BIBLIOGRAFIA

Convention on the Prohibition of the Development, Production, Stockpiling and use of Chemical Weapons and on their Destruction, «Technical Secretariat of the Organization for the Prohibition of Chemical Weapons - OPCW», The Hague 2005.
Chemical Facility Anti-Terrorism Standards; *Final Rule*, in «Secretary of Homeland Security, Department of Homeland Security - DHS», Washington DC 2006.
Risk-Based Performance Standards Guidance – Chemical Facility Anti-Terrorism Standards, «Department of Homeland Security - DHS», Washington DC 2008.
Prudent Practices in the Laboratory: Handling and Management of Chemical Hazards: Updated Version, «National Research Council (US) Committee on Prudent Practices in the Laboratory», National Academies Press, Washington DC 2011.
National Code of Practice for Chemicals of Security Concern, «Business Law Branch Attorney-General's Department, Attorney General's Department, Commonwealth of Australia», Barton, Australian Capital Territory 2014.
L. Caldwell, *Critical Infrastructure Protection, Observations on* DHS *Efforts to Identify, Prioritize, Assess, and Inspect Chemical Facilities*, «GAO - United States Government Accountability Office», Washington DC 2014.
A. Fasanella, *Perché i pinguini hanno volato e chi ha insegnato loro a farlo?*, «Osservatorio Sicurezza e Difesa CBRNe - Punti di Vista», Roma 2012.
M. Gismondo et al., *Handbook on chemical and biological waste management*, «UNICRI/EU CBRNe CoE», Roma 2014.
J.M. McComb, *Closing Pandora's Box: The Threat of Terrorist Use of Weapons of Mass Destruction*, «Global Security Studies», Volume 4, Issue 1, 2013.
R. Mugavero – V. Sabato, *Securing* CBRN*e*, WMD *and Dual-Use Laboratories and Researches: Emerging Issues and New Challenges*, «11° International Symposium on Protection against Chemical and Biological Warfare Agents», Stockolm 2013.
Osservatorio Sicurezza e Difesa Cbrn*e*, Scuola Interforze per la difesa nucleare, biologica, chimica, Università di Roma 'Tor Vergata' – Dipartimento di ingegneria elettronica, Università degli studi della Repubblica di San Marino – Centro universitario di formazione sulla sicurezza, *Corso* 'CBRN*e* I*ntelligence* I *Livello*', Rieti 2013; *Corso* 'CBRN*e* I*ntelligence* II *Livello*, Rieti 2014.
Presidenza del Consiglio dei Ministri – Comitato Nazionale per la biosicurezza, le biotecnologie e le scienze della vita, *Codice di Condotta per la Biosicurezza*, Roma 2010.
Presidenza del Consiglio dei Ministri – Dipartimento delle Informazioni per la Sicurezza – «Gnosis. Rivista italiana di intelligence», *Il Linguaggio degli Organismi Informativi – Glossario*, Roma 2013.
D.A. Shea, *Chemical Facility Security: Issue and Options for the 112th Congress*, Washington DC 2012.
R.P. Stickles – H. Ozog – S. Mohindr, *Security Vulnerability Assessment* (SVA) *Revealed*, ioMosaic Corporation Whitepaper, Salem, New Hampshire 2003.
M. Vaccaro, *Safety and Security*, «Commissione Tecnico Scientifica», Caserta 2005.

Rischio CBRN*e* e proliferazione WMDE

Scienza, ricerca, innovazione e sicurezza nazionale

Roberto Mugavero

Le nuove minacce per la sicurezza registrano l'uso di armi sia convenzionali che non convenzionali. Ciò evidenzia come gruppi criminali e terroristici possano ricercare nel campo scientifico, accademico e industriale un'importante fonte di competenze nell'uso di moderne tecnologie e di strumenti innovativi. In un'ottica di tutela della sicurezza nazionale, fondamentale si attesta una sempre maggiore protezione di tali ambiti, con specifica attenzione a quelli afferenti alla ricerca e alle applicazioni dual-use.

