11|2014

DRONE: SORVEGLIATO SPECIALE

A cura di
CISINT – Osservatorio Permanente di Ricerca

CISINT Centro Italiano di Strategia e Intelligence

LIMITAZIONE DELLA RESPONSABILITÀ

Le opinioni espresse nel presente documento, rilasciato a scopo informativo, sono di responsabilità esclusiva dell'autore e non riflettono necessariamente la posizione ufficiale del CISINT - Centro Italiano di Strategia e Intelligence.

www.cisint.org **info@cisint.org**

Sommario

INTRODUZIONE

In ambito militare, soprattutto nelle operazioni internazionali di contrasto al terrorismo, gli **APR**[1] hanno assunto un ruolo sempre più rilevante e incisivo. In particolare quest'ultimo decennio è stato caratterizzato da molteplici interventi militari portati a termine con successo grazie all'ausilio di droni: già dal 2004, ad esempio, nell'area FATA[2] del Pakistan questa tecnologia è stata ampiamente utilizzata dalle forze armate statunitensi nel corso della nota campagna "**War on Terror**", avviata dal Governo Bush, allo scopo di neutralizzare l'organizzazione terroristica Al Qaeda e i numerosi gruppi affini[3]. L'utilizzo di queste apparecchiature, tecnologicamente avanzate, è stato incentivato soprattutto dal progresso ottenuto nella miniaturizzazione e ottimizzazione dei componenti elettronici, da una maggiore affidabilità e responsività dei dispositivi meccanici di cui sono equipaggiate oltre che dai costi di produzione relativamente contenuti. Ciò ha conseguentemente permesso di ottenere una sensibile riduzione del numero di fatalità del personale militare operativo, dislocato nelle aree d'interesse ad alto rischio[4].

Occorre evidenziare che l'impiego dei droni si è diffuso ampiamente anche in contesti civili, nell'ambito di attività complesse e pericolose[5], come ad esempio nel caso di rilevazioni e perlustrazioni degli assetti territoriali, di investigazioni o di vigilanza per la security. Ciò ha favorito al contempo una consistente riduzione dei costi e dei rischi operativi annessi.

Il drone è quindi uno strumento tecnologico particolarmente versatile, caratterizzato da una capacità d'impiego "duale", proprio perché utilizzato sia in teatri operativi militari che civili. La versatilità e l'efficacia operativa dello strumento, nonché i costi di fabbricazione ridotti, sono alcuni dei fattori per i quali è lecito domandarsi se un drone possa essere utilizzato efficacemente come strumento di minaccia terroristica. Di fronte a tale eventualità, in che modo sarebbe possibile mitigare il rischio? Ancora, quali sarebbero le ripercussioni di un attacco terroristico alle infrastrutture critiche del nostro paese?

---

[1] APR: Aeromobile a Pilotaggio Remoto, comunemente indicato con il termine generico "drone".
[2] FATA: Federally Administered Tribal Areas
http://fata.gov.pk/
[3] Akbar Ahmed – "The Thistle and the Drone: How America's War on Terror Became a Global War on Tribal Islam" - Brookings Institution Press, 2013
[4] Mark Mazzetti - "The Way of the Knife: The CIA, a Secret Army, and a War at the Ends of the Earth" - Penguin Press, 2013
[5] Specificatamente per missioni di tipo "Dull, dirty and dangerous" (Noiose, sporche e pericolose).

Avviando un'attività di ricerca e di analisi, caratterizzata da un approccio multidisciplinare, il CISINT – Centro italiano di Strategia e Intelligence ha organizzato un **Osservatorio Permanente di Ricerca**[6], costituito da figure di elevata specializzazione aventi per obiettivo lo studio di tutti gli aspetti attinenti alla tecnologia APR, intesa come possibile minaccia terroristica. Ulteriore obiettivo è l'analisi delle possibili soluzioni di contrasto a tale minaccia, elaborando un adeguato documento conclusivo di riferimento, utile alle istituzioni, al settore industriale privato e al mondo accademico del nostro paese.

Si riportano di seguito alcuni estratti del documento ufficiale in fase di lavorazione, in merito alle tematiche oggetto di approfondimento.

