGER, CONSTRAINT
moz_uniqueid UNIQUE (name, host, path));
CREATE INDEX moz_basedomain ON moz_cookies (baseDomain);
```

SQLite ci consente di esportarli.

```
sqlite> .output google_cookies.txt
sqlite> select * from moz_cookies where baseDomain like
"%google%";
sqlite> .exit
select id, baseDomain, name, value, host, path, datetime(expi-
ry /1000000,'unixepoch', 'localtime'), datetime(lastAccessed
```

```
/1000000,'unixepoch', 'localtime'), datetime(creationTime
/1000000,'unixepoch', 'localtime'), isSecure, isHttpOnly from
moz_cookies where baseDomain like "%google%";
../22asgspj.default % cat google_cookies.txt
2|google.com|NID|67=W1QWYKFMdvqU2zPE8FRE2lHgcCEfqVVesM3mq
6sQnp9YYEMZxaPfFpwsD32ZxYphefbcwWExA1i1uQsqYNlYhoZ7iMwOQL
bwA_sA4jbWC234cWbfl0Q60WODwJCPmBDP|.google.com|/|1970-01-
01 01:23:26|2014-01-22 11:26:03|2014-01-22 11:25:01|0|1
14|google.com|PREF|ID=9f852e38784308a7:U=7265bf1409853526:FF=0:
TM=1390325832:LM=1390386317:S=J8Hu_SEmyiogNgjU|.google.com|/|19
70-01-01 01:24:13|2014-01-22 11:26:16|2014-01-21 18:37:25|0|0
42|google.com|__utma|247248150.264471248.1390386369.13903
86369.1390386369.1|.code.google.com|/|1970-01-01
01:24:13|2014-01-22 11:26:16|2014-01-22 11:26:09|0|0
43|google.com|__utmb|247248150.4.9.1390386376522|.code.google.com|
/|1970-01-01 01:23:10|2014-01-22 11:26:16|2014-01-22 11:26:09|0|0
44|google.com|__utmz|247248150.1390386369.1.1.utmcsr=google|utmccn
=(organic)|utmcmd=organic|utmctr=(not%20provided)|.code.google.com
|/|1970-01-01 01:23:26|2014-01-22 11:26:16|2014-01-22 11:26:09|0|0
```

4.15.8 Cache

La cache degli oggetti di Firefox può contenere informazioni utili ai fini d'indagine. Questi è analizzabile attraverso l'applicativo ff_cache_find[7], che richiede richiede libmime-types-perl.

```
% wget http://firefox-cache-forensics.googlecode.com/files/ff_cache_find_0.3.pl
—2014-01-24 16:08:55— http://firefox-cache-forensics.goo-
glecode.com/files/ff_cache_find_0.3.pl
Resolving firefox-cache-forensics.googlecode.com (fire-
fox-cache-forensics.googlecode.com)... 173.194.70.82,
2a00:1450:4001:c02::52
```

(7) - https://firefox-cache-forensics.googlecode.com/files/ff_cache_find_0.3.pl

```
Connecting to firefox-cache-forensics.googlecode.com (firefox-
cache-forensics.googlecode.com)|173.194.70.82|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 28029 (27K) [text/plain]
Saving to: `ff_cache_find_0.3.pl'
100%[======================================>]     28,029
4.02K/s  in 6.8s
2014-01-24 16:09:12 (4.02 KB/s) - `ff_cache_find_0.3.pl' saved [28029/28029]
% perl ff_cache_find_0.3.pl 22asgspj.default/Cache/_CACHE_MAP_
--------------
Request String: HTTP:https://www.google.com/images/nav_logo170_hr.png
Create time:                    Wed Jan 22 11:25:01 2014
Last Modified time:             Wed Jan 22 11:25:01 2014
Expire time:                    Thu Jan 22 11:25:01 2015
Fetch count:                    1
Server Response: request-method GET response-head HTTP/1.1 200 OK
  Alternate-Protocol: 443:quic
  Cache-Control: private, max-age=31536000
  Content-Length: 29887
<snip>
```

4.16 Attività del browser Chrome o Chronomium

Anche Google Chrome/Chromium utilizza SQLite per organizzare molte informazioni.

4.16.1 Informazioni sui profili

Le directory del profilo attenzionato sono:

- *$HOME/.config/google-chrome/Default*
- *$HOME/.config/chromium/Default*

```
/mnt/HD01/home % cd mirco/.config/chromium/Default/
../.config/chromium/Default % ls
```

```
Archived History    History                        Preferences
Archived History-journal  History-journal                README
Bookmarks           History Provider Cache      Session Storage
Bookmarks.bak       Last Session                  Shortcuts
Cookies             Last Tabs                  Shortcuts-journal
Cookies-journal     Local Storage                 Top Sites
Current Session     Login Data                 Top Sites-journal
Current Tabs        Login Data-journal   TransportSecurity
Extensions          Network Action Predictor     User StyleSheets
Favicons          Network Action Predictor-journal      Visited Links
Favicons-journal  Origin Bound Certs              Web Data
GPUCache          Origin Bound Certs-journal   Web Data-journal
```

4.16.2 Segnalibri

I segnalibri vengono memorizzati in formato JSON in un file testuale nel profilo.

```
../.config/chromium/Default % cat Bookmarks
{
  "checksum": "d2a60c194ff00edc1a6b7358de4174e3",
  "roots": {
   "bookmark_bar": {
     "children": [ {
      "date_added": "0",
      "id": "4",
      "name": "Debian.org",
      "type": "url",
      "url": "http://www.debian.org/"
     }, {
      "date_added": "0",
      "id": "5",
      "name": "Latest News",
      "type": "url",
```

```
       "url": "http://www.debian.org/News/"
      }, {
       "date_added": "0",
       "id": "6",
       "name": "Help",
       "type": "url",
       "url": "http://www.debian.org/support"
      } ],
      "date_added": "13034862044539058",
      "date_modified": "0",
      "id": "1",
      "name": "Bookmarks Bar",
      "type": "folder"
   },
   "other": {
      "children": [ ],
      "date_added": "13034862044539099",
      "date_modified": "0",
      "id": "2",
      "name": "Other Bookmarks",
      "type": "folder"
   },
   "synced": {
      "children": [ ],
      "date_added": "13034862044539114",
      "date_modified": "0",
      "id": "3",
      "name": "Mobile Bookmarks",
      "type": "folder"
   }
  },
  "version": 1
}
```

Che è stato aggiunto il giorno

```
sqlite> SELECT datetime(((13034862044539114/1000000)--
11644473600), "unixepoch", "localtime");
2014-01-22 12:00:44
```

A tal proposito si ricordi che Google Chrome utilizza il timestamp in formato in secondi trascorsi dal 01/01/1601 00:00:00.

4.16.3 History

La cronologia viene memorizzata all'interno delle tabelle urls e visits dell'archivio SQLite History (si noti che qui non c'è estensione).

```
../.config/chromium/Default % file History
History: SQLite 3.x database
../.config/chromium/Default % sqlite3 History
SQLite version 3.7.13 2012-06-11 02:05:22
Enter ".help" for instructions
Enter SQL statements terminated with a ";"
sqlite> .tables
downloads             meta                 urls
downloads_url_chains  segment_usage        visit_source
keyword_search_terms  segments             visits
sqlite> .schema urls
CREATE TABLE urls(id INTEGER PRIMARY KEY,url
LONGVARCHAR,title LONGVARCHAR,visit_count INTEGER DEFAULT
0 NOT NULL,typed_count INTEGER DEFAULT 0 NOT
NULL,last_visit_time INTEGER NOT NULL,hidden INTEGER
DEFAULT 0 NOT NULL,favicon_id INTEGER DEFAULT 0 NOT NULL);
CREATE INDEX urls_url_index ON urls (url);
sqlite> .schema visits
CREATE TABLE visits(id INTEGER PRIMARY KEY,url INTEGER NOT
NULL,visit_time INTEGER NOT NULL,from_visit INTEGER,tran-
sition INTEGER DEFAULT 0 NOT NULL,segment_id
INTEGER,visit_duration INTEGER DEFAULT 0 NOT NULL);
```

```
CREATE INDEX visits_from_index ON visits (from_visit);
CREATE INDEX visits_time_index ON visits (visit_time);
CREATE INDEX visits_url_index ON visits (url);
sqlite> SELECT urls.url, urls.title, urls.visit_count,
urls.typed_count,datetime(((urls.last_visit_time/1000000)
-11644473600),"unixepoch", "localtime"), urls.hidden,
datetime(((visits.visit_time/1000000)-11644473600),"uni-
xepoch", "localtime"), visits.from_visit,visits.transi-
tion FROM urls, visits WHERE urls.id = visits.url;
http://tools.google.com/chrome/intl/en/welcome.html|Getting
Started|1|0|2014-01-22 11:00:45|0|2014-01-22 11:00:45|0|268435462
https://www.google.com/intl/en/chrome/browser/welcome.html|Getting
Started|1|0|2014-01-22 11:00:45|0|2014-01-22 11:00:45|1|2684354566
http://localhost/|Materiale    didattico|2|2|2014-01-22
11:07:04|0|2014-01-22 11:01:07|0|838860801
http://localhost/|Materiale    didattico|2|2|2014-01-22
11:07:04|0|2014-01-22 11:06:45|0|855638017
<snip>
```

4.16.4 Download

Vediamo come ottenere informazioni sui file scaricati.

```
sqlite> SELECT id,full_path, url, datetime(start_time,'unixe-
poch','localtime') AS date, received_bytes, total_bytes, CASE
WHEN state=1 THEN 'complete' WHEN state=2 THEN 'incomplete' ELSE
'unknown' END AS state FROM downloads;
id,full_path,url,date,received_bytes,total_bytes,state
1,/home/sirfrancis/Scrivania/525009_540100799337472_59756
3617_n.jpg,http://sphotos-h.ak.fbcdn.net/hphotos-ak-
ash3/525009_540100799337472_597563617_n.jpg,"2012-11-03
16:01:17",77535,77535,complete
2,/home/sirfrancis/Scrivania/426091_399325840081636_41223
2381_n.jpg,http://sphotos-d.ak.fbcdn.net/hphotos-ak-
```

```
snc7/426091_399325840081636_412232381_n.jpg,"2012-11-03
16:01:31",68451,68451,complete
```

Dalla versione 26 la lista dei file scaricati è presente nelle tabelle download, downloads_url_chain sempre del database History.

```
sqlite> SELECT datetime(((downloads.start_time/1000000)-
11644473600),"unixepoch", "localtime"), downloads.target_path,
downloads_url_chains.url, downloads.received_bytes, downlo-
ads.total_bytes FROM downloads, downloads_url_chains WHERE
downloads.id = downloads_url_chains.id;
2014-01-22 12:04:58|/home/mirco/Scaricati/26131.c|http://www.exploit-
db.com/download/26131|4705|4705
2014-01-22 12:04:58|/home/mirco/Scaricati/26131.c|http://www.exploit-
db.com/download/26131/|4705|4705
2014-01-22 14:25:54|/home/mirco/Scaricati/02-Vulnerabilita_applicazioni-
parte3.pdf|http://weblab.ing.unimo.it/Lucidi_Sicurezza/02-
Vulnerabilita_applicazioni-parte3.pdf|760370|760370
```

4.17 Dati cancellati

Per esaltare i dati latenti utiliziamo il software exteundelete[8].

Poiché questi lavora solo sulle partizioni, con il comando dd estrarremo le singole partizioni d'interesse per l'indagine.

```
/media/evidence/HD01/raw % sfdisk -l -uS sdb.dd
Disk sdb.dd: cannot get geometry
Disk sdb.dd: 1044 cylinders, 255 heads, 63 sectors/track
Warning: extended partition does not start at a cylinder boundary.
DOS and Linux will interpret the contents differently.
Units = sectors of 512 bytes, counting from 0
   Device Boot   Start      End   #sectors        Id System
 sdb.dd1   *    2048   12810239   12808192   83        Linux
 sdb.dd2    12812286   16775167    3962882    5     Extended
```

(8) - http://extundelete.sourceforge.net/

```
 sdb.dd3          0          -          0     0        Empty
 sdb.dd4          0          -          0     0        Empty
 sdb.dd5   13651968   16775167   3123200    83        Linux
 sdb.dd6   12812288   13651967    839680    82 Linux swap / Solaris
```

Esportiamo la partizione di sistema, cioè la cartella "/"

```
/media/evidence/HD01/raw % dd if=sdb.dd of=sdb.part1.dd bs=512
skip=2048 count=1280819212808192+0 records in12808192+0 records
out6557794304 bytes (6.6 GB) copied, 248.784 s, 26.4 MB/s
```

Esportiamo il file system presente in "/home"

```
/media/evidence/HD01/raw % dd if=sdb.dd of=sdb.part2.dd bs=512
skip=13651968 count=31232003123200+0 records in3123200+0 records
out1599078400 bytes (1.6 GB) copied, 22.2038 s, 72.0 MB/s
```

Esportiamo la partizione di swap

```
/media/evidence/HD01/raw % dd if=sdb.dd of=sdb.part3.dd bs=512
skip=12812288 count=839680839680+0 records in839680+0 records
out429916160 bytes (430 MB) copied, 3.0923 s, 139 MB/s
```

Procediamo sulla prima partizione

```
% file sdb.part1.dd
sdb.part1.dd: Linux rev 1.0 ext4 file system data, UUID=184ea42f-
1bb7-4af7-b4db-0890481d46c9 (extents) (large files) (huge files)
```

Dall'analisi dell'UUID abbiamo conferma che stiamo lavorando sulla prima partizione. Ora recuperiamo i file.

```
/media/evidence/HD01/raw % ./extundelete —restore-all sdb.part1.dd
NOTICE: Extended attributes are not restored.
Loading file system metadata ... 49 groups loaded.
Loading journal descriptors ... 29395 descriptors loaded.
Searching for recoverable inodes in directory / ...552
recoverable inodes found.
Looking through the directory structure for deleted files ...
Unable to restore inode 261809
(var/lib/apt/lists/Debian%20GNU_Linux%207.3.0%20%5fWheezy%5f%20
-%20Official%20i386%20NETINST%20Binary-1%2020131215-
03:38_dists_wheezy_main_binary-i386_Packages): No data found.
```

```
Unable to restore inode 300576
(var/lib/dpkg/updates/0034): Space has been reallocated.
<snip>
```

Per un totale di

```
/media/evidence/HD01/raw/RECOVERED_FILES % ls -R | wc -l
662
```

Così ripartiti

```
/media/evidence/HD01/raw/RECOVERED_FILES % find ./ -type f | grep -E ".*\.[a-zA-
Z0-9]*$" | sed -e 's/.*\(\.[a-zA-Z0-9]*\)$/\1/' | sort | uniq -c | sort -n
1 .110
1 .99
<snip>
533 .gif
569 .bmp
610 .o
968 .h
2110 .c
```

Procediamo analogamente per il file system presente in /home

```
/media/evidence/HD01/raw % file sdb.part2.dd
sdb.part2.dd: Linux rev 1.0 ext4 file system data, UUID=cddf5c90-
df48-4084-b1b2-121a3386cd3a (extents) (large files) (huge files)
/media/evidence/HD01/raw % ./extundelete —restore-all sdb.part2.dd
NOTICE: Extended attributes are not restored.
Loading file system metadata ... 12 groups loaded.
Loading journal descriptors ... 6767 descriptors loaded.
Searching for recoverable inodes in directory / ...
199 recoverable inodes found.
Looking through the directory structure for deleted files
...
Unable to restore inode 1382 (mario/.config/dconf/user.VQZR9W):
Space has been reallocated.
Unable to restore inode 68 (mario/.cache/tracker/no-need-
mtime-check.txt.DFSI9W): Space has been reallocated.
```

```
Unable to restore inode 455 (mario/.cache/keyring-
EDp2ia/control): No undeleted copies found in the journal.
Unable to restore inode 715 (mario/.cache/keyring-
EDp2ia/gpg): Space has been reallocated.
```

Per un totale di

```
/media/evidence/HD01/raw/RECOVERED_FILES % ls -R | wc -l
34
```

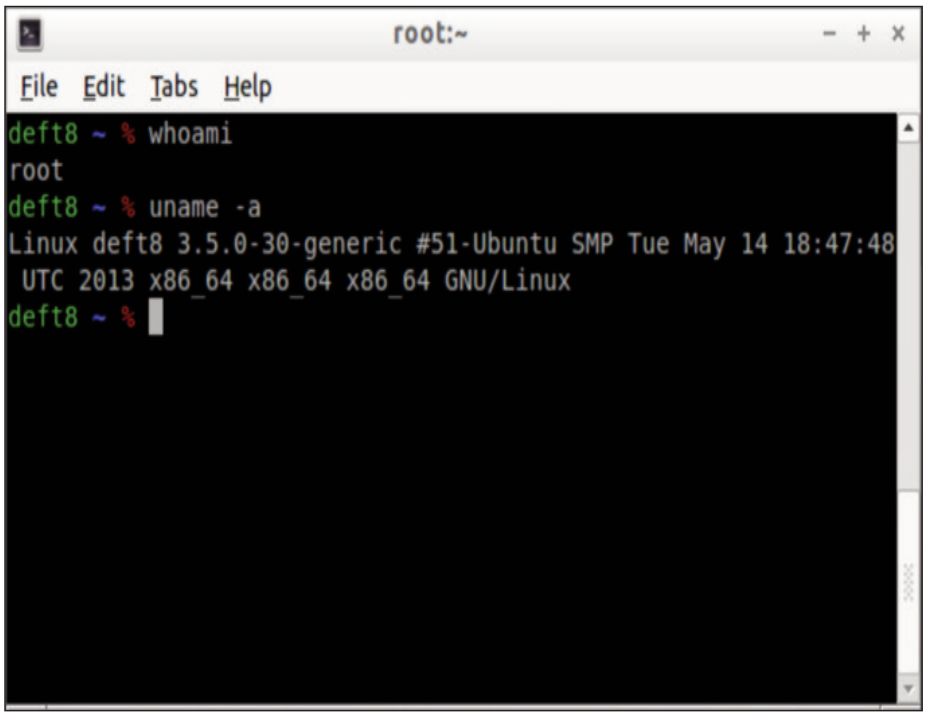
così ripartiti

```
/media/evidence/HD01/raw/RECOVERED_FILES % find ./ -type f | grep -E ".*\.[a-
zA-Z0-9]*$" | sed -e 's/.*\(\.[a-zA-Z0-9]*\)$/\1/' | sort | uniq -c | sort -n
   1 .1052
   1 .1122
<snip>
   1 .940
   1 .IBD39W
   1 .log
   1 .P48qZ8
   1 .pl
   1 .pset
   1 .writeability
   2 .cache
   2 .js
   2 .png
```

Per recuperare i file presenti nell'are di swap utiliziamo PhotoRec.

```
~/evidence/testdisk-6.14 % ./photorec_static /log
/media/evidence/HD01/raw/sdb.part3.dd
PhotoRec 6.14, Data Recovery Utility, July 2013
Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org
PhotoRec 6.14, Data Recovery Utility, July 2013
Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org
```

```
Disk ../sdb.part3.dd - 429 MB / 410 MiB (RO)
    Partition        Start     End   Size   in        sectors
  P Linux SWAP 2     0         0     1     52 68 16    839680
53 files saved in /root/evidence/RECOVERED_FILES_Part3/recup_dir directory.
Recovery completed.
```




```
You are welcome to donate to support further development
and encouragement
http://www.cgsecurity.org/wiki/Donation
```

di cui

