# La Francia non vuole Libra in Europa


***La criptovaluta di Facebook non sbarcherà mai sul suolo europeo***

Sin da quando è stata annunciata, Libra, la criptovaluta di Facebook, ha attirato sguardi poco benevoli da parte dell'Unione Europea, che il mese scorso ha iniziato a indagare sulla possibilità che essa violi le norme sulla concorrenza.
Degli Stati europei, in particolare è la Francia a essere la più critica verso Libra. Già durante l'estate aveva chiesto la creazione di uno speciale gruppo all'interno del G7 per studiare l'impatto delle criptovalute sull'economia, e per cercare un modo in cui le banche centrali possano regolamentarle.
Ora è anche più esplicita. Per bocca del proprio ministro dell'economia, Bruno Le Maire, ha fatto sapere che intende bloccare lo sviluppo di Libra in Europa, in quanto comporta dei «*rischi per la stabilità finanziaria*».

A rivelarlo è il quotidiano Le Figaro, che riporta le parole del ministro: *«Voglio dirlo con molta chiarezza: in queste condizioni, non possiamo autorizzare lo sviluppo di libra sul suolo europeo»*.
Le Maire teme *«la privatizzazione di una moneta, detenuta da un solo soggetto con oltre 2 miliardi di utenti sul pianeta»*. C'è in gioco – ha spiegato – *«la sovranità monetaria degli Stati»*.
Facebook non ha commentato ufficialmente l'uscita del ministro francese ma si sa che, dopo un inizio pieno di entusiasmo, ha preferito procedere con molta più cautela nel proporre Libra: le obiezioni avanzate sia dagli USA sia dalla UE hanno convinto il social network che non è il caso di forzare la mano, in quanto il terreno su cui si sta muovendo è molto delicato e può facilmente portare a reazioni aggressive da parte degli Stati, minacciati in una delle loro più importanti competenze.

---

# Thomas Cook, il chief executive Frankhauser chiede scusa ai dipendenti


“Voglio scusarmi con i miei 21mila colleghi, che immagino avranno  il cuore spezzato”. Così il chief executive di **Thomas Cook Peter Fankhauser** si rivolge ai dipendenti rimasti senza impiego, dopo la bancarotta del colosso del turismo organizzato.

Il manager esprime “**profondo rammarico**” per l’esito di mesi di trattative. “Abbiamo lavorato in modo estenuante per risolvere le questioni in sospeso su un accordo per garantire il futuro di Thomas Cook a dipendenti, clienti e fornitori”, ha dichiarato, riporta TravelMole. “Sebbene un accordo fosse stato ampiamente concordato – ha continuato -, una struttura aggiuntiva richiesta negli ultimi giorni di negoziati ha presentato una sfida che alla fine si è rivelata insormontabile. Vorrei scusarmi con i milioni di clienti, i dipendenti e i partner”.
“Questo – ha concluso – è **un giorno triste** per l’azienda che ha aperto la strada ai pacchetti turistici e ha consentito di

viaggiare a milioni di persone in tutto il mondo”.

## Articoli di approfondimento

23/09/2019 | Thomas Cook, le prime cifre del collasso del tour operator
23/09/2019 | Thomas Cook: Condor opera regolarmente
23/09/2019 | Air Malta in soccorso dei passeggeri Thomas Cook
24/09/2019 | Fallimento Thomas Cook: gli effetti sulle agenzie secondo Adv Unite

