Biomedicine & Prevention
An Open Access Transdisciplinary Journal

Dirty Bomb Drones, Physical-Logical Urban Protection Systems and Explosive/ Radiological Materials regulation's Challenges in the Age of Globalization

Pietro Rossetti,[1] Fabio Garzia,[2,3,4] Nicola Silverio Genco,[5] Cosimo Rossetti,[6] Simone Scolari[7]

[1] *University of Rome Tor Vergata, Rome 00173, Italy*

[2] *Safety & Security Engineering Group – University of Rome La Sapienza, Rome 00185, Italy*

[3] *Wessex Institute of Technology, Southampton SO40 7AA, UK*

[4] *European Academy of Sciences and Arts, Salzburg A-5020, Austria*

[5] *S.T.A.S.A. Studies Center, Rome 00137, Italy*

[6] *Ministry of Defence – Italian Air Force, Rome 00185, Italy*

[7] *Ministry of Defence – Italian Air Force, Rome 00185, Italy*

UAS' Radiological Threat: An Introduction

In the age of Globalization, information technology, international trade and investment, the commerce in R-sources and devices is conducted on a global scale. No country can effectively prevent from crossing its borders, the black market based on illicit used, misplaced, or stolen radioactive sources. The control of radioactive sources and contaminated products poses challenges on both national and international scales. After September 11th, 2001, the fear has increased: terrorist groups could use CBRN agents, since some of "dual-use" technologies and scientific knowledge, necessary for use in crude weapons, have become more easily available. In particular, Unmanned Aerial Systems (UASs), also known as drones, could be used not only to get information regarding professional, security, intelligence and logistics activities, but also to open up new threats and opportunities. Indeed, a drone might become a CBRNe "Tool" developed for terroristic warfare, working for example, as a Radiological Dispersal Device (RDD) carrier that generates R-contamination, or as a Radiological Exposure Device (RED) carrier releasing radiations, with the intent of inflicting severe injuries or financial and psychosocial costs. A "dirty" bomb UAS could be used in a "suicide mission", through detonation of conventional explosives payload and spreading a certain amount of a radioactive isotope. In this way, R-blast creates an area of low-radioactive contamination studied by atmospheric dispersion models. Hot-zone would be unsuitable for military, economic or other activities for a long time: the recovery of area is likely to be physically, financially, and psychologically "not sustainable".[1-7] On the one hand, UN Commission for Conventional Armaments' resolution of 12th August 1948 included "radioactive material weapons" as a form of weapon of mass destruction, along with lethal chemical and biological weapons and any weapons which have destructive effects to those of the atomic bomb. On the other hand, "a dirty bomb is not a "Weapon of Mass Destruction" but a "Weapon of Mass Disruption" where contamination and anxiety are the terrorists' major objectives" (Burton, 2017).[7-10] A "dirty" bomb is for jihadists, like a cyber-attack or a demonstration against a miniskirt or the halal food in public schools. What is important is intimidation, then hegemony comes, finally domain arrives. Attacks are also useful to increase the costs of our defenses, until making them economically ineffective, and finally blocking the European society" (Valori, 2017).[11]

Dirty Bomb UAS Materials and Manufacturing Methods

Possible radioisotopes "candidates" for a "Dirty bomb" project are the common radioactive materials used worldwide in waste from medical facilities, industrial plants, and nuclear power plants. The RDD Problem is related not only to the global fight against international terrorism, but also in countering criminal organizations that organize illicit trafficking of both radiological and nuclear material and high explosives smuggling. Such radiological materials could be divided into the following three groups, classified under the main types of radiation:[7,12]

"Dirty bomb" is one type of a RDD that combines conventional explosives with radioactive materials, which does not release enough radiation to kill people or cause severe illness. A RDD device easily transportable by a drone with the size of a small bottle weighing about thirty grams is capable of denying access to a critical infrastructure, multinational Corporates Head Offices, data centers, hospitals, government or military facilities, embassies, etc.[5,8,11,12] The following RDD could be simple and quite accessible to a terrorist organization: a blasting cap surrounded by a piece of detonating cord and few grams of ^{137}Cs, a beta-gamma emitter such as ^{60}Co, ^{192}Ir and ^{99m}Tc, the most commonly used radioactive material in nuclear medicine, which offer higher radiation output for a given volume. An abandoned radiotherapy machine can contain enough ^{137}Cs for a dozen such single/multiple/simultaneous attacks. Only 5 grams of ^{137}Cs produce