```
../RECOVERED_FILES_Part3 % find ./ -type f | grep -E
".*\.[a-zA-Z0-9]*$" | sed -e 's/.*\(\.[a-zA-Z0-9]*\)$/\1/'
| sort | uniq -c | sort -n
   1 .xml
   3 .elf
   50 .txt
```

	NOME COMANDO	FUNZIONE	POTENZIALITÀ	LIMITAZIONI/OSSERVAZIONI
1	`fsstat`	dettagli dei file system presenti	Descrizione metadati e contenuto	non accuratezza data/orario. Può essere sostituito dai comandi: - `dumpe2fs` in un contesto *post-mortem* - `tune2fs` su un sistema live
2	`mount`	Monta un disco fisico e volume logico	Verificare la lista dei dispositivi connessi alla workstation	In alternativa è possibile usare il comando `losetup` che crea dei device "virtuali"
3	`fdisk`	Manipolatore della tabella delle partizioni per Linux	Con il parametro-l fornisce la dimensione: - del disco/volume montato e le rispettive partizioni - del data unit	In alternativa è possibile usare sia il comando `sfdisk I -l -uS`, che `mmls -M` in modo tale da ottenere anche le partizioni vuote
4	`hdparm`	Consente la modifica avanzata dei parametri funzionali dei disposibivi ATA/IDE (hard disk, lettori cd/dvd)	Consente di ricavare informazioni relative all'hardware oggetto di analisi	Numeri seriali non sempre forniti correttamente
5	`md5sum`	Verifica l'integrità del contenuto informativo tramite l'algoritmo MD5	Funge da "sigillo elettronico"	Rischio di potenziali conflitti, il quale viene mitigato se combinato con l'algoritmo SHA1, il quale viene implementato mediante il comando `sha1sum`
6	`dcfldd`	Consente di realizzare un *forensic container* di tipo raw	Parallelizza le attività di copia e *multihashing*	*Fault tolerant* poco efficace non rende subito il *forensic container* in sola lettura
7	`cat`	Concatena i suoi ingressi e li scrive sullo standard output	Consente, tramite concatenazione, di realizzare un *forensic container* monolitico di tipo *raw*	Può essere sostituito dal comando affuse
8	`xmount`	Crea un file system virtuale usando FUSE, che contiene una rappresentazione virtuale dell'immagine del disco in ingresso.	Consente di emulare un *forensic containe*r in formato EWF come raw, VDI, …	
9	`img_stat`	Fornisce informazioni sulla tipologia di forensic container e rispettiva dimensione		

10	`dmesg`	Visualizza sullo *standard output* i messaggi contenuti nel buffer del kernel del sistema operativo		Verboso se non combinato con `grep`
11	`grep`	Ricerca in uno o più file (testo o binari) le linee che corrispondono ad uno o più modelli specificati con espressioni regolari o stringhe letterali		Va in crash su grosse mole di dati
12	`uname`	Mostra sullo standard output informazioni sul computer in uso e sul sistema operativo installato, quali ad esempio il tipo e la versione del sistema operativo installato, l'architettura del computer e il suo nome in rete		Solo su sistema live
13	`date`	Fornisce informazioni sulla data ed ora del sistema	Verifica le impostazioni del fuso orario	Solo su sistema *live*. In un contesto post-mortem viene sostituto dal comando `zdump`
14	`find`	consente la ricerca di file sulla base di: - nome - metadati…		
15	`blkid`	Estrapola informazioni da un dispositivo suddiviso in blocchi	Consente di ricavare gli UUID dei *file system* montati sulla macchina reale	
16	`who`	Fornisce informazioni sulle attività di *login*	Consente di ricavare le date di accensione e spegnimento della macchina	Solo su sistema *live*. In un contesto post-mortem viene sostituto dal comando `last reboot`
17	`sqlite3`	Consente di gestire *database sqlite*		
18	`wget`	Consente di acquisire una risorsa dal Web da riga di comando		
19	`file`	Fornisce informazioni sulla tipologia di file	Utile per rilevare eventuali attività di *antiforensics* (es. cambio estensione)	

Tabella 1 *Riassunto dei principali comandi*

5. Conclusioni

Come anticipato, non essendo l'intenzione quella di redigere una trattazione approfondita dell'argomento, si è proceduto con una panoramica teorica delle potenzialità delle indagini su sistemi Linux, seguita da un caso pratico di applicazione di alcuni dei metodi e strumenti illustrati. L'argomento è troppo vasto per poter entrare nei dettagli e si è quindi preferito fornire una panoramica d'insieme rendendo così il lettore autonomo nell'approfondimento delle aree di maggior interesse.

Purtroppo la bibliografia, nell'ambito della Forensics di sistemi Linux, è davvero poca e ove presente è piuttosto datata, quindi si ritiene superfluo fornire riferimenti a fonti di informazione per la Linux Forensics. I forum e le mailing list sono certamente una buona fonte di approvvigionamento per chi desidera approfondire: tramite motori di ricerca si troveranno le principali e quelle secondarie e minori. Alcune organizzazioni come il SANS pubblicano talvolta dei saggi su argomenti specifici e alcuni dei ricercatori hanno scritto alcuni approfondimenti interessanti su Linux e il suo file system.

LA NECESSITÀ DI DOTARSI DI UNA CAPACITÀ DI POLIZIA ROBUSTA NELLE MODERNE MISSIONI DI *PEACEKEEPING* E LE SUE SFIDE

Paolo NARDONE

Generale di Brigata
Direttore del Centro Eccellenza Stability Police Units
Vicenza

1. Introduzione

Kofi Annan, da Segretario Generale delle Nazioni Nite, lamentava il fatto che l'ONU fosse l'unica organizzazione che, per costituire il corpo dei vigili del fuoco, attendeva che venisse dichiarato l'incendio.

Ban Ki-Moon, da Segretario Generale dell'ONU, ha preso atto che, nel corso del tempo, la componente di polizia è quella che ha più rapidamente e massicciamente aumentato non solo le missioni ed il personale, ma anche le competenze ad essa assegnate. Questo è stato possibile perché innanzi alla mancanza di sicurezza che affligge i paesi usciti da conflitti o afflitti da gravi crisi interne, solo una adeguata componente di polizia robusta può consentire di svolgere i compiti assegnati dal mandato anche agli altri assetti della missione. Organizzazioni Internazionali diverse hanno riconosciuto l'intrinseco valore delle unità di polizia di stabilità, e seppur con nomi diversi ed assegnando loro compiti in parte diversi hanno condiviso un percorso comune in materia negli ultimi due decenni.

2. Operazioni di supporto alla pace e funzioni di stabilizzazione della componente di polizia

Le operazioni di supporto alla pace si inscrivono in un quadro in cui pace, sicurezza, rispetto dei diritti umani e sviluppo si intersecano in modo inestricabile, influenzandosi a vicenda.

Il ruolo riservato alla componente di polizia è, analogamente a quanto avviene nell'espletamento delle proprie funzioni in patria, quello di servire la comunità e di proteggerla. I compiti che sono stati assegnati a tale componente si sono progressivamente ampliati ed arricchiti nel corso degli ultimi vent'anni.[(1)]

Il persistere di conflitti in molti paesi in via di sviluppo fa sorgere delle domande circa le modalità più appropriate per assicurare pace e stabilità al fine di consentire parallelamente sviluppo sociale e crescita economica[(2)].

A livello di organizzazioni internazionali a carattere regionale, pure la dottrina dell'Unione Europea enfatizza il ruolo cruciale che lo sviluppo economico e sociale rivestono nell'assicurare pace e stabilità[(3)].-

(1) - Vedi per quanto concerne le mission delle Nazioni Unite UN DPKO/DFS Policy on UN Police in Peacekeeping and Special Political Missions, 1 febbraio 2014, pagg. 3-4 punti 6,7 e 9.

(2) - Vedi: "The causes of conflicts and the promotion of durable peace and sustainable development in Africa report". UNSG Kofi Annan. New York 1998.

(3) - Fin dall'adozione della EU's Security Strategy nel 2003, è stato riconosciuto che: "Security is a precondition to development."

Ogni analisi sui modelli di polizia di stabilità più idonei ad assicurare ordine e sicurezza pubblica e rispetto dei diritti umani fondamentali nelle aree di crisi non può ignorare e prescindere dal fatto che essi vadano inseriti in una cornice di ben più ampio respiro, una prospettiva più vasta e complessa, di cui la componente di polizia e le unità di polizia robusta rappresentano solo un lato, una dimensione della risposta.

L'approccio non può che essere, infatti, olistico nella consapevolezza del rilievo che tutte le componenti e tutti gli attori presenti in una missione di *peacekeeping* rivestono una importanza fondamentale. Nelle missioni integrate ogni elemento concorre a comporre un tassello del mosaico, nello sforzo complessivo per raggiungere un obiettivo condiviso.

L'aumento del numero di operazioni di mantenimento della pace in ogni area del globo, ed all'interno di esso l'aumento esponenziale della componente di polizia[(4)] ha messo in luce il bisogno della comunità internazionale di dotarsi della capacità di condurre delle complesse operazioni di supporto alla pace volte a mantenere o a ristabilire la sicurezza.

Si è avvertita come sempre più pressante la necessità di ampliare l'approccio, specie dopo l'*Agenda for Peace* del 1992, coinvolgendo tutte le componenti. Nel contempo alla componente militare veniva richiesto un sempre maggior coinvolgimento nel campo della stabilizzazione e delle sicurezza nelle aree di crisi o addirittura la imposizione *manu militari* dei deliberata del Consiglio di Sicurezza delle Nazioni Unite. Questo avveniva dopo i fallimenti degli anni novanta, in Bosnia e Ruanda, con il ripensamento complessivo delle attività di *peacekeeping* e l'elaborazione del c.d. Brahimi Report[(5)].

E' emerso, con sempre maggior chiarezza, che la stabilità e la sicurezza sono precondizioni imprescindibili al fine di poter assicurare ad un qualsivoglia paese benessere economico, pace sociale ed equilibrio politico.

La credibilità di una missione, nel senso di capacità di adempiere al mandato assegnato, in specie nell'assicurare una cornice di sicurezza adeguata, è

(4) - Vedi UN Peace Operations, Integrating Human Rights in UN Police Component Good Practioce and Lesons Learnt, 2013, pag 7: "UN Police the fastest growing component whithin UN peace operations".

(5) - UNGA, Report of the Panel on United Nations Peace Operations (The Brahimi Report), 2000.

venuta ad aggiungersi ai principi fondamentali che sorreggono le missioni di pace già elaborati dalla dottrina nel periodo precedente, e segnatamente: il consenso, l'imparzialità e il non uso della forza o l'uso minimo della forza nel caso della legittima difesa di se o di terzi. Le condizioni che suggeriscono lo schieramento di una missione di stabilizzazione possono sorgere sia prima che le tensioni si tramutino in un conflitto (c.d. *conflict prevention*), sia dopo che questo abbia avuto luogo. (c.d. *peacekeeping e peacebuilding*).

La comunità internazionale ha dato, nel corso del tempo, un rilievo sempre più ampio alla sicurezza ed alla protezione dei civili, anche superando la precedente concezione di protezione dei civili quale mera difesa da attacchi imminenti alla incolumità fisica ed alla vita delle persone[(6)].

Conseguentemente, negli ultimi due decenni, le operazioni di supporto alla pace di cui si è fatta carico la comunità internazionale sono aumentate enormemente sia in termini di numero, dimensione e di personale impiegato, che nello specchio di attività e responsabilità ad esse demandate[(7)].

I principi fondamentali che sorreggono tutte le tipologie di moderne operazioni di supporto alla pace[(8)], e non solo quelle onusiane per cui sono stati elaborati e compiutamente inseriti nella rispettiva dottrina, sono: l'imparzialità, il consenso, l'uso della forza solo per la legittima difesa o per la difesa del mandato[(9)], la legittimità, la legalità, la credibilità e la *local ownership*.

---

(6) - Vedi, ad es., A. De Guttry, F. Pagani, *Sfida all'ordine Mondiale*, Ed. Donzelli, Roma, 2002, che nelle pagg. 92-101 indica le tre generazioni di operazioni di supporto alla pace.
Vedi poi il documento *DPKO/DFS Operational Concept on the Protection of Civilians in United Nations Peacekeeping Operations*. In esso il concetto di protezione dei civili è articolato su tre livelli:
- *Tier 1: Protection through political process;*
- *Tier 2: Providing protection from physical violence.*
- *Tier 3: Establishing a protective environment.*

(7) - Vedi *The Protection of Civilians and the Post-Conflict Security Sector. A conceptual and Historical Overview*. Anreas Vogt, Benjamin de Carvalho, Petter Hojem, Marit Arntzen Glad. *NUPI Report Security in Practice,* n. 8, Norwegian Institute of International Affairs. Oslo 2008.

(8) - Fanno ovviamente eccezione le operazioni di peace enforcement in cui manca il consenso delle parti coinvolte nel conflitto o nella crisi nei confronti dello schieramento di una missione.

(9) - Il c.d. Brahimi Report sottolinea la necessità di un mandato più credibile e "robusto" e, corrispondentemente, la necessità di assetti capaci di dare effettività ad attività quali la protezione dei civili. La protezione dei civili è divenuta, conseguentemente, parte dei mandati delle operazioni di pace, consentendo ai peacekeepers di utilizzare la forza per proteggere civili sotto minaccia di attacchi violenti.

Durante le situazioni di crisi, spesso legate a conflitti o ad emergenze umanitarie, si generano sovente delle situazioni "fluide", con una repentina metamorfosi del tessuto sociale, economico e politico, percorso da tensioni emotive, istinti irrazionali, rancori mai sopiti, che vengono facilmente manipolate, e convogliate verso un presunto nemico, facendo leva si elementi classici identitari simbolici e generando gravi minacce nei confronti della popolazione locale. Minacce che di norma non rivestono più il carattere della aggressione militare tipica dei conflitti armati tradizionali[(10)].

Tali minacce a carattere non prettamente militare possono assumere le forme più disparate, dalla generale inosservanza delle leggi di ordine pubblico e pubblica sicurezza, alle vendette trasversali alle tensioni etniche, fino ai crimini più efferati, al disordine civile, alle insurrezioni ed agli attacchi terroristici. Al fine di poter meglio affrontare questa minaccia eterogenea e che non prefigura un confronto armato, si è coagulato un ampio consenso circa il bisogno di avere, in aggiunta alla componente militare che possiede le capacità per far fronte ad attività di combattimento, anche una componente idonea a favorire il processo di stabilizzazione e di ricostruzione[(11)]. Una mera forza militare infatti non è idonea e sufficiente ad assicurare una risposta adeguata in tali scenari[(12)].

Quando gli sforzi della diplomazia internazionale non riescono a prevenire la degenerazione delle tensioni interne, si possono prospettare diversi tipi di scenario, suscettibili di esporre la popolazione a gravi rischi e vulnerabilità, quali:

- prima dello scoppio della guerra, in un contesto di profonda crisi istituzionale, il rispetto della legge e la pace sociale vengono meno, l'apparato giudiziario e le forze di polizia perdono progressivamente la capacità di adempiere ai propri compiti istituzionali e diviene sempre più concreto il rischio di scivolare in una guerra civile o in un conflitto con territori vicini;

---

(10) - Negli ultimi decenni la quasi totalità dei conflitti è rappresentata da conflitti interni e non più da conflitti armati internazionali come nel passato.

(11) - *Aspetti di dottrina militare delle Multinational Specialized Units*, in *RASSEGNA DELL'ARMA DEI CARABINIERI,* Seminar on the Multinational Specialized Units, pagina 174 della versione in lingua italiana e 161 della versione in lingua inglese, Andrea Margelletti.

(12) - *A New Partnership Agenda, Charting a new horizon for UN peacekeeping*, UN DPKO and UN DFS, New York, July 2009, page 38, draws: *Military peacekeeping rarely succeeds without a civilian component - but finding sufficient and highly qualified civilian staff is often as hard, or harder, than finding troops*".

- con lo scoppio di un conflitto, le forze contrapposte non rispettano, nell'uso della forza armata, i principi di distinzione, di proporzionalità, necessità militare e di umanità, causando inaccettabili danni collaterali su vasta scala o attaccando deliberatamente la popolazione civile, o parte di essa, in base ad uno o più elementi scriminanti (etnici, religiosi e/o linguistici);

- la crisi porta al fallimento completo delle strutture statuali ed ad una situazione di totale anarchia in cui gruppi etnici, tribali, religiosi, politici, eversivi o criminali si affrontano in un conflitto senza quartiere e senza regole, ove l'obiettivo principale degli attacchi sono le varie fazioni avverse o la popolazione civile appartenente a gruppi etnici, tribali, religiosi, linguistici, eccetera, opposti[13];

- alla cessazione del conflitto, che può essere sia interno che internazionale, o al cambiamento radicale di un regime che ha governato il paese per un tempo relativamente lungo, la fazione uscita vittoriosa dallo scontro armato o dalla rivoluzione, che è riuscita a sconfiggere o spodestare la controparte, utilizza le potestà di governo senza fornire alcuna tutela, nel nuovo assetto di potere, agli appartenenti al gruppo della parte soccombente.

Nel corso di un conflitto, o in una situazione di grave crisi, le opposte fazioni riescono a concordare una tregua, un cessate il fuoco o un accordo di pace, che abbisogna però di un supporto esterno, in funzione di garanzia o di rafforzamento delle capacità, per essere consolidata.

Le varie organizzazioni internazionali impegnate nelle missioni di supporto alla pace hanno elaborato proprie dottrine di riferimento per intervenire in questi vari scenari, sia prima che durante e dopo l'esplosione di un conflitto[14].

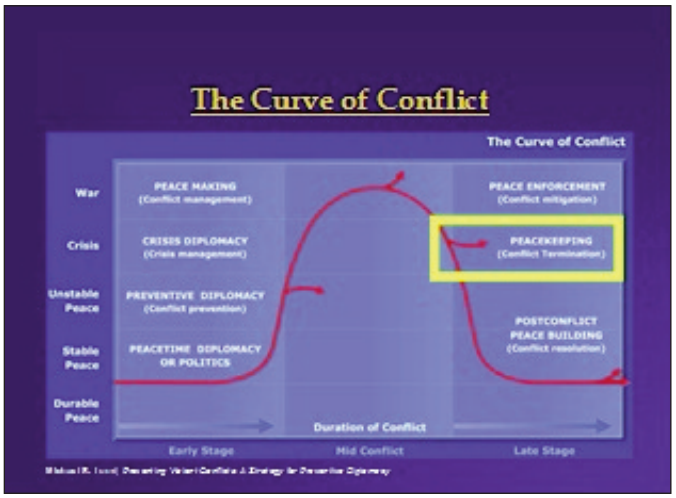
---

(13) - Si pensi ad esempio alla crisi libica e, prima di essa alla perdurante crisi in Somalia.

(14) - Con riferimento al *crisis management,* ad esempio, il nuovo *NATO Strategic Concept* adottato dai Capi di Stato e di Governo a Lisbona, nel novembre 2010 afferma: "*NATO has a unique and robust set of political and military capabilities to address the full spectrum of crises – before, during and after conflicts. NATO will actively employ an appropriate mix of those political and military tools to help manage developing crises that have the potential to affect Alliance security, before they escalate into conflicts; to stop ongoing conflicts where they affect Alliance security; and to help consolidate stability in post-conflict situations where that contributes to Euro- Atlantic security". The lessons learned from NATO operations, in particular in Afghanistan and the Western Balkans, make it clear that a comprehensive political, civilian and military approach is necessary for effective crisis management. The Alliance will engage actively with other international actors before, during and after crises to encourage collaborative analysis, planning and conduct of activities on the ground, in order to maximize coherence and effectiveness of the overall international effort.*

Nella fase in cui il conflitto è ancora in corso ed ove le parti in conflitto non fornissero il loro consenso allo schieramento della missione, non si tratterebbe di una operazione di supporto alla pace, ma di imposizione della pace. In tale circostanza il ruolo della componente di polizia non potrebbe che essere molto limitato e marginale, a favore della componente militare. Tutt'al più potrebbe ritagliarsi uno spazio la componente di gendarmeria, sotto comando e controllo del comandante della forza della componente militare.

La gran parte delle moderne operazioni di supporto alla pace contemplano l'intervento della comunità internazionale, con il coinvolgimento più ampio possibile dei diversi attori, per stabilizzare il paese ed assicurare la necessaria assistenza nell'immediato dopoguerra, non appena le parti coinvolte nel conflitto siglano, una tregua, un cessate il fuoco o un accordo di pace ed acconsentono (o meglio direttamente richiedono), alla comunità internazionale di schierare una missione sul terreno.



La curva del conflitto di M.S. Lund

Nell'analisi del modello che rappresenta il *continuum* tra la destabilizzazione, la guerra, e il percorso verso una pace sostenibile, è possibile identificare diversi punti potenziali di ingresso per l'intervento della comunità internazionale così come di uscita.

Un sistema flessibile, sia per il coinvolgimento internazionale sia per la rimessione della gestione della crisi nelle mani delle autorità locali[15].

Nello svolgimento di una missione di supporto alla pace, per una adeguata risoluzione delle varie emergenze che si possono presentare, occorre far ricorso all'impiego di tutto l'ampio spettro di strumenti, mezzi, personale messi a disposizione dalle autorità nazionali e dai partner internazionali. Dall'assistenza umanitaria, alla ricostruzione, al supporto alle attività di combattimento qualora necessario, alla realizzazione di un quadro di sicurezza ed ordine pubblico adeguato, alla riforma e riorganizzazione degli apparati di sicurezza, alla smobilitazione, disarma mento e reintegrazione degli ex combattenti, fino alla facilitazione della riconciliazione tra le popolazioni locali o tra gruppi dislocati in diverse aree del territorio, alla gestione degli sfollati e dei rifugiati, fino all'assistenza al loro ritorno e ristabilimento nei luoghi di origine, favorendo il processo di ricostruzione dell'architettura sociale, economica e politica nella fase di transizione verso una governance locale riconosciuta come legittima dalla gran parte della popolazione, ad esito di un processo elettorale corretto, democratico e trasparente.

Le esperienze recentemente maturate nei vari teatri di operazione hanno evidenziato come i casi in cui gli obiettivi di carattere prettamente militare sono stati concepiti, nel quadro complessivo delle operazioni, come separati rispetto agli obiettivi posti dalle altre attività (diplomatici, civili, economici, ecc…), l'obiettivo politico finale (una pace duratura), si palesa estremamente difficile da aggiungere.

La comunità internazionale è arrivata quindi a trovare un certo consensus sulla necessità di perseguire un approccio integrato, con una visione olistica (c.d. *comprehensive approach*) ed a pianificare la fase della ricostruzione e dello sviluppo delle capacità delle autorità locali fin dai primi istanti della missione.

Una raccomandazione da indirizzare ai responsabili dei processi di pianificazione per la gestione delle situazioni di crisi è di iscrivere le attività di peace

(15) - Tratto da:*Policekeeping to Peace: Intervention, Transnational Administration and the Responsibility to do it right*, Graham Day and Christopher Freeman, working paper, September 2003: "*By studying the model of the continuum from war to sustainable peace, one can identify potential entry and exit points for intervention by the international community, a system of trigger and release points of engagement*".

building e quelle di nation building in un quadro strategico ed operativo più ampio, onnicomprensivo e non meramente come una seconda fase del tutto indipendente, concepita e condotta solo al termine delle ostilità una volta ottenuta la stabilizzazione del paese affetto dalla crisi[(16)].

Presupposto fondamentale per la realizzazione sul campo di un approccio integrato è la sussistenza di condizioni minime di sicurezza (c.d. *safe and secure environment*). E' evidente infatti che questo è un prerequisito rispetto allo schieramento di componenti non militari.

Il concetto di stabilizzazione si è evoluto nel corso del tempo. Dalla mera osservazione del rispetto di una tregua, come è stato per le prime missioni di *peacekeeping* in medio oriente e per quella ancora in atto tra Pakistan ed India, è maturata sempre più forte la consapevolezza di doversi dotare di una capacità di *peacekeeping* "robusto". Questo punto in particolare è stato al centro delle discussioni e degli sviluppi dottrinali nel corso degli ultimi 20 anni.

Il principale attore internazionale in tema di *peacekeeping*, le Nazioni Unite, ha seguito un percorso analogo a quello delle organizzazioni internazionali a carattere regionale. Le operazioni di mantenimento della pace dell'ONU si sono rapidamente e progressivamente estese, specie nell'ultimo decennio e continuano ancora ad evolversi.

I conflitti contemporanei sono soprattutto conflitti interni e non più a carattere internazionale, sono rivolti piuttosto al controllo della popolazione, delle risorse, del territorio. Le parti più vulnerabili della popolazione, quali donne e bambini, vengono deliberatamente fatti oggetto di attacchi dal gruppo etnico, linguistico o religioso avverso. La tradizionale presenza statica di forze sul terreno con compiti di osservazione e di monitoraggio circa il rispetto di quanto convenuto negli accordi di pace[(17)] o di interposizione, non rappresenta più lo strumento più idoneo per stabilizzare una situazione.

---

(16) - *Aspetti di dottrina militare delle Multinational Specialized Units*, in *RASSEGNA DELL'ARMA DEI CARABINIERI*, Seminar on the Multinational Specialized Units, 2004, pag. 175 della versione in italiano e 160 della versione in inglese, Andrea Margelletti.

(17) - Gli osservatori militari tradizionalmente osservavano il rispetto di tregue, cessate il fuoco o accordi di pace in cui venivano stabilite delle linee di separazione, delle zone di separazione e/o delle aree in cui era interdetto l'ingresso con armamenti pesanti. Inoltre, ovviamente, osservavano il rispetto del cessate il fuoco stesso.