ANALISI DI SCENARIO

Il vocabolo "drone" ha origini etimologiche presumibilmente elleniche. Il significato più antico attribuito al termine è quello di "fuco – maschio dell'ape" (dall'inglese antico "dran", derivato a sua volta dal tedesco "drohne").

Il concetto di "drone", inteso come veicolo aereo da combattimento pilotato a distanza, risale alla Seconda Guerra Mondiale dall'idea degli americani Lee De Forest e Ulises Armand Sanabria, i quali nel 1940 hanno diffuso un articolo intitolato "**Robot Television Bomber**", pubblicandolo su una rivista specializzata anglosassone (Popular Mechanics).

Un primo impiego effettivo di questa tecnologia, ancora priva di armamenti, è avvenuto nel 1973 da parte dello Stato d'Israele nei confronti dell'Egitto, durante la guerra dello Yom Kippur. In quest'azione militare l'esercito israeliano, senza registrare alcun decesso nei propri schieramenti militari, è riuscito a penetrare le difese egiziane utilizzando un drone target (modello "**Firebee**", di fabbricazione della società americana Ryan Aeronautical Company), dirottando in tal modo l'attenzione della contraerea egiziana.

I droni sono stati inizialmente concepiti per svolgere attività di ricognizione e di sorveglianza, ma col passare del tempo hanno assunto anche una funzionalità di attacco, subendo sensibili modifiche strutturali per soddisfare necessità di carattere militare. Molti paesi europei, tra cui l'Italia, possiedono e producono droni. Anche Cina, Russia e Iran hanno sviluppato propri modelli, commercializzandoli: Teheran, ad esempio, è uno dei maggiori produttori di **UAV**, con quattro modelli all'attivo, progettati e sviluppati dall'esercito o da centri di ricerca vicini al regime.

[6] L'Osservatorio Permanente di Ricerca è attualmente costituito da: dott. Vincenzo Iavarone, dott. Mario Avantini, dott. Claudio Todaro, dott. Federico Sesler.

L'utilizzo diffuso dei droni richiede una meticolosa attenzione in merito alle questioni di sicurezza e privacy della popolazione. Tali sistemi infatti avrebbero la capacità di sorvolare aree appartenenti a infrastrutture critiche e strategiche di un paese. Teoricamente questi sistemi tecnologici potrebbero violare aree ad accesso ristretto, diventando quindi un'arma a disposizione di terroristi, anarchici insurrezionalisti, movimenti indipendentisti ma anche singoli individui potrebbero sferrare attacchi pressoché imprevedibili contro "palazzi di potere", luoghi di culto religioso e rilevanti centri di aggregazione sociale.

L'ISIS, ad esempio, potrebbe essere in possesso di droni? Alcuni analisti esperti hanno tentato di rispondere a tale quesito: dai filmati propagandistici diffusi dallo Stato Islamico si è potuto riscontrare che le riprese aeree della base militare siriana ad Al Ragga (città ora appartenente al califfato) sono state effettuate tramite un drone. A quanto pare dunque **l'ISIS sarebbe molto verosimilmente in possesso di almeno un drone, per il momento non armato**. Non è possibile escludere che l'arsenale venga ampliato in un prossimo futuro. Come è vero che quasi tutti gli Stati produttori di droni, Iran compreso, sono schierati contro il califfato è altrettanto vero che il califfato stesso ha dato dimostrazione di possedere una notevole capacità di sviluppo tecnologico, non solo in attività di propaganda (tramite comunicazioni nei social media e divulgando filmati in alta definizione) ma anche dal punto di vista militare.

L'utilizzo dei droni pone in essere anche altre questioni indubbiamente rilevanti: si discute ampiamente in merito alla legittimità degli interventi militari tramite APR, oppure in merito al reale livello di sicurezza di questi veicoli, la cui efficacia operativa è essenzialmente garantita dal corretto funzionamento delle apparecchiature elettroniche di bordo, le quali potrebbero subire manomissioni e sabotaggi esattamente come qualsiasi altra strumentazione.