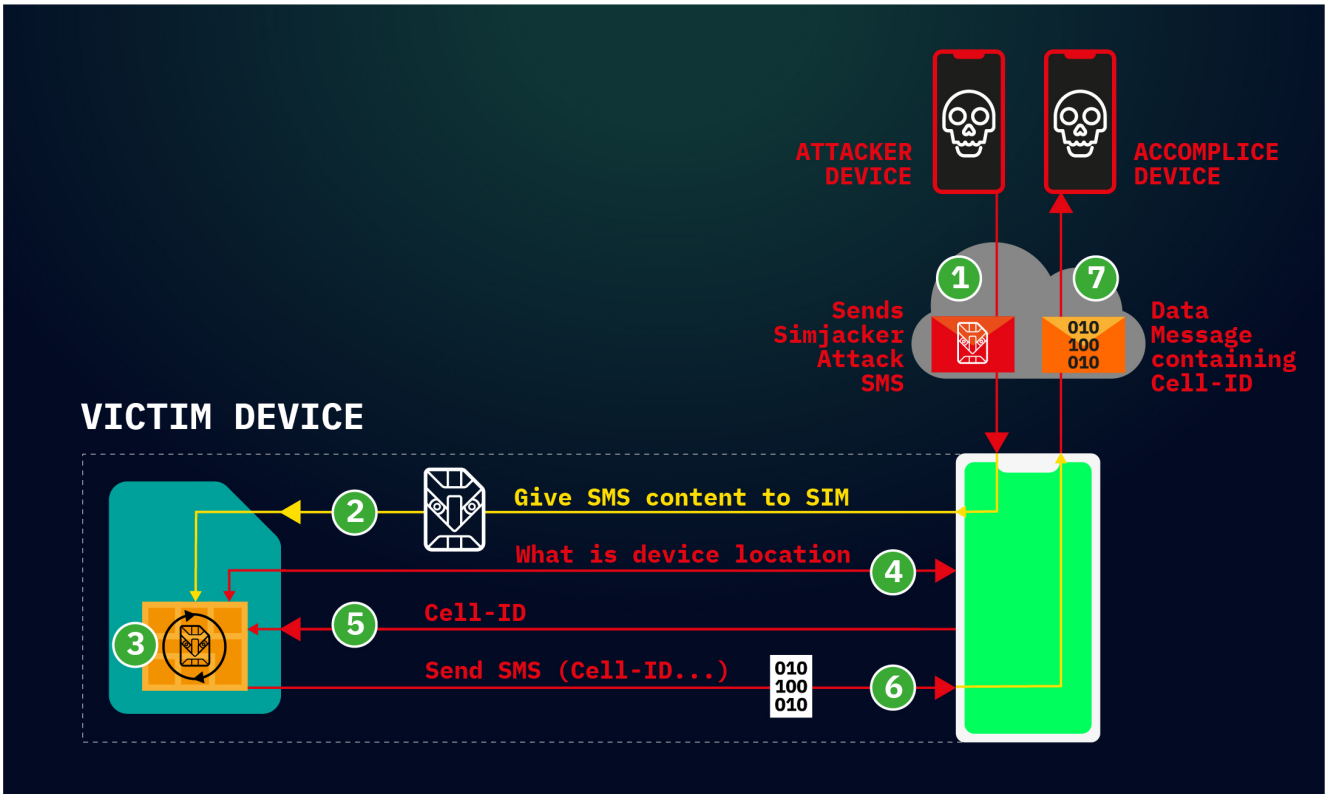
---

# Sim sotto attacco hacker: il virus trasforma lo smartphone in una microspia

***Attraverso l’uso della funzione S@t Browser, lo spyware Simjacker prende il possesso della sim card e la istruisce per rivelare informazioni sensibili. A rischio 1 miliardo di***

***utenti***

La soluzione più semplice, si suol dire, è sempre la migliore. E la regola vale anche quando la soluzione ha scopi tutt'altro che benevoli. È il caso di un **attacco informatico che sfrutta gli sms**. Già, i messaggini di cui ormai ci siamo dimenticati, soppiantati dalle chat, sono il cavallo di Troia di un **codice tipo spyware**, che **istruisce la sim card** perché prenda il controllo del dispositivo ed effettui operazioni sensibili, **spiando le informazioni** e spedendole all'attaccante.
La falla è stata scoperta da **Adaptive Mobile Security**, azienda di sicurezza informatica di Dublino specializzata in telecomunicazioni. **Simjacker**, questo il nome con cui è stato ribattezzato l'attacco, rappresenta una minaccia per almeno un **miliardo di proprietari di telefoni, in 30 paesi** in tutti i continenti. E, come se non bastasse, c'è già chi l'ha sfruttata. "*Crediamo che questa vulnerabilità sia stata* ***utilizzata da almeno due anni*** *da un gruppo di attacco altamente sofisticato*", mettono nero su bianco i ricercatori. Nello specifico, "*una* ***compagnia privata che lavora con i governi*** *per monitorare individui*".
Una vera e propria **operazione di spionaggio**, che mette milioni di persone a repentaglio, perché si basa su una funzione non più aggiornata dal 2009 e perché può colpire indiscriminatamente tutti i modelli e le marche di smartphone sono esposti. I ricercatori di Adaptive Mobile hanno osservato che Simjacker può prendere in ostaggio **cellulari Apple, Zte, Motorola, Samsung, Google e Huawei** e persino dispositivi internet of things che montano sim card, ma anche e-sim. Una situazione che rende ancora più complesso mettere una toppa.