Sebbene i principi cardine del *peacekeeping* rimangono gli stessi: consenso, imparzialità, uso della forza solo per la legittima difesa o in difesa del mandato, si impone nel contempo un mutamento paradigmatico per permettere ai *peacekeepers* di dissuadere o impedire agli oppositori al processo di pace di far deragliare dal sentiero disegnato per la transizione e per affrontare in modo credibile coloro i quali costituiscono una minaccia diretta per la missione o per la popolazione locale.

Come abbondantemente sottolineato nel Rapporto del Panel sulle Operazioni di Pace delle Nazioni Unite (c.d. *Brahimi report*), quando le forze ONU vengono schierate per supportare la pace, devono esser anche capaci di fronteggiare eventuali gruppi che pervicacemente minassero la stabilizzazione ricorrendo ad attacchi armati e violenze nel tentativo di ricondurre al conflitto.

Il contingente deve avere la determinazione e la capacità per sconfiggere tali avversari. Infatti, ogni qualvolta forze vengono schierate in operazioni di pace sorge la legittima aspettativa in seno alla popolazione di essere da loro protette[(18)].

Il punto cardine e qualificante di tali principi è che la sicurezza rappresenta il fondamento e la precondizione dalla quale discendono e dipendono tutti gli altri aspetti delle operazioni di pace e le attività di stabilizzazione. Purtroppo, invece, numerose missioni internazionali di pace hanno evidenziato, a causa delle difficilissime condizioni sul terreno, dei deficit consistenti proprio sul piano della pubblica sicurezza.

(18) - *Robust peacekeeping: exploring the challenges in doctrine, commitments and conduct of operations*, UN. Report on Wilton Park Conference WP973 14 – 16 May 2009 , New York: *UN peacekeeping operations have rapidly expanded over the last decade, and are constantly evolving. Contemporary conflicts are overwhelmingly intra-state, not inter-state disputes, involving competition for control of population as much as territory, and deliberate targeting of the most vulnerable, women and children. A traditional static presence of peacekeeping forces to observe and monitor compliance with the end of hostilities is no longer a sufficient response. The fundamental principles of peacekeeping remain the same: consent, impartiality and the use of force only in self-defence or in defence of the mandate. At the same time, a paradigm shift is needed to enable peacekeepers to deter or prevent 'spoilers' derailing peace processes, or those who threaten the mission or local population. As underlined in the Report of the Panel on United Nations Peace Operations (Brahimi report), when UN forces are sent to uphold the peace they must be prepared to confront the lingering forces of war and violence, with the ability and determination to defeat them. Whenever there is a UN presence, local people have an expectation it will provide protection.*

Le lezioni apprese dalla comunità internazionale nella gestione dei vari teatri di operazione, *in primis* con le stragi di Srebrenica e il genocidio in Ruanda, per quanto attiene al mandato ed alla capacità di adempierlo, hanno anche identificato delle evidenti mancanze, dei gap di sicurezza, tra la componente civile e quella militare. Vuoti di capacità che hanno rischiato di compromettere l'intera missione di pace.

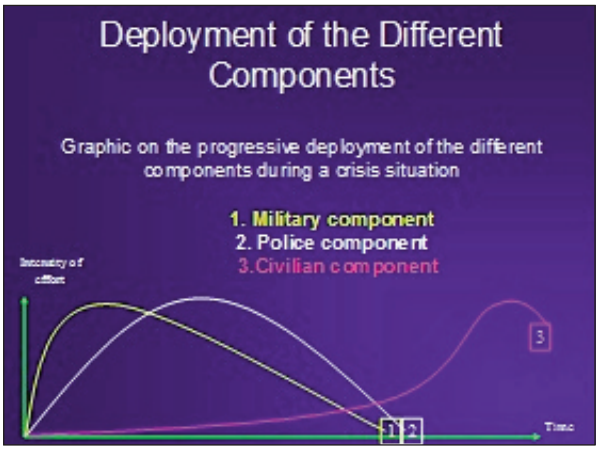
Le missioni di polizia, o il ruolo della componente di polizia nelle missioni integrate, vengono considerate cruciali nella gestione delle crisi, tuttavia si trovano innanzi delle sfide immense, essendo chiamate, al contempo, a gestire la crisi nell'immediato e pure a contribuire allo sviluppo ed alla democratizzazione nel più lungo termine[(19)].

In linea di massima, lo schieramento delle tre componenti in una missione di pace segue una sequenza logica e cronologica. Anzitutto la componente militare assicura una adeguata cornice di sicurezza, quindi la componente di polizia assicura le funzioni di ordine pubblico e pubblica sicurezza nel rispetto delle leggi (c.d. *law and order*), ed infine la componente civile avvia il processo di ricostruzione del paese. Più che di una successione con fasi distinte, si tratta del contributo, in termini di sforzo relativo, dato da ciascuna componente in un continuum temporale.

Nel caso di una missione in cui l'apparato di sicurezza del paese ospite è totalmente collassato e l'ambiente, se non ostile, è quanto meno poco permissivo, si ha anzitutto il dispiegamento in teatro della componente militare. Essa si articola, di norma, in tre stadi: pacificazione, stabilizzazione e rinnovamento istituzionale. Nell'ambito della prima di queste fasi la sicurezza (c.d. *safety and security*) è assicurata dai militari del contingente internazionale di pace, la seconda fase vede invece l'ordine pubblico e la pubblica sicurezza gestiti o da una forza di polizia internazionale (dotata di poteri esecutivi oppure solo in supporto alle autorità locali) o da un corpo di polizia *ad interim* che nel tempo sarà destinato a subire una importante trasformazione nell'ambito della più complessiva riforma del settore della sicurezza, ed infine, all'ultimo stadio, tali fun-

(19) - Tratto da: *From Congo to Kosovo*, ANNIKA HANSEN, IISS: *The lessons learned by the International Community in managing the peacekeeping operations have identified security gaps between military and civilian that have repeatedly jeopardized stability operations. The police missions are considered crucial in civilian crisis management, but they are challenged because they are tasked both with immediate crisis management, and with developmental assistance and democratization.*

zioni saranno assicurate da una ricostituita polizia locale ed un ruolo preminente viene ricoperto dalla componente civile, che assiste le autorità locali nel loro sforzo di profonda riorganizzazione gli apparati statuali[20].



Talvolta, invece, la comunità internazionale preferisce - o comunque sceglie - di inviare una missione politica, oppure una missione dedicata esclusivamente allo sviluppo delle capacità, senza dotarla, quindi, di compiti esecutivi e senza seguire la successione logico-temporale suindicata.

Tuttavia, spesso per le materiali condizioni che si hanno sul terreno alla fine del conflitto e per la elevata volatilità delle condizioni ambientali, dello scenario, per l'elevato rischio, il personale che viene schierato nella primissima fase è personale militare con capacità di combattimento. Non va trascurato che a fronte di elevate capacità prettamente militari, tali forze spesso ha dimostrato di non possedere le specifiche capacità di per gestire i non combattenti[21].

(20) - Tratto da: *Democratizing the Police Abroad: What to Do and How to Do It. Issues in International Crime*" David H. BAYLEY. U.S. Department of Justice Office of Justice Programs. June 2001, pag. 53 :T*he sort of peacekeeping that occurs in complex emergencies, where intervention begins with military action, has three stages: pacification, stabilization, and institutionalization. During the first phase, public security is provided by the international military; in the second, it is provided either by an international police force or by an interim local police; and in the third, it is provided by a reconstituted local police.*

(21) - Vedasi: *Policing Post Conflict Cities*, Alice HILLS, Zed Books ltd. London and New York. 2009: *the circumstances in which conflict ends and the volatility of the environment mean that the troops involved are usually war fighters. Additionally their transitional skills may be unequal to the demands of managing non-combatants.*

Oltre a dover avere piena consapevolezza delle effettive potenzialità, ruolo e funzioni di ciascuna delle tre diverse componenti, la comunità internazionale deve assolutamente essere capace di schierarle molto rapidamente nel teatro di operazioni, onde evitare la creazione, a causa del ritardo, di vuoti di potere che potrebbero successivamente comportare l'impossibilità di raggiungere gli obiettivi assegnati alla missione.

Infatti, quando in una stato l'intero ordinamento istituzionale collassa e le autorità sono incapaci o non hanno la volontà e la determinazione per esercitare con effettività i poteri esecutivi, legislativi e giudiziari, viene lasciato un enorme spazio vuoto che, verosimilmente, sarà immediatamente occupato da chi ha la forza per imporsi e cioè dalla criminalità organizzata e da altri sodalizi illeciti o criminali.

Il sistema giudiziario è sovente disintegrato, con obiettive difficoltà di fare riferimento a giudici o procuratori, le forze di sicurezza esistenti sono spesso militarizzate o fortemente politicizzate, il sistema carcerario è collassato e con ciò vi è la oggettiva impossibilità di applicare le leggi esistenti.

Si soggiunge che trattati o accordi di pace, o politiche adottate per adeguarsi a raccomandazioni provenienti dalla comunità internazionale causano una repentina e brusca riduzione degli organici delle forze di sicurezza, talvolta inscrivendosi nel quadro del processo di demilitarizzazione, oppure a causa del vetting che espelle il personale che non riunisce determinati requisiti o perché direttamente legato alle violazioni dei diritti umani perpetrate dal precedente regime, o ancora, perché prima della cessazione delle ostilità erano parte di una forza di occupazione o fondati su criteri di discriminazione etnica[(22)].

Mentre la componente militare può, nella gran parte dei casi, essere schierata con un termine di preavviso molto ristretto, non vi è una forza di polizia internazionale in grado di schierarsi in tempi rapidi per supportare una operazione di mantenimento della pace.

I poliziotti sono di solito impiegati nei rispettivi paesi di appartenenza, ove sono adibiti allo svolgimento di normali compiti di polizia.

(22) - Vedasi *The Protection of Civilians and the Post-Conflict Security Sector. A conceptual and Historical Overview*, Andreas VOGT, Benjamin DE CARVALHO, Petter HOJEM, Marit ARNTZEN GLAD. NUPI Report Security in Practice nr. 8, Norwegian Institute of International Affairs. Oslo 2008.

Il loro schieramento in teatro di operazioni è alquanto costoso e soprattutto non è tempestivo, anche perché debbono essere reclutati da reparti diversi[23].

Si deve ricordare, inoltre, come i poliziotti schierati individualmente[24] svolgono in ambito della missione uno spettro di attività abbastanza limitato. Le attività che li vedono impegnati sono essenzialmente quelle compendiate nell'acronimo SMART (*support, mentor, advise, report e train*). Il concetto di impiego dei poliziotti internazionali sintetizzato in SMART è stato per la prima vota coniato nel 1995, nel manuale sulle linee giuda per i diritti umani dei poliziotti delle Nazioni Unite[25]. SMART significa infatti:

- supporto al rispetto dei diritti umani ed all'assistenza umanitaria;
  monitoraggio sulle autorità locali, sui centri di detenzione e pena, sull'apparato giudiziario e sul rispetto degli accordi per implementare il processo di pace;
- assistenza e consulenza (*Advising e Mentoring*) a favore della polizia locale sulla base degli standard internazionalmente riconosciuti, anche al fine di riformare e ristrutturare l'apparato di sicurezza esistente *in loco*;
- rapportare situazioni ed eventi;
- training/addestramento della polizia locale, con particolare riferimento al rispetto alle corrette procedure di polizia e dei diritti umani fondamentali.

Le attività ricomprese nel concetto SMART erano concepite per essere svolte da singoli ufficiali di polizia, non armati, privi di poteri e funzioni esecutive, coordinati dalla sezione di polizia del Dipartimento delle Operazioni di Mantenimento della Pace dell'ONU. Questo concetto di spettro di attività SMART condusse comunque ad un incremento delle responsabilità riconosciute in capo alla componente di polizia internazionale, offrendo assistenza e monitoraggio in numerose operazioni di pace in cui veniva richiesto alla comunità internazionale di contribuire al processo di ricostruzione dell'architettura istituzionale del paese affetto dalla crisi[26].

---

(23) - Tratto da: *The Protection of Civilians and the Post-Conflict Security Sector. A conceptual and Historical Overview.* Anreas VOGT, Benjamin DE CARVALHO, Petter HOJEM, Marit ARNTZEN GLAD. NUPI Report Security in Practice nr. 8, Norwegian Institute of International Affairs. Oslo 2008. pag 8.

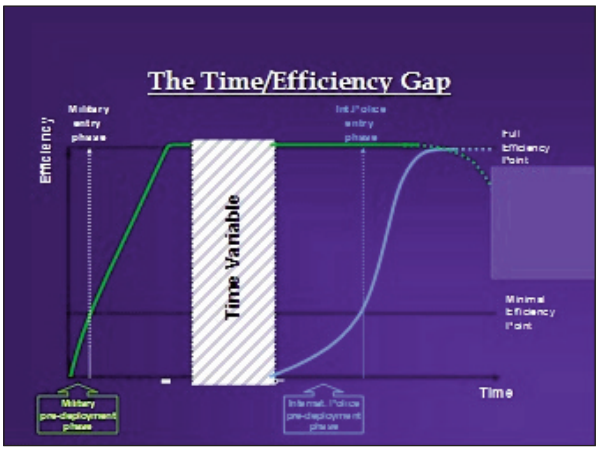
(24) - Generalmente indicati come individual police offiers o CIVPOL.

(25) - UN DPKO Trainer's manual on the human rights basic guidelines for UNCIVPOL, 1995.

(26) - Tratto da: *Policing Peace: The European Gendarmerie Force*, Claudio CATALANO, Marzo 2005 pag. 8. Vedi anche: "EU policing for peace operations: what does it mean?", European Interdependence Research Unit discussion paper 023, Renata Dwan, July 2002.

Per quanto concerne l'approccio della componente di polizia nello missioni di supporto alla pace va altresì rammentato come mobilitare poliziotti da ogni parte del globo (selezionarli, addestrarli, equipaggiarli e schierarli) richiede molto tempo e ciò determina un impatto incontrovertibilmente negativo per l'efficacia della missione[(27)].

Tra lo schieramento della componente militare e quella di polizia vi era, perciò, un chiaro *gap* temporale.



The deployment gap

Per affrontare e risolvere tali sfide e riempire i vuoti di capacità nella componente di polizia occorre sviluppare una dottrina condivisa e predisporre un addestramento specialistico standardizzato. Dottrina ed addestramento che sarebbero direttamente rivolti alla creazione di una capacità da parte della comunità internazionale di schierare rapidamente una componente di polizia robusta ed arricchita con elementi specializzati in grado di svolgere un ampio spettro di funzioni di polizia e dotata di equipaggiamento ed addestramento tali da consentirgli di svolgere al meglio i compiti assegnatigli.

(27) - Ad eccezione della NATO, che si era dotata di una propria capacità anche nello schierare una componente di polizia, sebbene sotto catena di comando militare, almeno fino alcuni anni fa, nessun altro attore sulla scena internazionale si era dimostrato in possesso di capacità di pianificazione e condotta di operazioni a livello strategico, né si era palesato capace di affrontare e gestire sfide su larga scala che coinvolgessero la componente di polizia.

Va sottolineato che ristabilire lo stato di diritto nel più breve tempo possibile costituisce una priorità assoluta, dipendendo ogni passo successivo definito nell'agenda politica e nella pianificazione strategica da esso. Senza stato di diritto lo sviluppo economico, la democratizzazione e lo sviluppo della società civile sono inconcepibili ed inattuabili[28].

L'insieme di queste considerazione ha fatto progressivamente emergere l'idea che fosse necessario generare e schierare una parte della componente di polizia della missione come forza di intervento con peculiarità e caratteristiche sue proprie, idonea a riempire quel gap di sicurezza che altrimenti è destinato giocoforza a manifestarsi nei contesti altamente destabilizzati.

Non si tratta certo di una capacità che può essere espressa da una forza militare tradizionale, orientata al combattimento, alla soppressione di fazioni o gruppi armati che si oppongono al processo di pace, né di una missione di polizia di tipo tradizionale, costituita dalla somma di poliziotti individuali incapaci di gestire minacce significative alla incolumità propria o della popolazione o di fronteggiare situazioni su larga scala come moti di piazza che si possono verificare sul terreno.

Ciò di cui emerge chiaramente il bisogno, è di una organizzazione di polizia robusta, in grado di compiere missioni di polizia con personale ben articolato e strutturato, inquadrato in una chiara linea di comando e controllo, capace di condurre azioni anche con unità organiche e di assolvere compiti altamente specializzati coordinandosi con gli altri elementi dell'unità di polizia di quella missione o con le unità militari presenti, a seconda delle circostanze. In sintesi, vi è bisogno di unità organiche di polizia che riescano a ristabilire ed a mantenere l'ordine e la sicurezza allorquando le forze di polizia locali siano incapaci o non intendano farlo.

Il contesto in cui vengono schierate le moderne missioni di pace è infatti troppo complesso, rischioso, spesso troppo violento per essere efficacemente fronteggiato da singoli poliziotti internazionali schierati individualmente.

(28) - *Policing Post Conflict Cities,* Alice HILLS, Zed Books ltd. London and New York. 2009, page 57. Rule of Law "*Everything else depends on it: a functioning economy, a free and fair political system, the development of civil society and public confidence in police and courts*", "*Bearing in mind that establishing rule of law as soon as possible is the first priority*".

Essi non possono affrontare da soli sistemi giudiziari disintegrati, forze di sicurezza locali altamente militarizzate e politicizzate, o del tutto smantellate, l'assenza di un sistema penitenziario, scontri e dimostrazioni tra fazioni avverse,situazioni di sostanziale anarchia o di mera affermazione della legge del più forte.

E' di tutta evidenza, poi, che l'incapacità o il fallimento nel tentativo di risolvere queste situazioni in modo concreto e tempestivo, è destinato a generare un vuoto di potere che lascia enormi spazi e margini di manovra per le infiltrazioni della criminalità organizzata, di milizie e di altri attori che si oppongono al processo di pace[29].

Alcuni autori sono fermamente convinti che la componente di polizia internazionale non dovrebbe schierare i singoli poliziotti individuali nella missione di pace fino a quando l'area è ancora interessata da combattimenti e sacche di resistenza armata.

Come corollario a tale scuola di pensiero possiamo affermare che delle unità di polizia robusta, ben addestrate ed equipaggiate, che possono essere denominate Unità di Polizia di Stabilità, o meglio, con terminologia anglosassone, *Stability Police Units* o SPU[30], rappresentano lo strumento più idoneo, se non addirittura ottimale, per ridurre i deficit di sicurezza (c.d. *security gap*) che si rinvengono nelle are destabilizzate.

Tali forze - o unità organiche di polizia di stabilità - debbono essere strutturate in modo da poter assicurare la efficace condotta di un ampissimo spettro di operazioni di polizia, che variano dall'imposizione della legge in termini di polizia giudiziaria, fino alla capacità di resistere ad atti ostili o a vincere delle resistenze esprimendo delle capacità di combattimento tipiche della fanteria leggera.

---

(29) - Vedasi: *The Protection of Civilians and the Post-Conflict Security Sector. A conceptual and Historical Overview.* Anreas VOGT, Benjamin DE CARVALHO, Petter HOJEM, Marit ARNTZEN GLAD. NUPI Report Security in Practice, n. 8, Norwegian Institute of International Affairs. Oslo 2008, pag. 7.

(30) - SPU è semplicemente uno schema teorico per indicare in modo onnicomprensivo i diversi modelli attualmente esistenti (MSU, IPU, FPU) che condividono simile struttura e assunti dottrinali. Inoltre SPU è pure l'acronimo delle formed police units schierate dall' UNMIK in Kosovo nel 2000.

The security Gap

E' di tutta evidenza come in fasi post conflitto o comunque di crisi generalizzata dell'ordine pubblico, i gruppi di dimostranti, in mezzo alla folla o servendosi di essa, possono celare delle minacce compiendo improvvisamente degli attacchi, anche armati e ben organizzati, con caratteristiche in tutto assimilabili alle operazioni militari. Questo è uno dei motivi principali per cui uno dei modelli di SPU (*Stability Police Unit*), la *Multinational Specialized Unit* (meglio nota con l'acronimo MSU), possiede delle capacità (in termini di addestramento, equipaggiamento, motorizzazione ed armamento) di fanteria leggera, tali da poter condurre delle operazioni di stabilizzazione risolutive di situazioni ad alto rischio.

Il modo in cui una SPU ricorre allo spettro di possibilità nell'uso della forza è profondamente diverso rispetto a quello di unità che, pur potendo apparire per certi versi simili nella struttura o nell'equipaggiamento, appartengono alla componente militare della missione. La differenza fondamentale risiede nel fatto che mentre la componente prettamente militare è, in linea di massima, autorizzata, addestrata e - si può ragionevolmente presupporre - pronta all'uso della forza letale innanzi ad una possibile minaccia, le SPU, ragionando, per forma mentis, in termini di *amicus-hostis*, avendo una attitudine ed una formazione mentale tipica della forza di polizia, considererà principalmente l'uso di una forza e di mezzi di coazione non letali, anzitutto ricorrendo alla persuasione, alla negoziazione ed alla mediazione.

Pur accogliendo tali assunti, è ben chiaro che anche una SPU, esperiti tutti i mezzi non letali proporzionali alla minaccia, farà uso, in ultima istanza, alla forza letale per difendere se stessa o la popolazione o per adempiere in altro modo al mandato quando previsto.

La SPU, proprio in quanto unità di polizia, possiede nel proprio patrimonio genetico le capacità ed attitudini necessarie per interagire e relazionarsi con la popolazione e con le autorità locali, cementando la fiducia reciproca e costruendo una fattiva collaborazione. Tali qualità trovano origine proprio nel tradizionale modus operandi delle forze di polizia, le quali in ogni contesto sociale ed istituzionale (con l'ovvia eccezione dei casi di degenerazione ed uso distorto a fini politici delle forze dell'ordine) cercano sempre di stabilire una forte, chiara ed aperta relazione e collaborazione con la cittadinanza, animati da spirito di servizio, per svolgere la tipica e quotidiana attività di polizia.

Il Professor Bayley ricorda e ci insegna che una forza di polizia, quando opera in modo legittimo - e ciò vale sia nel proprio paese sia nelle missioni di pace-, deve essere anzitutto:

- disponibile/presente (*available*);
- utile, nel senso di essere capace di risolvere i problemi della popolazione (*useful*);
- comportarsi in modo rispettoso della persona e dei suoi diritti (*respectful*).

L'approccio e la interrelazione con la popolazione e le autorità locali, anche in teatro di operazione, è assolutamente cruciale sotto ogni punto di vista. Per di più, le capacità di raccolta di informazioni, anche con riferimento ad attività o sodalizi criminali e l'idoneità a prevenire la commissione di atti illeciti, che si iscrivono nel circolo della quotidiana attività per ogni agente di polizia, può ben supportare le nuove istituzioni locali, emergenti dal conflitto, in alcune aree molto sensibili e di grande vulnerabilità, consentendo loro di intraprendere le contromisure adeguate per fronteggiare attività o pressioni illecite che se non tempestivamente indirizzate potrebbero considerevolmente minare il percorso di uscita dalla crisi.

Tenendo a mente lo scenario complessivo che ci si trova a fronteggiare nelle fasi iniziali di una missione di pace, un approccio integrato e flessibile tra la componente militare da un lato e quella civile e di polizia (sia locale che internazionale) dall'altro, va considerato come priorità di ordine logico e metodologico.

Per una risposta efficace a delle crisi complesse è opportuno che operino fin dal principio sia la componente militare che quella di polizia, pertanto la loro capacità di interrelazione e di dar luogo ad un processo di pianificazione effettivamente integrato costituisce una indiscutibile priorità. L'interazione tra componente militare e di polizia è fondamentale perché se ruolo e specifici compiti assegnati nel quadro della missione possono essere diversi, essi sono indubbiamente anche complementari e correlati. Volendo ora esaminare quanto è emerso in occasione di gravi crisi internazionali che han indotto allo schieramento di missioni internazionali di pace, come per il Kosovo, la Bosnia, l'Iraq, l'Afghanistan, il Mali e la Repubblica Centrafricana, alcuni fattori di criticità meritano di essere evidenziati:

- la componente militare internazionale ha gestito l'intervento militare ed ha cercato di assicurare un ambiente sicuro per la popolazione;
- in linea di principio, le unità militari tradizionali, si son palesate capaci di affrontare con competenza ed efficacia la sfera attinente l'attività di combattimento di forze contrapposte mentre, invece, si sono rivelate assai meno efficaci nell'assicurare la pubblica sicurezza ed il controllo dei fenomeni criminali;
- le forze dell'ordine dei paesi che hanno ospitato le missioni di pace nella fase post conflitto (e qui l'elenco degli esempi sarebbe veramente lungo), erano del tutto inesistenti, smantellate, corrotte o comunque incapaci e non propense a svolgere i propri compiti istituzionali.

In questi contesti la chiave del successo è rappresentata dal forte consenso interno ed internazionale che la missione può vantare. E' richiesta poi una grande capacità info-investigativa, che permei l'intero specchio di attività della missione, e consenta di identificare e di localizzare gli obiettivi, la guerriglia, i gruppi terroristi, al fine di poterne neutralizzare le capacità operative, di minimizzare il rischio di danni collaterali nella conduzione di operazioni e di focalizzare l'attenzione sul rispetto dei diritti umani e sull'assicurazione alla giustizia di coloro i quali si sono macchiati della loro violazione in modo grave, massiccio e sistematico. Quanto prima va riavviata l'operatività delle forze di polizia locali, che abbisognano di un considerevole sforzo in termini di vetting, di addestramento e di *mentoring*.