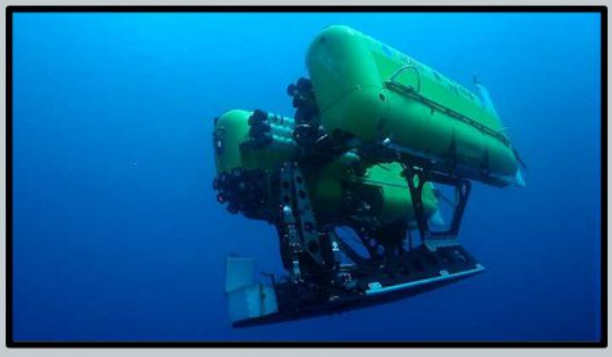
Nel caso di impieghi civili, anche le aziende private hanno annunciato la volontà di avvalersi di droni per svolgere i propri servizi, ciò con un evidente impatto sulla privacy e la sicurezza dei cittadini.

ANALISI TECNOLOGICA ED ECONOMICA

Occorre innanzitutto distinguere la categoria dei droni RPA - Remotely Piloted Aircraft (oppure UAV - Unmanned Aerial Vehicle, ROA - Remotely Operated Aircraft), che afferisce specificatamente ai mezzi aerei pilotati a distanza, da quella più generica degli RPV - Remotely Operated Vehicle (oppure UVS - Unmanned Vehicle System) nella quale sono contemplati anche mezzi subacquei (UUV - Unmanned Underwater Vehicle), anfibi (UAV - Unmanned

Amphibious Vehicle), terrestri (UGV – Unmanned Ground Vehicle) e acquatici (USV - Unmanned Surface Vehicle) a controllo remoto.






I costi di produzione dei droni variano considerevolmente, sia per le peculiarità che li caratterizzano che per l'utilizzo cui sono destinati:

- Droni preposti allo svolgimento di attività d'intelligence militare - fino a 93 milioni di Dollari (modello: Global Hawk – produttore: Northrop Grumman);
- Droni preposti allo svolgimento di attività di vigilanza - fino a 100 mila Dollari (modello: ScanEagle – produttore: Insitu);
- Droni per impieghi in ambito civile, ad esempio per attività di supporto all'agricoltura - dai 10 mila ai 15 mila Dollari (modello: Lancaster Hawkeye – produttore: PrecisionHawk);
- Droni per impieghi in ambito civile, ad esempio per attività di rilevamento fotografico - circa 1.300,00 Dollari (modello: Phantom Vision +2 – produttore: DJI).

Nel caso ipotetico in cui un gruppo terroristico decidesse di dotarsi di un drone per sferrare un attacco improvviso a una infrastruttura critica di un paese, non incontrerebbe particolari

difficoltà realizzative. Sarebbe sufficiente utilizzare un "**delivery drone**" (drone postino), appartenente alla categoria degli RPA.

Opportunamente modificato affinché possa trasportare materiale esplosivo, un RPA si trasformerebbe facilmente in un vettore di elevatissima pericolosità. Dal lato puramente operativo, sarebbero disponibili due modalità realizzative differenti:

- **Modalità 1**: Acquisto di un RPA commercializzato su larga scala e quindi facilmente reperibile, pre-assemblato e per uso amatoriale o semiprofessionale, il cui costo si aggira intorno alle poche migliaia di Euro. Equipaggiandolo opportunamente di carica esplosiva e relativo detonatore, sarebbe in grado di danneggiare e compromettere gravemente aree strategicamente rilevanti;
- **Modalità 2**: Possedendo conoscenze basilari di elettronica, è possibile reperire l'occorrente per assemblare autonomamente un drone postino. Oltre ai componenti strettamente necessari (chassy, sistema di propulsione ad elica, strumentazione di volo, regolatori di velocità, ricevitore radio e sistema di alimentazione) potrebbe essere provvisto, ad esempio, di un meccanismo "**grabber**", in grado cioè di afferrare, trattenere/trasportare e depositare/rilasciare un ordigno esplosivo dove stabilito.