Negli ultimi decenni, tra i molteplici settori strategici per la sicurezza nazionale, rilievo prioritario hanno assunto anche gli ambiti relativi a scienza, ricerca, tecnologia e innovazione, soprattutto per l'importanza che essi hanno sulla vita, sullo sviluppo e sulla crescita del Paese e dei suoi interessi. Ma come si pongono dinanzi alle attuali minacce, caratterizzate dalla volontà di provocare danni e vittime con un profondo impatto psicologico sulla collettività?
Interessante è comprendere i possibili fattori di vulnerabilità nel campo scientifico, accademico e industriale rispetto alla tutela degli interessi nazionali e alla protezione della popolazione, delle infrastrutture e del territorio. Tali considerazioni valgono con riferimento ai temi correlati agli agenti chimici, biologici, radiologici, alle attività nel campo nucleare (Cbrn*e* e al rischio esplosivo), che risultano essere sempre più appetibili per la criminalità e il terrorismo.
Per intendere appieno le ragioni della crescita dei nuovi rischi, bisogna considerare i grandi cambiamenti avvenuti in ambito geopolitico, contrassegnati da ampi processi di transizione in molti Paesi del Nord Africa e nelle aree più instabili del Medio Oriente. Tali mutamenti hanno condotto anche all'estremizzazione di radicalismi e fondamentalismi che si sono manifestati in azioni aggressive e violente.

L'attrazione verso le armi non convenzionali, in funzione di attacchi terroristici, è testimoniata da numerosi episodi.
Nel 2009 è stato sventato un attacco contro la metropolitana di New York, che prevedeva l'impiego di Wmd, organizzato da elementi affiliati ad Al Qaeda, tre dei quali identificati, arrestati e condannati.
Le capacità dell'organizzazione terroristica nel campo dell'armamento non convenzionale erano già emerse in precedenti occasioni. Nell'aprile 2004 le Forze di polizia giordane avevano sequestrato a otto membri di Al Qaeda una vasta gamma di armi chimiche, tra cui agenti soffocanti, vescicanti e gas nervino. Prima dell'11 settembre 2001, d'altra parte, era stato sperimentato in Afghanistan un programma di armamento chimico testimoniato dalla scoperta, durante il conflitto, di laboratori e di video nei quali membri del gruppo islamista testavano gas su alcuni cani.
Nell'agosto 2014, nel quadro di un'offensiva contro elementi dell'Isis, in un villaggio della Siria è stato rinvenuto un computer portatile già appartenente a un membro tunisino, esperto in chimica e fisica, con materiale riguardante lo sviluppo e l'impiego di armi biologiche. Il pc conteneva, tra gli altri, un documento illustrativo dei vantaggi riconducibili all'uso di tali agenti rispetto alle armi convenzionali (economicità, a fronte di un alto numero di potenziali vittime) e una *fatwa*, pronunciata dallo studioso e religioso jihadista saudita Nasir Al-Fahd, nella quale si approvava l'uso di armi di distruzione di massa contro gli infedeli laddove si fosse ravvisata l'impossibilità di sconfiggerli con altri mezzi. L'organizzazione non governativa Syrian Observatory for Human Rights ha poi confermato il lancio da parte dell'Isis, nel giugno 2015, nei pressi della città di Al-Hasakah, di razzi a caricamento chimico su civili e milizie curde.
Questi richiami danno conto del crescente interesse da parte del terrorismo fondamentalista verso nuove strategie offensive, e pongono gli Stati di fronte alla necessità di assicurare un'adeguata diffusione e condivisione del sapere, garantendo la riduzione dei rischi che ne derivano. È evidente come si debba essere sempre più indirizzati verso una logica comprensiva e integrata, ove anche attività del campo scientifico e tecnologico costituiscano uno dei fronti sui quali le strategie di sicurezza del Paese devono interrogarsi.
Ciò anche in ragione di un sempre maggiore coinvolgimento del settore dell'intelligence preposto alla controproliferazione – dedicato, cioè, alla prevenzione e al contrasto della realizzazione di armi di distruzione di massa – attivo con iniziative tese a individuare traffici di materiali, tecnologie e know-how e a identificare quei fattori che possano rappresentare, per le proprie peculiarità, elementi da proteggere e salvaguardare.