Gli sforzi info investigativi richiedono degli assetti di polizia e delle capacità che le *Stability Police Units* possono pure mettere a disposizione, in termini di competenze specifiche, delle autorità civili e della polizia locale per supportarne l'attività.

Nelle operazioni di supporto alla pace, l'ampio spettro delle capacità di polizia (ed in primis quello di proteggere la popolazione civile), che delle unità organiche di polizia riescono ad esprimere anche in contesti altamente destabilizzati è conosciuto come capacità di polizia robusta, o, utilizzando la terminologia anglosassone *robust policing*. Le forze che vengono inviate per sostenere i processi di pace debbono essere in grado di affrontare efficacemente le persistenti sacche di resistenza armata e di violenza, possedendo la determinazione e la capacità per sconfiggerle[(31)].

Ovunque vi sia la presenza di forze dell'ONU o di un'altra organizzazione internazionale che schiera propri *peacekeepers,* la popolazione locale fa legittimo affidamento sul fatto che esse saranno in grado di assicurare loro protezione. Oggi ben 9 delle 16 missioni di *peacekeeping* dell'ONU prevedono ad esempio la protezione dei civili, ad esempio, tra i compiti assegnati dal mandato. La componente di polizia deve essere abbastanza capace ed affidabile per sapersi destreggiare adeguatamente in tale realtà[(32)].

3. Il ruolo di una componente di polizia robusta negli scenari più destabilizzati

Lo scoppio di numerose e disastrose crisi in molte parti del globo è anche e forse soprattutto la conseguenza di profondi mutamenti geopolitici occorsi nella storia recente. La fine della logica dei due blocchi contrapposti, che aveva caratterizzato per mezzo secolo la c.d. Guerra Fredda, ha visto la proliferazione di crisi locali, guerre, atti di terrorismo internazionale sempre più sanguinosi ed eclatanti.

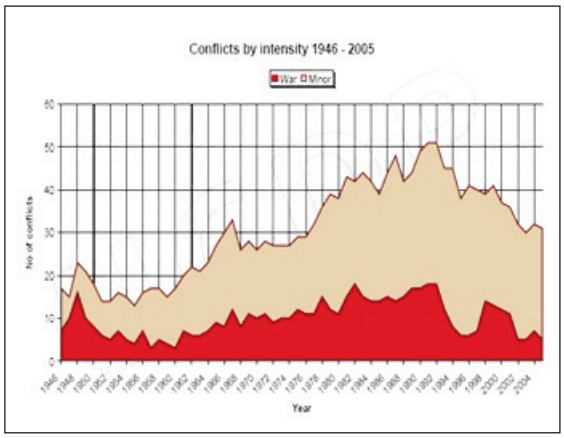
---

(31) - Brahimi Report. Report of the Panel on UN Peace Operations, A/55/305/-S/2000/809 21 August 2000. Le forze ONU che sono inviate per mantenere la pace: *must be prepared to confront the lingering forces of war and violence, with the ability and determination to defeat them.*

(32) - Report on Wilton Park Conference WP973 robust peacekeeping: exploring the challenges in doctrine, commitments and conduct of operations, 14 - 16 May 2009 , New York, riferendosi soprattutto alla component militare ed al concetto di robust peacekeeping scrive: *There is broad consensus that robust UN peacekeeping is not and can never be an instrument of peace enforcement. Rather, it comprises the tactical show or use of force to change behaviour and create conditions for a political process. Thus it is not only a military issue, but a political and economic one. It aims to further a broader strategy to achieve a transition from conflict to peace and strengthen fragile states, a strategy backed by the UNSC and TCCs. It is also an attitude of mind, demonstrating the UN stands firm and is not to be intimidated. A 'strategic guidance note' explaining robust peacekeeping philosophy and response expectations from TCCs would be useful.*

Spesso le attività eversive, terroristiche o i movimenti insurrezionali che hanno dato vita a conflitti interni sono risultati legati a doppio filo con sodalizi criminali impegnati nel traffico illecito di armi, stupefacenti o addirittura - si pensi all'attuale crisi libica - alla tratta ed al traffico di esseri umani[33].

La comunità internazionale si trova così ad affrontare delle situazioni di destabilizzazione sempre più gravi e complesse, con minacce per la sicurezza che talora trascendono il singolo paese in cui si verificano gli scontri armati.



Dalla Guerra ai conflitti a minore intensità ed alle minacce asimmetriche[34]

Questo nuovo panorama e le situazioni di crisi che sono scoppiate nelle più diverse parti del globo, hanno richiesto la predisposizione ed il supporto da parte di un apparato di sicurezza capace di trascendere la risposta a carattere meramente militare nella gestione della crisi, al fine di meglio fronteggiare emergenze mutevoli ed evitare che situazioni di fragilità scivolino verso il riaccendersi o l'aggravarsi di conflitti. E' proprio in capo a tale apparato di sicurezza che va rimessa la responsabilità di neutralizzare e recidere i legami tra reti terroristiche, sodalizi criminali e movimenti eversivi e insurrezionali.

Attori che condividono sovente l'interesse nel mantenere condizioni di marcata instabilità nelle rispettive aree di manovra, sia per i lauti profitti generati per

(33) - Cfr. SINCONI, ALBANO, VOLPICELLI, POLITI, BONIFAZI, *addressing Human Trafficking in Peace Support Operations, Reference Material to design Training Sessions for International Peacekeepers*, in *RASSEGNA DELL'ARMA DEI CARABINIERI*, Roma, 2015

(34) - Fonte: Uppsala University.

alcuni nel corso delle economie di guerra, sia per i consistenti traffici illeciti che nell'era dell'economia globalizzata riescono ad infiltrarsi con maggiore agilità nei vari angoli del globo e sono favoriti dall'assenza di un controllo funzionale e capillare da parte di autorità statuali nel territorio in cui operano. In sintesi, la situazione di instabilità consente alle reti terroristiche di raggiungere il loro obiettivo politico ed a quelle criminali di sviluppare floridi commerci illeciti con i conseguenti imponenti profitti che ne conseguono. Al movimento eversivo o insurrezionale offrono, poi, la prospettiva concreta di un rovesciamento del regime e/o della conquista e del futuro esercizio del potere politico sul territorio. Spesso tali reti sono interconnesse, in una sorta di area grigia, che si supporta ed alimenta reciprocamente, sebbene gli obiettivi finali possano essere anche radicalmente divergenti.

La emersione di scenari operativi in cui reti criminali, movimenti insurrezionali, cellule terroristiche, signori della guerra, milizie private, gruppi religiosi fanatici, si presentano congiuntamente nel medesimo teatro di operazione, ha fatto sorgere nuovi interrogativi circa le risposte che una missione internazionale di pace deve essere in grado di fornire. Lo stesso discorso vale per gli stati falliti, come ad esempio la Somalia e la Libia, ove il collasso delle istituzioni è terreno fertilissimo per tali *peace spilers* (Al Shabaab o Isis che siano). Ciò importa un ripensamento del concetto di *peacekeeping* moderno, che va visto in tutta la sua multiforme poliedricità [35].

(35) - Nel 2015 è in atto il c.d. Brahimi Report II (*High-Level Independent Panel on Peace Operations*) che a settembre 2015 informerà degli esiti l'Assemblea Generale dell'ONU. Vedasi la comunicazione del Segretario Generale dell'ONU datata 31 ottobre 2014: "*The Panel will make a comprehensive assessment of the state of UN peace operations today, and the emerging needs of the future. It will consider a broad range of issues facing peace operations, including the changing nature of conflict, evolving mandates, good offices and peacebuilding challenges, managerial and administrative arrangements, planning, partnerships, human rights and protection of civilians, uniformed capabilities for peacekeeping operations and performance. The last major external review of peace operations was undertaken in 2000 and led by Mr. Lahkdar Brahimi. In addition, this will be the first such panel to examine both peacekeeping operations and special political missions. As we approach the 15-year anniversary of the Brahimi report, we must acknowledge that peace operations today are increasingly called on to confront politically complex and challenging conflicts, often in volatile security environments where operations are directly targeted. We must take stock of evolving expectations and consider how the Organization can most effectively advance peace, assist countries caught in conflict and ensure that our peacekeeping operations and special political missions remain strong and effective in a changing global context. The Panel will work closely with the main UN Departments concerned, as well as with Member States and the UN system as a whole. The Panel's recommendations to me will be available for consideration by the General Assembly at its 2015 General Debate*".

La comunità internazionale si è trovata così a decidere e sperimentare mandati sempre più articolati e complessi, che ponevano al centro la protezione dei civili e la ricostruzione e la stabilizzazione di aree minacciate da conflitti interni o internazionali o da questi appena devastati o che avevano conosciuto la barbarie di regimi sanguinari che avevano violato i più fondamentali ed elementari diritti umani (si pensi al regime talebano in Afghanistan o alle atrocità dell'Isis).

Spesso le guerre o i processi di transizione da regimi totalitari hanno disarticolato l'intero tessuto sociale ed istituzionale del paese, lasciandolo privo di alcuna capacità di assicurare lo stato di diritto con le proprie forze dell'ordine. Da quanto precede si comprende come oggi le vere sfide superino la semplice prevenzione dei conflitti, il supporto nell'assicurare il rispetto di tregue o cessate il fuoco o anche l'intervento diretto per imporne la fine, magari con l'impiego della forza armata, ma sono costituite dalla costruzione di un assetto istituzionale che sia idoneo a mantenere stabilmente nel tempo la pace, basato su relazioni di tipo non violento tra i gruppi esponenziali delle varie anime della società, sull'equilibrio tra poteri ed istituzioni. In sostanza, è necessario essere pronti a stabilizzare dei paesi in cui possiamo essere chiamati ad intervenire, nella consapevolezza che la controparte, o meglio la minaccia da gestire, non proverrà da forze armate tradizionali, ma piuttosto da un variegato insieme di soggetti che hanno peraltro facile gioco nel nascondersi tra la popolazione stessa che siamo chiamati a proteggere.

Le *Stability Police Units* (SPUs) sono chiamate ad intervenire a favore della stabilizzazione dell'area, assicurando il rispetto della legge, l'ordine e la sicurezza pubblica, precondizioni imprescindibili per la ricostruzione del paese, anche supportando il ristabilimento ed il funzionamento delle forze di polizia locale, dell'apparato giudiziario e del sistema penitenziario.

Questo scenario così difficile e ricco di insidie richiede inoltre, ad un tempo, delle competenze di polizia e una elevata capacità di autoprotezione e presuppongono persino la capacità di ingaggiare forze avverse onde resistere ad attacchi o per condurre operazioni ad alto rischio, quali la cattura di criminali di guerra, il disarmamento di fazioni ribelli, la protezione di sfollati da attacchi di bande o milizie.

Durante il manifestarsi di una crisi si possono distinguere diverse fasi, in particolare il passaggio dalla destabilizzazione, al conflitto, alla sigla di una accordo di pace, alla stabilizzazione, fino (idealmente), alla ricostruzione ed alla ripresa della piena funzionalità degli apparati dello stato. In ciascuna fase il ruolo di ciascuna componente varia sensibilmente e l'intensità dello sforzo profuso da ciascuna di esse può essere osservato facendo riferimento alle principali linee di azione che si articolano nel corso del processo.

Il ruolo delle SPU inizia quando le attività di combattimento decrescono o cessano, spesso a seguito della firma di un accordo di pace o di un cessate il fuoco cui hanno aderito le parti precedentemente coinvolte nel conflitto. La funziona principale delle SPU è quella di contribuire al processo di stabilizzazione e ricostruzione, nel grafico rappresentato dalla linea verde. Tuttavia, permane sempre uno sforzo, sebbene di minore intensità, dedicato a supportare la ricostruzione di emergenza (ad esempio i c.d. *quick impact projects*, o le attività di collaborazione civile e militare svolte anche da branche specializzate di SPU quali la *Multinational Specialized Unit*). Del pari un contributo, sebbene indiretto e marginale, viene fornito anche a favore dello sforzo della missione rivolto alla ricostruzione degli assetti istituzionali (specie con riferimento ad attività rientranti nella competenza del ministero degli interni o della giustizia) ed alla c.d *good governance*.

La ricaduta della situazione nel conflitto, anche se sporadicamente, o gravi attacchi al personale della missione stessa, costituisce un freno enorme che giunge quasi a paralizzare tutti gli sforzi di stabilizzazione, ricostruzione, *nation building*, eccetera, causando un ritardo nella tempistica della transizione dei pieni ed effettivi poteri a favore delle autorità locali emerse dopo la crisi, secondo il doppio binario, del passaggio delle funzioni da organismi militari a favore di quelli civili e da organismi internazionali a quelli locali. Tenendo a mente che, in ossequio al principio della *local ownership*, tale transizione dovrebbe avvenire il più presto possibile.

Per questi motivi la nuova e più pressante minaccia è rappresentata proprio dal terrorismo, dalla criminalità organizzata, dai gruppi organizzati che non condividono il processo di pace (c.d. *peace spoilers*), dalla corruzione e da tutti gli altri elementi che hanno un impatto diretto sulla sicurezza.

Se poi tali minacce comportano attività di combattimento, esse di fatto bloccano ed impediscono tutti gli altri sforzi di ricostruzione ed i processi di transizione. A complicare il quadro è la costatazione che spesso si tratta di una minaccia che, sebbene molto pericolosa, non è chiaramente identificabile e quindi fronteggiabile. Questo tipo di aspetti, in cui si fronteggiano parti tra loro assolutamente diverse per organizzazione, mezzi, metodi di combattimento e scopi vengono ricondotti al concetto di guerra o di minaccia asimmetrica. Tali sfide richiedono incontrovertibilmente la presenza in seno alla missione di unità di polizia in possesso di una elevata attitudine nelle indagini criminali.

Nel passato, invece, le forze militari convenzionali si sono dovute misurare con questi elementi combattenti non convenzionali, milizie, gruppi ribelli, guerriglie e gruppi criminali con tutti i limiti più sopra illustrati (e senza neppure mezzi e mandato idonei a farvi fronte). Pertanto, per affrontare e sconfiggere questo nemico sfuggente che si può rinvenire nelle zone di crisi e che può ricorrere a mezzi e metodi asimmetrici di combattimento, è necessario fornire delle capacità addizionali alle forze schierate rispetto a quelle in uso secondo i paradigmi dell'approccio operativo convenzionale, caratterizzato da una prospettiva tipicamente militare convenzionale.

Il tipo di capacità cui ci si riferisce può essere fornito proprio dalle *Stability Police Units*, capaci di raccogliere informazioni e di svolgere attività investigative onde identificare e localizzare gli obiettivi e le forze avverse (terroristi, gruppi criminali, eversivi, ecc..) neutralizzandoli nel pieno rispetto dei principi di proporzionalità e di discriminazione nell'uso della forza. Questi due principi del diritto internazionale umanitario non vanno rispettati solo perché così imposto dal diritto e perché rappresentano imperativi categorici di natura etica, ma anche per la incontrovertibile necessità di mantenere il consenso da parte della popolazione in favore del personale impiegato nella missione di pace.

Una repressione indiscriminata delle forze avverse presenti sul terreno, o azioni che potrebbero lasciare il sapore amaro della rappresaglia, sono verosimilmente destinati a risvegliare istinti vendicativi, desideri di rivincita, sentimenti, propaganda e retorica contrarie alle forze schierate nella missione, giustapponendo la popolazione civile al personale internazionale, con ciò rendendo impossibile il raggiungimento degli obiettivi della missione.

L'accusa di uso eccessivo della forza da parte dei *peacekeepers* dell'ECOWAS[36] in Liberia agli inizi degli anni '90 o il fallimento, per incapacità di agire o meglio di reagire in Bosnia Herzegovina (UNPROFOR), Sierra Leon (UNAMSIL) e Ruanda (UNAMIR) sono a titolo esemplificativo alcuni chiari esempi di come la credibilità della comunità internazionale è stata seriamente compromessa, specie con riferimento al dovere di proteggere i civili[37].

Se è vero, come è vero, che la creazione di un ambiente stabile e sicuro (in linguaggio anglosassone si parla di *safe and secure environment*) rappresenta il principale obiettivo finale di ogni missione, e pertanto il suo raggiungimento o meno determina il discrimine tra una missione che può essere considerata un successo ed una che invece ha fallito nel suo intento, è di evidenza intuitiva che guadagnarsi la fiducia e quindi il consenso della popolazione è una delle necessarie precondizioni indispensabili per realizzare i passi successivi, isolando, se del caso, le piccole fazioni estremiste che non intendono partecipare al processo di pace dalla massa della popolazione.

In questo contesto le SPU offrono, come modello concettuale, uno strumento operativo caratterizzato dall'essere pre-organizzato, robusto e rapidamente schierabile in teatro di operazioni.

In grado di compiere uno specchio amplissimo di compiti di polizia, così come richiesto da ciascun specifico scenario operativo, anche in ambienti ostili e poco permeabili, adatto a stabilizzare situazioni caotiche e destabilizzate ma senza generare sentimenti di odio e desideri di vendetta.

Come si vede, le *Stability Police Units* possono sia, di regola, apportare delle competenze e capacità addizionali, complementari a quelle fornite dalla componente militare nella missione di supporto alla pace di tipo integrato, sia, possono agire indipendentemente, qualora non vi fosse la compresenza della componente militare nell'area.

---

(36) - *Economic Community of Western African Countries.*

(37) - Vedi sul punto *The impossible Mandate?*, Victoria K. HOLT & Tobias C. BERKMAN, *Military Preparedness, The Responsibility to Protect and Modern Peace Operations*, The Henry L. Stimson Center, Washington, 2006, anche con riferimento nel suo incipit alla misione in Sudan.

Importante caratteristica delle SPU deve essere la loro abilità nell'interagire con l'apparato di sicurezza esistente sul posto, che, verosimilmente, potrebbe essere incapace di agire da solo e di svolgere in autonomia le operazioni, e che abbisogna, quindi, del supporto esterno qualificato di queste Unità.

L'azione delle SPU in qualità di supporto operativo alle forze locali, peraltro, consente di eliminare alcuni limiti che si potrebbero rivelare insormontabili in caso di missione con un mandato privo di poteri esecutivi (che, peraltro, costituisce la regola per le attuali missioni di pace se si eccettua, nel recente passato, Timor Est e ancor oggi, seppur solo in modo parziale, il Kosovo).

Il mantenimento dell'ordine pubblico e della pubblica sicurezza, in mancanza di una forza di polizia del paese ospite capace di provvedervi, non va da un lato demandato alla componente militare, per forma mentis, esperienza e per procedure di impiego non usa a farlo, né può essere rimesso ad elementi individuali, come i singoli esperti di polizia, non in grado di provvedere alla propria sicurezza e tanto meno capacità di far fronte ad una manifestazione violenta.

4. L'approntamento di una unità di polizia robusta tipo SPU

Nell'ambito dell'approntamento di una unità di polizia che si prepara per essere schierata come SPU vi sono una serie di attività che si susseguono e che si possono rinvenire a prescindere dall'organizzazione o paese che si appresta a inviare tale tipo di unità. Esse sono:

- attività preliminari (tra cui la raccolta di informazioni, comprese quelle relative alla copertura finanziaria ed allo stato degli assetti da mettere a disposizione dell'organo competente a prendere decisioni in merito allo schieramento di una SPU);

- missione in area per raccogliere direttamente informazioni in loco (*Fact Finding Missions o Technical Assessment Mission*)[38];

(38) - Queste missioni vengono svolte sia prima di schierare una intera missione sia prima di schierare una singola SPU, per poter raccogliere gli elementi informativi di rispettiva competenza.

- l'esatto inquadramento legale, anche con riferimento alla presenza di una mandato che autorizzi la missione e poi lo schieramento di una SPU[(39)] e, se del caso, l'adozione di strumenti giuridici che rendano chiaro lo *status* giuridico delle forze schierate, compresi privilegi ed immunità del personale impiegato;

- la pianificazione strategica[(40)], in cui deve essere chiara non solo la effettiva situazione sul terreno e la missione da assegnare agli assetti che saranno schierati, ma anche quale è l'intento e lo schema di manovra che si intende seguire, attribuendo i diversi compiti secondo una tempistica precisa, onde conseguire il raggiungimento dell'end state (e deve inoltre disegnare da subito una exit strategy ed indicatori per la transizione);

- la decisione di schierare una (o più) SPU[(41)];

- la nomina di un Police Commissioner (e di un *Deputy chief of operations* per FPUs nelle missioni onusiane)[(42)] o di un *Force Commander* (per le MSU o IPU nella ipotesi che quest'ultima venga schierata sotto catena di comando militare);

(39) - *In primis* la decisione dell'organo politico competente ad autorizzare la missione, come ad esempio la Risoluzione del Consiglio di Sicurezza dell'ONU o la *Council Decision* (già *Joint Action*) del Consiglio Europeo o il Communiqué del Peace and Security Council dell'Unione Africana o ancora la decisione del North Atlantic Council. Vedasi UN DPKO United Nations Peacekeeping Operations Principles and Guidelines (*Capstone Doctrine*) 2008, pagG. 13-14; United Nations Force Headquarters Handbook, novembre, New York, 2014, pag. 2. Tutte le organizzazioni internazionali, NATO inclusa, riconoscono una *primacy* al Consiglio di Sicurezza dell'ONU nel fornire legittimità all'azione in caso di mancato consenso da parte del paese ospite.

(40) - Per l'ONU trattasi di pianificazione integrata (*Integrated Mission Planning Process*), che già coinvolge tutte le tre componenti, vedasi UN DPKO United Nations Peacekeeping Operations Principles and Guidelines (*Capstone Doctrine*) 2008 pagg. 52-57. Per l'Unione Europea può trattarsi di una Missione di Gestione Civile delle Crisi quando le FPU o IPU di tipo A o B si trovano sotto catena di comando e controllo civile ed in cui il Capo Missione dipende dal *Civilian Planning and Conduct Capability* (CPCC) oppure di una Missione Militare quando l'IPU di tipo A o di tipo B, o le FPU si trovano, in via di eccezione, inquadrate sotto comando e controllo militare in cui il Force Commander dipende dal *Crisis Management Planning Directorate* (CMPD).

(41) - Alcune SPU, come le FPU, sono su base nazionale, altre, come le MSU, sono su base multinazionale. Nel processo di generazione della forza, anche dopo che l'organizzazione internazionale o la coalizione di stati ha deciso lo schieramento di tale tipo di unità, serve comunque l'ulteriore passaggio, presso ciascun paese contributore, della decisione di fornire effettivamente proprio personale.

(42) - Nelle missioni ONU si nominano le posizioni più elevate, c.d. *senior mission leadership*, che si affiancano all'inizio della missione al *UN Country Team*.

- la pianificazione operativa[43];

- il processo di generazione della forza (per generare ed attivare una assetto in grado di esprimere tutte le capacità, anche altamente specializzate, che vengono richieste all'unità per l'assolvimento dei suoi compiti ed in conformità con il piano operativo). Va fatta attenzione nella scelta di personale di paesi contributori che per motivi storici, politici, religiosi od altri ancora, possano essere considerati come ostili anziché come imparziali dalla popolazione locale o dalle parti in conflitto nell'area di crisi;

-l'assegnazione di responsabilità e competenze logistiche[44]. Qualora si decida lo schieramento di una unità a composizione multinazionale (come ad es. l' MSU e l'IPU di tipo A), può ritornare molto utile considerare il concetto di Leading Nation[45]. Anche quando il contingente dell'SPU è però su base esclusivamente nazionale (come per le FPU) si pone il problema di scegliere il sistema di *wet lease o di dry lease*, per le missioni ONU minuziosamente dettagliato nel *Contingent Owned Equipment Manual*, con le logiche conseguenze in tema di maggiore o minore capacità ed autonomia logistica;

- lo schieramento (con tutte le problematiche afferenti, oltre al trasporto in teatro del personale ed all'equipaggiamento, anche alla sicurezza ed alla sistemazione della base con tutte le misure di difesa attiva e passiva);

- la gestione del personale, dei mezzi e materiali e delle attività in teatro di operazioni. Oltre alla mera rotazione del personale ed alla sua amministrazione, un fattore di criticità è individuato nel rispetto del codice di condotta;

---

