SCENARIO

Il concetto di Security e gli scenari di minaccia: le nuove tecnologie e la Security sociale

Il presente articolo descrive brevemente il concetto di security, il suo significato attuale e le implicazioni che derivano dalla sua applicazione. Le minacce più probabili vengono prese in esame, passando in rassegna gli agenti biologici e chimici utilizzati in situazioni di conflitto, e considerando gli esplosivi assieme ai relativi precursori, questi ultimi particolarmente adatti alla costruzione di dispositivi esplosivi improvvisati (IED, Improvised Explosive Devices). Sono inoltre illustrate tutte le minacce di tipo CBRNe (chimiche, biologiche, radiologiche, nucleari ed esplosive) ed è brevemente spiegato l'incubo della "bomba sporca".
Vengono quindi descritte le attività di ricerca e sviluppo tecnologico per la security, così come previste a livello europeo nei programmi attuali e precedenti, a livello sia internazionale che italiano. Infine, alcuni scenari di riferimento, con particolare attenzione alla security del trasporto di massa, sono qui esposti con particolare riguardo ai casi in cui lo sviluppo tecnologico potrebbe diventare più efficace nell'immediato futuro.

Security concept and threat scenarios: New technologies and social security

The concept of security with its current meaning and the implication of its implementation are shortly introduced here. A threat analysis is presented reviewing biological and chemical warfare agents, explosive compounds and their precursors, the latter being suitable to the construction of improvised explosive devices (IED). All Chemical, Biological, Radiological, Nuclear and explosive (CBRNe) threats are considered, and the "dirty bomb" nightmare is introduced.
Research and Technology Development (RTD) for Security is discussed as foreseen at the European level, in both former and current programs, as well as at a higher international level and in the Italian surroundings.
Reference scenarios, with special attention to mass transport security, are discussed trying to foresee where technology development might become more and more effective in the near future.

DOI: 10.12910/EAI2014-85

R. Fantoni, A. Palucci

Contact person: Roberta Fantoni
roberta.fantoni@enea.it

Il concetto di Security

Con il termine Security si fa riferimento al grado di protezione da qualunque tipo di danno o pericolo. Tale concetto è applicabile a qualunque bene vulnerabile e di valore: singoli individui, una comunità, una nazione o un'organizzazione. Il concetto di security viene generalmente associato al rischio, cioè alla possibilità che si verifichi un evento dannoso, e alla minaccia, l'azione che rende il rischio una realtà concreta. I sistemi di security dovrebbero tenere adeguatamente conto dei rischi e contrastare le minacce. Nella maggior parte dei sistemi di security, l'anello più debole della catena è quello più importante. Le minacce terroristiche sono tipicamente asimmetriche, poiché il "difensore" deve coprire tutti i punti di possibile attacco, mentre l'"attaccante" ha solo bisogno di individuare un punto debole sul quale concentrare gli sforzi perturbatori.

Ad ogni campo di azione corrisponde uno specifico problema di security. Un esempio di possibile lista di aspetti relativi alla security potrebbe essere il seguente:

- *Information Technology (IT): security per applicazioni, sistemi informatici, dati, informazioni, reti.*
- *Security fisica: aeroporti e porti, filiera alimentare e approvvigionamenti, case, infrastrutture, scuole, centri commerciali, beni culturali, aree sportive.*
- *Security politica, sociale e monetaria: sicurezza nazionale, internazionale, pubblica, finanziaria.*

Il presente articolo prende in esame gli aspetti fisici della security, in particolare quelli relativi ai progressi delle attività di ricerca e sviluppo tecnologico.

Storicamente i diversi aspetti della security sono stati trattati singolarmente, in genere da diversi operatori pubblici o privati dotati di dipartimenti specificamente dedicati alla security per sistemi IT, protezione fisica e prevenzione di frodi. Oggi è generalmente riconosciuta una correlazione dei requisiti per la security e viene preferibilmente seguito un approccio olistico, che comporta una gestione del rischio integrata di tipo "all hazards". La convergenza delle discipline della security verso questo tipo di approccio ha avuto ampio impulso dallo sviluppo delle tecnologie di videosorveglianza digitale, dalla digitalizzazione e dalle reti di sistemi fisici di controllo, quali, ad esempio, i sistemi SCADA (Supervisory Control And Data Acquisition) di controllo, supervisione e acquisizione dati [1].

The concept of Security

Security is the degree of protection from any harm or danger. It applies to any vulnerable and valuable asset, such as single persons, community, nation, or organization. The concept of Security is usually associated with risk, i.e. the possibility that some hazardous events concretize, and with threat, i.e. the action that triggers the risk actualization. Security systems should adequately take risks into account and counteract threats. In most security systems, the "weakest link in the chain" is the most important. Terroristic threats are usually asymmetric since the "defender" must cover all points of possible attack, while the attacker only needs to identify a single weak point upon which to concentrate the disruptive efforts.

Different realms can be considered dealing with specific security problems. An example of possible security categorization is given in the following:

- *Information Technology (IT) aspects:* Application security, Computing security, Data security, Information security, Network security.
- *Physical aspects:* Airport and port security, Food and Supply chain security, Home security, Infrastructure security, School security, Shopping center security, Cultural Heritage and Sport area security.
- *Political, social and monetary aspects:* Homeland security, Human security, International security, National security, Public security, Financial security.

This paper is focused on the physical aspects of security, in particular dealing with possible security improvements expected from RTD activities.

Various aspects of security were historically addressed separately, usually by different public or private operators with specific departments for IT security, physical security, and fraud prevention. The interconnected nature of security requirements is nowadays generally recognized, and a holistic approach to security, involving an "all hazards" management, is preferentially followed. The convergence of security disciplines into an integrated approach to Security was largely pushed by the development of digital video surveillance technologies and by the digitization and networking of physical control systems (e.g., by Supervisory Control And Data Acquisition systems - SCADA) [1].

A picture of the complexity of Security needs to consider the players, that take decisions and perform actions, the technological tools adopted to prevent or fight the threats, the technology developers whose role is to study and build these tools.

The main players are:

- government authorities, mostly concerned with political and social issues,
- the army, involved in military operations at the borders as well as in

Per avere un quadro della complessità della security occorre considerare gli attori, cioè coloro che prendono le decisioni e le attuano, gli strumenti adoperati per prevenire o combattere le minacce e gli sviluppatori di tecnologie, che hanno il compito di studiare e realizzare tali strumenti.