Per tale motivo, la comunità gravitante attorno a settori attigui alle tematiche dell'armamento non convenzionale non può esimersi dal promuovere politiche di gestione responsabili, ove il principale riferimento sia costituito da specifiche normative, linee guida, codici etici e di condotta in grado di realizzare il giusto equilibrio tra la corretta crescita tecnologica per usi civili e l'esigenza di impedirne un impiego per finalità criminali e/o terroristiche.
Alcuni eventi rappresentano un esplicito richiamo a rischi concreti.
Il primo episodio risale all'autunno del 2001 quando, negli Stati Uniti, spore di *bacillus antracis* vennero inviate per posta, causando il decesso di cinque persone e il contagio di molte altre. Il ceppo di antrace utilizzato fu l'*ames*, uno dei più letali tra quelli noti e i gruppi di specialisti incaricati di scoprirne l'origine formularono conclusioni ben diverse. Una parte sostenne che si trattava di un agente che qualsiasi microbiologo avrebbe potuto produrre con strumentazioni scientifiche di base e locali di fortuna. Altri dichiararono che il materiale poteva essere prodotto solo con capacità e tecnologie molto avanzate. In ogni caso l'evento fu seguito dall'adozione del Federal Select Agent Program che, da allora, sovrintende al possesso, all'uso e al trasferimento di agenti biologici e tossine che rappresentino una potenziale minaccia per la salute pubblica e che prevede, per tutto il personale operante, preventive valutazioni di sicurezza.
Il secondo episodio, divenuto pubblico nel 2008, ha visto come protagonisti i Servizi britannici che hanno appurato come negli anni, più di un centinaio di sospetti terroristi, nelle vesti di laureati e dottorandi, abbiano tentato di infiltrarsi in laboratori chimici, biologici e nucleari del Paese con l'obiettivo di acquisire mezzi cognitivi, metodologici, tecnologici e strumentali per la realizzazione di armi di distruzione di massa. Ciò ha determinato un innalzamento dell'allarme da parte dell'MI5 e del Foreign and Commonwealth Office in merito al rischio di reclutamento, da parte di organizzazioni terroristiche, di scienziati e studenti universitari con accesso a laboratori specialistici per materiali e tecnologie correlati ad agenti Cbrn*e*. Il Regno Unito, peraltro, ritenendo già concreti simili tentativi, aveva introdotto a partire dal novembre 2007, un piano denominato Academic Technology Approval Scheme (Atas), volto alla certificazione di studenti stranieri provenienti da nazioni extra Ue e richiedenti l'ingresso nel Paese per motivi di studio o ricerca su tematiche e tecnologie sensibili in campi quali la chimica, l'ingegneria, la fisica, la biofisica, la metallurgia e la microbiologia. Per tali tipologie di studenti il conseguimento di un certificato Atas – rilasciato solo in assenza di legami dei richiedenti con programmi di proliferazione Wmd e di elementi di rischio per la sicurezza nazionale – costituisce un prerequisito per ottenere il visto d'ingresso. L'Atas è quindi, a livello europeo, una delle prime concrete iniziative adottate per evitare la diffusione di conoscenze e capacità utilizzabili anche per scopi non pacifici o terroristici. Già nel primo periodo di applicazione ha determinato il respingimento di circa 20.000 domande.