- ***Pure Alpha emitters***
  - **Plutonium-238 (^{238}Pu) - research and well logging and in RTGs for space missions;**
  - **Americium-241 (^{241}Am) - industrial gauges and well logging;**
  - **Radium-223 (^{223}Ra) - cancer treatment of bone metastases.**
- ***Pure Beta emitter***
  - **Strontium-90 (^{90}Sr) - radioisotope thermoelectric generators (RTGs), used to make electricity in remote areas;**
- ***Pure Gamma emitter***
  - **Technetium-99m (^{99m}Tc) – diagnostic imaging in nuclear medicine**
- ***Beta/Gamma emitters***
  - **Cobalt-60 (^{60}Co) - cancer therapy, industrial radiography, industrial gauges, food irradiation;**
  - **Cesium-137 (^{137}Cs) - same uses as Cobalt-60 and well logging;**
  - **Iridium-192 (^{192}Ir) - industrial radiography and medical implants for cancer therapy.**
  - **Iodium-131 (^{131}I) - differentiated thyroid cancer therapy and other thyroid conditions**

Figure 1. Radioisotopes "candidates" for a "Dirty bomb" project.

a radiation field of 140 R/h, 1,4 Sv per hour at 1 meter (Radiotherapy session' Equivalent dose is about 1,5-2,0 Sv).[1,7] Despite fear, the explosion of a dirty bomb is likely to have a little biological effect on populations, unlike the blast effects which can cause serious injuries and property damages in a close area, from less than a city block to several square miles. A dirty bomb can easily be carried by a wide variety of commercial UASs. Indeed, the average specifications of UASs under 5,000 euros, provide up to 40 minutes of flight time on a single charge, 6 kg. payload and about 5,000 meters of operating range. Recent modular UASs designs are easy to configure and ready to use in a few minutes: equipped with engines self-cooled and customize flight batteries, to ensure prolonged use over 15-20 flight time minutes with a transmission range of a few kilometers.[1,7,13,14]

Dirty Bomb UAS: A Regulation Point of View

The regulation, presented below, preventing nuclear and radiological material missing, international illegal trafficking, unauthorized removal/handling/smuggling of RN-material and sabotage against transport of nuclear material and facilities:

- "Convention on the physical protection of the nuclear material and nuclear facilities" (1979 and amendments 2005) – unauthorized removal and sabotage against transport of nuclear material and installation; IAEA "Nuclear security recommendation on physical protection of nuclear material and nuclear facilities" (INFCIRC/225/Revision 5) – concerning at point 2, the objectives of a State's physical protection regime.
- Italian Law Acts No. 58/2015 – introduction of the "new" "Attempt on the security of nuclear installations" crime; Italian Law Acts No. 153/2016 – introduction the crime of " Nuclear Terrorism", in case of financing people for purposes of terrorism; procurement of radioactive material; creation/possession of a "nuclear weapon" such as Nuclear Explosive Devise, RDD or RED; use of radioactive material or nuclear weapon; use or damage nuclear plants with the release or danger of releasing radioactive material.[17-22]

The National and International legal framework preventing and contrasting the illegal activities related explosives and their precursors – such as high explosive trafficking/smuggling, manufacturing of Homemade explosives and "Residual Explosive Remnants of War" search/detention/smuggling – collects the following regulations:[14]

- European Parliament Regulation (EU) No. 98/2013 of the Council of 15th January 2013 concerning the Marketing and Use of Explosive Precursors establishes harmonized rules about the making available, introduction, possession and use of substances or mixtures that could be used for the illicit manufacture of explosives, ensuring that appropriate reporting of suspicious transactions and thefts;
- Consolidated act of National Public Security Laws (TULPS); the Italian Legislative Decree of April 4th, 2010, No. 58 – concerning the market regulation of pyrotechnic articles and Italian Legislative Decree of May 19th, 2016, No. 81 – concerning the market regulation and control of explosives for civil use;
- Italian Law Act of October 2nd, 1967, No. 895, concerning arms explosive, chemical, aggressive, or other murderous devices control provisions. The Law provides punishes with imprisonment and a fine, everyone who is unlicensed by the authority manufactures, possesses or introduces into the State, also for sale, any war or warships or parts of them, warlike, explosive, chemical, aggressive, or other murderous devices, or collects them; provides instructions in any form, including anonymous or via telematics, regarding preparation or use of explosive materials, is punished with imprisonment from one to six years;
- Italian Ministerial Decree of May 11th, 2015, No. 82 – Regulation for the establishment of criteria for the assessment of the suitability of companies for the purposes of registration of companies specializing in remediation of explosive "remnants of war" pursuant the Law of October 1st, 2012, No. 177.