Gli attori principali sono:

- *le autorità di governo, che si occupano soprattutto di problematiche politiche e sociali;*
- *l'esercito, coinvolto in operazioni militari al confine e in interventi specifici in caso di catastrofi nazionali su larga scala;*
- *corpi civili pubblici (vigili del fuoco e protezione civile);*
- *corpi di polizia, per interventi di routine contro il terrorismo e il crimine organizzato.*

Creare opportune interazioni tra gli attori della security a livello nazionale e internazionale è una sfida oggi esplicitamente tenuta in grande considerazione, come dimostrano i tanti Master Courses di specializzazione nella security, tenuti nella maggior parte dei paesi industrializzati [2, 3].

Passiamo ora alla disamina degli strumenti disponibili per contrastare le minacce. È ben noto che lo spazio e la difesa nazionale siano universalmente ritenuti i principali propulsori dello sviluppo di nuove tecnologie. La duplice applicazione (militare e civile) delle tecnologie per la security ha sicuramente tratto beneficio dalle principali ricadute della ricerca in campo militare. Ad esempio, gli strumenti tecnologici sviluppati per la protezione di un accampamento militare in uno scenario bellico, quali sistemi di videosorveglianza, visione notturna, riconoscimento biometrico, possono essere utilizzati per la protezione di infrastrutture critiche (vedi, ad es., [4]). La crittografia è un ulteriore esempio di ricaduta tecnologica: originariamente sviluppata per proteggere le telecomunicazioni durante la seconda Guerra mondiale, è oggi alla base dei protocolli informatici di comunicazione e di scambio digitale di dati.

Gli sviluppatori di tecnologie rappresentano il terzo elemento critico di cui tenere conto nell'organizzazione di un sistema di security per la difesa nazionale. Se da un lato è estremamente necessario indirizzare la ricerca verso dispositivi rapidi, sensibili e selettivi per il rilevamento di possibili minacce aree, riducendo al massimo l'interferenza con le attività ordinarie ivi portate avanti, dall'altro i terroristi si evolvono parallelamente, perlopiù acquisendo le informazioni pubbliche disponibili, che consentono loro di mettere a punto minacce più

specific interventions for large-scale national disasters,

- non-military public organization (such as firemen and civil protection),
- the police, for routine interventions counteracting terrorism and organized crime.

To apply an appropriate interaction among security players, both at the national and international level, is a challenge explicitly considered nowadays in the security specializations master courses held in the most industrialized countries [2, 3].

The available tools to counteract the threats are the next issue. It is well known that space and army are worldwide acknowledged as the main drivers of technology developments. Security implementations may profit of major fallouts from military research, as far as dual technologies (military/civilian) are concerned. For instance, the technology tools developed to protect a military camp in a war theatre may be successfully utilized for critical infrastructure protection (video surveillance, night view, biometric recognition, etc.) see, e.g., [4]. As a further example, we can mention cryptography, first developed to protect telecommunication during World War II and nowadays at the basis of computer secure communication protocols and digital data exchange.

Technology Developers represent the third critical element in organizing a Security Homeland system. On the one hand it is really necessary to address research towards fast, sensitive and selective devices for detection of potential threats in crowded areas, minimizing the interference with the ordinary activities there carried on. On the other hand, terrorists evolve in parallel, mostly through public available information which allows them to choose more sophisticated threats or adopt new weapons (e.g., plastic knives to fool metal detectors, liquid precursors to be mixed on board for quickly assembling IEDs) [5].

Threat analysis

Biological (B) and chemical (C) warfare agents

Biological terrorism dates as far back as ancient Roman civilization, but now it is a primary concern in the States' political agendas. According to the Global Terrorism Database (GTD) of the National Consortium for the Study of Terrorism and Responses to Terrorism (START) [6], biological and chemical attacks account for nearly 0.2% of terror attacks perpetrated worldwide between January 1st, 1970 and December 31st, 2011 [7]. Despite the ban, Weapons of Mass Destruction (WMD) have actually been used in warfare, as in the Iran-Iraq war in 1984/88: Iraq made use of chemical warfare agents [8] and in some terroristic attacks. Not only do biological agents affect specific targets but they can also potentially induce mass hysteria on the society exposed to them [9]. Malicious letters containing Bacillus anthrax, addressed in the U.S. to

sofisticate o di utilizzare nuove armi come, ad esempio, coltelli di plastica non rilevabili dai metal detector, precursori in forma liquida da miscelare una volta a bordo per assemblare rapidamente dispositivi esplosivi improvvisati, i cosiddetti IED (Improvised Explosive Devices) [5].

Analisi della minaccia

Agenti chimici per guerra biologica (B) e chimica (C)

Sebbene il terrorismo biologico risalga ai tempi dell'antica civiltà romana, oggi rappresenta il principale elemento di preoccupazione all'ordine del giorno nell'agenda politica dei vari stati. Secondo il Global Terrorism Database (GTD) del National Consortium for the Study of Terrorism and Responses to Terrorism (START) [6], gli attacchi biologici e chimici equivalgono a circa lo 0,2% degli attacchi terroristici perpetrati in tutto il mondo tra l'1 Gennaio 1970 e il 31 Dicembre 2011 [7]. Malgrado siano state bandite, in realtà le armi di distruzione di massa (WMD) sono state usate in scenari bellici quali, ad esempio, la guerra tra Iran e Iraq nel 1984/88: l'Iraq ha fatto uso di sostanze chimiche [8] durante la guerra e in occasione di alcuni attacchi terroristici.

Tali sostanze biologiche non solo colpiscono obiettivi specifici, ma possono anche potenzialmente portare a fenomeni di isteria di massa nella società ad esse esposta [9]. Lettere contaminate, contenenti il bacillo dell'antrace, sono state spedite negli Stati Uniti a diversi uffici di testate giornalistiche e a due senatori dell'ala democratica, uccidendo cinque persone e infettandone altre 17 [10].

Negli ultimi cinque anni, il traffico illegale di merci, persone e sostanze ha portato ad accrescere fortemente il livello di controllo contro gli attacchi terroristici, in particolare contro la contaminazione biologica delle merci [11]. L'adozione di questo tipo di misure di security diventa di primaria importanza in aree al confine come, ad esempio, le aree portuali, dove meno del 5% dei container sono analizzati allo scanner e merci potenzialmente contaminate da sostanze biologiche vengono consegnate tramite una intricata catena di distribuzione. Tuttavia, anche altre strutture civili strategiche possono costituire un facile obiettivo: metro, supermarket, reti di distribuzione idrica.

I nuovi strumenti tecnologici devono essere mirati al rilevamento e al riconoscimento a distanza di diversi materiali biologici pericolosi (bat-

several news media offices and two Democratic Senators, killed five people and infected 17 others [10].

During the last few years, the flow of illegal goods, people and substances has strongly forced to increase the level of control against terrorist attacks, in particular for infection of goods with biological agents [11]. This is a primary need in the border security area, i.e. harbors, where less than 5% of containers are scanned and the goods, possibly contaminated by biological attack, are distributed in a tangled supply chain. Nonetheless, other strategic civil structures (metro, supermarkets, hydric supply chains, etc.) can be affected, too.