L'interrogativo, con risposta potenzialmente inespressa e assolutamente attuale, permane sul numero di elementi (terroristi veri e propri, così come studenti a cui sia stato offerto un finanziamento per la frequenza ai corsi in cambio dell'utilizzo delle conoscenze apprese) sospettati di aver già infiltrato la rete di laboratori, sia del Regno Unito che degli altri Paesi europei, tanto da rendere urgente l'adozione delle misure di protezione delle attività scientifiche e tecniche di settore, con particolare attenzione al personale operante. Va rilevato, in ogni caso, come per la realizzazione di un attacco terroristico con l'uso di sostanze chimiche, biologiche e radiologiche sia necessario l'apporto di specifiche competenze (scienziati, professionisti e tecnici) nonché l'impiego di idonee strumentazioni e tecnologie (laboratori).

L'acquisizione di sostanze, di tecnologie e di capacità relative all'armamento non convenzionale vede, d'altra parte, due possibili principali fonti: l'eredità dei pregressi programmi di proliferazione e l'insieme delle attività destinate a usi e applicazioni pacifiche civili.

Relativamente al primo aspetto è noto come, nel corso degli anni, la strategia bellica offensiva abbia pensato alla creazione di un vero e proprio arsenale, costituito dai cosiddetti 'agenti Cbrn da guerra', capace di consentire aggressioni sempre più efficaci ed efficienti. Di qui i programmi per la proliferazione di Wmd (con cui numerosi Paesi hanno sviluppato virus, batteri, tossine, composti chimici, sostanze radioattive e ordigni atomici letali) dei quali si ha conoscenza, sia per ammissione degli stessi proliferanti sia per le prove acquisite nel tempo; in altri casi se ne sospetta l'esistenza senza però disporre di elementi che consentano di dichiararne l'effettiva presenza. In tale ambito, il problema dell'acquisizione illecita di competenze e capacità frutto di pregressi programmi di proliferazione trova la sua massima espressione, anche come caso di studio, nella dissoluzione dell'Unione Sovietica.

Tale evento epocale ha visto la frammentazione delle strutture e degli arsenali Cbrn e Wmd nelle diverse Repubbliche sovietiche e negli Stati indipendenti venutisi a costituire. Il controllo centralizzato di Mosca è progressivamente scemato e la comunità internazionale – preoccupata per la possibile fuga di scienziati e tecnici disponibili al reclutamento e allarmata dalla ridotta vigilanza sul particolare tipo di armamento – ha accentuato il proprio intervento nel contrasto alla possibile acquisizione di competenze, materiali e tecnologie per scopi militari e/o terroristici. L'impegno si è concretizzato nell'attuazione di progetti, in diversi Paesi dell'ex Urss, volti alla reintegrazione nella comunità scientifica internazionale degli esperti già operanti nei settori d'interesse.

In tale ambito, gli Stati Uniti hanno definito un modello di gestione della problematica con la legge Nunn-Lugar che, nel 1991, ha istituito il Cooperative Threat Reduction Program, finalizzato ad assistere gli Stati ex sovietici per la protezione di capacità e di competenze, per la distruzione delle riserve di armamento biologico e chimico nonché per lo smantellamento degli ordigni nucleari. Il programma, sin dall'inizio, ha operato attraverso la Defense Threat Reduction Agency (Dtra) – dipendente dal Dipartimento della Difesa – che ha seguito i progetti in collaborazione con i governi partner e con le agenzie governative statunitensi interessate.

I risultati ottenuti sono stati riconosciuti a distanza di quasi vent'anni dall'avvio del programma, nel 2009, allorché l'Accademia Nazionale delle Scienze americana – in un report redatto su mandato del Congresso e dal titolo E*ngagement Global Security: a new model for Cooperative Threat Reduction* – ha raccomandato l'applicazione più estesa del modello Nunn-Lugar, in quanto efficace strumento di contrasto alla minaccia terroristica Cbrn*e* e alla proliferazione Wmd nel XXI secolo.