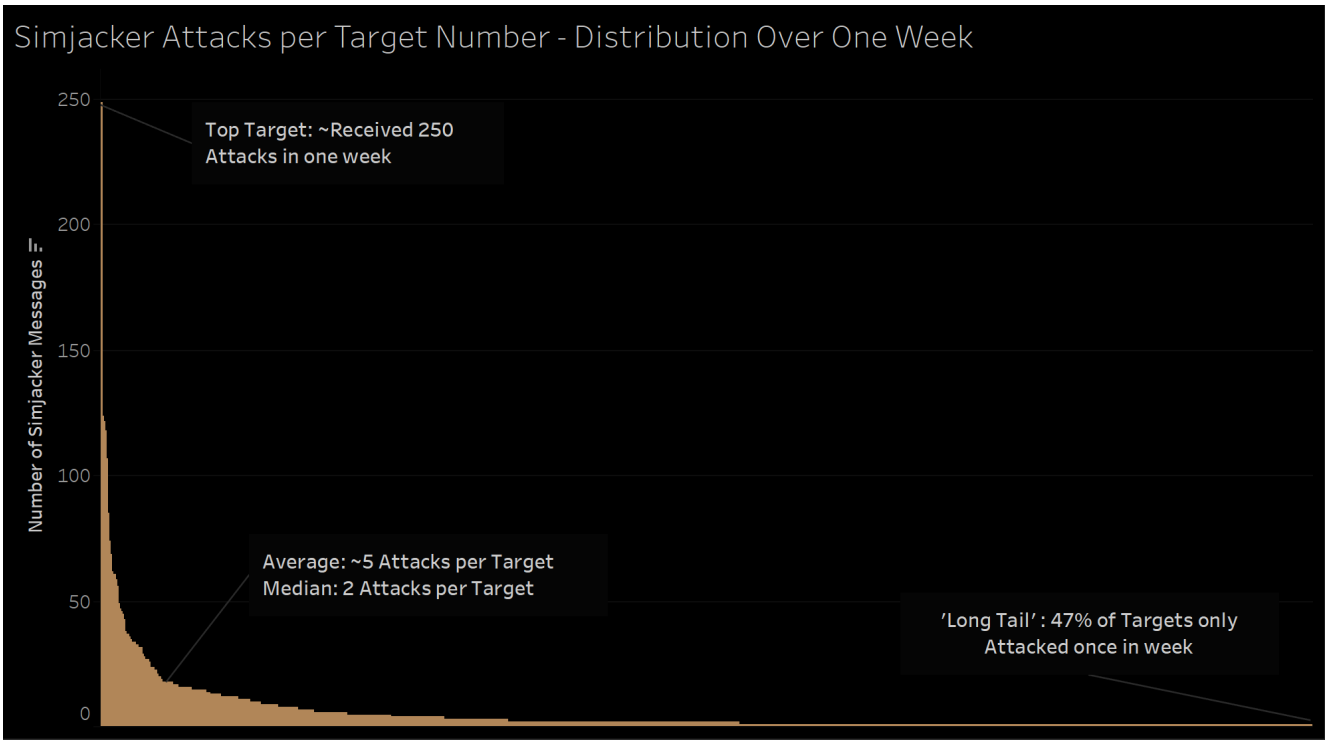
Il funzionamento dell'attacco Simjacker alle sim (Adaptive Mobile Security)

## Come funziona l'attacco

Il cavallo di Troia è un **sms**, che contiene le **istruzioni per la sim card**, di cui sfrutta una funzione, il S@t Browser. Il codice maligno raccoglie informazioni sulla localizzazione del dispositivo e sul numero Imei (International mobile equipment identity), che lo identifica, e le spedisce all'attaccante. Il tutto avviene all'**insaputa del proprietario** del cellulare, perché nelle caselle degli sms ricevuti o inviati non c'è traccia di queste comunicazioni.