(43) - In linea di massima il *Police Commissioner* abbozza un *Operational Plan* (OPLAN), che poi sottopone all'autorizzazione e nel quale possono essere presenti (o meno) unità organiche di polizia, indicandone compiti e funzioni. Successivamente allo schieramento, viene poi elaborato un *Mission Implementation Plan* che aggiorna l'OPLAN.

(44) - Mentre la considerazione degli aspetti logistici ha luogo fin dal principio del processo di pianificazione.

(45) - Nella dottrina della NATO, l'Allied Joint Logistic Doctrine AJP-4 (A), dicembre 2003, unclassified, specificsa tale concetto: *Section II, NATO's logistic support concept*, dice che: Logistic support will be based on national provisions and may include degrees of multinational support as agreed by those nations. While each nation takes responsibility for the provision of support to its forces, Host Nation Support, if available, lead nation, role specialisation, mutual assistance, and use of Multinational Integrated Logiostic Units (MILUs) and/or Multinational Integrated Medical Units (MIMUs) may be employed when considered to be more advantageous.

- la gestione dell'attività operativa quotidiana, con emissione di *Fragmentary Orders* o di *Operational Orders*, facilitata dal riferimento a quanto già pianificato a livello strategico ed operativo, cui deve conformarsi[(46)];

- la richiesta di eventuali modifiche nel mandato o nella documentazione della pianificazione da esso discendente (ad esempio la richiesta alla catena di comando di mutare le regole di ingaggio o le direttive sull'uso della forza);

- la gestione di eventuali modifiche del mandato, con l'adattaemnto conseguente di tutta la documentazione e struttura della missione, ivi compresa, se del caso, la SPU;

- la pianificazione di contingenza, per stabilire, *ex ante*, come comportarsi in caso di mutamento del quadro di situazione o di eventi ipotizzabili[(47)];

- la fine della missione (per scadenza del mandato, o per cambiamento sostanziale del mandato, o per eventi che causano il ritiro dell'unità SPU). Ogni organizzazione internazionale quando schiera una propria SPU segue ovviamente il proprio processo di pianificazione, utilizzando una diversa terminologia e riconoscendo responsabilità decisorie e pianificatorie ad organi ed uffici diversi, tuttavia, il concetto di fondo permane in linea di massima sempre lo stesso.

Ad esempio, nella dottrina ONU, semplificando al massimo, per lo schieramento di una FPU, il processo si articola nelle fasi seguenti:

- decisione di inviare una Technical Assessment Mission (TAM) per verificare la situazione a seguito di un determinato evento;

- autorizzazione da parte del 5° Comitato dell'Assemblea Generale ONU alla spesa per la TAM;

- rapporto al Segretario Generale;

- rapporto del segretario Generale al Consiglio di Sicurezza;

- adozione di una risoluzione del Consiglio di Sicurezza che autorizza per

(46) - FRAGO e OPORDER sono concettualmente sempre iscritti secondo quanto indicato nel Concetto di Operazione (CONOPS) e nel Piano di Operazione (OPLAN o Mission Plan), che a loro volta non possono divergere da quanto stabilito nel mandato.

(47) - I *Contingency Plans* possono (e dovrebbero) essere elaborati fin dall'inizio dell'attività di pianificazione. Poi vi sono anche gli *Emergency Plans*, che pianificano le attività da compiere ad esempio in caso di una catastrofe naturale o di una altro evento che costringe ad abbandonare immediatamente il teatro di operazione.

un certo tempo, in un certo teatro di operazione, un certo numero di FPU (*Formed Police Units*) per l'assolvimento di alcuni compiti sommariamente ivi indicati (la Risoluzione del Consiglio segue infatti la fase di studio sul paese in crisi ed il relativo rapporto presentato dal Segretario Generale al Consiglio di Sicurezza che conclude quelle che potremmo indicare come attività preliminari);

- invito[48] ai Paesi Membri dell'ONU a contribuire inviando una o più FPU;
- sopralluogo (c.d. *Technical Reconnaissance*) da parte del paese possibile contributore di FPU;
- negoziazione di un protocollo di intesa (c.d. *Memorandum of Understanding* - MOU) tra Dipartimento di Mantenimento della Pace e Dipartimento per il Supporto alle Operazioni (DPKO/DFS) e paese contributore;
- visita ispettiva del personale ONU (FPAT), prima dello schieramento con validazione della unità[49] a seguito di una addestramento pre-schieramento basato sui moduli addestrativi standardizzati dell'ONU e, nuovamente, visita ispettiva sul posto subito dopo lo schieramento (per verificare prontezza operative e mezzi e materiali che saranno, peraltro, soggetti a rimborso in base al *Contingent Own Equipment Manual*);
- firma del protocollo di intesa (MOU)[50];
- schieramento della FPU[51];
- rotazione con altra FPU del paese contributore[52] o rientro della FPU per fine mandato e liquidazione della posizione.

---

(48) - Da parte del Sottosegretario dell'ONU, a capo del Dipartimento per le Operazioni di Mantenimento della Pace, e, per la componente di polizia, operato in particolare dal Police Advisor.

(49) - Secondo la *Standard Operational Procedure* (SOP) *Assessment of Operational Capability of Formed Police Unites for service* in *United Nations Peacekeeping Operations*. Ref. 2012.11, datata 1 settembre 2012 che illustra nel dettaglio come un *Formed Police Assessment Team* (FPAT) valuta la capacità operative delle FPU.

(50) - In cui sarà stabilito anche se il sistema di rimborso sarà c.d. *wet lease*, per cui l'unità avrà effettiva autonomia logistica, provvedendo da se anche a riparazioni e manutenzione, oppure *dry lease*, e quindi farà riferimento ad altre entità dell'ONU per eseguire queste attività.

(51) - La FPU può poi siglare degli accordi tecnici per l'eventuale fornitura di beni e servizi con altri paesi contributori o con terzi.

(52) - Ogni 6, o, preferibilmente per l'OUN, 12 mesi.

Al fine di ridurre il tempo necessario per schierare in teatro una SPU è altamente auspicabile avere il personale potenzialmente schierabile già identificato ed adeguatamente addestrato prima che giunga la possibile richiesta di intervento. La SPU dovrebbe infatti già essere organizzata in termini di personale, mezzi, equipaggiamento e capacità operative.

Appare in tutta la sua evidenza come avere del personale già individuato ed inquadrato in una unità organica, addestrato ed equipaggiato favorisce enormemente il taglio dei tempi necessari per il dispiegamento dell'unità sul terreno e, con l'accorciamento del gap temporale, fornisce un impatto altamente positivo a favore del successo della missione.

Prima della missione sarà così sufficiente impartire il *pre-deployment training,* seguire eventuali cicli vaccinali del personale e completare la dotazione organica di mezzi e materiali. Passi particolarmente critici nel costituire l'unità organica SPU sono:

- la fase di identificazione dello spettro di capacità di polizia che l'unità deve saper esprimere per poter adempiere ai compiti, anche specialistici ed impliciti, assegnati all'SPU nel mandato della missione (in pratica è l'analisi del compito che quell'unità sarà chiamata ad assolvere che consentirà di definire capacità e articolazione di dettaglio che la SPU dovrà possedere, un c.d. *demand driven approach*). Per l'ONU la lista delle capacità è predeterminata in modo più limitativo rispetto ad altre unità di polizia di stabilità (mantenimento O.P., protezione di personale, mezzi ed infrastrutture dell'ONU, supporto operativo); ma può tuttavia arricchirsi di elementi ulteriori (EOD, unità cinofile, SWAT, *close potection*, ecc…) secondo le esigenze;

- individuare il tipo di personale più idoneo a poter esprimere le capacità individuate e selezione dello stesso (spesso capita chi è addestrato e preparato per le missioni poi non viene schierato e chi non è stato addestrato viene invece schierato);

- addestramento *pre-deployment* (individuale per le competenze specialistiche ed al livello di unità per le tecniche di ordine pubblico/operazioni ad alto rischio);

- la fornitura di equipaggiamento e materiali in alcuni casi, come per le FPU dei paesi africani, questo diventa un momento insuperabile, poiché il paese

contributore deve prima dotarsi di mezzi, materiali, armamento ed equipaggiamento e solo dopo alcuni mesi viene rimborsato[53];

- addestramento in teatro (c.d. *induction training* nella fase iniziale dell'immissione in teatro e successivamente l'ulteriore *in-mission training* per il mantenimento delle capacità operative).

Gli esperti stanno attualmente insistendo soprattutto sull'importanza del *capability driven approach*, cioè dell'inviare in missione esattamente il personale con le competenze e conoscenze e mezzi idonei a rispondere alle esigenze della missione e non, invece, ciò di cui i potenziali paesi contributori dispongono o hanno interesse a schierare. La risoluzione di questa criticità consente di evitare delle chiare carenze una volta già schierate le forze.

La corretta pianificazione (concetto certamente più familiare e meglio investigato dal punto di vista dottrinale da parte della componente militare ed invece alquanto nuovo e talora ostico per la componente di polizia e sovente sconosciuto per quella civile) è momento assolutamente fondamentale in vista del raggiungimento degli obiettivi finali stabiliti dal mandato per la missione[54].

Sul punto va detto che, in linea di massima, le forze di gendarmeria possiedono di norma un quadro ufficiali più preparato in tema di pianificazione strategica ed operativa rispetto alle forze di polizia a statuto civile.

---

(53) - In ambito di gruppo di esperti in peacekeeping e peacebuilding del G8 si era ipotizzata la possibilità di creare un meccanismo di prestiti ponte che tuttavia non è mai (ufficialmente) entrato in vigore anche perché contrasta con disposizioni amministrative onusiane.

(54) - Il processo di pianificazione prevede in particolare, dopo la scelta tra le opzioni strategiche, l'adozione di una decisione politica in forma di mandato, quindi la sua traduzione in un concetto di operazione (CONOPS) e/o un *integrated mission plan*, quindi si cala dal livello strategico a quello operativo, producendo il piano operativo o piano della missione (*Operational Plan – OPLAN o Mission Plan*). Il piano specificherà anche la situazione nell'area, l'obiettivo della missione, l'intento del comandante, lo schema di manovra secondo cui si intende raggiungere l'obiettivo finale, i compiti assegnati alle varie componenti, nelle varie fasi della missione, tra cui quelli di competenza della SPU, il coordinamento con gli altri attori presenti nell'area, eccetera. Se vi sono più componenti nella missione (polizia, militare e civile) ciascuna di esse avrà il suo piano operativo, allegato al quale vi saranno gran parte dei documenti fondamentali che regolano le attività nella missione, incluse le regole sul l'uso della forza. La pianificazione poi si sposta a livello tattico, per l'assegnazione dei compiti tattici da svolgere di volta in volta.

In caso di una missione a carattere internazionale, guidata da un organizzazione internazionale o formata *ad hoc* da una coalizione di Stati, a seconda delle normative nazionali e del quadro regolatorio e dottrinale della organizzazione internazionale che la schiera sul terreno, la SPU può essere inquadrata, oltre che all'interno di una missione esclusivamente di polizia, o all'interno della componente civile o di polizia in una missione dotata di più componenti, anche sotto catena di comando e controllo della componente militare.

Questo avviene:

- sempre per la MSU (*Multinational Specialized Unit*, modello di SPU della NATO);

- temporaneamente e come circostanza eccezionale per la IPU (*Intergrated Police Unit*, modello di SPU dell'Unione Europea, che, tuttavia, quando si è schierato nei Balcani è stato posto proprio sotto comando militare);

- mai per le FPU (modello di SPU dell'ONU, oltre che dell'Unione Africana e pure dell'Unione Europea).

Per essere efficace una SPU deve essere:

- inserita in una chiara struttura di commando e controllo, con tecniche tattiche e procedure (TTPs) che ne consentano l'interoperabilità con gli altri assetti della missione e con degli standard che siano comuni a quelli della più ampia organizzazione nell'ambito della quale la SPU viene inserita (sul punto la PFU viene talvota criticata poiché chi ne dirige e coordina l'impiego - l'FPU coordinator - non esercita su di loro azione di comando, ma solo, appunto, di coordinamento);

- dotata di una capacità logistica che le consenta di curare tutti gli aspetti tecnici connessi al mantenimento in efficienza di tutti i mezzi e materiali, dei veicoli, dell'equipaggiamento individuale e di reparto, dei eventuale equipaggiamento o armamento pesante o altamente specializzato se utilizzato nella specifica missione.

In sintesi, una SPU deve avere una efficace struttura di comando e controllo, evitando sovrapposizioni o incertezze sull'attribuzione delle competenze e delle responsabilità ai vari livelli, (c.d. C2, *command and control*)[55] e di una struttura di supporto interna che ne garantisca l'autonomia logistica.

(55) - Anche indicate come C3, command, control and communication o ancora C3IS. Gli apparati di comunicazione si sono rivelati un anello debole della catena sia durante le varie esercitazioni su larga scala della component di polizia, sia nelle missioni effettivamente schierate.

La SPU deve poi essere addestrata ed equipaggiata in modo da poter reagire adeguatamente e proporzionalmente in caso di attacco, o per proteggere i civili, assicurando una forza sufficiente, credibile e potenzialmente deterrente. Deve cioè consentire tanto la legittima difesa dell'unità quanto quella dei civili eventualmente fatti segno di attacchi da gruppi semi organizzati dotati di armi leggere (soglia limite estrema, oltre la quale le SPU debbono cedere il passo alla componente militare della missione).

Come logica conseguenza dei compiti e del ruolo spettante alle unità organiche di polizia nell'ambito delle missioni di supporto alla pace, così come si sono più sopra tratteggiati, queste sono le caratteristiche principali che le SPU debbono possedere:

- *Robustezza*: una SPU deve avere dimensioni e capacità operative che le consentano di svolgere la propria missione anche in contesti altamente destabilizzati e pericolosi. Si pensi oggi alle FPU dell'Unione Africana in Somalia piuttosto che alla IPU dell'Unione Europea schierata da maggio 2014 a marzo 2015 nella Repubblica Centrafricana. Per questo motivo personale, equipaggiamento ed armamento devono permettere di affrontare un ampio spettro di minacce, fattori ed elementi ostili. L'autonomia logistica deve essere parametrata allo sforzo operativo richiesto, commensurandosi ai particolari compiti che la missione assegna all'unità;

- *Rapida schierabilità:* la SPU deve essere in grado di dispiegarsi nell'area della missione in tempi molto rapidi (circa 30 giorni) da quando viene presa la decisione di schierarla da parte del paese contributore;

- *Flessibilità*: è la capacità di adattarsi alle mutevoli evoluzioni dello scenario, operando in modo efficace nelle più disparate situazioni (idealmente tanto all'interno di una catena di comando civile quanto di una catena di comando militare), e, del pari, di essere in grado di passare da una missione in cui il mandato assicura poteri esecutivi in sostituzione di forze dell'ordine locali inesistenti o inidonee (c.d. *substitution o executive mission*)[56], in una missione di supporto a favore delle autorità locali (c.d. *strengthening o non-executive mission*)[57]. Specie in caso di mandato esecutovo deve poter adempiere a tutte le principali funzioni

(56) - *A mission with executive police/law enforcement powers.*

(57) - *A mission without executive powers, based on training, mentoring, monitoring and advising local police.*

di polizia, anche in ambiente destabilizzato o poco permeabile o ostile. Poiché di norma non è già predisposto un bacino di riserva da cui attingere una o più unità da impiegare per una specifica missione, già dotate di tutte le caratteristiche necessarie per assolvere il mandato, la generazione della forza, anche con riferimento alle SPU, deve essere in tutto attagliata, di volta in volta, alla specifica missione. La composizione di dettaglio e le dotazioni vanno quindi definite solo dopo che area di intervento, situazione e compito assegnato siano ben identificati. Si pensi, ad esempio, alla differenza di mezzi e materiali a seconda si operi in contesto urbano o desertico o tra una area ormai stabilizzata ed una ostile. Il processo di generazione della forza deve cioè considerare, oltre al tipo di mandato ed ai specifici compiti assegnati:

- le condizioni ambientali locali (climatiche, economiche, sociali ecc…);
- il livello di intensità del conflitto, con particolare riguardo agli aspetti afferenti la presenza o meno di una minaccia da parte di gruppi militarmente organizzati ed al livello della criminalità organizzata e comune;
- la soglia della tensione tra le parti che hanno partecipato al conflitto o la crisi interna che ha portato alla missione internazionale.

Anche un identico modello di SPU può suggerire cambiamenti nell'articolazione e nella specializzazione del personale da inviare. Ad esempio l'ultima MSU ancora oggi schierata nei Balcani non è affatto identica a quella ben più robusta degli anni novanta o a quella schierata a suo tempo in Iraq. Si pensi che nei Balcani ci si è dotati di capacità specializzate per la protezione dell'ambiente, mentre in Iraq, invece, per la tutela dei beni culturali. Per la stessa gestione dell'ordine pubblico, nei Balcani ormai stabilizzati le operazioni di ordine pubblico potevano essere ben gestite dal personale dei battaglioni mobili, mentre in Iraq risultavano più idonei i carabinieri del reggimento paracadutisti;

- *Struttura efficace di commando e controllo (e comunicazione)*: è costituita dalla capacità di governare e dirigere le unità dipendenti verso gli obiettivi che sono stati posti. Quando si schiera una SPU occorre anche che i paesi contributori la dotino di idonei appartati di comunicazione e di *information technology,* sia per i collegamenti tra le varie articolazioni della SPU per eseguire quanto disposto dal comandante, sia per potersi all'occorrenza coordinare con i superiori comandi o con altre unità ed attori presenti in teatro.

La disponibilità di un efficiente sistema per la gestione del flusso di comunicazioni ed informazioni è un fattore certamente critico per il successo della missione. Una struttura di comando ben identificata, con responsabilità e competenze chiaramente allocate, priva di sovrapposizioni o eccessivamente lunga, è requisito indispensabile di ogni missione. La struttura e le competenze assegnate ai vari livelli debbono essere congruenti con i compiti che vengono demandati alle unità ed anche alla dislocazione geografica delle unità sul territorio. Sovente ogni contingente nazionale utilizza una propria maglia radio con propri apparati e canali che non consentono di comunicare con i contingenti di altri paesi. Per le SPU formate su base multinazionale è necessario che la possibilità di comunicare tempestivamente sia assicurata in ogni istante e nell'intera area di responsabilità (AoR);

- *Interoperabilità*: costituisce la idoneità di organizzazioni, sistemi, unità e forze di fornire supporto ad altre organizzazioni, sistemi, unità e forze e, viceversa, di esserne supportati, operando e cooperando efficacemente in modo congiunto. L'obiettivo della interoperabilità può essere raggiunto primariamente attraverso la elaborazione di tattiche, tecniche e procedure comuni nonché attraverso una struttura di comando e controllo che sia interoperabile[58]. L'addestramento congiunto consente di amalgamare le unità e di esaltare la capacità di operare congiuntamente negli interventi. Importante è che la lingua ufficiale della missione sia pure la lingua condivisa dalle strutture di comando e controllo (tenendo peraltro a mente che le comunicazioni via radio o telefono sono molto più difficili di quelle tra interlocutori compresenti). Anche la logistica può essere un fatto che impedisce o esalta la interoperabilità delle unità/forze;

- *Multinazionalità*: è data dalla partecipazione di un elevato numero di paesi alla missione, che in tal modo, specie se provenienti da diverse regioni del globo, ne incrementano e consolidano la percepita legittimità. Le SPU possono essere sia un assetto nazionale (come accade per il modello FPU) oppure possono essere multinazionali, specie se con un paese che si presenta come l*eading nation* e altri che contribuiscono con alcune componenti (*plotoni, squadre*) o con personale specializzato (è il caso dei modelli MSU ed IPU). Poiché è opportuno

(58) - *Communications and Information System (CIS) assets.*

e necessario garantire un elevato livello di imparzialità ed evitare che l'unità organica di polizia sia percepita come espressione dell'interesse del paese contributore, è altamente auspicabile che le SPU di maggiore dimensione, che si pongono come missioni di polizia, aventi responsabilità e competenza sull'intero teatro di operazioni (è il caso della MSU della NATO, dell'IPU dell'Unione Europea e del SPF teorizzata dagli esperti statunitensi), siano costituite da più paesi e quindi a carattere multinazionale. Inoltre, al fine di favorire atteggiamenti positivi e consenso della popolazione locale nei confronti dell'SPU, i paesi di provenienza andrebbero bilanciati quanto più possibile per assicurare anche elementi di affinità culturale, linguistica e religiosa rispetto alla popolazione locale. Questo vale anche nelle missioni in cui sia il paese ospite ad aver chiesto l'intervento di un paese amico per assistere nella stabilizzazione.

5. Articolazione di un modello ipotetico generico di SPU

La SPU è un modello teorico, cui ci si riferisce in questa sede, privo di una precisa struttura organizzativa decisa da una autorità competente e sviluppato in documenti dottrinali[(59)].

Ogni organizzazione internazionale si è dotata di un proprio modello, denominandolo in modo diverso e dotandolo di alcune proprie peculiarità. Raramente, peraltro, quando un paese contributore ha schierato una SPU a favore di una missione guidata da una determinata organizzazione internazionale o coalizione di Stati, la composizione della propria SPU ha rispecchiato fedelmente l'organigramma ufficialmente approvato. Questo vale anche, più in generale, per ogni missione, che, sebbene abbia una struttura tipo elaborata nel quadro della relativa dottrina di riferimento di ciascuna organizzazione internazionale, poi si attaglia in modo diverso a seconda del contesto in cui è schierata. La partecipazione ad una missione con proprie unità rimane sempre una prerogativa dello stato contributore, non essendo previsto alcun meccanismo per costringere i paesi a fornire personale.

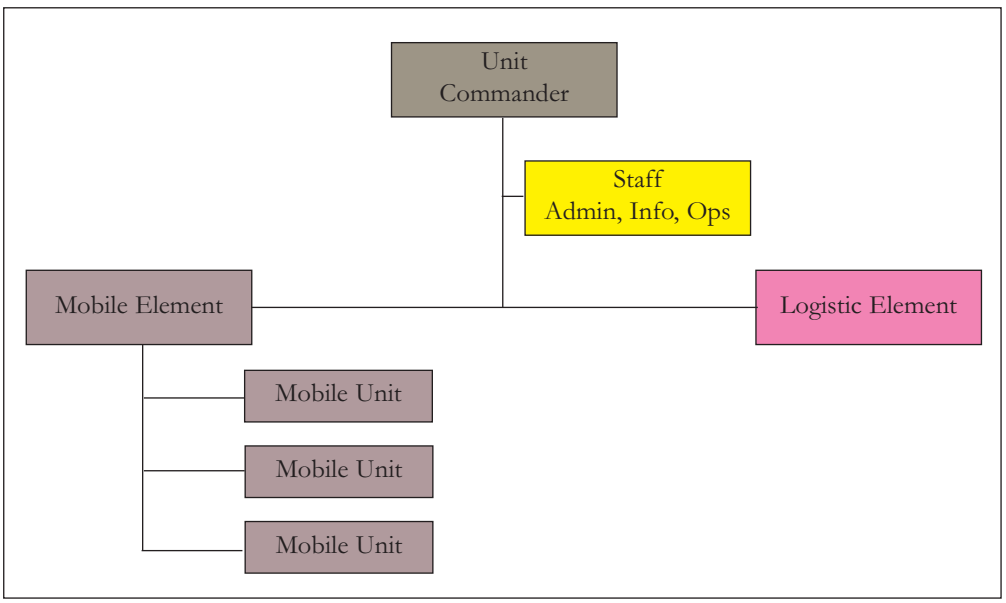
(59) - SPU o *Special Police Unit* fu il primo nome adottato dalle Nazioni Unite per le unità organiche di polizia che successivamente furono denominate FPU. Le SPU ONU vennero schierate per la prima volta nel 2000 in Kosovo.

Le dimensioni ed articolazione di dettaglio dell'unità saranno quindi adattate alle diverse specifiche situazioni, missioni e scenari. Tuttavia queste unità possiedono una ossatura di base largamente condivisa dai vari modelli. Si possono così sintetizzare e semplificare al massimo le capacità minime e la struttura base di un ipotetica SPU. Essa si può articolare in due diversi sottotipi o modelli fondamentali:

- SPU con una struttura basata su una unità mobile (c.d. *Mobile Element*) supportato da un elemento logistico (*Logistic Element*) e dallo staff (che è il modello seguito dalle FPU dell'ONU);

- SPU che, oltre alla component mobile poggia su un secondo pilastro operativo, costituito da unità specializzate con competenze di polizia specifiche (c.d. *Specialized Element* o *Special Police Element*) in grado di condurre attività di polizia altamente specializzate ed attività investigativa di elevato livello, supportate da un elemento logistico e dallo staff (è il modello seguito dalla MSU della NATO e dal IPU di tipo "A" dell'Unione Europea).

L'organigramma del primo modello può essere rappresentato come nel grafico qui illustrato.



Organigramma di base di una SPU (concetto utilizzato per le FPU)