Si fa presente che **l'innesco di un esplosivo può essere effettuato anche tramite un comunissimo telefono cellulare GSM**. I modelli più evoluti potrebbero essere provvisti di sistemi di comunicazione criptati, immuni da attacchi di tipo "**spoofing**" e "**jamming**" sul segnale GPS o da qualsiasi azione di disturbo delle comunicazioni e delle funzionalità hardware/software (anche tramite eventuali **malware injection** lato codice, operazione estrema ma non impossibile).

Inoltre, **ipotizzando un attacco sincronizzato su larga scala, verso molteplici obbiettivi strategici dello stesso paese, sarebbe possibile seminare distruzione e morte in breve tempo, mettendo così in ginocchio un intero paese**.

ATTUALE QUADRO NORMATIVO ITALIANO PER L'UTILIZZO DEI DRONI

L'Unione Europea ha stimato che il mercato dei droni raggiungerà i 15 miliardi di Euro entro i prossimi dieci anni. A livello mondiale il mercato potrebbe invece raggiungere i 130 miliardi di Dollari.

In Italia nell'aprile 2014 è entrato in vigore il Regolamento ad hoc per i "**Mezzi Aerei a Pilotaggio Remoto**", elaborato da **ENAC – Ente Nazionale per l'Aviazione Civile**[7].

La disciplina è stata illustrata e commentata in modo vario, ponendo particolare interesse nei confronti della tipologia di droni utilizzati in attività commerciali o professionali: per il monitoraggio di zone agricole e di impianti industriali, per le riprese video-fotografiche oppure per mansioni di pubblica sicurezza.

Il Regolamento non si limita a disciplinare l'utilizzo degli apparecchi **SAPR** (Sistemi **Aeromobili** a Pilotaggio Remoto), destinati all'impiego in operazioni specializzate ma interessa anche la categoria degli "**Aeromodelli**" (*non sono considerati aeromobili ai fini del loro assoggettamento alle previsioni del Codice della Navigazione e possono essere utilizzati esclusivamente per impiego ricreazionale e sportivi*[8]).

Le norme elaborate dall'Ente potrebbero essere migliorate attraverso l'armonizzazione con quanto previsto in altri stati e con l'ampliamento dei casi di applicazione (ad esempio, manca una distinzione tra aeromodelli e giocattoli).

La differenza tra SAPR e aeromodelli dipende in buona sostanza dall'utilizzo effettivo del mezzo. Si potrebbe facilmente ipotizzare che in breve tempo i droni per uso civile transiteranno in aree di bassa quota, necessitando quindi di una normativa che ne regolamenti l'accesso, oltre alla idoneità di chi effettua le manovre di pilotaggio da terra. Occorre specificare che ENAC distingue i SAPR in due categorie, a seconda del peso.

[7] https://www.enac.gov.it/La_Normativa/Normativa_Enac/Regolamenti/Regolamenti_ad_hoc/info-1226715l2.html

[8] Definizione fornita dall'art 1 del Regolamento ENAC.

Una prima categoria comprende modelli provvisti di una massa al decollo inferiore a 25 Kg, utilizzati in operazioni di volo non critiche.
In questo caso per operare occorre solo un'autocertificazione e la responsabilità ricade sull'operatore. Nel caso questi apparecchi siano impiegati in operazioni critiche, è necessario possedere un'autorizzazione rilasciata dall'ente (sulla base di opportuni accertamenti) il quale fornisce anche una distinzione, definendo critiche quelle operazioni che comprendono il sorvolo di aree congestionate e infrastrutture industriali, mentre sono operazioni non critiche quelle in cui l'apparecchio, in caso di malfunzionamento, non può causare danni a terzi.

La seconda categoria include i SAPR con una massa al decollo compresa tra i 25 e i 150 Kg.
In questo caso, a prescindere dal tipo di attività svolta, è richiesto il possesso di una certificazione del mezzo aereo e un'autorizzazione all'impiego per l'operatore (permesso di volo SAPR): il pilota del drone deve aver compiuto la maggiore età, deve conoscere le regole e le procedure di volo applicabili e deve aver portato a compimento un programma di addestramento specifico per il modello di SAPR utilizzato.

Occorre inoltre possedere un certificato medico di seconda classe. Il Regolamento impone anche una polizza assicurativa per danni verso terzi.