Per la prima volta, sottolineano i ricercatori, è stato **scoperto un attacco malware via sms**. In precedenza con i messaggini arrivava il link a una pagina web da cui scaricare il virus. In questo caso, invece, il pacchetto è completo.
"*Il S@t Browser permette generalmente alle sim card di implementare* ***servizi a valore aggiunto***", spiega a *Wired* Pierluigi Paganini, responsabile tecnologico della società di sicurezza informatica Cybaze e membro di Enisa, l'agenzia europea della cybersecurity. Per esempio, è

adoperato dalle compagnie telefoniche per inviare via sim card il credito telefonico della propria utenza. “*È un protocollo adoperato dagli operatori di telecomunicazioni*”, ricorda Alessio Pennasilico, componente del comitato tecnico di Clusit, l’associazione nazionale della cibersicurezza.
Tuttavia, come osservano da Adaptive Mobile, è poco conosciuto, abbastanza vecchio e **non è stato aggiornato dal 2009** ma sopravvive nelle pieghe delle tecnologie mobili. Tanto che gli analisti hanno stimato che è adoperato dalle compagnie telefoniche di almeno 30 Paesi di Europa, Asia, Africa e Americhe e si stima che almeno un miliardo di persone siano a rischio attacchi.



Numeri di attacchi alle sim con Simjacker (Adaptive Mobile Security)

## Le conseguenze dell’attacco

Conoscere **posizione e numero identificativo dello smartphone** è già una cattiva notizia. “*Io posso mandare il messaggio infetto a un utente, creare gruppi omogenei e, attraverso questo malware, conoscere gli spostamenti, le intersezioni e le interconnessioni tra queste persone*”, aggiunge Pennasilico.
Ma c’è di più. Debitatamente istruito, Simjacker può ordinare

alla sim card operazioni più complesse. Come "*recuperare le email; accedere a un browser e scaricare malware; far sì che il telefono chiami un numero quando si inizia una conversazione e usarlo come microspia, oppure che componga numeri a pagamento per attività fraudolente*", elenca Paganini. Il tutto senza che la vittima se ne accorga e, di conseguenza, possa prendere delle contromisure. È un attacco che si presta a **campagne di spionaggio industriale, sabotaggio, disinformazione e sorveglianza** di massa.
Tanto che gli analisti hanno già visto il malware all'opera. Un'azienda privata di sorveglianza, al soldo dei governi, lo usa da due anni per spiare target specifici. In un paese, si legge nel rapporto di Adaptive mobile, circa **100-150 persone ogni giorno erano vittime di ripetuti attacchi Simjacker**. In alcuni il controllo durava settimane, in altre era un raid fulmineo. Nel complesso, gli analisti non la descrivono come "*un'operazione di controllo di massa, ma come una progettata per monitorare un ampio numero di individui per vari motivi*". E quando l'attacco non andava a buon fine, la società tirava fuori dal cilindro altri malware simili, meno sofisticati.
Per Paganini "*è tra i peggiori attacchi rivelati di recente*". "*La **falla di Whatsapp** di qualche mese fa era un attacco spaventoso, ma richiedeva attrezzature specifiche e quindi è presumibile che fosse indirizzato a target puntuali. Questo attacco invece colpisce tutti*", osserva Pennasilico.

## Le contromisure

E difendersi è complicato. L'ampia varietà di modelli e di dispositivi rende complesso individuare una soluzione. E disabilitare la funzione incriminata potrebbe rivelarsi controproducente. Gli analisti hanno allertato l'associazione Gsm, che riunisce gli operatori, e la Sim alliance, che associa i produttori di card, perché drizzino le antenne sul traffico di sms sospetti con comandi S@t browser e perché **aggiornino le protezioni.**
Nel frattempo il 3 ottobre, alla presentazione ufficiale della

ricerca alla Virus bulletin conference di Londra (incontro di cibersicurezza), Adaptive Mobile fornirà più dettagli sull'attacco. "*Trattandosi di* ***sim card, ci vorrà tempo***", riconosce Paganini. E quindi il rischio che la falla sia adoperata da altri malintenzionati o spioni cresce.
In generale nel 2019 malware e ransomware sono aumentati. E secondo il rapporto Trend Micro, l'Italia è il quarto paese al mondo per numero di malware intercettati nella prima metà del 2019. In parallelo nel Belpaese sta **calando l'uso degli sms**. L'Autorità per le telecomunicazioni ha calcolato che nel 2018 l'invio è sceso del 27% rispetto al 2017. Ridotto a 12 miliardi di unità, circa la metà del 2012. Di contro, sono sempre più utilizzati dalle aziende per le lo comunicazioni. A cominciare dalle banche.