I modelli di SPU di cui le varie Organizzazioni Internazionali (o coalizioni di Stati) si possono avvalere (e di cui si sono avvalsi nel recente passato), grazie alle rispettive elaborazioni dottrinali sono quelli della MSU (*Multinational Specialized Unit*), concepito in ambito NATO (ed attuato sotto la guida dei carabinieri), quello della IPU (*Integrated Police Unit*) dell'Unione Europea, a sua volta suddiviso in due sotto modelli di diversa dimensione, di cui è stato testato nei Balcani solo quello più robusto (ed anche in questo caso con un ruolo guida da parte dei carabinieri), quello delle FPU (*Formed Police Units*) concepito dal DPKO dell'ONU ed ampiamente utilizzato nelle missioni di *peacekeeping* condotte direttamente dalle Nazioni Unite e identico al modello di FPU adottato pure dall'Unione Europea e quello delle SPU (*Special Police Units*)[(60)] schierate dalle Nazioni Unite nei Balcani già nel 2000. L'EGF (*European Gendarmerie Force*), invece, non è in sé una unità organica di polizia ma uno Stato Maggoire permanete che che può avvalersi di unità tipo IPU o FPU (che si trovano in condizioni di approntamento presso i diversi Stati parte del trattato di Velsen del 2007), oppure che può supportare l'avvio di una missione sotto propria egida, sempre facendo riscorso a tali assetti di polizia robusta, per compiere le missioni che gli vengono assegnate. Infine, modello emergente, su cui si stanno concentrando notevoli sforzi dottrinali, è quello delle FPU dell'Unione Africana concettualmente riconducibili alle FPU dell'ONU, seppure con alcune minime varianti, attualmente schierate in Somalia e Repubblica Centrafricana. E', infatti, in parallelo alla concezione ed allo schieramento in missione di questi modelli tra loro simili (e soprattutto dalle lezioni apprese dalle diverse missioni in cui sono stati schierati) che si è evoluta la dottrina delle SPU, affinandosi e modernizzandosi, fino a giungere ai più recenti traguardi dottrinali, raggiunti con la policy per l'impiego delle FPU (*Formed Police Units*) delle Nazioni Unite, nel marzo 2010[(61)].

(60) - *The UN SPU model is explained in the "Handbook for UN Special Police Units", Department of Peacekeeping Operations, Civilian Police Unit, United Nations Headquarters and Office of the Special Advisor to the Commissioner, UNMMIK Civilian Police Headquarters 15 genniao 2001.*

(61) - *UN DPKO/DFS, Policy (Revised) Formed Police Units in United Nations Peacekeeping Operations.* Rf. 2009.32. 1 marzo 2010. L'Ambasciatore Alain Le Roy, *Under Secretary General dell'UN DPKO* al tempo, ha adottato nel 2010 il nuovo inquadramento dottrinale delle FPU dell'ONU, beneficiando in particolare delle risultanze dei lavori del *UN DPKO Doctrinal Development Group on FPUs,* cui han partecipato un gran numero di esperti già schierati in missioni di pace con funzioni di rilievo in tutti i diversi modelli di unità organiche sopra richiamati.

L'adozione nel febbraio 2014 di una nuova *policy* ONU per l'impiego della componente di polizia porterà a breve ad un ulteriore ripensamento ed avanzamento di tale processo. Nel quadro della *Strategic Global Framework Guidance*, si sta infatti tentando di produrre in modo organico l'intero spettro dei documenti a monte della policy, incluso quelli relativi alle linee guida, alle procedure operative standardizzate (SOP) ed ai curricula addestrativi relativi alle FPU[(62)].

Il principale elemento di differenziazione tra i diversi modelli, che va da subito sottolineato, è dato dal fatto che le FPU dell'ONU vanno necessariamente ed esclusivamente considerate parte della componente civile e solo e soltanto all'interno di una catena di comando e controllo civile (che si articola lungo la catena Segretario Generale, Rappresentante Speciale del Segretario Generale dell'ONU/Capo Missione, *Police Commissioner* e comandante della FPU), ma i fondamenti teorici e gli assunti logici le accomunano in tutto, come si vedrà più avanti, agli altri modelli. Inoltre il coordinamento per l'impiego delle FPU è rimesso ad un FPU coordinator, che non è in line ma esercita solo il coordinamento, mentre le altre SPU hanno una catena di comando e controllo prettamente gerarchica. Infine, la MSU e l'IPU di tipo "A" sono unità tendenzialmente destinate ad operare sull'intero teatro di operazione e come una missione di polizia (cosa mai occorsa), o come componente di polizia di una missione (cosa avvenuta nel quadro delle missioni militari NATO e UE nei Balcani).

Quando si organizza una SPU sulla base di un mandato internazionale i modelli MSU e IPU sono a composizione multinazionale, mentre il modello FPU è costituito su base nazionale dai singoli paesi contributori[(63)].

Per le MSU e IPU, in linea di massima, ogni qualvolta sia possibile, si ritiene che il personale dello staff debba essere a composizione multinazionale.

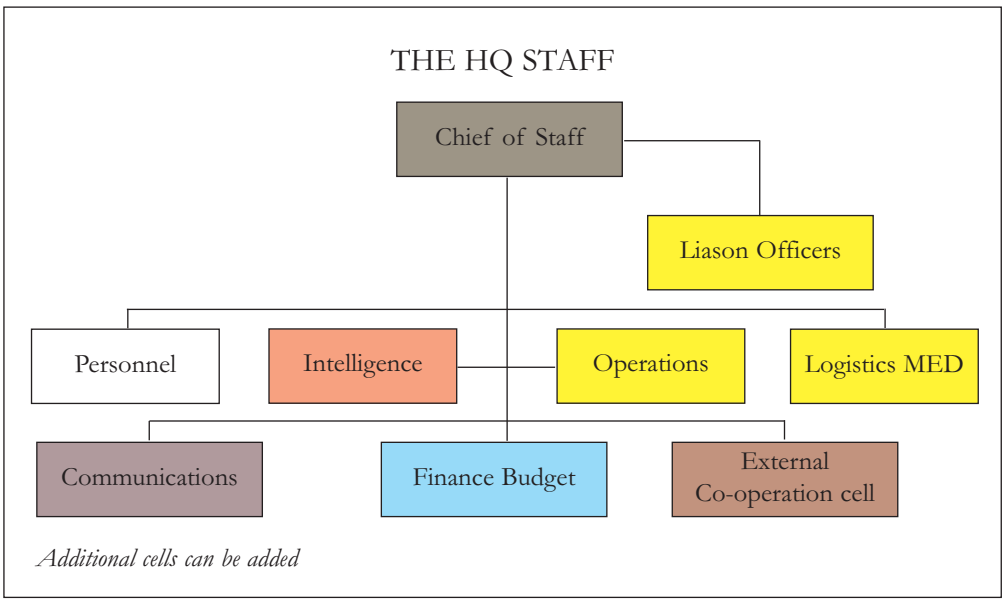
La componente mobile e quella specializzata della SPU possono essere, auspicabilmente, multinazionali ma per le unità di più piccole dimensioni (squadre e/o plotoni) è invece opportuno che siano costituite su base nazionale (anche per motivi di comprensione linguistica e di identità di tecniche, tattiche e procedure).

(62) - *UN DPKO/DFS Policy on United Nations Police in Peacekeeping Operations and Special Political Missions*, Ref. 2014.01, Febbraio 2014.

(63) - La FPU italiana ha visto tuttavia a fianco dei carabinieri personale israeliano inquadrato nella stessa unità ed ara prevista altresì la partecipazione di personale serbo.

Schematicamente, le componenti della SPU da essere prese n considerazione sono le seguenti:

- *Staff* (o stato maggiore), che deve essere composto da ufficiali di polizia con specifica competenza ed esperienza nelle branche in cui sono inseriti o di cui hanno la responsabilità. Quando la SPU è a composizione multinazionale debbono essere ripartite in modo equilibrato tra i paesi che costituiscono la SPU;



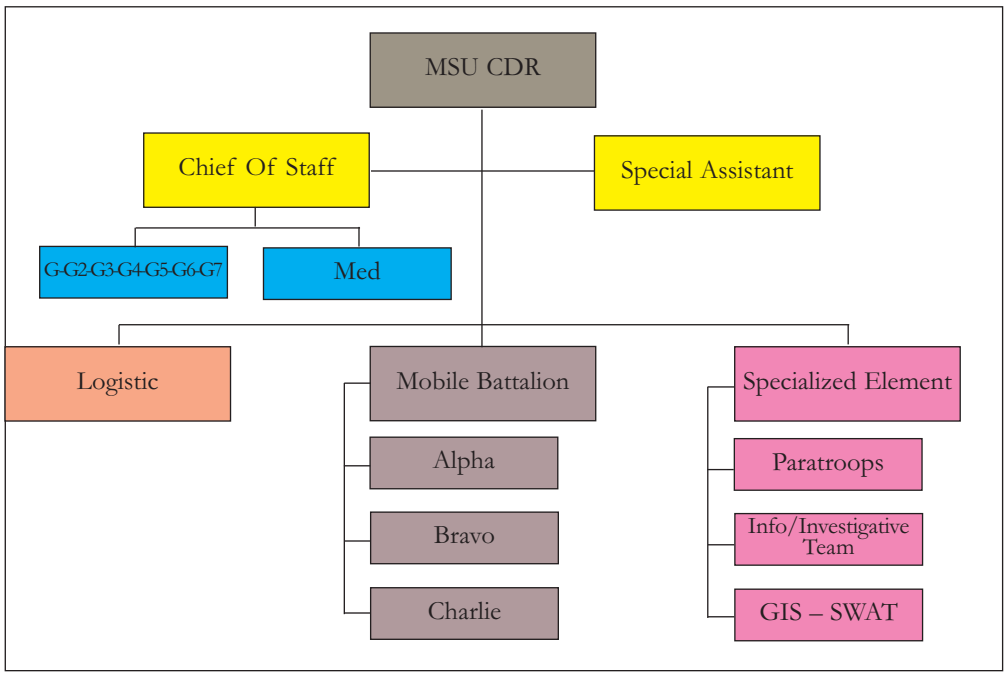
Organigramma di uno generico Stato Maggiore di una SPU[64]

- *Componente Mobile* che può essere articolata, a sua volta, in diverse unità mobili di minore livello. Ad esempio le Formed Police Unit (FPU) che sono unità tattiche di livello compagnia (e costituite su base nazionale) sono poi suddivise in plotoni e questi, a loro volta, in squadre. La squadra rappresenta per esse il minor livello di impego del personale, non essendo previsto l'impiego a livello individuale che farebbe venir meno il significato stesso di FPU;

(64) - Questa è la composizione in caso di SPU di notevoli dimensioni, ben strutturata, mentre per le unità più piccolo numero di branche e di personale addetto è significativamente più limitato.

- *Elemento Logistico*, strutturato essenzialmente su base nazionale anche quando l'unità è multinazionale, secondo i concetto logistico di "*Leading Nation*". Le SPU di più grandi dimensioni, quali ad esempio la MSU e l'IPU che sono state schierate nei Balcani ed in Iraq, aggiungono al modello organizzativo di base appena accennato un altro fondamentale pilastro: l'Elemento Specializzato (*Specialized Element*);

- *Elemento Specializzato* è una componente di enorme importanza e valore, costituita da personale specializzato nel compimento di azioni risolutive ed ad alto rischio (SWAT), di protezione di VIP, di disattivazione e rimozione di ordigni esplosivi, di investigazioni criminali basate su elevate capacità info-investigative ed ulteriori capacità specializzate di polizia ove necessario. Qualora richiesto dal mandato, tale componente può provvedere anche all'addestramento, al *mentoring* ed all'*advising* in favore della polizia locale (mentre per la componente mobile si può configurare di solito solo attività di servizi congiunti con *la local police* o esercitazioni congiunte a finalità didattico-addestrative).



Organigramma di una SPU generica di tipo più robusto (MSU schierata nei Balcani)

L'Elemento Specializzato può essere costituito da diverse unità/teams forniti dai diversi paesi che costituiscono la SPU in base alle loro specifiche e magari internazionalmente riconosciute competenze in particolari settori di impiego. Si pensi, a titolo esemplificativo, alle competenze, quasi ineguagliabili, che l'Italia può esprimere in indagini svolte in ambiti peculiari come l'antisofisticazione alimentare (NAS), la contraffazione monetaria (NOAM), la tutela del patrimonio artistico e culturale (TPC), controterrorismo ed eversione (ROS), le investigazioni scientifiche (RaCIS), la tutela dell'ambiente, eccetera.

La *policy* adottata dal DPKO dell'ONU è quella di far svolgere l'attività info-investigativa e l'addestramento della polizia locale a personale specializzato individualmente considerato (c.d. *individual* UNPOL, in passato individuati anche come o CIVPOL), collocati gerarchicamente sotto il commando di un comandante regionale e di impiegare, invece, le unità organiche di polizia, le FPU, solo per compiti di ordine pubblico, di controllo della folla, di scorta, di protezione di personale mezzi e materiali della missione o di supporto agli elementi specializzati o alle operazioni delle forze di polizia del paese ospite. Al contrario, la *policy* della NATO con le MSU e dell'Unione Europea con le IPU è stata quella di collocare Elemento Mobile ed Elemento Specializzato all'interno della stessa unità organica di polizia, possedendo così la capacità di compiere con tale unità l'intero spettro di capacità di polizia richiesto dalla missione.

Nell'approntare personale ed equipaggiamento di un Elemento Specializzato, vanno preventivamente considerate le particolari capacità di cui si vuol dotare ed i compiti specifici che ad esse si intendono attribuire. Per ciascuna capacità specialistica che si voglia esprimere va considerata poi la disponibilità di equipaggiamento specialistico adeguato e di personale specializzato.

6. Addestramento delle SPU

L'addestramento è il principale fattore di successo per un efficace impiego delle forze di polizia, e questo vale tanto per lo svolgimento del servizio nel paese di origine quanto per adempiere le funzioni di polizia fuori area. Il livello adeguato di addestramento necessario per compiere correttamente i propri

compiti all'estero è tuttavia ancora più elevato di quello richiesto in patria. Infatti le condizioni ambientali e di sicurezza all'estero sono generalmente assai più dure. Ma soprattutto il quadro giuridico di riferimento, con norme di diritto internazionale come la Risoluzione del Consiglio di Sicurezza che definisce il mandato, lo *status of forces agreement/status of mission agreement* o le regole di ingaggio/direttive sull'uso della forza e l'ordinamento giuridico dello Stato ospite, che si sovrappongono alle norme di ciascun paese contributore e vincolano il *peacekeeper* ad una condotta nell'espletamento del servizio significativamente diversa da quanto uso fare in patria è molto più complessa l'opera cui il *peacekeeper* è chiamato. Si pensi che per i crimini comuni (che non riguardino minacce diretta ai *peacekeepers*), la norma che deve essere applicata è quella del *locus commissi delicti*, scritta in codici e lingue spesso del tutto sconosciuti ai *peacekeeper*.

Per poter operare correttamente ed in modo efficace in un simile contesto la qualità dell'addestramento pre-schieramento è assolutamente fondamentale e ricomprende anche molti aspetti non presenti nell'addestramento per il servizio in patria (ad es. *cultural awareness*, campi minati, ecc…).

Per di più, l'addestramento a favore di personale da impiegare in una MSU/IPU/FPU è ancora più articolato e complesso rispetto a quello da fornire ad un *individual civil police officer* che dovrà essere immesso in teatro di operazione per lavorare individualmente. Infatti nel nostro caso bisogna addestrare per affinare diversi aspetti, quali:

- le conoscenze, capacità e professionalità per svolgere i "normali" compiti di polizia;
- la capacità a lavorare ed integrarsi perfettamente in una unità (tanto nelle attività di ordine pubblico quanto nella raccolta, condivisione e alimentazione del flusso informativo o ancor più nell'espletamento di compiti specialistici);
- la capacità di comprendere ruolo e funzioni delle diverse componenti dell'unità;
- la capacità di operare in complementarietà con forze, unità o elementi di altri paesi/organizzazioni;
- l'utilizzo di una lingua (inglese o francese) spesso diversa da quella madre.

Tutto ciò nell'ottica di operare per un periodo prolungato lontano dai propri luoghi di origine e dalle proprie famiglie.

Le esigenze addestrative di queste unità sono uniche nel loro genere ed estremamente ampie per le competenze che coinvolgono. Inoltre, considerato che tutte le moderne missioni di supporto alla pace hanno sempre carattere multinazionale, è importante condividere una visione comune, standardizzare tecniche, tattiche e procedure, ma anche preparare il personale secondo la corretta *forma mentis* per servire come operatore delle forze dell'ordine in una missione internazionale, nel rispetto di principi, standard e regole fissati dalla Nazioni Unite e delle altre Organizzazioni Internazionali talvolta distanti dal patrimonio culturale e dalla esperienza personale maturata da rappresentanti di paesi di solo più recente vocazione democratica).

Per ottenere questi obiettivi è allora necessario provvedere ad un vero e proprio "indottrinamento" e formazione sia nel corso dell'addestramento pre-impiego dell'unità che precedentemente. Poiché la durata del *pre-deployment training* non può essere lunga come un corso di istruzione di base (la FPU cinese segue l'addestramento pre-impiego di 9 mesi, in assoluto il più lungo), e in un arco temporale breve non si può variare la *forma mentis*, occorre fornire un addestramento adeguato, ancor prima dell"affinamento della preparazione nell'approntamento pre-impiego.

Affinché gli ufficiali di polizia siano in grado di adempiere correttamente i propri compiti anche in modo autonomo ed indipendente (come spesso accade) in assenza di specifici ordini per compiere una determinata attività o fronteggiare un evento improvviso, è necessario che abbiano una profonda comprensione dei principi e valori fondamentali che debbono sorreggere la loro azione, specie in tema di rispetto dei diritti umani e delle libertà fondamentali che di norma sono estremamente importanti in un area di impiego che è stata appena afflitta da un conflitto o che è comunque destabilizzata ed ogni errore del *peacekeeper* può riverberarsi con un impatto molto maggiore rispetto a ciò che accadrebbe in patria.

L'addestramento del personale, almeno fino allo schieramento in teatro, è sempre responsabilità del paese contributore.

Alla responsabilità del paese contributore viene poi a sommarsi quella dei comandanti da cui dipendono le forze messe a disposizione durante la missione (oltre ovviamente a quella dei singoli *peacekeeper* che non possono esimersi dal

dovere deontologico di informarsi e formarsi). L'addestramento relativo alle conoscenze di base dell'ufficiale di polizia non rientra comunque nell'addestramento all'impiego fuori area, si dà giustamente per acquisito (ma non deve essere dato per scontato) e rientra sempre nelle responsabilità della nazione che mette a disposizione il proprio personale.

Il contenuto e taglio addestrativo per approntare una MSU/IPU/FPU dipendono anche dal tipo di mandato della specifica missione in cui stanno per schierarsi, che, ad esempio, per la dottrina dell'Unione Europea può essere distinto in due diversi ruoli da poter assegnare alle FPU o IPU:

- missione esecutiva (o di sostituzione), in cui le unità son chiamate a svolgere tutta l'ampia gamma di compiti che generalmente debbono svolgere pure nel paese di origine (sono i casi delle missioni svolte in Kosovo o a Timor Est);

- missioni non-esecutive (o di supporto, c.d. strengthening missions), dove le unità si limitano solo a fornire supporto operativo alle autorità locali o a componenti della missione, monitorano la situazione, eventualmente addestrano le forze locali e contribuiscono allo sviluppo delle capacità della polizia locale, del sistema giudiziario e penitenziario.

Simili differenziazioni del mandato sono rinvenibili nella tripartizione operata dalla dottrina dell'ONU[(65)] che suddivide in:

- *Interim Policing and Law Enforcement;*

(65) - Per la dottrina delle Nazioni Unite i police keeping mandates sono suddivisi e definiti nel modo seguente:
- Interim Policing and Law Enforcement (including patrolling, confidence-building, investigations, arrests, detentions, on-the-job mentoring, advising, training, transition and support);
- Operational Support (including public order, crowd control, anti-riot, capacity-building, mentoring, training and protection of UN facilities and personnel);
- Reform, Restructuring and (Re)Building (including efforts related to legislation, systems, procedures, codes, values, organization, management, vetting, training, basic material, logistics, communications etc).
Come si vede, essenzialmente il primo rappresenta le missioni c.d. "*executive*" o "*substitution*" mentre il secondo e terzo alinea rappresentano le missioni con mandato c.d. "*non-executive*" o *strengthening*".
Anche per la dottrina dell'Unione Africana I mandate si suddividono in tre gruppi:
- Non-executive authority (including advice, monitoring and mentoring of local police);
- Full or partial authority (including contributing to the reform, restructuring and rebuilding, including training, of a national police force and other LEAs);
- Full executive authority (including interim law enforcement, security support to a national police force and other LEAs).
Dal punto di vista concettuale le similitudini tra le tre diverse suddivisioni dei diversi mandati assegnabili nelle missioni alla componente di polizia sono evidenti.

- *Operational Support;*
- *Reform, Restructuring and (Re)Building);*

nonché da quella dell'Unione Africana che distingue in:

- esecutive;
- non-esecutive;
- parzialmente esecutive.

L'addestramento che precede l'impiego dell'unità (c.d. *pre-deployment training*) si deve attagliare a questi due diversi tipi di mandato. Poiché si tratta di un addestramento molto articolato e complesso, che presuppone compiti molto vasti e differenziati.

I centri addestrativi che si occupano della preparazione pre-impiego di unità organiche di polizia debbono essere, a loro volta, flessibili ed in grado di fornire di volta in volta un addestramento perfettamente attagliato alle specifiche esigenze ed al mandato della concreta missione.

Per certi versi pare più difficile svolgere attività addestrativa per le missioni in cui non esiste potere esecutivo rispetto alle altre, in quanto l'approccio dell'operatore diviene in teatro sostanzialmente diverso da quanto chiamato a fare in patria.

7. Conclusioni

La realtà sul terreno ha portato diverse organizzazioni internazionali a seguire un modello di polizia robusta che è stato testato per la prima volta nei Balcani dalla NATO.

Con nomi diversi e con articolazioni e capacità leggermente diverse tutte queste SPU rispondono ad una comune esigenza di stabilizzare un territorio assicurando lo stato di diritto come nessun altro assetto riesce a fare. Sfide a difficoltà sono enormi.

Tuttavia, l'individuazione di tratti comuni e uno sforzo adeguato nell'addestramento e nell'equipaggiamento delle forze può assicurare il successo della missione. Il modello NATO e successivamente quello della UE hanno visto storicamente un indiscusso ruolo guida dell'Arma dei carabinieri.

Ma, attraverso l'addestramento delle FPU onusiane e di quelle dell'Unione Africana, anche in questo campo l'Arma si è ritagliata un ruolo di primo piano a livello internazionale con oltre settemila *peacekeepers* che fanno riferimento a questi modelli di polizia robusta addestrati nel corso di un decennio al CoESPU di Vicenza.

VITA DELLA SCUOLA

Cambio al Comando della Scuola Ufficiali Carabinieri

Il 3 luglio 2015, il Gen. D. Luigi Robusto ha ceduto il comando della Scuola al Gen. D. Vittorio Tomasone.

Alla cerimonia ha presenziato il Comandante delle Scuole dell'Arma dei Carabinieri, Gen.C.A. Umberto Pinotti.

Visita di una delegazione della Polizia Armata Cinese

L'8 luglio 2015, nell'ambito dell'attività di cooperazione tra l'Arma dei Carabinieri e la Cina, una delegazione della Polizia Armata Cinese ha visitato la Scuola.

Chiusura dell'Anno Accademico 2014/2015

Il 28 luglio 2015, alla presenza del Capo di Stato Maggiore della Difesa, del Comandante Generale dell'Arma dei Carabinieri, del Comandante delle Scuole dell'Arma, del Corpo docente dell'Istituto e degli Ufficiali frequentatori, si è svolta la cerimonia di chiusura dell'Anno Accademico 2014/2015.

Visita di una delegazione della Polizia Nazionale Colombiana

Il 7 settembre 2015 una delegazione della Polizia Nazionale Colombiana, accompagnata dal Col. Jorge Gallego, Ufficiale di collegamento presso l'Ambasciata colombiana in Italia, ha visitato la Scuola.

ATTUALITÀ E COMMENTI

CONTROLLO DEL TERRITORIO E ATTIVITÀ INFORMATIVA

PRIMI STRUMENTI DI CONTRASTO AL TERRORISMO DI MATRICE RELIGIOSA(*)

1. Introduzione

Il terrorismo è un fenomeno antico, in continua evoluzione, intrinsecamente complesso e articolato e, per questo, di difficile interpretazione. Soprattutto, sotteso al concetto di terrorismo, vi è quello di lotta non convenzionale, o guerra asimmetrica, intesa come conflitto ad armi impari in cui una delle parti in causa è costretta a difendersi da un nemico invisibile, trovandosi dunque in una condizione di palese svantaggio.

Dal dopoguerra a oggi il nostro Paese è stato interessato da fenomeni di terrorismo di matrici diverse, politico-territoriale (irredentismo altoatesino), ideologica (brigate rosse, NAR), religiosa (integralismo islamico). Ma è solo dall'attentato "delle Torri Gemelle" dell'11 settembre 2001 che l'attenzione si è concentrata in particolare sulle organizzazioni fondamentaliste musulmane.

In realtà, la nostra penisola aveva già subito attacchi portati da esponenti del radicalismo religioso, anche se le motivazioni erano riconducibili più che altro alla questione palestinese: si citano, ad esempio, la "strage di Fiumicino" del 1973, quando un commando dell'OLP uccise trentaquattro persone, ferendone altre quindici, tutti passeggeri di un volo PANAM, proseguito poi con un dirottamento. La "seconda strage di Fiumicino" del 1985 dove sempre un gruppo di terroristi palestinesi aprì il fuoco sui passeggeri in coda al check-in di un volo della El Al, la compagnia di bandiera israeliana (diciassette morti).

L'*escalation* vera e propria di attacchi portati sul suolo europeo da parte di estremisti islamici iniziò con gli attentati di Madrid del 2004, proseguendo con quelli di Londra del 2005 e di Parigi dei giorni scorsi.

È quindi da circa un decennio che l'attenzione degli apparati di sicurezza e di *intelligence* dei paesi del Vecchio Continente si sono focalizzati su questo nuovo fenomeno, sentito come un nemico subdolo e strisciante, che non si palesa con armate di carri armati e flotte di bombardieri, bensì con piccole unità di uomini armati in maniera leggera, se non addirittura con mezzi improvvisati (IED, *Improvised Explosive Device*).

(*) - Ciclo addestrativo 2015. Conferenza al personale del Comando Provinciale di Forlì-Cesena.

Proprio per la connotazione asimmetrica della minaccia, per le sue capacità di infiltrazione nel tessuto sociale e il basso profilo, questa nuova tipologia di guerra non si combatte con schieramenti di truppe, ovvero con le forme più classiche di arte militare, bensì con un soldato atipico: l'operatore di polizia. Infatti, l'attore principale di questa guerra al terrore è l'apparato di sicurezza interno di un Paese, più che le sue Forze Armate.

E, nella realtà italiana, nell'ambito delle Forze dell'Ordine, l'Arma dei Carabinieri è l'Organizzazione che può fare la differenza; per la capillarità che la contraddistingue e per quella coscienza informativa che fu in passato punto di forza della nostra Istituzione e che oggi va necessariamente riscoperta e incrementata.

2. Pillole di Islam

L'islam è una religione nata nella Penisola Arabica agli inizi del 600 d.C. per predicazione del suo profeta Maometto. Essa si basa su un libro sacro, il Corano (Qur'an, "recitazione") formato da 114 "sure" (capitoli), distribuite in 6226 versetti. Nel 622 d.C. Maometto si reca presso Medina (Madinat al-Nabi, "la città del profeta") con i suoi discepoli, chiamati muslimûn: questo viaggio è chiamato higra, "egira", "emigrazione", e da lì parte il calendario musulmano (infatti, questo è l'anno 1436).

La religione dell'Islam consiste nella fede (al-īmān) e nella pratica (al-dīn). I cinque pilastri dell'Islam (Arkān al-Islām) è l'espressione usata per indicare i cinque obblighi fondamentali di ogni musulmano, uomo o donna, in base alla legge religiosa (Sharī'a) che il musulmano devoto è tenuto a osservare, ritenendoli atti essenziali per compiacere Dio (Allah) che li ha ordinati.

Tali obblighi sono:

1. La testimonianza di fede (Shahada);
2. Le preghiere rituali (Salah);
3. L'elemosina (Zakat);
4. Il digiuno durante il mese di Ramadan (Sawm o Siyam);
5. Il pellegrinaggio a La Mecca almeno una volta nella vita per tutti quelli che siano in grado di affrontarlo (Hajj).

L'islam riconosce la sacralità della Bibbia, perché è un libro "rivelato"; cristiani ed ebrei sono "Le Genti del Libro", come i musulmani. Inoltre riconosce l'esistenza di Gesù Cristo, ma non come Figlio di Dio, bensì come suo profeta.

Nel 630 d.C. Maometto guida un esercito di diecimila uomini contro Mecca; la città si arrende senza combattere ed egli, dopo aver distrutto gli idoli pagani, proclama "Allah akbar", "Dio è grande!", imponendo il monoteismo. La formula di conversione è "non vi è altro Dio che Dio e Maometto è il suo profeta".

Dopo la morte di Maometto, avvenuta nel 632 d.C., inizia una disputa tra i suoi successori riguardo al leader della ummah (la "comunità dei fedeli"), cioè il "califfo": la maggioranza sosteneva la tesi dell'elezione del successore del profeta (in seguito chiamati "sunniti"); ma una minoranza insisteva sul fatto che il califfato dovesse essere riservato al cugino e genero di Muhammad, Ali ibn Abi Talib, e alla discendenza di questi e di sua moglie Fatima.