ANALISI DEI RISCHI

Un'attività fondamentale per la valutazione della minaccia terroristica attraverso l'utilizzo dei droni è costituita dall'analisi dei rischi.

A tal proposito si è ritenuto opportuno adottare un protocollo per l'**analisi dei rischi AS/AT (Antisabotaggio/Antiterrorismo)**, già sviluppato per esigenze di Sicurezza Nazionale[9] e come tale particolarmente adatto allo scenario di minaccia oggetto del presente studio[10].

L'attività di analisi sarà effettuata attraverso vari passaggi operativi che consentiranno l'elaborazione di una adeguata valutazione dei rischi:

- Comprensione dello scenario (volta all'individuazione della tipologia dei potenziali obiettivi nazionali a opera della minaccia terroristica considerata);
- Comprensione dei dati prestazionali dei droni utilizzabili per un'azione terroristica (in termini di quote di volo, velocità, raggio d'azione, carico utile, sistemi di comando e controllo, ecc.);
- Individuazione delle molteplici modalità di minaccia (per tipologia di drone, per profilo di missione, per tipologia di "strumento di offesa" trasportato, ecc.);
- Individuazione dei fattori di rischio e delle relative vulnerabilità di sistema per ciascuna della configurazioni di minaccia considerate (valutando molteplici tipologie di infrastruttura, selezionate come potenziale obiettivo di attacco);
- Determinazione delle probabilità di accadimento per ciascuna modalità di attacco individuata;
- Revisione degli effetti (impatto) che l'attacco terroristico potrebbe provocare a ciascuna delle infrastrutture considerate;
- Studio delle possibili strategie difensive e preventive;
- Valutazione del rapporto costi/benefici nella strategia di protezione AS/AT applicabile ai contesti considerati.

In base a quanto già previsto dal protocollo sopra menzionato, la valutazione dell'impatto avverrà secondo la scala di valutazione riportata nella tabella seguente, ove per "organizzazione" si intende il soggetto responsabile dell'infrastruttura considerata (obiettivo dell'attacco terroristico).

[9] Claudio Todaro/Vincenzo Iavarone – "Protocollo per la Valutazione del Rischio Sicurezza AS/AT" – Novembre 2012
[10] Vincenzo Iavarone/Claudio Todaro/R. Carìa – "La Protezione delle Infrastrutture Critiche" – Rivista Militare nr. 1/2013

VALUTAZIONE	CRITERIO
Trascurabile	Le conseguenze possono consistere in interruzione di breve durata per alcune delle attività senza danni economici sensibili per l'Organizzazione.
Minore	Le conseguenze possono consistere in ferite di piccola entità del personale dell'Organizzazione, danneggiamento di beni strumentali e ritardi delle attività con danni economici limitati per l'Organizzazione.
Moderato	Le conseguenze possono consistere in ferite di piccola entità del personale dell'Organizzazione, danneggiamento di beni strumentali, perdite di informazioni sensibili e ritardi delle attività con danni economici sensibili per l'Organizzazione.
Severo	Le conseguenze possono consistere in ferite di grave entità del personale dell'Organizzazione, perdite di beni strumentali, perdite di informazioni sensibili e cancellazione delle attività con danni economici gravi per l'Organizzazione.
Critico	Le conseguenze possono consistere in ferite di grave entità e decessi del personale dell'Organizzazione, perdite di beni strumentali, perdite di informazioni sensibili e cancellazione completa delle attività con gravissimi danni economici e d'immagine per l'Organizzazione.