Per quanto concerne l'acquisizione di capacità connesse ad armamenti non convenzionali attingendo da attività pacifiche civili, la situazione attuale vede un costante incremento della minaccia. La prevenzione dell'uso terroristico di armi Cbrn*e* oggi passa anche attraverso lo sviluppo di una cultura che consenta di annullare o, almeno, di mitigare i possibili rischi; ciò anche nell'ottica di un'azione complementare al sistema di sicurezza nazionale. Le strategie che mirano alla tutela del patrimonio tangibile e intangibile necessitano dell'adozione di regole e di linee guida che delimitino il perimetro entro cui il settore è chiamato a operare quotidianamente per la difesa della comunità e degli interessi del Paese. A tal proposito possiamo individuare due diversi aspetti della problematica: la responsabilità istituzionale e quella individuale. Per la prima è opinione condivisa a livello internazionale che ricerche, studi, innovazione e formazione nel campo Cbrn necessitino di una preventiva valutazione tesa a verificare, secondo criteri oggettivi, se le attività svolte si prestino realmente a un potenziale duplice uso, ovvero posseggano una particolare attrattività da parte di gruppi criminali o terroristici, tanto da indurli a ricercarne l'accesso. Qualora la verifica abbia sortito esito positivo, le istituzioni devono poter supervisionare le attività predisponendo una serie di misure che, nel garantire il perseguimento degli obiettivi prefissati, consenta di proteggere il personale, le infrastrutture, i prodotti e il know-how. A monte del percorso è necessario provvedere alla definizione di conoscenze e capacità presenti, di processi e metodi utilizzati, di agenti e materiali sviluppati, lavorati e conservati e di sistemi, strumenti e tecnologie impiegati.

Una volta identificato il 'capitale' tangibile e intangibile da proteggere, si potrà, in relazione alle attività da svolgere, procedere con:
– l'analisi delle vulnerabilità, delle criticità e delle minacce;
– l'identificazione dei rischi;
– la definizione delle potenziali, possibili conseguenze di eventi dannosi;
– la formalizzazione di un programma volto a individuare le misure per l'azzeramento, la riduzione e la mitigazione dei rischi e dei relativi effetti;
– l'attuazione delle misure necessarie per il miglioramento dei livelli di protezione con complessivo aumento delle capacità di resistenza e resilienza.

In tale ambito i più comuni e concreti pericoli possono essere determinati da:
– furto o appropriazione di prodotti, materiali, sistemi, tecnologie e apparecchiature;
– azioni e attacchi interni e/o esterni con acquisizione, rilascio non controllato o perdita di informazioni, dati sensibili e conoscenze;
– attentati o sabotaggi che possano determinare dispersione, rilascio o esposizione intenzionale a sostanze pericolose.

Tra le misure minime di garanzia applicabili ad attività potenzialmente duali si riportano:
– informazione e formazione di tutto il personale sulle tematiche relative ai rischi di security;
– censimento, controllo e accreditamento, di personale, materiali e strutture;
– tracciabilità degli agenti;
– revisione periodica delle *clearance* per l'accesso alle attività;
– controllo e sorveglianza di siti e ambienti, con adozione di misure per la limitazione degli accessi, al solo personale autorizzato;
– tenuta di registri relativi a possesso, utilizzo e movimentazione di sostanze, attrezzature e sistemi;
– monitoraggio e autorizzazione allo specifico utilizzo di capacità e beni;
– svolgimento delle attività con potenziale duplice uso, soprattutto presso università, ospedali e istituti di ricerca pubblici e privati, in luoghi non aperti al pubblico e con procedure di verifica per dipendenti e visitatori;
– garanzia di una facile e veloce comunicazione in caso di violazioni o di minaccia;
– adozione di una politica formale che vieti lo svolgimento di attività senza il consenso del responsabile principale o del supervisore della struttura o del progetto;
– revisione di manoscritti, articoli e pubblicazioni prima della presentazione a giornali scientifici o conferenze pubbliche al fine di verificare il potenziale rischio di uso non pacifico dei contenuti;
– costante attenzione alla possibilità di illecito prelievo, sottrazione o diversione di conoscenze e beni per finalità criminali o terroristiche.