The technology tools to be developed are addressed towards the stand-off detection and recognition of different dangerous biological materials (bacteria and viruses), tracing their presence in the air. Noxious B-agents to be considered for bio-terrorism are in the most dangerous class A, like Bacillus anthracis (Anthrax), Yersinia pestis (pneumonic plague), and Variolavirus (Smallpox).

Chemical warfare agents are gases, such as Yperite (from World War I). Nevertheless, gases are nowadays seldom used by terrorists. A remarkable exception was the attack with sarin gas at the Tokyo metro in 1995 [12].

teri e virus), tracciandone la presenza nell'aria. Agenti biologici nocivi da considerare in caso di bioterrorismo sono quelli di classe A, quella più pericolosa: Bacillus anthracis (antrace), Yersinia pestis (peste), e Variolavirus (vaiolo).
Le sostanze usate per la guerra chimica sono gas come l'iprite, utilizzata per la prima volta durante la Prima Guerra Mondiale. Tuttavia, attualmente i gas non sono usati spesso dai terroristi, eccezione esemplare fu l'attacco alla metropolitana di Tokio, perpetrato con gas sarin nel 1995 [12].

Esplosivi e precursori (inclusi IED e bombe sporche)

La definizione comunemente usata per il termine esplosivo è: un materiale, o singola sostanza pura, o una miscela di sostanze, in grado di generare un'esplosione mediante la sua stessa energia. Solitamente gli esplosivi sono specie chimicamente stabili che richiedono uno stimolo esterno, come un colpo o una scintilla, per liberare la propria energia. I vari stimoli ai quali rispondono gli esplosivi e le modalità di risposta nel produrre esplosioni forniscono una base conveniente per la loro classificazione. In alternativa, si utilizzano classificazioni basate sulla composizione chimica, in particolare sulla presenza di un gruppo nitrogenato attivo (NO, NH, C-N etc.) o perossido (O-O).
Sebbene le minacce CB abbiano un forte impatto sui media e sulla mente della popolazione, lo strumento preferito in assoluto dai terroristi resta sempre l'uso di armi esplosive, principalmente perché sono economiche, disponibili dappertutto e relativamente semplici da maneggiare. Il database START [6] riporta attacchi con bombe per circa il 49% degli atti terroristici perpetrati in tutto il mondo tra l'1 Gennaio 1970 e il 31 Dicembre 2011, vedi Figura1. La figura mostra chiaramente i problemi sorti a seguito dell'evento dell'11 Settembre, che ha scatenato una escalation di attacchi esplosivi.
La maggior parte degli esplosivi sono caratterizzati da una pressione di vapore bassissima e persino rilevatori altamente sensibili di tracce di gas non riescono a reagire alla loro presenza. La prima sfida tecnologica per la security è stata riconosciuta nella possibilità di rilevare con rapidità e affidabilità tracce di esplosivo nei punti di transito (varchi in aree affollate), al fine di sostituire l'unico rilevatore di gas naturale sensibile e selettivo: il naso del cane. Il rilevamento spettroscopico della composizione degli

Explosives and precursors (including IED and dirty bombs)

A common definition of explosive is: a material, either a pure single substance or a mixture of substances, which is capable of producing an explosion by its own energy. Explosives are usually chemically stable species which commonly require some stimulus, like a blow or a spark, to liberate their energy. The various stimuli to which explosives respond and the manners of their responses in producing explosions provide a convenient basis for their classification. Alternatively, classifications based on chemical composition, particularly on the presence of the active nitrogenated (NO, NH, C-N etc.) or peroxide (O-O) group, are utilized.
Although the CB threats bear a strong impact on the media and impression on the minds of the population, the most preferred terrorists' tool still remains the use of explosive weapons, mainly because these are low-cost, available everywhere and relatively easy to handle. In the START database [6] bombing attacks account for about 49% of the terroristic actions perpetrated worldwide between January 1st, 1970, and December 31st, 2011, see Figure 1. The figure clearly depicts the problems come out after 9/11 event, which triggered an escalation of explosive attacks.
The majority of explosives are characterized by a very low vapor pressure, and even high sensitivity gas phase trace detectors cannot react to their presence. The first technology challenge for Security has been recognized in fast and reliable trace detection of explosives at

elementi o l'individuazione di gruppi funzionali, ad esempio, tramite la tecnica LIBS [13] nel primo caso e quella Raman nel secondo [14], sembra attraente per la possibilità di rilevamento remoto automatico e il monitoraggio a distanza, evitando qualunque problema dovuto alla possibile stanchezza di operatori umani o animali.

In ogni caso la tecnologia progredisce e i terroristi sostituiscono gli esplosivi commerciali con gli IED, costruiti con esplosivi non disponibili in commercio, il più delle volte preparati in loco partendo da sostanze chimiche innocue. La definizione di uno IED concordata internazionalmente è la seguente: "Un qualunque dispositivo fabbricato in modo improvvisato che incorpora esplosivi o sostanze chimiche distruttive, letali, nocive, pirotecniche o incendiarie, progettato per distruggere, sfigurare, distrarre od ostacolare" [15].

Le informazioni incontrollate disseminate nel web e la presenza simultanea di persone altamente formate e laureate consente a un grande numero di individui di preparare e costruire IED contenenti esplosivi improvvisati (IE). Gli IE possono essere fabbricati in casa, con prodotti che possono essere acquistati senza alcuna autorizzazione specifica (ad es., nitrato di ammonio, pepe nero, perossido di idrogeno e altre sostanza chimiche). Tali sostanze sono comunemente definite come precursori di esplosivi. Ne consegue che la sfida tecnologica diventa il rilevamento di possibili precursori di esplosivi in luoghi imprevisti (ad es., una gran quantità di fertilizzanti nel garage di un appartamento di città) [5].

Il 22 luglio 2011 Anders Behring Breivik, di nazionalità norvegese, uccise 8 persone facendo esplodere un'autobomba (un VBIED, "dispositivo esplosivo improvvisato incorporato in un autoveicolo") nel quartiere governativo di Oslo (Norvegia). Il caso Breivik illustra che i precursori chimici di esplosivi sono facilmente ottenibili da chiunque sia in grado di inventare una ragione plausibile per procurarseli.