- Scala di valutazione dell'impatto –

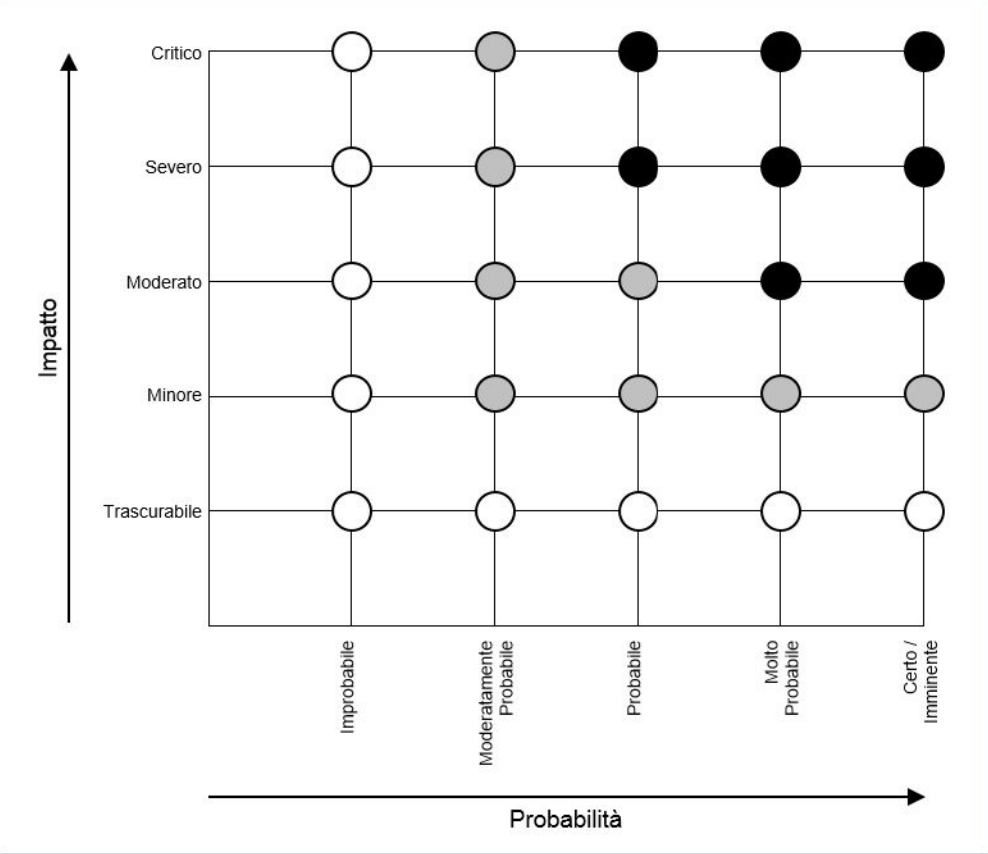
La valutazione della probabilità sarà effettuata secondo la scala di valutazione riportata nella tabella seguente, ove il criterio (da "**Improbabile**" a "**Certo/Imminente**") farà riferimento alla situazione di scenario geopolitico indicato nella sezione specifica, all'interno dello studio.

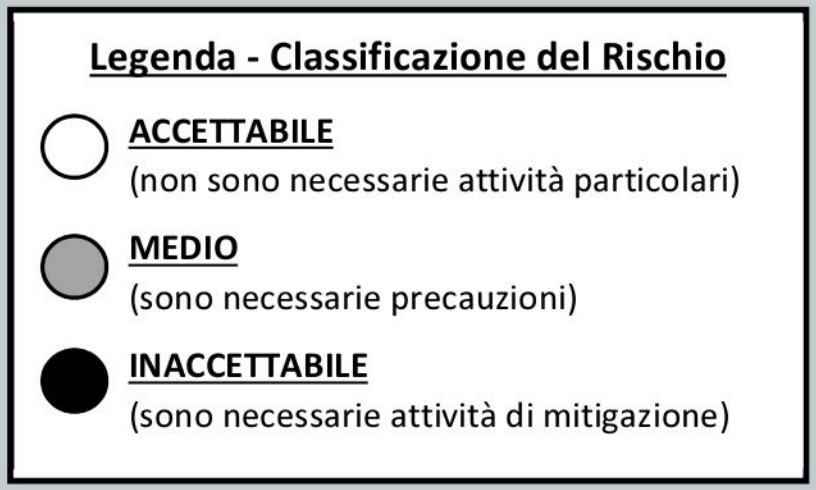
VALUTAZIONE	CRITERIO
Improbabile	L'evento è considerato privo di una realistica probabilità di accadimento.
Moderatamente probabile	L'evento è considerato con una ragionevole probabilità di accadimento.
Probabile	L'evento è considerato con una elevata probabilità di accadimento.
Molto probabile	L'evento è considerato con una probabilità di accadimento molto elevata.
Certo/Imminente	L'evento è considerato di imminente accadimento.