In questo è fondamentale definire gli elementi che possano diminuire o compromettere i livelli di protezione del sistema nel suo insieme, fra cui è possibile includere:
– la limitatezza di risorse economiche e finanziarie per la realizzazione di idonee politiche di tutela delle attività;

– il continuo avvicendamento di ricercatori, specialisti, tecnici, impiegati, studenti e stagisti;
– la carenza, tra il personale operante, di appropriata informazione e formazione.

Passando alla responsabilità individuale nella protezione di capacità con potenziale uso duale, tutto il personale collocato in ambiti sensibili, in base al proprio livello di partecipazione e di contributo, dovrebbe agire attivamente per annullare o ridurre le conseguenze dovute a un difetto di valutazione dei rischi e alla mancata adozione delle opportune cautele. Ciò sottintende l'adozione di misure idonee a realizzare una cornice di prevenzione e controllo, secondo il principio dell'autogoverno, che annovera i seguenti provvedimenti:
– l'autovalutazione delle potenzialità dual-use di un'attività con l'individuazione delle possibili conseguenze negative;
– l'identificazione delle diverse implicazioni legali, etiche e sociali;
– la predisposizione di ogni adeguata protezione nell'accesso alla conoscenza, alle sostanze, alle apparecchiature e ai sistemi sensibili;
– l'adozione di idonee cautele nella diffusione di dati, anche nello svolgimento di attività didattiche e formative, nella stesura di pubblicazioni e articoli nonché nella partecipazione a progetti, gruppi di lavoro, conferenze, convegni, workshop, seminari ecc.;
– l'informazione, la formazione e l'aggiornamento continui sulle normative e sulle indicazioni nazionali e internazionali di settore;
– l'applicazione delle norme di legge e delle prassi comuni;
– l'adozione delle opportune azioni di supervisione, controllo e verifica in merito a competenza e affidabilità del personale subordinato;
– la segnalazione alle autorità preposte di attività che violino le disposizioni di settore.

Ciò evidenzia come le future politiche volte a coniugare scienza, ricerca, innovazione, formazione e sicurezza nazionale dovranno essere sempre più caratterizzate dall'integrazione di attività istituzionali e individuali, in un contesto ove i princìpi di consapevolezza, responsabilità e informazione siano, oltre che basilari e condivisi, anche fondanti di una cultura in grado di sconfiggere le multiformi dimensioni delle odierne minacce

G

SITOGRAFIA

Terrorist Plots Targeting New York City, «New York Police Department», New York 28.7.2015, <www.nyc.gov> [28/07/2016].
H. Doornbo – J. Moussa, *Found: The Islamic State's Terror Laptop of Doom. Buried in a Dell computer captured in Syria are lessons for making bubonic plague bombs and missives on using weapons of mass destruction*, «Foreign Policy» 28.8.2014, <www.foreignpolicy.com> [28/07/2016].
A. Sims, *Isis uses poisonous gas on Kurdish forces*, «The Independent», London 18.7.2015, <www.independent.co.uk> [28/07/2016].
R. Solomon, ISIS' *Threat: Chemical and Biological. Intelligence researcher Ronen Solomon analyzes the reports of* ISIS' *threats to commit attacks in the subway in Paris and New York. What really drives the West to act against the Islamic State organization*?, «Israel Defense» 28.9.2014, <www.israeldefense.co.il> [28/09/2014].
M. Townsend, *Terrorists try to infiltrate* UK's *top labs*, «The Guardian», London 2008, <www.theguardian.com> [28/07/2016].