La Comunità Europea ha recentemente limitato la vendita sul mercato di precursori di esplosivi con il regolamento n. 98/2013 [16], nel quale sono elencate le sostanze che non saranno più rese disponibili al pubblico in generale, né da sole né miscelate, o sostanze che le includano, tranne nel caso in cui la concentrazione sia uguale o inferiore ai valori limite prefissati. Vi sono inoltre riportate le sostanze, da sole o miscelate, o contenute in composti che potrebbero indurre a transazioni sospette relative alla

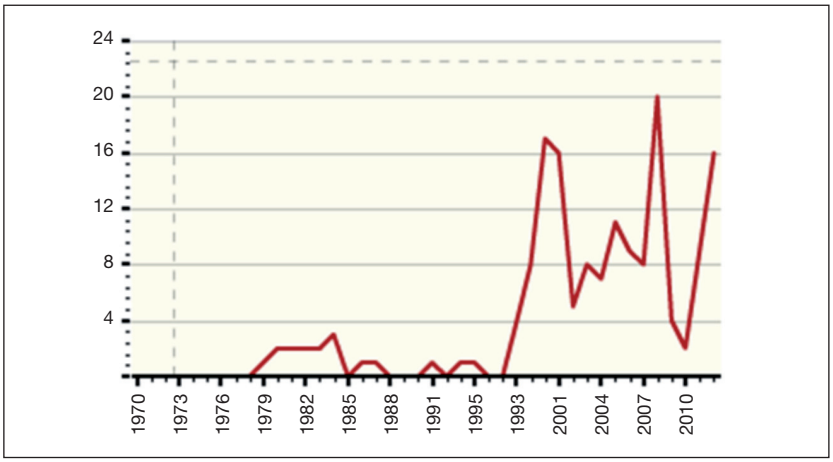


FIGURE 1 Worldwide explosives incidence from 1970 to 2010 year
Incidenza degli attacchi terroristici mediante esplosivi nel mondo dal 1970 al 2010
Source: [6]

transit points (gates in crowded areas) in order to replace the only sensitive and selective enough natural gas detector: the dog nose. Alternative spectroscopic detection of elemental composition or identification of functional groups, e.g. by LIBS [13] in the first case and by Raman in the second [14], appear appealing because of the chance of automatic remote detection and stand-off monitoring, without any problems related to the possible tiredness of human or animal operators.

Anyhow, technology is in progress and bombs made with commercial explosive are being replaced by terrorist with IEDs, where non-commercial explosives are utilized, most of the time produced in situ starting from harmless chemicals. The definition internationally agreed of an IED is the following: "Any device that is fabricated in an improvised manner, incorporating explosives or destructive, lethal, noxious, pyrotechnic, or incendiary chemicals, designed to destroy, disfigure, distract or harass" [15].

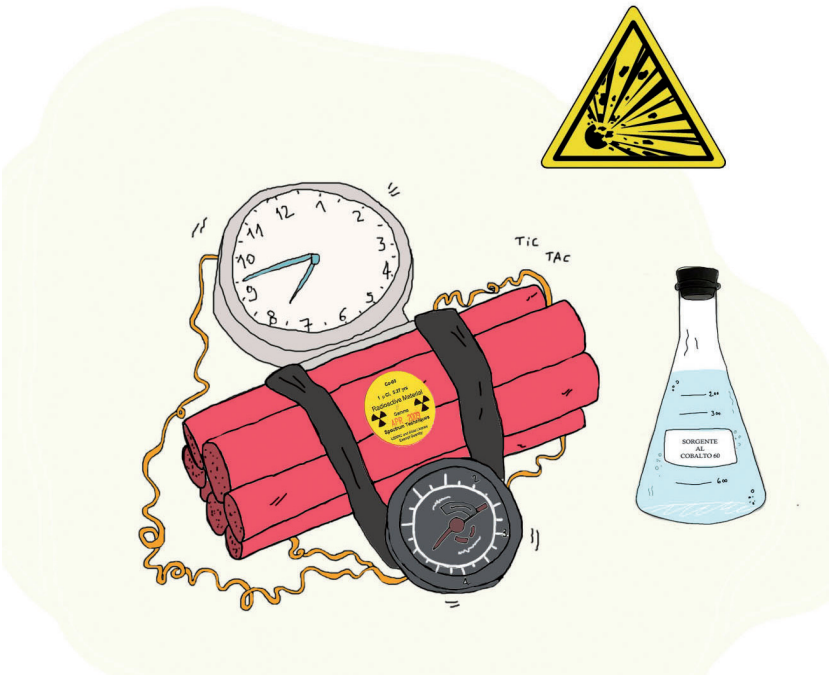
The uncontrolled information disseminated in the web and the simultaneous presence of highly trained and graduate personnel enables a large number of people to prepare and build IEDs containing Improvised Explosives (IE). IE can be realized at home, using products that can be bought without any specific authorization (e.g., ammonium nitrate, black pepper, hydrogen peroxide, and other chemical substances). These substances are commonly referred as explosive precursors. Hence, the technology challenge becomes the detection of possible explosive precursors at unexpected locations (e.g., large quantity of fertilizers in the garage of a city flat) [5].

compravendita e all'uso di precursori di esplosivi.
Il panorama degli attacchi terroristici con armi CBRNe si complica maggiormente con il concetto di "bomba sporca", che richiede un'ulteriore spiegazione. Una bomba sporca è un'arma radiologica ipotetica che combina materiale radioattivo con esplosivi convenzionali. Lo scopo di tale arma è di contaminare l'area circostante il cosiddetto "agente di dispersione" o '"esplosione convenzionale" con materiale radioattivo, fungendo primariamente da dispositivo per il divieto di accesso dei civili a una data area. L'uso di questo tipo di bomba sporca, basata sul Cesio-137, è stato rivendicato dai ribelli ceceni nei due attacchi falliti del 1995 a Mosca e del 1998 nei pressi di Grozny [17].
Tuttavia, è improbabile che una bomba sporca causi molte vittime da esposizione a radiazioni. Il suo scopo è presumibilmente quello di creare danni psicologici più che fisici, facendo leva sull'ignoranza e innescando meccanismi di panico e terrore di massa. Inoltre l'isolamento e la decontaminazione di migliaia di vittime, nonché la decontaminazione dell'area colpita potrebbero richiedere tempi e costi notevoli, rendendo tale area parzialmente inutilizzabile e causando pesanti danni economici. Per tale ragione oggi l'individuazione a distanza rapida e affidabile di bombe sporche rappresenta una importante sfida tecnologica.