Questa fazione era conosciuta come Shi'at Ali, «i seguaci di Ali». Il termine «imam» è importante per comprendere le differenze dottrinali tra sunniti e sciiti. Tutti i musulmani usano questa parola per indicare la «guida della preghiera», chi conduce la congregazione nel culto. Ma la maggior parte degli sciiti usa il termine imam in un senso più ristretto, per riferirsi al legittimo leader spirituale dell'intera ummah, che deve essere un diretto discendente di sangue del profeta. Il primo di questi imam, fu Ali e il terzo suo figlio Husain.

Per i sunniti, invece, indica qualunque leader religioso di qualunque comunità. Gli sciiti furono la parte perdente in questo scontro, e rappresentano non più del 10-15% dell'intera popolazione musulmana (circa un miliardo e seicento milioni), concentrata in particolar modo in Iran e in Iraq.

3. L'integralismo

Alle origini il Salafismo un movimento profondamente e sinceramente religioso che si batteva per il recupero di un Islam puro, privo dei tradizionalismi religiosi che contraddistinguevano l'Islam ufficiale fino al XIX secolo.

I primi salafiti propugnavano una Nahda, una rinascita culturale islamica, e proponevano una lettura ambivalente dell'Islam. Da un lato erano contrari a una sua lettura troppo tradizionalista, dall'altra criticavano alcune correnti sufi, i mistici dell'Islam sunnita che erano spesso considerati degli eretici a causa della loro lettura allegorica del Corano.

I sufi valorizzavano principalmente il batin, il significato interiore del Corano, piuttosto che lo zahir, quello esteriore. Per i salafiti, questi mistici erano complici degli invasori occidentali che avevano colonizzato anche culturalmente l'Egitto, diffondendo nuovi usi e costumi.

Il significato del termine salafita è gradualmente cambiato e oggi è utilizzato per indicare coloro che vogliono implementare la shari'a, la legge islamica, ritenendo corretta una lettura integrale e letterale del Corano e della sunna, l'insieme del comportamento e degli insegnamenti del Profeta Maometto.

Per questo i salafiti dicono di essere i veri seguaci dell'Islam: perché emulano i primi pii musulmani, i salaf, professando la versione a loro avviso più autentica dell'Islam. Rifiutando l'adesione a ciascuna delle quattro tradizionali scuole giuridiche - hanafita, hanbalita, malikita, shafiita - i salafiti sono stati influenzati dalla lettura di Muhammad Ibn Abd al-Wahhab, il severo sapiente islamico cui si legò Muhammed Ibn Saud per dar vita al Regno dell'Arabia Saudita, a metà del XVIII secolo.

Abd al-Wahhab è anche l'uomo attorno al quale è nato il wahabismo, un movimento islamista dogmatico prevalentemente saudita. Il movimento salafita si ispira infatti a sapienti radicali come Ibn Taymiyya, importante teologo siriano del XIII secolo e fervente sostenitore della jihad, che divenne un simbolo per Abd al-Wahhab.

Il wahabismo è la corrente che più di ogni altra ispira gli integralisti, e quindi i terroristi, odierni. Osama bin Laden era un wahabita, così come Abu Bakr Al-Baghdadi, il sedicente califfo dello Stato Islamico (IS o ISIS o ISIL).

Esistono forme di integralismo anche tra gli sciiti.

Basti pensare a Hezbollah, organizzazione combattente libanese legata all'Iran, di confessione sciita come la religione ufficiale di Teheran. All'interno del mondo fondamentalista rimane, però, predominante e preponderante la componente sunnita di matrice wahabita.

In un articolo presente nel sito web di Elaph (Īlāf, "L'Alleanza"), giornale ritenuto uno dei più letti su internet, Othman Al-Omeir, il suo Direttore, denuncia il fondamentalismo wahabita per il suo aspetto anti-cristiano all'interno scrivendo che ogni giorno, nelle moschee, gli imam incitano i fedeli all'odio contro i cristiani.

Così scrive: "Quegli imam diffondono un Credo totalitario intriso di violenza, che trova eco persino in alcuni documenti ufficiali del governo di Ryad, la Capitale dell'Arabia Saudita. Si sostiene che è un obbligo religioso per ogni musulmano odiare i cristiani e che non bisogna imitarli, né fraternizzare con loro né aiutarli in alcun modo. Guai a salutarli per primi, guai a porgere gli auguri a Natale.

La democrazia è anti-islamica e dunque va respinta. I 'Fratelli' che si trovano nelle terre dei miscredenti devono comportarsi come se fossero in missione dietro le linee nemiche, acquisendo nuove conoscenze e fondi da usare per la Guerra Santa o facendo proselitismo.

Qualunque altra ragione non è ammessa. E chi osa convertirsi al cristianesimo sappia che sarà ucciso. Così si parla nelle moschee e nelle scuole coraniche wahabite".

4. Il processo di radicalizzazione

La minaccia terroristica può provenire da formazioni ben conosciute, già autrici di attentati e attacchi in varie parti del mondo (Al-Qaida, ISIS, Boko Haram), per il tramite di elementi organici all'organizzazione, e da questa addestrati, armati ed equipaggiati. Questi soggetti sono inviati direttamente dai campi di addestramento e dalle basi dei gruppi terroristici a compiere la propria missione. Tale forma di minaccia è paradossalmente più prevenibile e fronteggiabile, poiché, soprattutto dopo l'"11 settembre", le *intelligence* di tutte la Nazioni (occidentali, ma anche dei Paesi musulmani) investono notevoli risorse nel controllo e monitoraggio di queste organizzazioni, individuandone le filiere di reclutamento e riuscendo, così, a sventarne la maggior parte delle minacce.

Altro problema, invece, è rappresentato da quei singoli elementi, o gruppi di poche persone, già presenti sul territorio nazionale, che, a seguito di un processo di radicalizzazione ideologica, si convertono alla jihad e si equipaggiano per compiere attentati.

È su questo tipo di soggetti, definiti *lone actors*, che si deve concentrare l'attenzione delle forze dell'ordine che presidiano il territorio.

Fino ad oggi il nostro Paese ha conosciuto pochi casi di atti terroristici compiuti da elementi solitari che hanno maturato il loro proposito all'interno dei confini nazionali. Il primo ebbe luogo a Modena nel dicembre 2003, quando un trentatreenne di origini palestinesi, Muhannad al-Khatib, riempì la sua Peugeot 205 con due taniche di benzina e una bombola di Gpl e la parcheggiò di fronte alla sinagoga nel centro del capoluogo emiliano.

Al-Khatib dapprima cercò di dar fuoco alla macchina dall'esterno, poi, non riuscendovi ed essendo sopraggiunta una volante della polizia, entrò in macchina e si fece esplodere, morendo, ma non causando altri feriti o danni.

Al-Khatib era sconosciuto alle autorità e non risulta avesse idee o legami estremisti. I suoi conoscenti di allora lo descrivono come cronicamente depresso e dicono avesse espresso il desiderio di uccidersi.

Un episodio molto simile avvenne a Brescia la sera del 28 marzo 2004, quando un trentaseienne marocchino, Moustafa Chaouki, parcheggiò la sua Fiat Tempra nella corsia "drive through" di un McDonald's della città lombarda e la fece esplodere.

Come a Modena, l'esplosione uccise l'attentatore ma non causò altri feriti o ingenti danni.

Due giorni dopo l'esplosione, la questura di Brescia ricevette una lettera scritta da Chaouki in cui il marocchino rivendicava l'atto, indicava che nessuno lo aveva aiutato e che aveva compiuto il gesto per vendicare le sofferenze delle popolazioni arabe, in particolare in Palestina e in Iraq. Come al-Khatib, Chaouki era sconosciuto alle autorità antiterrorismo. Aveva vissuto in Italia sin dal 1989, lavorando come manovale e autista nel bresciano e nel bergamasco, non aveva precedenti penali e i suoi padroni di casa e datori di lavoro lo descrivono come un soggetto irreprensibile.

La separazione dalla moglie nel 2002 lo portò a chiudersi in se stesso, limitando i contatti con i suoi fratelli che erano in zona e andando a vivere da solo in un camper. Poche settimane prima di uccidersi aveva perso il lavoro e aveva detto ai fratelli che si sentiva un fallimento nella vita privata e in quella professionale.

Nei primi mesi del 2003 Chaouki aveva preso contatto con un'organizzazione di Brescia che fornisce supporto psicologico contro la depressione e si era incontrato in varie occasioni con una loro esperta. Dopo l'incidente al McDonald's, la donna disse agli inquirenti che Chaouki non aveva mai espresso astio contro l'Italia e che non aveva dato segnali né di forti passioni politiche o religiose né di tendenze suicide.

Questi due soggetti hanno agito come prototipi di lone actor, non coinvolgendo nessuno in alcuna fase del loro piano, e pare che nessuno sapesse dell'intenzione di ciascuno dei singoli attentatori di compiere quel gesto.

I soggetti non appartenevano nemmeno marginalmente ad alcun nucleo militante e non era nota alcuna loro simpatia fondamentalista.

È ovviamente molto difficile capire queste dinamiche a posteriori, ma è possibile che al-Khatib e Chaouki abbiano voluto mascherare la loro intenzione di commettere suicidio - un atto considerato riprovevole, oltreché un peccato gravissimo nella loro cultura - per motivi personali con la scelta di modalità che avrebbero potuto rendere il loro un gesto eroico agli occhi di parte della loro comunità.

Negli anni 2000 l'Europa è stata segnata da numerosi attacchi terroristici di matrice jihadista (Madrid, Londra), mentre l'Italia ne è rimasta sostanzialmente estranea. Un insieme di fattori spiega quest'eccezione a livello europeo.

La pressione esercitata dalle autorità italiane contro le filiere jihadiste presenti sul territorio è probabilmente il principale.

Continue ondate di arresti che iniziarono nel 2000 smantellarono numerose cellule in Lombardia e nel resto del Paese.

Una volta arrestati gli obiettivi principali di un'indagine, le autorità italiane solevano aprire una nuova inchiesta contro i soggetti marginali, smantellando così nuclei interi. Grazie a questo approccio investigativo estremamente tenace, decine di estremisti furono arrestati, nella maggior parte dei casi (con importanti eccezioni) condannati a pochi anni di prigione e in seguito espulsi verso il paese d'origine. Altri furono semplicemente espulsi dal territorio nazionale per motivi di ordine pubblico, non per via processuale, ma con un decreto amministrativo.

Nel 2007 una serie di indagini svolte dimostrò che il fenomeno jihadista in Italia stava cambiando. La prima inchiesta fu resa pubblica nel luglio di quell'anno, quando quattro marocchini che risiedevano in provincia di Perugia furono arrestati in base all'articolo 270 quinquies del Codice penale. L'articolo, come si vedrà, fu introdotto nel luglio del 2005 e punisce individui che forniscono o ricevono addestramento su esplosivi, armi oppure ogni altra tecnica che possa essere utilizzata per fini terroristici. L'operazione "Hammam" della DIGOS di Perugia svelò una sorta di "scuola jihadista" tenuta da Mostapha el-Korchi, il quarantenne imam della piccola moschea al-Nour di Ponte Felcino, una frazione del capoluogo umbro. Il marocchino, terminate le funzioni religiose, organizzava delle "lezioni" a porte chiuse a pochi giovani selezionati, durante le quali inneggiava alla guerra santa e faceva visionare filmati di addestramento alle tattiche di guerriglia e di propaganda estremista religiosa. L'indagine è molto simile ad altre due compiute nel milanese (a Macherio, "Operazione Shamal") e in Calabria (Sellia Marina, "Operazione Hanein") nei mesi successivi. Nella prima, conclusa nel dicembre 2008, la Digos di Milano arrestò due marocchini, accusandoli di pianificare attacchi contro vari obiettivi a Milano e in Brianza. Nella seconda, le autorità rinviarono a giudizio tre marocchini, incluso l'imam della locale moschea, in base all'articolo 270 quinques.

Questi tre casi presentano numerosi punti in comune tra di loro. I tre nuclei, infatti, operavano indipendentemente da gruppi strutturati. Inoltre, anche se è vero che la maggior parte dei militanti della scena tradizionale faceva ampio uso di internet, i tre gruppi in esame sembrano che avessero posto il web al centro delle loro attività. Internet era l'unico modo in cui questi nuclei, non avendo solidi contatti con il mondo jihadista globale e operando, nel caso di Ponte Felcino e Sellia Marina, geograficamente isolati da altri nuclei jihadisti italiani, potevano approfondire la loro conoscenza dell'ideologia jihadista, imparare tattiche e celebrare le azioni di vari gruppi jihadisti.

Inoltre, in tutti e tre le indagini la moschea, anche se si tratta più di piccole sale di preghiera improvvisate, svolge un ruolo fondamentale al punto che in tutti e tre i casi l'imam era la forza trainante del nucleo. Nonostante frequenti eccezioni, la nuova generazione di jihadisti autoctoni europei tende, invece, a non essere affiliata ad alcun luogo di preghiera. Va infine evidenziato che il livello di sofisticazione dei nuclei era alquanto ridotto. In sostanza possono essere visti semplicemente come aggregazioni informali di giovani ai margini della società, senza previe connessioni con il jihadismo e che hanno seguito un leader carismatico, egli stesso privo di forti legami con gruppi jihadisti strutturati.

L'episodio che demarca un cambiamento significativo delle dinamiche del jihadismo in Italia avvenne il mattino del 12 ottobre 2009 presso la caserma Santa Barbara, un'estesa struttura militare alla periferia occidentale di Milano. Alle ore 7:40, quando il cancello della porta carraia all'entrata principale della caserma era aperto per favorire l'afflusso delle macchine del personale di servizio, un uomo cercò di varcare la soglia a piedi. Viste le guardie all'ingresso, l'uomo si chinò e fece esplodere una scatola nera che teneva sotto il braccio, urlando qualcosa in una lingua (con ogni probabilità l'arabo) che nessuno comprese. Le autorità stabilirono in seguito che l'esplosione dei 4,6 chilogrammi di una sostanza esplosiva a base di triacetontriperossido (Tatp) che il soggetto trasportava si ridusse a causa del cattivo stato di conservazione della sostanza e del basso potere d'innesco del detonatore. L'esplosione comunque causò ferite serie agli occhi dell'attentatore, che perse anche la mano destra. Due soldati invece riportarono alcune lievi ferite. La polizia arrivò sulla scena pochi istanti dopo l'esplosione. Nonostante le ferite, l'uomo riuscì a sussurrare al primo poliziotto che lo soccorse: «Ve ne dovete andare via dall'Afghanistan». Mentre gli agenti lo perquisivano aggiunse: «Non ho nient'altro... niente... mi chiamo Game e sono della Libia». L'indagine che seguì rivelò che l'uomo si chiamava Mohammed Game ed era, in effetti, un libico nato a Benghazi nel 1974. Game era arrivato in Italia nel 2003, dopo aver studiato da perito elettronico nel suo paese. Game non era conosciuto alle autorità dell'antiterrorismo italiane e l'indagine rivelò che la sua radicalizzazione era avvenuta di recente. Sua moglie e suo fratello Imad raccontarono agli inquirenti che Game aveva avuto un attacco cardiaco nel 2008 e che da allora la sua vita era cambiata completamente. Imad raccontò che Game aveva iniziato a frequentare la moschea di Viale Jenner, all'epoca considerata la più integralista della realtà italiana.

I tecnici informatici della polizia scoprirono che Game era un avido consumatore di materiale jihadista e che aveva salvato sul suo computer 788 file su questo tema. Game inoltre aveva consultato materiale di varia natura, ma sembrava che fosse rimasto particolarmente affascinato dagli scritti di Abu Musab al-Suri, del quale scaricò 185 file. Al-Suri, uno dei più celebrati ideologi del movimento jihadista globale, è particolarmente noto per aver elaborato il concetto di resistenza senza leader e di jihad tramite terrorismo individualizzato. Formulando un'idea che è stata adottata poi da altri vari leader e gruppi del movimento jihadista globale, al-Suri propugnava un sistema operativo in cui individui o piccoli gruppi isolati potessero operare autonomamente senza stabilire contatti tra loro. Ciò che, secondo al-Suri, avrebbe unito questi soggetti sarebbe stato semplicemente «un obiettivo comune, un programma dottrinario condiviso e comprensivo di (auto-)educazione». Gli scritti di al-Suri, la maggior parte dei quali datati anni Novanta, sono visti come la teorizzazione della fase attuale del jihadismo autoctono in Occidente.

5. Prevenzione e controllo del territorio

Dall'analisi dei casi fino a qui tracciati si può dedurre che la minaccia alla sicurezza pubblica può derivare, in sintesi, da tre tipologie di terroristi: elementi addestrati, armati ed equipaggiati da organizzazioni ben strutturate, di livello internazionale (Al-Qaeda, Al Nu'sra…); soggetti che sono indottrinati e parzialmente equipaggiati da cellule indipendenti, già presenti sul territorio (imam di Perugia); *lone actor*, che si autoindottrinano tramite internet e si procurano armi e materiali in autonomia (Game).

Mentre il primo tipo di minaccia è contrastato principalmente con attività di intelligence da parte delle Agenzie nazionali a ciò preposte, le cellule indipendenti e i *lone actor* sono invece, in larga parte, obiettivo delle Forze di Polizia.

È infatti tramite un incisivo e costante controllo del territorio e un'approfondita e puntuale attività informativa che realtà come quella di Perugia o soggetti come il Game vengono allo scoperto.

In questo senso, la Forza che più di ogni altra ha la possibilità di incidere in maniera significativa sulla sicurezza nazionale è l'Arma dei Carabinieri, per quella già richiamata capillarità che la contraddistingue.

Si rende pertanto necessario, da parte di ogni componente dell'Organizzazione territoriale, dalla più piccola Stazione fino ai Comandi più grandi, acquisire una mentalità che, sebbene nuova negli obiettivi, in realtà è antica quanto l'Arma.

La coscienza informativa, infatti, è patrimonio dell'Istituzione e suo punto di forza da due secoli, e forse mai come oggi va riscoperta e applicata. Nella lotta al terrorismo di matrice religiosa, però, tale attività deve essere focalizzata su alcuni aspetti, che devono essere tenuti in considerazione.

Il primo è che la comunità musulmana tende ad essere attrattiva per la maggior parte delle persone che appartengono a quella fede. Anche per il fatto di essere stranieri o figli di immigrati in terra straniera, i cittadini provenienti dai Paesi musulmani tendono a raggrupparsi e frequentare i Centri islamici o le moschee.

È pertanto necessario intrattenere costanti e rispettosi rapporti con i leader di tali comunità che, va ricordato, sono per la quasi totalità dei religiosi moderati che per primi hanno interesse ad isolare elementi integralisti e pericolosi.

Vi è poi il massivo uso di internet da parte di soggetti che si sono avvicinati a idee fondamentaliste. Partendo dal presupposto che tendenzialmente i soggetti immigrati usano la Rete per comunicare con i famigliari nei loro Paesi d'origine e per tenersi informati su cosa vi avviene, l'utilizzo dello strumento telematico è ancor più frequente da parte di coloro che intendono aderire alle idee più integraliste o che vogliano addestrarsi al confezionamento di ordigni rudimentali e altri mezzi offensivi.

Da quanto detto sopra, deriva che l'operatore di polizia, e in particolare il carabiniere appartenente all'Organizzazione territoriale, dovrà usare maggiori attenzioni nel relazionarsi con persone di fede islamica, valutando se si trova di fronte a un soggetto credente sì, magari anche praticante, ma dalle idee e dai comportamenti assolutamente leciti; o se, al contrario, si è imbattuto in un elemento già radicalizzato o in corso di radicalizzazione. I segnali di questo mutamento, già avvenuto o in corso, possono essere evidenti (barba, abiti e copricapi tradizionali, moglie coperta da niqab, abaya o addirittura burqa) oppure possono essere assolutamente invisibili. Quest'ultima possibilità rientra nel concetto di "occultamento" (kitman o taqiyya), ovvero nella possibilità che colui che intende diventare martire della fede (l'impropriamente detto "kamikaze", ma che in lingua araba si definisce shahid, "colui che testimonia la fede islamica" fino alla morte) possa adottare degli atteggiamenti contrari alla shari'a per celare i suoi intendimenti. Questi soggetti, pertanto, vestono all'occidentale, bevono alcool, magari mangiano anche il maiale, il tutto per confondere l'avversario (kafir, l'infedele), comportandosi come lui ed inducendolo a fidarsi.

Imbattersi in una persona che, pur apparendo del tutto non praticante, abbia invece sul proprio computer diversi filmati sulla jihad o intrattenga contatti telematici con soggetti o gruppi fondamentalisti, deve immediatamente attivare l'attenzione dell'operatore di polizia, che attuerà tutte le misure del caso (informare, nel caso dell'Arma, il Nucleo Informativo Provinciale, redigendo apposita annotazione di polizia giudiziaria).

Vedremo, ora, gli strumenti giuridici a disposizione degli agenti e ufficiali di polizia giudiziaria nel contrasto a questo fenomeno.

6. Strumenti normativi

Storicamente, la maggior parte dei jihadisti arrestati in Italia è stata accusata di associazione con finalità di terrorismo (articolo 270 bis del Codice penale). L'articolo, così come modificato nel dicembre 2001, dice che «chiunque promuove, costituisce, organizza, dirige o finanzia associazioni che si propongono il compimento di atti di violenza con finalità di terrorismo o di eversione dell'ordine democratico è punito con la reclusione da sette a quindici anni. Chiunque partecipa a tali associazioni è punito con la reclusione da cinque a dieci anni. Ai fini della legge penale, la finalità di terrorismo ricorre anche quando gli atti di violenza sono rivolti contro uno Stato estero, un'istituzione e un organismo internazionale».

Il dettato normativo, però, nasce dall'esigenza di contrastare fenomeni di terrorismo in cui si possa riconoscere un'organizzazione tradizionale, ben strutturata. Le problematiche maggiori provengono dalla gestione di fattispecie che riguardino piccoli nuclei indipendenti (Imam di Perugia) o i lone actor. Se da un lato vi è la necessità non solo di monitorare questi soggetti ma anche, in certi casi, di arrestarli prima che compiano atti immediatamente preparatori a un attacco, tale esigenza è controbilanciata da quella di non criminalizzare quei soggetti solo per delle opinioni espresse. Nel 2005 il legislatore italiano optò per una soluzione che pende maggiormente nella direzione delle esigenze di sicurezza e introdusse l'articolo 270 quinquies del Codice penale. L'articolo punisce con la detenzione fra i cinque e i dieci anni chiunque «addestra o comunque fornisce istruzioni sulla preparazione o sull'uso di materiali esplosivi, di armi da fuoco o di altre armi, di sostanze chimiche o batteriologiche nocive o pericolose, nonché di ogni altra tecnica o metodo per il compimento di atti di violenza ovvero di sabotaggio di servizi pubblici essenziali, con finalità di terrorismo, anche se rivolti contro uno Stato estero, un'istituzione o un organismo internazionale».

La norma, in sostanza, cerca di punire comportamenti che precedono e sono funzionali alla commissione del reato e punisce sia colui che fornisce le informazioni, "addestratore" e "informatore," sia colui che le riceve, cioè l'"addestrato", anche se il soggetto che ha ricevuto le informazioni non le mette in pratica e perfino se non le ha intese (sentenza Corte di Cassazione, Sezione Penale I, caso 872, 12 luglio 2011, Korchi e altri).

Una delle più serie difficoltà che presenta l'applicazione di questa norma nella lotta contro la nascente minaccia del jihadismo autoctono in Italia, però, è data dal fatto che, sebbene sembri impossibile accusare lone actor di un reato di natura associativa come quello previsto dall'articolo 270 bis, tuttavia anche l'articolo 270 quinquies è inevitabilmente soggetto a una forte discrezionalità interpretativa da parte giudiziale, essendo una norma che punisce comportamenti che non sono necessariamente collegati ad atti violenti. La serie di condotte attuate da un soggetto, infatti, possono per un giudice essere sufficienti a configurare il reato, per un altro esprimere un mero interesse ad argomenti "scabrosi", ma che non sottintende necessariamente una volontà di delinquere.

7. Conclusioni

Come in ogni altro Paese europeo, la radicalizzazione d'ispirazione jihadista in Italia riguarda solo una frazione statisticamente insignificante della popolazione di fede musulmana. Ma il fenomeno in Italia sembra essere ridotto anche quando paragonato con altri Paesi europei. Non è certo il perché di questa peculiarità italiana, ma la relativa tranquillità che il nostro Paese ha attraversato finora sotto questo aspetto non deve indurci ad abbassare la guardia.

I recenti fatti di Parigi, infatti, ci costringono ad occuparci del fenomeno in maniera ancor più incisiva e, come detto, l'Arma deve essere in prima linea nella lotta a queste forme di minaccia. Dopo l'intelligence, che ha di fronte un lavoro enorme di prevenzione dagli attacchi che possono essere portati entro i confini nazionali, lo strumento di contrasto più efficace rimane l'attività informativa messa in essere dai nostri reparti territoriali. Opera che potrà fare la differenza se incrementata e attuata con precisione e scrupolo.

Diego Polio
Maggiore dei Carabinieri,
Comandante della Compagnia Carabinieri di Cesena

Riferimenti bibliografici

- Paul Balta, *L'islam*, ed. 2006, Armando ed.;

- Khaled Fouad Allam, *Il jihadista della porta accanto*, Piemme ed.;