---

# Google, fuori le pseudoscienze dall'advertising

Google modifica le regole per l’advertising ponendo nuovi limiti per la pubblicità di cure e medicinali sul motore di ricerca: decida la scienza.

Sebbene **Google** poggi sostanzialmente gran parte dei propri introiti sull’**advertising**, non può esimersi dal mantenere sano e pulito il mercato nel quale va ad attingere. Ecco perché con un nuovo aggiornamento il gruppo ha tracciato un nuovo limite oltre il quale i clienti non potranno andare, soprattutto in ambito “**sanità e farmaci**“.

## Google, limiti all’adv sul biomedicale

Quando un utente cerca su Google, si trova di fronte sulle SERP una commistione tra risultati e advertising: la logica con cui è costruita la pagina è tale per cui si considerano le pubblicità in qualche modo correlate alla parola cercata, poiché è proprio su tale logica che si basa l’offerta pubblicitaria del gruppo. Ogni singola pubblicità prevede pertanto una quota di responsabilità in capo a Google e ignorare questo aspetto equivale ormai a nascondere la testa

sotto la sabbia. Così non vuole fare il motore di ricerca, che con una presa d'atto della situazione ha voluto invece bloccare ogni residua tolleranza e portare a compimento una **nuova policy e nuovi limiti sul mondo biomedicale**.
La regole (vedi la policy) **proibiscono d'ora innanzi la vendita di pubblicità per servizi, prodotti e teoremi che non sono improntati su basi scientifiche**. Qualsivoglia trattamento che non abbia supporti scientifici clinici sufficienti, insomma, non potranno raggiungere le masse: la validazione scientifica diventa un limite oggettivo oltre il quale ogni para-scienza non potrà arrivare.

## L'importanza di una nuova policy

Si tratta di una modifica di grande importanza poiché il tema della salute implica il trattamento di un ambito di grande sensibilità. Le ricerche coinvolte dalle modifiche alla policy sono infatti legate spesso a problemi alla salute, coinvolgendo pertanto utenti in una particolare situazione psico-fisica. L'attitudine al click può portare facilmente tra le braccia di pseudoscienziati, pseudomedici, truffatori, alchimisti della cura miracolosa e venditori di placebo.
Non solo: quando un nuovo farmaco o una nuova cura sono ancora nell'alveo dello **sperimentale**, poco senso avrebbe una vendita tra le masse, senza l'intermediazione di medici e senza la necessaria consapevolezza su rischi e opportunità: la nuova policy regolamenta pertanto anche quell'area grigia della scienza sperimentale, laddove nuove cure sono in fase di test per una validazione che consenta l'uso di massa.
Un intervento meritevole da parte di Google, quindi, e l'auspicio è che possa giungere anche a realtà concorrenti come Facebook: troppo spesso l'advertising è farcito di pubblicità di questo tipo, ove diete miracolose e farmaci mirabolanti promettono insperate guarigioni. Lucrare sulla disperazione altrui è qualcosa di inqualificabile e le piattaforme non possono più esimersi dal porre un freno a derive di questo tipo. L'oggettiva co-responsabilità di chi

veicola annunci di questo tipo, infatti, è ormai conclamata e troppo ingombrante per poter essere ignorata.

## Omeopatia

Una curiosità rimane pendente: come sarà giudicata l'omeopatia? Gli studi che ne dimostrano la totale inefficacia saranno sufficienti per proibirne l'advertising su Google? Questo aspetto andrà verificato nel tempo. Ad oggi una verifica estemporanea non sembra ancora bloccare pubblicità su questo tema, ove con ogni probabilità sarà sancito un limite concreto e visibile tra cosa è scienza e cosa non lo è, tra cosa è tollerato e cosa non lo è, tra cosa è parte del compromesso e cosa ne è irrimediabilmente fuori.

---

# Esercitazione Borea 2019, la comunicazione nella gestione delle situazioni di crisi

Si è svolta a Trieste, nelle giornate del 5 e 6 dicembre 2019,

l’esercitazione di Difesa Civile per posti di comando BOREA 2019, organizzata dal Ministero dell’Interno e sotto il controllo della NATO.