Ricerca e sviluppo tecnologico per la security

Dal PASR-6PQ fino a Horizon 2020 tramite il 7PQ – Il panorama europeo

Il bisogno di un maggiore sforzo della ricerca europea per la security ha acquisito maggiore importanza dal 2002 al 2007, durante il Sesto Programma Quadro (6PQ). Attenzione è stata dedicata fin dall'inizio a bilanciare tale sforzo, affiancando i miglioramenti nelle forme di controllo con il rispetto della privacy e della libertà individuale. Bandi di progetto sono stati dedicati agli aspetti relativi alla security, in particolare allo spazio e all'aeronautica, nonché all'ICT. Inoltre, nello stesso periodo (2004-2006) è stata lanciata l'azione dedicata PASR (Preparatory Action for Security Research), che ha finanziato la realizzazione di progetti pilota. La lista delle misure di security nel 6PQ e nel PASR è disponibile in [18].
Nel frattempo, due commissioni (ESRIF - European Security Research and Innovation Forum, and ESRAB - European Security Research Advi-



On July 22nd, 2011, the Norwegian national Anders Behring Breivik killed 8 people through the explosion of a car bomb (a "vehicle-borne improvised explosive device", VBIED) in the government quarter of Oslo (Norway). The Breivik case illustrates that precursor chemicals are easily obtainable for anyone capable of inventing a plausible reason to procure them.
The EC has recently limited the market sale of explosive precursors with the 98/2013 regulation [16]. Substances which shall not be made available to members of the general public on their own, or in mixtures, or substances including them, except if the concentration is equal to or lower than the limit values set out, are listed. Furthermore, also substances on their own, or in mixtures, or in substances for which suspicious transactions referring to the marketing and use of explosives precursors are reported.
The terroristic attack panorama, based on CBRNe weapons, is further complicated by the concept of "dirty bomb", which requires an additional explanation. A dirty bomb is a speculative radiological weapon that combines radioactive material with conventional explosives. The purpose of the weapon is to contaminate the area around the "dispersal agent"/"conventional explosion" with radioactive material, serving primarily as an area denial device against civilians. The use of such a type of dirty bomb (based on Caesium-137) has been claimed

sory Board), composte da specialisti e strateghi altamente qualificati, hanno stilato le linee strategiche per la ricerca europea sulla security, suggerendo i principi e i meccanismi per la loro adozione all'interno del Settimo Programma Quadro (7PQ) per la Ricerca della Commissione Europea.
Nel 7PQ è stata aggiunta una priorità tematica (tema 10) sulla Security, quale specifico programma di cooperazione, ponendo l'attenzione sulle quattro missioni della Security suggerite dall'ESRAB [19]:

- *security dei cittadini;*
- *security delle infrastrutture e dei servizi pubblici;*
- *sorveglianza intelligente e security di confine;*
- *ristabilire condizioni di security e sicurezza personale in caso di crisi.*

Inoltre, sono state considerate tre attività trasversali: Integrazione, interconnettività e interoperabilità dei sistemi di security; Security e società; Coordinamento e strutturazione della ricerca sulla security.
Oggi, i temi relativi alla security sono ritenuti della massima importanza nei programmi di cooperazione internazionale. L'argomento relativo alla protezione dei cittadini è incluso nel programma di ricerca europeo Horizon 2020 (H2020). In particolare, appartiene ad uno dei tre maggiori pilastri, l'unico relativo alla società sicura, finalizzato alla protezione della libertà e della security dell'Europa e dei suoi cittadini.
La sfida sulla security posta da H2020 consiste nell'intraprendere tutte le attività di ricerca e di innovazione necessarie alla protezione dei cittadini, della società e dell'economia, nonché di servizi e infrastrutture, della prosperità, della stabilità politica e del benessere. Secondo la dichiarazione ufficiale della Comunità Europea riportata in [20], gli obiettivi primari della sfida per una società sicura sono:

- *migliorare la resistenza della nostra società contro le catastrofi naturali e quelle causate dall'uomo;*
- *combattere il crimine e il terrorismo;*
- *migliorare la security ai confini;*
- *fornire una migliore security telematica.*

Altri promotori internazionali della security

L'Agenzia Europea per la Difesa (AED) è il luogo di riferimento per la cooperazione per la difesa europea sin dal 2004, anno della sua fondazione. Tra i suoi impegni istituzionali, l'AED

by Chechen rebels in two failed attacks in 1995 and 1998, the first in Moscow and the second near Grozny [17].
However a dirty bomb is unlikely to cause many deaths by radiation exposure. Its purpose would presumably be to create psychological, not physical, harm through ignorance, mass panic, and terror. Additionally, containment and decontamination of thousands of victims, as well as decontamination of the affected area might require considerable time and expense, rendering areas partly unusable and causing economic damage. For this reason, nowadays fast and reliable remote identification of dirty bombs is a significant technological challenge.

RTD for security

From PASR-FP6 through F7 to Horizon 2020 – The European panorama

The needs to increase European research effort on security became significant during the 6th Framework Programme (FP6) in 2002-2007 period. Attention was paid to balance it, which implied enhanced forms of control, with the respect of privacy and individual freedom. Calls for projects were dedicated to aspects concerning security, especially for aeronautic and space, and for ICT. Additionally, in the same period (2004-2006) the dedicated PASR (Preparatory Action for Security Research) action was launched, funding pilot projects. A review of security measures in FP6 and PASR can be found in [18].
Meanwhile two commissions (ESRIF - European Security Research and Innovation Forum and ESRAB - European Security Research Advisory Board), composed by highly qualified specialists and strategists, have drawn the strategic lines for European security research and advised on the principles and mechanism for its implementation within the Commission's 7th Framework Programme (FP7) for Research.
In FP7 a thematic priority (theme 10) on Security was added, as a specific cooperation programme. The focus was set on the four Security missions suggested by ESRAB [19]:

- Security of citizens,
- Security of infrastructure and utilities,
- Intelligent surveillance and border security,
- Restoring security and safety in case of crisis.

Furthermore three cross cutting activities were considered: Security systems integration, interconnectivity and interoperability, Security and Society, Security Research coordination and structuring.
Nowadays, the themes related to security are of utmost importance in international cooperation programs. The topic, relevant to Citizen protection, is included in Horizon 2020 (H2020), the current European research programme. In particular, it belongs to one of the three major pillars, the one relevant to Secure society, aimed at protecting freedom and security of Europe and its citizens.

porta avanti anche progetti di ricerca e sviluppo tecnologico, iniziative a supporto dell'industria europea della difesa e un metodo innovativo di duplice utilizzo. Il Ministero della Difesa dei rispettivi paesi membri assicura il proprio supporto ai nuovi progetti.
Il programma Science for Peace and Security (SPS), originariamente nato come programma scientifico della NATO negli anni Cinquanta, offre finanziamenti per attività di progetti di collaborazione, workshop e formazione, che coinvolgono scienziati provenienti dai paesi membri della NATO e dai paesi partner. L'SPS è uno strumento politico per migliorare la cooperazione e il dialogo con tutti i partner e costituisce una palestra interessante per i giovani ricercatori, che collaborano anche con paesi extra NATO.
Parallelamente, varie lobby europee sono attive nel panorama della security, promuovendo i bisogni e le nuove aspettative degli operatori o dei portatori di interesse che intendono avere un dialogo specifico con la CE. Tra queste, l'AeroSpace and Defense Industries Association of Europe rappresenta le maggiori industrie europee nel campo dell'aeronautica, spazio, difesa e security. Diversamente, l'Integrated Mission Group for Security (IMG-S) è un forum pubblico che riunisce gli esperti di tecnologie provenienti da industria, PMI, Organizzazioni di Ricerca e Sviluppo e dal mondo universitario. IMG-S fornisce il proprio supporto alla Commissione Europea e agli Stati Membri nella costruzione di capacità tecnologiche europee di classe mondiale.