- Limes, rivista italiana di geopolitica, *Le maschere del califfo*, n. 9, settembre 2014;

- Lorenzo Vidino, *Il jihadismo autoctono in Italia: nascita, sviluppo e dinamiche di radicalizzazione*, European Fondation for democracy, Istituto per gli studi di politica internazionale, ed. 2014.

Sitografia

- http:storiografia.me/2013/11/21/un-movimento-sunnita;

- http://www.ispionline.it.

L'ARMA NELLA GRANDE GUERRA

Prof. Renato Lopresto

A tutti sono note le funzioni conformi alla sua tradizione che l'Arma svolse durante la Guerra 1915-1918, vale a dire quei compiti connessi alla sua stessa nascita, avvenuta nel lontano 1814, ad opera di Vittorio Emanuele I di Savoia, deciso a ristabilire l'ordine nel regno e a contrastare il ricordo di Napoleone e della Rivoluzione francese.

Attività di polizia militare, di assistenza alle popolazioni costrette ad abbandonare le proprie case, di salvaguardia delle strutture d'interesse strategico (come ferrovie e ponti), di spionaggio e controspionaggio, di opposizione ai fenomeni di ribellione e di diserzione che in certi periodi critici del conflitto coinvolse interi reparti: particolarmente triste a questo riguardo l'episodio della brigata Catanzaro accaduto il 15 luglio 1917 quando, impiegata a lungo e gloriosamente su vari fronti, durante un periodo di meritato riposo, si ribellò all'ordine di rientrare in prima linea. Ne seguì la decimazione.

Ma quanti sanno che i carabinieri presero parte attiva alle operazioni di guerra con la divisa grigioverde? Furono infatti impegnati in unità combattenti fin dai primi giorni del conflitto. Del resto, dal 1914 lo Stato maggiore dell'Esercito aveva previsto per l'Arma la duplice funzione di polizia militare e di forza combattente.

Il 24 maggio 1915 il Reggimento Carabinieri Reali Mobilitato, composto da militi che provenivano dalle diverse Legioni Territoriali, partì per raggiungere il settore orientale italiano per poi attestarsi, secondo gli ordini ricevuti, sulle pendici del Monte Podgora, alle dipendenze del Comando della Brigata Pistoia e quindi del 6° Corpo d'Armata. Lo comandava il colonnello Antonio Vannugli che nel suo Diario di guerra, in data 19 luglio 1915, scrive: "Il Reggimento Carabinieri deve conquistare la cresta di Quota 240, corrispondente al proprio fronte ed ivi rafforzarsi."

Il Reggimento era formato da nove compagnie e comprendeva sessantacinque ufficiali e duemilacinquecento tra sottufficiali e truppa. Presto vennero aggiunti un Gruppo Squadroni, 257 Plotoni e 168 Sezioni, che insieme raggiungevano cinquecento ufficiali e poco meno di ventimila tra sottufficiali e truppa. I Plotoni e le Sezioni, a differenza del Reggimento e degli Squadroni, avevano solo compiti di polizia militare. Il fronte era quello dell'Isonzo che il Comandante Supremo generale Cadorna considerava primario, anche per la corretta osservazione della natura del terreno, in certi punti meno impervio rispetto a quello degli Altipiani. Ma dopo i primi modesti successi, ottenuti a caro prezzo, la sua strategia si rivelò inefficace. L'obiettivo di Cadorna era raggiungere Lubiana e da lì puntare su Vienna. Ci volle invece un anno per conquistare Gorizia (agosto 1916) e le undici sanguinose battaglie dell'Isonzo, insieme con le pessime condizioni di vita e la disciplina inflessibile e, per certi aspetti disumana, imposta dall'alto, servirono solo a logorare il fisico e il morale dei nostri combattenti. Seguì il disastro di Caporetto (ottobre 1917), che costrinse Vittorio Emanuele III a sostituire Cadorna con Diaz.

Tra il 23 giugno e il 7 luglio 1915 si era svolta la prima battaglia dell'Isonzo, la prima delle famose spallate che avrebbero dovuto aprire al nostro esercito la strada per Vienna: i reparti italiani avevano ricevuto l'ordine di puntare su Gorizia, Tolmino e il Carso, dove era forte la linea di difesa austriaca. L'impeto dei nostri fanti fu smorzato dall'insufficienza della nostra artiglieria, per cui la battaglia si concluse senza esiti positivi. Dieci giorni dopo giunse l'ordine d'una nuova offensiva, che dette inizio alla seconda battaglia dell'Isonzo (18 luglio - 3 agosto 1915). L'obiettivo principale era la conquista del Monte San Michele nel gruppo del Carso, da dove il nemico difendeva Gorizia. Il Reggimento Carabinieri avrebbe ricevuto lo stesso compito: effettuare un'azione dimostrativa per favorire l'attacco sul Carso. Gli italiani raggiunsero alcune posizioni che non poterono mantenere, sempre a causa dell'insufficienza dell'artiglieria. Fu in questo scenario che si distinsero e si sacrificarono i nostri carabinieri. Non era la prima volta che l'Arma affrontava la linea del fuoco. Si era già distinta in diverse occasioni ancora prima della nostra unità nazionale, particolarmente durante le guerre d'indipendenza a Pastrengo, a Montebello, a Palestro, a Magenta, a San Martino.

Ai piedi del Monte Podgora, nel luglio del 1915, la situazione era molto difficile e pericolosa: nel territorio l'acqua scarseggiava, nelle trincee le condizioni igieniche precarie, i mezzi disponibili insufficienti, il nemico in posizione dominante in cima al monte, le speranze di farcela scarse. Quando fu in zona, partito il 5 luglio da Udine, dov'era acquartierato, passando per Cormons, il Reggimento Carabinieri dovette farsi carico di costruire sbarramenti, organizzare posti di blocco, assolvere compiti di polizia militare, prima di raggiungere e sistemarsi alla meglio nelle trincee di fronte a Quota 240, sotto il tiro degli austriaci.

Anche qui i carabinieri provvidero a costruire opere di fortificazione e di collegamento fra le trincee, col rischio continuo rappresentato dalle batterie nemiche, che provocarono non pochi feriti, e con l'incubo delle malattie diffuse in quel luogo malsano.

Tuttavia, quando giunse l'ordine del Comando del 6° Corpo d'Armata di passare all'attacco, verso le ore 11 della mattina del 19 luglio, il colonnello Vannugli intimò l'assalto e, subito dopo il grido del tenente colonnello Pranzetti "Alla baionetta!", l'8° Compagnia del capitano Vallaro, la 7° del capitano Losco e la 9° del capitano Lazzari, che componevano il 1° Battaglione, a breve distanza tra loro, si lanciarono verso l'alto sotto i colpi furiosi degli austriaci. Gli ordini ricevuti erano appunto quelli di assaltare all'arma bianca.

Seguirono perdite gravissime, soprattutto sul fianco destro del Battaglione, senza che i militi desistessero dall'impresa disperata.

L'intenso fuoco nemico riuscì a rallentare ma non a fermare l'avanzata dell'8° Compagnia, che occupava la prima linea, nonostante il ferimento del capitano Vallaro. Ebbe però l'effetto d'arrestare in parte la seconda linea, quella della 7° Compagnia del capitano Losco, che riuscì a riprendersi e addirittura ad avvicinarsi ai reticolati austriaci, dove fu costretta a fermarsi per la violenta reazione nemica: durante l'azione il capitano Losco cadde eroicamente. La stessa sorte toccò al comandante della 9° Compagnia, che rappresentava la terza linea, il capitano Lazzari. Ma il tenente Mazzerelli, assunto il comando, proseguì fino a pochi metri dai reticolati, dove anche lui fu costretto a fermarsi.

Intorno alle ore 13 fu mandato all'attacco il 2° Battaglione con la 4° e la 5° Compagnia, sotto un fuoco violento che uccise un numero elevato di uomini. Vista l'impossibilità d'insistere, anche perché gli austriaci erano riusciti a piazzare una mitragliatrice in posizione strategica e sicura, colpendo alle spalle i nostri, alle ore 15 circa giunse l'ordine di fermare l'assalto e difendere le posizioni raggiunte. Quindi il Comando della Brigata Pistoia decise di mandare in aiuto tre Compagnie del 36° Fanteria, ripetendo l'ordine di riprendere l'assalto. Ma più tardi il Comando del 6° Corpo d'Armata, resosi conto della situazione priva di speranza senza un appoggio adeguato dell'artiglieria, lo revocò.

Dopo la cruenta e sfortunata battaglia il Reggimento Carabinieri, oltre all'elogio ufficiale degli alti Comandi, ricevette nove medaglie d'argento, trentatré di bronzo e tredici croci al valore militare, ma contò cinquantatré morti, 143 feriti e dieci dispersi. Il suo sacrificio purtroppo non fu compensato dalla vittoria: anche la seconda battaglia dell'Isonzo si concluse, come la prima e come le nove che seguirono, con un nulla di fatto. Ma il 9 agosto 1916, nella sesta battaglia dell'Isonzo (6-17 agosto 1916), i carabinieri avranno la soddisfazione di entrare per primi nella sospirata città di Gorizia.

Nel Regolamento Organico infatti si disponeva che fossero i carabinieri a entrare per primi nelle località conquistate, per "verificare", come scrive nella sua "Storia documentale dell'Arma dei carabinieri" il generale A. Ferrara, "che non vi fossero appostati dei cecchini avversari, stanarli e procedere all'arresto di personaggi ritenuti pericolosi ai fini dello spionaggio; occorreva porre in salvo la cassa comunale e proteggere le proprietà dei cittadini lasciate incustodite dallo sciacallaggio dilagante; occorreva disporsi immediatamente alla vigilanza di ogni struttura utile militarmente, come ponti, stazioni ferroviarie, aeroporti o centrali idriche ed elettriche; occorreva individuare e recuperare armi e munizioni abbandonate dal nemico; occorreva regolare il traffico sugli stradali e coordinare l'afflusso in prima linea dei reparti, evitando dannosi ingorghi."

È sufficiente questo stralcio per dare un'idea delle grandi responsabilità e degli innumerevoli compiti che venivano assegnati all'Arma negli anni tormentati del conflitto.

Il 5 giugno 1920, la bandiera dell'Arma dei Carabinieri ottenne la prima Medaglia d'Oro al Valor Militare, con la seguente motivazione: «Rinnovellò le sue più fiere tradizioni con innumerevoli prove di tenace attaccamento al dovere e di fulgido eroismo, dando validissimo contributo alla radiosa vittoria delle armi d'Italia».

Riferimenti bibliografici

- G. Oliva, *Storia dei Carabinieri*, Mondadori 2002;
- G. Breccia, *Nei secoli Fedele*, Mondadori 2014;
- A. Ferrara, *Storia documentale dell'Arma dei Carabinieri*, Arma dei Carabinieri 2004;
- G. Rochat, *Breve storia dell'esercito italiano 1861-1943,* Einaudi 1978;
- G. Rochat, *L'Italia nella Prima Guerra Mondiale*, Feltrinelli 1976;
- M. Isnenghi - G. Rochat, *La Grande Guerra*, La Nuova Italia 2000;
- E. Forcella - A. Monticone, *Plotone d'esecuzione,* Laterza 2008.

LIBRI

Notkerus Claudus

I Fiori del Silenzio

Edizioni dell'Eremo
2015, pag. 72

La poesia religiosa appartiene ad un filone letterario che ha origini antiche.
Quando, nel 1200, comparvero i primi movimenti eretici (che erano sorti, anche comprensibilmente, in contrapposizione alla corruzione e alla ricchezza del Clero, dedito, tra le altre cose, alla vendita degli uffici sacri e delle indulgenze), l'atteggiamento iniziale della Chiesa fu di totale intolleranza, involutosi, ben presto, nella dura repressione.
Al riguardo, basti pensare alla crociata condotta da Innocenzo III contro gli Albigesi e alla volontà di Gregorio IX di istituzionalizzare l'inquisizione - già nata sotto il pontificato di papa Lucio III - con le vesti formali dei tribunali, da lui appositamente creati.
Successivamente, nell'ambito della riforma che caratterizzò il XIII Secolo, la compagine ecclesiastica adottò una linea volta alla riscoperta di una certa spiritualità interiore, mostrandosi quindi più accomodante nei confronti dei movimenti eretici, sebbene mai in termini arrendevoli, abbandonando gradualmente la via delle soppressione, percorrendo strade alternative di natura squisitamente dottrinale. Si avvalse, a tal uopo, dell'opera di frati predicatori ai quali fu affidato il compito di diffondere la Parola tra il popolo (rinnovando la formula dell'epoca, per tutto l'Alto Medioevo limitata alla comunicazione attraverso le arti figurative). Fu pertanto scelto un archetipo della moderna catechesi che si concretizzò in tre differenti esternazioni - le prediche, la lauda drammatica, il poemetto di argomento religioso - forme artistiche indirizzabili sia ad una platea illetterata, sia ad esponenti della media borghesia.
Questa introduzione storica è oltremodo necessaria parlando de "I fiori del Silenzio", un'opera concepita proprio da un monaco eremita, Fra Claudio (alias Notkerus Claudus), che vive nell'Eremo della Beata Vergine del Soccorso (a Minucciano, nel Lucchese), edificio la cui iniziale costruzione risale al XV secolo.
Il frate - che è anche musicista, intagliatore e scultore di legno e marmo - è autore di versi semplici, non soltanto privi di qualsivoglia velleità letteraria, ma lontani dalle regole metriche della poesia. La cosa assume le caratteristiche di una vera e propria contraddizione, per un musicista, se si pensa che la metrica è alla base della "musicalità" che caratterizza il verso e che distingue la poesia dalla prosa. A dirla tutta, infatti, i testi di questo libello rappresentano un genuino esempio di sintesi letteraria che si colloca perfettamente a metà strada tra la poesia e la prosa.
Nondimeno, il valore intrinseco dei versi supera ogni incertezza letteraria: ciò che conta, per l'Autore, non è la volontà di presentarsi quale intellettuale dallo stile avvincente e seducente, ma strumento nelle mani di Dio.

Ne consegue che, in perfetta armonia con i prodromi che hanno caratterizzato la nascita della poesia religiosa descritti in apertura (forma artistica genuina ma profonda, diretta ad una platea non necessariamente acculturata), quest'opera si segnala per la sua efficacia senza pari nella estesa compagine della letteratura poetica nazionale, in particolare religiosa.

Al riguardo è sufficiente richiamare alcuni versi estremamente rappresentativi di questo inusuale modus comunicativo. Ne "I Dieci Comandamenti", ad esempio, parlando del decimo ("Desiderar la roba d'altri non è l'Amore"), Fra Claudio ci comunica: "Obbedirò! Non per un comando e in modo scaltro, ma per amor ad un altro". Si tratta di un modo di vedere il precetto che è tanto rivoluzionario quanto profondo: non è forse vero che il comandamento ci è stato tramandato per anni in termini di mero precetto, rispettato per mero senso del dovere piuttosto che per intima convinzione? Qui, invece, il frate ci invita ad una riflessione importante che richiama e sintetizza in poche righe il senso della Parola di Gesù Cristo: il furto, cioè, non è vietato in quanto lesivo del concetto di proprietà (concetto che è un caposaldo dell'odierno ordinamento penale nazionale, mutuato, peraltro, dal diritto romano), ma in quanto atto privo di Amore, lesivo di un sentimento altissimo ma imprescindibile. E difatti, il lettore noterà che, nel verso sopra citato, la nozione di proprietà privata è certamente superata, né citata, né sottintesa.

Un altro esempio dell'efficacia dell'arte comunicativa di questo frate lo si trova in maniera esemplare nella poesia "Il diavolo?". Già il punto interrogativo fa intuire una certa attitudine di matrice sovversiva (negare l'esistenza del diavolo vuol dire negare anche quella di Dio), giacché egli mette in dubbio la presenza del maligno fin dal titolo, sebbene in maniera chiaramente provocatoria. Si converrà che la via scelta dall'Autore per invitare il lettore alla riflessione sullo specifico argomento, è quantomeno inusuale per un prelato. "Il diavolo non esiste! È un discorso così triste! È un'altra invenzione dei soliti preti che con le loro paure fan stare tutti quieti. Cosa vuoi che esista un angelo ribelle che a tutti i costi vuole la tua pelle (.) In questa vita puoi fare ciò che vuoi: arraffa, ruba… uccidi più che puoi (.) Se Gesù ti dice che il diavolo c'è, non ascoltarlo, ascolta me!". In questo stile più vicino alla novella di collodiana memoria, pur in presenza di versi successivi certamente più elementari ("via delle fiamme già al sesto girone, c'è un posto per te anche se un po' tontolone"), il frate compie una ribellione comunicativa che è senza precedenti. Egli, prelato per vocazione, veste incredibilmente i panni del diavolo tentatore e, facendo leva sul suo status di religioso, ovviamente conosciuto dal lettore, spinge quest'ultimo alla riflessione profonda, vestendola anche di sottile vena ironica.

Insomma, alla fine della lettura, egli schernisce chi schernisce il religioso allorquando mette in guardia i fedeli parlando del diavolo, facendolo apparire un maldestro imbonitore da strada.

Non tutto è perfetto, naturalmente: versi come "O icona scritta col sangue a perenne memoria", dedicati alla Sindone, in un periodo storico ove ci sono più elementi che portano a dubitare della sua autenticità, sono espressione di una non condividibile volontà di voler rappresentare in maniera univoca talune cose.

Tuttavia, la forza di questi scritti sta anche nella loro capacità di generare alcune contrarietà: l'autore, cioè, riesce tanto a rafforzare la fede nei credenti, quanto a far riflettere in maniera attenta e intelligente il non credente.

Per questi motivi, l'opera presenta una forte potere comunicativo che anche un giornalista laico, per giunta ateo, come il sottoscritto, non può non esaltare.

Ten Col. CC Gianluca Livi

Il titolo non è in vendita essendo distribuito gratuitamente dai frati dell'Eremo, previa richiesta da formulare al seguente indirizzo: Frate Claudio, c/o Eremo della Beata Verginedel Soccorso, 55034 Minucciano(Lucca). Il richiedente può eventualemente fare una donazione in denaro.

RIVISTE

Rivista Militare

Del n. 3/2015, maggio-giugno, segnaliamo la pubblicazione degli articoli di Vittorfranco PISANO "L'Europa sotto attacco", Arduino PANICCIA "Geopolitica e geoeconomia dell'Iran", Antonio CIABATTINI LEONARDI "Le forze nucleari degli Stati Uniti, Daniele CELLAMARE "La radicalizzazione jihadista in Medio Oriente", Ugo GAETA "Le capacità cinofile dell'Esercito Italiano", Claudio BEGGIATO "La guerra elettronica -3^ parte", Massimiliano BAR "L'Esercito Australiano si rinnova. Il Piano Beersheba", Bruno VIO "Transalpine Bond 2014", Cinzia FUGGETTI "La nuova fisionomia dei conflitti armati. Confronto con DIU", Francesca CANNATARO e Valentina COSCO "Dove si addestra l'uomo soldato", Pietro BATACCHI "L'Artiglieria oggi", Flavio RUSSO "La prima mitragliatrice meccanica".

Nel n. 4/2015, luglio-agosto, è stata pubblicata l'intervista, a cura di Monia SAVIOLI, all'Onorevole, Gen.C.A. Luigi Ramponi "Minaccia cyber: ultima frontiera delle ostilità", a seguire gli articoli di Tommaso GIORGINO "L'evoluzione dei rapporti Italia-Libia", Daniele CELLAMARE "Stati Uniti e Cuba …. Test per la pace", Pietro MAZZAGATTI e Paolo PICCIONI "I fenomeni migratori", Arduino PANICCIA "L'Egitto nel quadro geostrategico mediorientale", Antonio CIABATTINI LEONARDi, Pietro TORNABENE e Antonino MIDOLO "Force Protection", Dario PORFIDIA "Corpi Tecnici: proposta di una futura evoluzione", Vincenzo GELOMINI e Amodio CARLEO "I rimborsi ONU in ambito UNIFIL", Antonello FOLCO BIAGINI e Antonello BATTAGLIA "1915. A un anno dallo scoppio: l'Europa e l'andamento degli scontri", Flavio RUSSO "Il lanciafiamme", Leonardo PRIZZI "Il D'Annunzio soldato", Maurizio GALLO "Ricordando D'Annunzio", Ernesto BONELLI "Le origini dell'Esercito Italiano", Alessandro FONTANA di VALSALINA "I samurai", Giorgio BATTISTI "La via italiana alla controguerriglia".

Rivista Marittima

Nel numero di luglio-agosto 2015 sono stati pubblicati gli articoli di Mario Rino ME "La Terza Guerra Mondiale a pezzi e la Bagarre multipolare - 1^ parte", Florence GAUB "La Counterinsurgency: non una specialità araba", Ezio FERRANTE "La rivoluzione dei Choke Points", Michele COSENTINO "La strategia di Pechino per la colonizzazione insulare del Mar Cinese Meridionale", Patrizio RAPALINO "Diplomazia navale", Paolo PEZZUTI "Operazione Atalanta", Giuliano DA FRÉ "Guerra yemenita: la dimensione navale del conflitto", Domenico VECCHIONI "Gli ammutinati del Bounty", Paolo BEMBO "Pittori di Marina nella Grande Guerra", Enrico CERNUSCHI "Partita a scacchi nell'Egeo maggio-agosto 1848".

Rivista Aeronautica

Nel n. 4/2015 sono stati pubblicati lo "Speciale 55° anniversario Frecce Tricolori", gli articoli di Riccardo NICCOLI "Nevatim air base", Remo GUIDI "Anatolian Eagle 2015", Gennaro DI NAPOLI, Andrea FRATICELLI e Luciano PICCIONE "Project Management: capacità e competenze dell'A.M.", Pompilio SAMMACICCIO "EATT 2015", Stefano COSCI "EPRC That others may live", della Redazione "Consegnato l'HH-101- Caesar", Pierluigi DE PAOLIS "Store integration & safe separation", Luca RICCI e Emanuele SALVATI "RIAT 2015", Stefano COSCI "Fly party 2015", Ugo VICENZI "Un C-54 memoria del ponte aereo di Berlino", Alberto DE RUBEIS e Antonello GERMINARIO "Antartide: la nuova sfida dell'Aeronautica Militare", Antonio CALABRESE "Sopravvivere in ambienti estremi", Stefano COSCI "Pronto… .Samantha?", Antonio CALBRESE "A protezione della Terra".

Rivista della Guardia di Finanza

Nel n. 3, maggio-giugno 2015, segnaliamo la pubblicazione degli articoli di Antonio Felice URICCHIO "Spunti per una ricostruzione della natura tributaria dei contributi ai consorzi obbligatori in materia di rifiuti", Alessandro GIOVANNINI "Elusione fiscale, abuso del diritto e sanzione", Tommaso RAFARACI "Reati tributari con soglia di punibilità e applicazione dell'art. 220 disp.att. c.p.p.: la Cassazione rimarca i diritti della difesa", Paolo CENTORE "L'attività delle Commissioni di studio dell'Associazione Italiana Dottori Commercialisti", Nicola QUIRINO "The recent pubblic health spending trend in Europe", Piergiorgio VALENTE e Danilo Massimo CARDONE "L'azione dell'Amministrazione finanziaria di contrasto all'esterovestizione", Camillo SACCHETTO "Documenti fiscali digitali: regole tecniche e conservazione a norma", Stefano SCREPANTI "La strategia nazionale di contrasto alle frodi IVA", Rosario SCALIA "Il controllo delle spese effettuate dai gruppi consiliari nelle Regioni", la tesi di laurea di Gennaro Antonio COLARUSSO "L'elusività del conferimento di ramo d'azienda seguito dalla cessione di quote da parte del soggetto conferente".

Nel n. 4, luglio-agosto 2015, sono stati pubblicati il testo dell'audizione del Comandante Generale della G. di F., Gen.C.A. Saverio CAPOLUPO, sui "Flussi migratori in Europa attraverso l'Italia, modelli di accoglienza e prospettive di riforma", l'analisi del Presidente dell'A.N.AC., Dott, Raffaele CANTONE, su "L'attività di prevenzione e contrasto della corruzione, a tutela dei cittadini, delle Istituzioni, dei mercati e della democrazia", gli articoli di Alessandro TRAVERSI "Brevi note in tema di autoriciclaggio", Sergio RICCI "Le ONLUS: inquadramento generale e casi peculiari", Pasqualino SILVESTRE "Il sequestro dei beni conferiti in trust nella giurisprudenza penale", Piergiorgio VALENTE e Giampiero IANNI

"Economia digitale: principi impositivi e questioni aperte", Camillo SACCHETTO e Marco CARROZZINO "La cooperazione internazionale in materia tributaria: sistemi informatici e contrasto all'evasione fiscale internazionale", Nicola BIA e Armando TADINI "Confisca di prevenzione in fattispecie di evasione fiscale", Marco THIONE e Marco BARGAGLI "Aggressive tax planning: profili soggettivi e oggettivi", la tesi di laurea di Andrea CASAMASSIMA "Evasione interpretativa e da alterazione della realtà nei rapporti internazionali".

Rivista di Polizia - Rassegna di dottrina tecnica e legislazione

Nel fascicolo V, maggio 2015, sono stati pubblicati gli interventi tenuti nell'ambito del convegno "Le dimensioni della sicurezza", tenutosi presso la Scuola Superiore di Polizia, 25 marzo 2015, del Pref. Alessandro PANSA, Prof. Giuliano AMATO, On. Angelino ALFANO, gli articoli di Alessandro COVIELLO "Lotta al terrorismo e tutela dei diritti umani fondamentali", Vincenzo DI LEMBO "Le minacce alla sicurezza informatica. Gli attacchi di ingegneria sociale", Danilo RIGONI "Salute e sicurezza nei luoghi di lavoro. Il Servizio di Prevenzione e Protezione e la riunione periodica".

GNOSIS - Rivista Italiana di Intelligence

Il n. 3/2015 presenta gli articoli di Alain CHARBONNIER "Rochefort vinse a Midway, fu sconfitto a Washington", Gianandrea GAIANI "Isis un anno dopo. Punti di forza e debolezza del Califfato", Dario FABBRI "L'approccio imperiale di Obama nel caos mediorientale", Corrado Maria DACLON "Globalismo nuova frontiera della politica", Barbara CONTINI "L'immigrazione e l'espansione della religione islamica in Europa. Una prospettiva in chiaroscuro per molti Stati europei", Matteo MARCONI "Come la geopolitica approdò sulla terra: Rudolf Kjellén e Karl Haushofer (III parte), Alessandro PANSA "Sviluppo tecnologico e distribuzione del potere internazionale", Giampaolo RUGARLI "Il magazzino dell'agente segreto", Filippo ARAGONA "Il fenomeno della 'ndrangheta nel dopoguerra e l'affermazione dei valori costituzionali", Antonio D'AMATO "La camorra dal contrabbando di sigarette al traffico internazionale di stupefacenti, fino alle infiltrazioni nei pubblici poteri", Manoela PATTI "Mafia e antimafia nell'Italia repubblicana", Roberto ADRIANI "Wikyleaks e il mito della trasparenza. L'influenza dei mass media e new media nelle relazioni internazionali", Giuseppe ARCANGELI "Ixp e privacy nelle telecomunicazioni", Raffaele AZZARONE "Cyber Vademecum (V parte). Panorama normativo e organizzativo nazionale", Marco BALDI e Michele ELIA "La crittografia. Da raffinata arte rinascimentale a moderna scienza", Roberto GANGANELLI "Sufficit unum. Un geniale codice e una medaglia mai coniata".

a cura del Lgt. Remo Gonnella