Tutta l’esercitazione si è tenuta presso il palazzo della Prefettura di Trieste dove, per l’occasione, si sono incontrati e hanno lavorato a stretto contatto, coordinati dal Prefetto, le Forze dell’Ordine, i Vigili del Fuoco, il Servizio Sanitario, la Protezione civile, l’Arpa, la Regione Friuli Venezia Giulia, il Comune di Trieste, l’Autorità portuale.
L’esercitazione ha simulato un attacco N.B.C.R. (Nucleare, Battereologico, Chimico, Radiologico) con la presenza di terroristi in azione in contemporanea, in diverse zone sensibili della città.
Gli attori presenti in Prefettura si sono suddivisi in tre tavoli con tre competenze differenti: un tavolo decisionale, coordinato dal Prefetto di Trieste Valerio Valenti, che valutava la situazione minuto per minuto, decidendo quali strategie adottare e quali azioni intraprendere, un tavolo tecnico, in cui si valutavano eventuali azioni per mitigare gli effetti dell’attacco sul territorio, ed infine, un tavolo dedicato alla comunicazione.
Proprio di quest’ultimo mi soffermo ad analizzare l’intensa, difficile e delicata attività svolta dovendo informare costantemente la popolazione.

Prima dell’inizio dell’esercitazione era stato redatto dal Capo di Gabinetto del Comune di Trieste Vittorio della Marra un Piano di Comunicazione di Crisi che, forse per la prima volta in Italia, ha dato un forte peso ai canali di comunicazione forse più utili in caso di crisi come questa, i social media. I social infatti sono già stati testati come efficienti canali comunicativi durante vari attacchi terroristici in Francia, Germania e Inghilterra, permettendo un raggiungimento capillare delle informazioni, dei consigli,

delle indicazioni necessarie in queste situazioni. Costruire in “tempo di pace” un piano di comunicazione organizzato – che assegni ruoli specifici e che tenga conto dei diversi canali di comunicazione, inclusivi della stampa nazionale che, in situazioni come questa, va necessariamente aggiornata costantemente in modo da condividere informazioni corrette e condivise – permette di non trovarsi impreparati davanti ad eventi così gravi ed inaspettati.
L’esercitazione è iniziata intorno alle 8.30 del mattino del 5 dicembre e il tavolo sulla comunicazione ha, da subito, iniziato la simulazione informando i cittadini di quello che stava succedendo, cercando, per quanto possibile, di far mantenere ordine e calma e fornendo precise istruzioni su come ci si doveva comportare, quali azioni intraprendere per limitare al massimo situazioni di pericolo per se stessi e per gli altri e elencando tutti i canali ufficiali dove venivano fornite le informazioni.
In questi casi la disinformazione delle persone assieme al panico generato da un attacco di questa entità, potrebbero compromettere il piano di messa in soccorso degli eventuali feriti o, addirittura, procurarne di nuovi. Diventa quindi fondamentale comunicare tempestivamente fornendo indicazioni sicure e verificate e rivolgendosi a tutte le tipologie di cittadini e specificando i diversi comportamenti da tenere che, spesso, vanno in contrasto con le azioni istintive delle persone.
L’esercitazione prevedeva costanti e pressanti injects per rendere più realistica la simulazione, aumentandone lo stress e distraendo i partecipanti con azioni di disturbo. Sul fronte della comunicazione gli injects avevano la forma delle fake news, con tweet lanciati da presunte persone autorevoli che però fornivano informazioni non corrette e che, se non contrastate immediatamente dai canali di comunicazione istituzionali, avrebbero messo ancora più in allarme la popolazione aumentando il caos generale e compromettendo il lavoro di informazione corretta e puntuale fatto fino a quel momento. L’azione costante di monitoraggio dei social in casi

del genere diventa fondamentale come è fondamentale che tutti i canali dedicati all'emergenza comunichino con un'unica voce autorevole.
Gli organizzatori dell'esercitazione sono stati estremamente bravi a creare una simulazione così drammaticamente reale riuscendo a coinvolgere a tal punto i partecipanti, che la tensione in Prefettura era palpabile. Risulta necessario infatti immedesimarsi il più possibile, durante questi eventi, per testare l'organizzazione ma anche se stessi in situazioni così stressanti e drammatiche che richiedono nervi saldi e capacità di lavorare in team.
Un plauso dunque al Ministero dell'Interno che organizza sul territorio nazionale queste simulazioni avendo ben chiaro come sia necessario essere pronti e organizzati in possibili situazioni di crisi, anche e soprattutto sul fonte della comunicazione, spesso messo in secondo piano ma, se ben organizzato, fondamentale per gestire una situazione di crisi.