Lo scenario italiano

Vari paesi europei come, per citarne alcuni, Germania, Gran Bretagna, Olanda, Svezia, hanno incluso nel proprio programma nazionale dedicato il supporto alla ricerca sulla security, in maniera analoga, ma non speculare, ai Programmi Quadro europei. Al contrario, in Italia non è disponibile alcuna opportunità di finanziamento, malgrado la security per la difesa nazionale sia citata nel Programma di Ricerca Nazionale 2011-2013.
A livello nazionale, la piattaforma italiana per la security SERIT (Security Research in Italy) è un'iniziativa congiunta lanciata da CNR e Finmeccanica, che riunisce industrie italiane (grandi industrie e PMI), università, centri di ricerca e utenti finali. L'obiettivo è lo stesso del suo gemello IMG-S, ma con un legame più forte con le autorità nazionali.

The challenge on security afforded by H2020 is about undertaking research and innovation activities needed to protect our citizens, society and economy as well as our infrastructures and services, our prosperity, political stability and wellbeing. According to the official European Community statement reported in [20], the primary aims of the Secure Societies Challenge are:

- *to enhance the resilience of our society against natural and man-made disasters;*
- *to fight crime and terrorism;*
- *to improve border security;*
- *and to provide enhanced cyber-security.*

Other international security promoters

The European Defense Agency (EDA) is the place to go for European defense cooperation since its foundation in 2004. EDA, among its institutional commitments, conducts also RTD projects, works on initiatives in support of the European defense industry, and advances an innovative dual-use approach. The Ministry of Defense of the respective member states assures the support of the new projects.
The Science for Peace and Security Programme (SPS) originally founded as the NATO Science Programme in the 1950s, offers grants for collaboration projects, workshops and training involving scientists from NATO member states and partner countries. SPS is a policy tool for enhancing cooperation and dialogue with all partners, and is an interesting palaestra for young researchers to collaborate also with extra NATO countries.
In parallel, different European lobby organizations are active in the Security panorama, fostering the needs and new expectations from the operators or stakeholders that intend to have a specialized dialogue with the EC. Among them the AeroSpace and Defense Industries Association of Europe represents the major aeronautics, space, defense and security industries in Europe. Conversely, the Integrated Mission Group for Security (IMG-S) is an open forum bringing together technology experts from Industry, SMEs, Research and Technology Organizations (RTOs) and Academia. IMG-S aims to support the European Commission and its Member States to build world-class European technological capabilities.

The Italian background

Different European countries, Germany, Great Britain, Holland, Sweden, just to mention a few, have included in their own dedicated national program the support to Security research, analogous but not mirrored to the EU Framework Programs. Conversely, in Italy no specific funding opportunities are available, although the Homeland Security is indicated in the National Research Program 2011-2013.

Scenari di riferimento

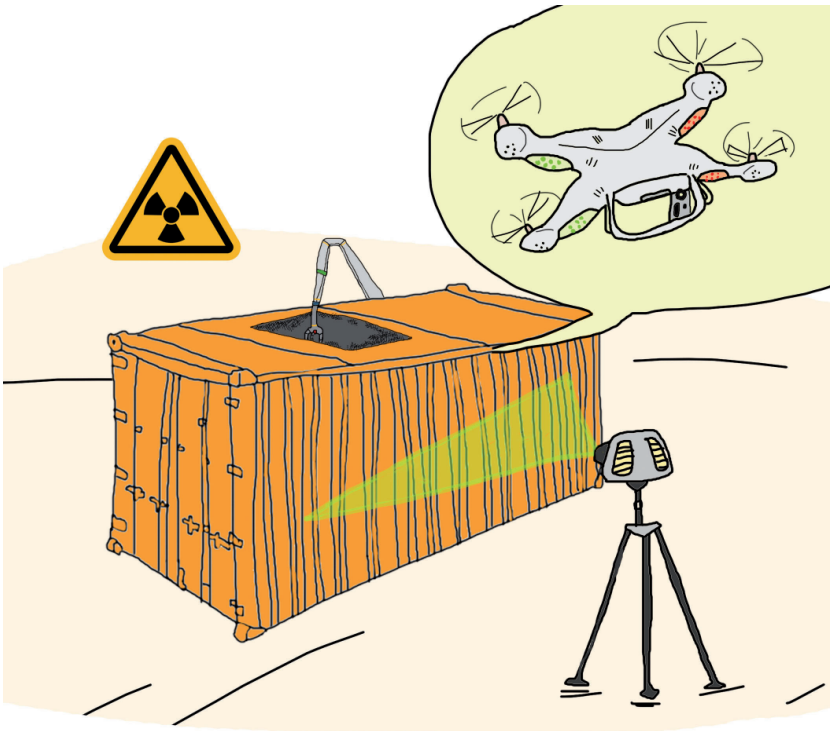
Security per il trasporto di massa e la gestione delle folle

La mobilità globale è una conquista importante della società industriale moderna, che comporta una rete complessa di infrastrutture, nelle quali il flusso di gente, informazioni e merci è stato molto semplificato. Le criticità emergono là dove le minacce attuali a cui è sottoposta la società sono numerose e complesse. In siti molto affollati come, ad esempio, i punti di scambio per il trasporto, le operazioni vengono spesso eseguite al limite della capacità delle infrastrutture, rendendole in tal modo maggiormente vulnerabili a eventuali attacchi.

La società, viceversa, non è chiamata a far fronte a una singola minaccia o pericolo, ma a numerose prove, quali terrorismo, crimine organizzato, instabilità regionale e calamità naturali, che esigono altrettante azioni tecnologiche e non tecnologiche di natura preventiva e contromisure. Ne consegue che la tecnologia e le metodologie utilizzate per identificare la varietà delle minacce devono essere rapide e versatili, capaci di rilevare quantità massicce o tracce di agenti CBRNe e armi nascoste, senza causare disordine o ritardi eccessivi.