- Scala di valutazione della probabilità di accadimento –

Infine, il "**Livello di Rischio**" sarà definito dalla **Matrice dei Rischi** riportata di seguito, secondo la classificazione specificata:

- **Accettabile;**
- **Medio;**
- **Inaccettabile.**





Per ciascun "Livello di Rischio" sarà stabilita l'eventuale necessità di intervento di mitigazione e la relativa priorità, da attuarsi (con riferimento all'infrastruttura, potenziale obiettivo dell'attacco) secondo le opzioni seguenti:

- Organizzative (con riferimento al personale impiegato nell'infrastruttura);
- Operative (con riferimento alle procedure adottate nell'infrastruttura);
- Tecnologiche (con riferimento ai dispositivi tecnologici adottati nell'infrastruttura);
- Legislative (con riferimento a eventuali interventi di carattere normativo, al fine di consentire un contrasto efficace della minaccia in fase preventiva).

L'attività di analisi dei rischi costituirà il "**focus operativo**" dell'Osservatorio Permanente di Ricerca. In questa fase saranno vagliati attentamente tutti gli scenari di contesto possibili e le tecnologie impiegabili dai potenziali soggetti ostili.

CONCLUSIONI

Tramite l'analisi sin qui sinteticamente esposta si è voluto evidenziare la **peculiarità "dual use" che caratterizza la tecnologia APR**, volgendo l'attenzione soprattutto sulla semplicità con cui potrebbe essere utilizzata per fini terroristici. Trattandosi quindi di una minaccia concreta è necessario che le istituzioni, coadiuvate dal settore privato e accademico, elaborino e attuino una strategia di prevenzione e contrasto, sufficientemente adeguata ed efficace, a salvaguardia delle priorie infrastrutture critiche, al contempo tutelando la sicurezza dei propri cittadini.

Il CISINT – Centro Italiano di Strategia e Intelligence, costituendo il proprio Osservatorio Permanente di Ricerca, ha l'ambizione di creare un pool di esperti arricchito e impreziosito in futuro anche dalla collaborazione di ulteriori figure di elevata specializzazione, assurgendo al ruolo di eccellente punto di riferimento a livello nazionale sulla tematica descritta. Analizzando gli aspetti e le necessità tecnologiche e normative, oltre a recepire eventuali indicazioni/necessità di carattere istituzionale, industriale e accademico, l'Osservatorio Permanente di Ricerca procederà definendo una possibile architettura di sistema per un contrasto efficace della minaccia.

L'AUTORE

Osservatorio Permanente di Ricerca

L'Osservatorio Permanente di Ricerca è costituito da CISINT – Centro Italiano di Strategia e Intelligence. Composta da analisti e ricercatori altamente qualificati e operanti in seno all'Associazione, questa struttura è pronta ad accogliere contributi da parte del mondo istituzionale in qualità di principale attore di contrasto a eventuali minacce terroristiche, nonché del mondo industriale e accademico per un'attenta valutazione circa la disponibilità di adeguate tecnologie di contromisura. In tal modo è possibile caratterizzare una minaccia con un elevato grado di attendibilità, considerando anche l'accessibilità da parte di "soggetti ostili" alle varie tecnologie disponibili sul mercato. In qualità di referente, CISINT – Centro Italiano di Strategia e Intelligence rende fruibile da parte degli organi istituzionali e dell'industria di settore il risultato degli studi effettuati dall'Osservatorio Permanente di Ricerca, come utile strumento per l'individuazione e la definizione di efficaci strategie operative e di piattaforme tecnologicamente adeguate.

Osservatorio Permanente di Ricerca:
Dott. Vincenzo Iavarone
Dott. Mario Avantini
Dott. Claudio Todaro
Dott. Federico Sesler

Via Clelia 45, 00181 - Roma

Tel/Fax: (+39) 06 7808035

Email: info@cisint.org

www.cisint.org