Lo sviluppo di strumenti multiuso per il rilevamento rapido di immagini con il riconoscimento automatico della minaccia è l'obiettivo finale adatto a un comune scenario di varchi per il trasporto di massa e, più in generale, a punti di controllo. Nel primo caso, varchi attivi o passivi dovrebbero essere utilizzati per passeggeri e bagagli a mano; nel secondo, i portali dovrebbero consentire lo screening del contenuto di valigie di varie dimensioni, da quelle personali ai container che viaggiano su grandi aerei, navi e treni merci. I requisiti di protezione della sicurezza personale e della privacy sono molto diversi nei due casi, con pesanti restrizioni per l'uso di radiazioni ionizzanti e potenzialmente nocive (persino nella regione microonde - THz) su esseri umani, tuttavia la rapidità è fondamentale in entrambi. Oltre alle armi e agli esplosivi, i materiali da identificare possono essere diversi, inclusi, ad esempio, i precursori di IED sui passeggeri o i radionuclidi nascosti nelle merci [21].

Etichettare persone e oggetti sospetti durante il percorso di imbarco sarebbe una procedura appropriata che consentirebbe di eseguire le successive misure di conferma utilizzando



At the national level, the Italian Security platform SERIT (Security Research in Italy) is a joint initiative launched by CNR and Finmeccanica, bringing together Italian industries (both large industries and SMEs), academia, research centers and end-users. Its final aim is the same as that of the twin IMG-S but with a stronger connection with the national authorities.

Reference scenarios

Mass transport security and crowd management

Global mobility is a significant achievement of the modern industrial society involving a complex network of infrastructures, where people, information, and goods can easily flow. Critical points emerge where current threats facing society are numerous and complex. In very crowded sites, such as transport hubs, operations often proceed at the limit of the infrastructure capability, thus increasing its vulnerability to attacks. Conversely, society is not called to face a single threat or hazard, but a variety of challenges such as terrorism, organized crime, regional instability and natural disasters, that demand a corresponding variety of non-technological and technological actions, of a preventive

tecnologie alternative, riducendo drasticamente il numero di falsi positivi. La lunghezza del percorso da seguire durante le suddette procedure e i tempi richiesti svolgono un ruolo significativo nella selezione delle diverse tecnologie per i controlli successivi. A questo riguardo, lo scenario del trasporto urbano è di gran lunga più severo di quello relativo al traffico aereo.

Per ottenere la massima attenzione dell'opinione pubblica, un gruppo terroristico tende a colpire aree affollate, dove la quantità di agenti disturbatori presenti potrebbe consentire di raggiungere la massima distruzione. In caso di panico, proprio il comportamento della folla potrebbe causare ulteriori vittime, anche in conseguenza di una minaccia di minima entità.

La gestione delle folle richiede che siano considerati tutti gli elementi di un evento, partendo dalla sua tipologia (spettacolo circense o sportivo o teatrale, concerto, rally, parata, ecc.), le caratteristiche della struttura e suoi accessi, le comunicazioni disponibili, la dimensione e il comportamento della folla, le possibilità di un suo controllo anche nello smaltimento delle code. Come accade per ogni tipo di gestione, occorre tenere conto della pianificazione, l'organizzazione, il reclutamento di personale la direzione e la valutazione. Particolarmente importanti per la gestione delle folle sono la definizione dei ruoli delle parti coinvolte in un evento, la qualità delle risorse di intelligence avanzata e l'efficacia del processo di pianificazione.

Lo sviluppo tecnologico nella gestione delle folle è mirato sia alle misure preventive, sia agli interventi. Lo screening delle folle mediante il rilevamento automatico di comportamento sospetto (insolito), che fa scattare i sensori per minacce specifiche su un target selezionato (potenziali terroristi), appartiene al primo gruppo, mentre la pronta attivazione automatica di vie di fuga, assistita da dispositivi autonomi non gestiti da operatori umani e tramite strumenti di ICT, è un esempio del secondo gruppo.

Sistemi di reti di rilevamento e accettazione etica

Gli scenari fin qui presentati sono molto complessi a causa della loro grande variabilità e di minacce rilevanti che, nella maggior parte dei casi, sono quasi imprevedibili. Diverse tecniche di rilevamento, che nel caso dei sensori

nature as well as counter measures. Consequently the technology and the methodologies used to identify the variety of threats must be fast and versatile - capable of dealing with the detection of hidden bulk and trace of CBRNe agents and concealed weapons, without causing excessive disruption or delay.

The development of multipurpose instrumentation for fast imaging with automatic recognition of the threat is the final objective suitable for a common scenario at mass transport gates, and more generally at custom controls. In the former case, active or passive gates should be utilized on people and their hand luggage, in the latter portals should permit the screening of the content of differently-sized luggage, from personal suit cases to containers travelling on large cargos planes, ships and trains. Safety and privacy requirements are largely different in the two cases, with heavy restrictions to the use of ionizing and potentially harmful radiation (even in the microwave - THz region), however speed is crucial in both cases. Apart from weapons and explosives, the target materials to be detected might be different, including for instance IED precursors on passengers or radionuclides hidden with goods [21].

Labelling suspect persons and items during a loading path is a successful procedure that might permit to perform successive confirmation measurements by alternative technologies in order to drastically reduce the number of false positives. The length of the path to be followed during the boarding procedures and the time required do play a significant role in selecting different technologies for successive checks. To this respect the scenario for urban transport is by far more stringent than that relevant to airport traffic.

With the aim of maximizing the attention from public opinion, a terroristic group tends to strike in a crowded area, where the same quantity of disruptive agents could allow to achieve the most destruction. In case of panic the crowd behavior itself can cause additional loss of human lives, even as a consequence of a very minor threat.

Crowd management must take all the elements of an event into account, especially the type of event (circus, sporting, theatrical, concert, rally, parade, etc.), characteristics of the facility, size and demeanor of the crowd, methods of entrance, communications, crowd control, and queueing. As in all management, it must include planning, organizing, staffing, directing and evaluating. Particularly critical to crowd management is defining the roles of the parties involved in an event, the quality of the advance intelligence, and the effectiveness of the planning process.

Technologic development in crowd management is addressed to both preventive measures and interventions. Crowd screening with automatic detection of suspect (unusual) behavior triggering sensors for specific threats on a selected target (potential terrorists) belongs to the first group, while prompt automatic activation of escape route

elettro-ottici coprono l'intero spettro elettromagnetico, possono essere utilizzate per fornire informazioni rapide ed efficaci sulla eventuale presenza di sostanze sospette.
Il metodo emergente per far fronte alla security in tutti i tipi di scenario consiste nell'integrare le informazioni (video, chimiche, fisiche), raccolte da una rete di vari sensori e sistemi di consapevolezza ambientale, e convogliarle in un Centro di Comando e Controllo supportato dalle tecnologie Expert System. La rete deve garantire la confidenzialità dei dati ed essere predisposta per accogliere la futura integrazione di nuovi dispositivi, che consenta la realizzazione di una cosiddetta 'architettura aperta'.
Attualmente, il modello di security adottato negli aeroporti è forse l'esempio migliore per l'intenso lavoro normativo eseguito dall'International Civil Aviation Organization, dove le necessità emergenti vengono discusse e le contromisure individuate e proposte mediante norme che ne definiscono le caratteristiche logistiche e tecniche. Ovviamente i diversi scenari andranno modificati in modo che in futuro possano essere progettati con proprie infrastrutture di security già incorporate. È prevedibile che tecnologie a distanza, basate su radiazioni non-ionizzanti, svolgeranno un ruolo sempre più importante senza però sostituire completamente il rilevamento puntuale, necessario per la conferma locale, i successivi interventi delle autorità competenti e l'uso in campo forense.
Tutte queste tecnologie di screening non riscuotono l'accettazione immediata da parte della società civile, a causa dell'invasione della privacy che potrebbe limitare la libertà individuale. Ne consegue necessariamente che, per un risultato soddisfacente occorre trovare un equilibrio tra l'applicazione di misure efficaci per migliorare la security e il rispetto dei diritti civili.

(traduzione di Carla Costigliola)

assisted by unmanned autonomous vehicles and by available ICT tools is an example of the second one.

Networked Detection Systems and ethical acceptance

The scenarios presented above are very complex having a large variability, and relevant threats are in most cases almost unpredictable. Numerous different detection techniques, covering all the electromagnetic spectrum in case of electro-optical sensors, can be utilized to supply rapid and effective information on the presence of suspicious substances.
The emerging approach to face security in all the scenarios is to integrate the information collected from a network of various sensors and systems of environmental awareness (video, chemical, physical), and to merge it in a Command and Control center supported by Expert System technologies. The network has to ensure the confidentiality of the data and to be open to the future integration of new devices, in a so-called open architecture.
Presently, the security model adopted in the airports is perhaps the best example due to the intense regulation work performed by International Civil Aviation Organization, where the emerging needs are discussed and the countermeasures regulated in both logistic and technical characteristics. Obvious modifications to the different scenarios have to be adopted, so that in the future they already have to be designed with their own security infrastructures embedded. It is predictable that stand-off technologies based on non-ionizing radiations will play an increasing role, without completely replacing the point-detection necessary for local confirmation, next authorities intervention and forensic use.
These screening technologies are not so immediately acceptable by the civil society, due to the privacy invasion that can affect the individual freedom. A balance between implementing effective measures to improve security and respecting civil rights is mandatory to obtain a satisfactory result.

Roberta Fantoni
ENEA, Technical Unit for the Development of Applications of Radiation

Antonio Palucci
ENEA, Technical Unit for the Development of Applications of Radiation - Diagnostics and Laser Metrology Laboratory

references & notes

[1] M. Minichino et al, Quality of service of an electrical grid under cyber attacks on its Supervisor Control and Data Acquisition System (this issue).

[2] F. Padoani, A. Rizzo, Developing the human dimension of security by means of centres of excellence (this issue).

[3] A. Malizia et al, Building a Chemical-Biological-Radiological-Nuclear, Eplosive events tech advisor and first responders team to support top decision makers during the emergencies (this issue).

[4] V. Rosato et al, Decision support system aimed at improving the "physical protection" of critical infrastructures against natural events (this issue).

[5] L. Fiorani et al, Lidar/DIAL detection of explosive precursors by OPO/OPA laser systems (this issue).

[6] National Consortium for the Study of Terrorism and Responses to Terrorism (START), Global Terrorism Database, http://www.start.umd.edu/gtd [Accessed 3 November 2013].

[7] D. J. Dire, 2013, CBRNE - Biological Warfare Agents, Medscape, New York, NY.

[8] United Nations - Security Council, 2006, Twenty-sixth quarterly report on the activities of the United Nations Monitoring, Verification and Inspection Commission in accordance with paragraph 12 of Security Council resolution 1284 (1999), United Nations, New York, NY. http://www.un.org/en/ga/search/view_doc.asp?symbol=S/RES/1284(1999)

[9] J. Du, 2002, Bioterrorism: How Has It Been Used? What Can It Do? How Prepared Are We? UCLA, Los Angeles, CA– http://www1.international.ucla.edu/article.asp?parentid=1352

[10] Federal Bureau of Investigation, Famous Cases and Criminals: Amerithrax or Anthrax Investigation, FBI, [Online]. Available: http://www.fbi.gov/about-us/history/famous-cases/anthrax-amerithrax [Accessed 3 November 2013].

[11] A. Lai et al, Innovative devices for biohazards and food contaminants (this issue)

[12] H. Murakami, 2003, Underground. Racconto a più voci dell'attentato alla metropolitana di Tokyo, Einaudi, ISBN 978-88-06-16521-5.

[13] V. Lazic et al, 2011, "Detection of explosives in traces by laser induced breakdown spectroscopy: Differences from organic interferents and conditions for a correct classification", Spectrochim. Acta Part B, 66 ,644–655.

[14] A. Palucci et al, Raman spectroscopy for the detection of trace amounts of energetic materials for counterterrorism issues (this issue).

[15] NATO STANAG AAP6-6+Interagency Intelligence Committee on Terrorism – From Enhancing the security of explosives – Report of the explosive security experts task force, Brussels, 28 June 2007, http://nso.nato.int/nso/

[16] Regulation (EU) No 98/2013 of the European Parliament and of The Council of 15 January 2013 on the marketing and use of explosives precursors. http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:039:0001:0011:EN:PDF

[17] J. Bale, 2004, The Chechen resistance and radiological terrorism, Global Security Newswire, Article, April 1st 2004 - http://www.nti.org/analysis/articles/chechen-resistance-radiological-terror

[18] D. Bigo, J. Jeandesboz, 2008, DG Internal Policies of the Union, briefing note PE 393.289 (May 2008), http://edz.bib.uni-mannheim.de/daten/edz-ma/ep/08/EST21149.pdf

[19] European Security Advisory Board (ESRAB), Meeting the Challenge: the European Security Research Agenda, Office for Official Publications of the European Communities, Luxembourg, 2006 - http://cordis.europa.eu/fp7/security/about-security_en.html

[20] http://ec.europa.eu/programmes/horizon2020/en/h2020-section/secure-societies-%E2%80%93-protecting-freedom-and-security-europe-and-its-citizens

[21] Di Lazzaro et al, Marking and tracking radioactive materials: a possible Hi-TECH solution (this issue).