In order to prevent and contrast Illicit UASs Operations – for example, hardware attacks; wireless attacks; spoofing against sensors; illegal use of images and data; espionage; sabotage; illicit/hazardous substances transportation – in March 2015, European Aviation Safety Agency (EASA) presented a new regulatory approach for Remotely Piloted Aircraft (RPAS) targeted on the type of drone "operations" and safety requirements needs. However, EASA has no mandate for security, data protection and privacy. Main results of the research stressed the aspects of security technologies analysis; comprehensive knowledge of 27 EU members' citizens, about privacy and security topics; c) a new model of criteria of surveillance based security technologies Decision Support System (DSS). From a point of view of the prevention of illicit acts committed by drones, the Italian Civil Aviation Authority – ENAC Remotely Piloted Aircraft regulation Ed.2 - Em.3 - March 24th, 2016" allows Critical operations with UASs under 25 kg. over urban areas under several conditions and an acceptable level of safety – for example a command and control system whose software complies with the EUROCAE ED-12 standards (reliability level D, at least); flying over groups of people remains forbidden in any case (in open/confined spaces). Possibility to fly anywhere however corresponds to the difficulty of detection/real-time identification "homemade drone" (self-built or modified drone) or hidden pilot.

Urban Protection and Dirty Bomb Drone: Discussion on an Integrated Technological System Framework

Due to the continuous growth and variation of threats, security management needs continuous enhancing, using comprehensive and integrated technological prevention and protection countermeasures powerful tools. RDD and UAS combined together in a new CBRNe system developed for terroristic warfare, become a CBRNe threat working as a "dirty bomb" carrier, both in open-air and internal urban areas. The prevention and protection activities can be done using wide range and multidisciplinary technological tools, all interconnected and interacted reciprocally, according to the security, cost and benefit optimization needs:

- *physical* technologies: illicit drone intrusion detection, identification and tracking, jammer devices, R-detection, (Stand-Off or mobile-drone commercial version) explosives and other chemical compounds detection (Laser Direct Structuring (LDS), laser based spectroscopy method), access control, analog/digital video surveillance, etc.; *logical* technologies: illicit drone intrusion detection systems, anti-viruses; Closed Circuit Television (CCTV) and multi-sensors integrated system; robotic vision, human and drone similarity detection, clustering and classification system;
- *physical* barriers: drone physical capture devices (drone-mounted net cannon snags other drones) border patrol drone, air conditioning air intakes' automatic shut off system; *logical* barriers: firewalls, cyber-attack and intrusion detection systems.

The following figure shows a simplified Integrated Technological System Framework (ITSF) example: integrated technological prevention/protection countermeasures, facing not only an ongoing dirty bomb drones attack, but also the probability that such event could occur, by reporting any critical situation to the operators. In the scheme, counter-drone defense system, and "Flying" dirty bomb detection system (drone-mounted R-detection system) with illicit drone detection, identification and tracking systems, are integrated together. The system is characterized by a high flexibility and modularity, increasing the protection of the system against illicit drones, cyber-attacks and RDD/RED and the security level of the communication among security personnel, control personnel, maintenance personnel, visitors, etc. The ITSF allows the addition of any CBRN and explosives detectors both in stand-off and mobile versions, counter-drone sensors, alarms and protection system, robotic vision, CBRN defense systems and more physical/logical technologies and barriers elements. ITSF is designed to be a general system available for the majority of organizations, according to the security needs in an urban environment, that may be integrated in the Internet of Everything (IoE) system, considering the presence of the public and the external visitors. As shown in the ITSF scheme, due to security reasons, the workstations used to perform supervision and observation of area (WS1), CBRNe detectors, intrusion sensors, alarms management and illicit drones protection system (WS2), systems management (WS3) are based on a properly dedicated LAN with the high survival Server (HSS). WSs and HSS are distinguished by both a physical and a logical point of view, including all the countermeasures necessary to prevent cyber-attacks, using firewall, intrusion detection system and anti-virus devices properly installed, and capable of controlling flying patrol-drones and "explosives and chemical compounds detection-drone" for security and emergency management. The system could be able to communicate with all the "IoE objects" on the field and supplied to the personnel of control room, security personnel, maintenance personnel, Police, Fire Brigades, drones pilots and operators, signaling in real time any critical, dangerous or anomalous situation (illicit drones, explosives or R-materials detection) using any kind of communication medium.[22,24]

Conclusions

In conclusion, as described above, the crucial issues in dirty bomb-drone prevention, could be founded on the adoption of a strict regulatory control regime for UAS' Security and serious considerations about radioactive waste management and nuclear terrorism intelligence; prevention the radicalization of Islamic subjects related to radionuclide production or storage sites; quick management and processing of information in the EU area about search and securing orphan sources; public information and contrast to the illicit trafficking of radioactive waste and radiological sources. From the point of view of the prevention of illicit acts committed by drones in no-fly zone, the UK authorities intend to use the "geo-fencing" – the definition of "fenced" areas where flight is prohibited – defined by GPS and stored in drones – in order to protect critical areas. Another countermeasure could be the traceability (buyer identification) of drones and accessories in all

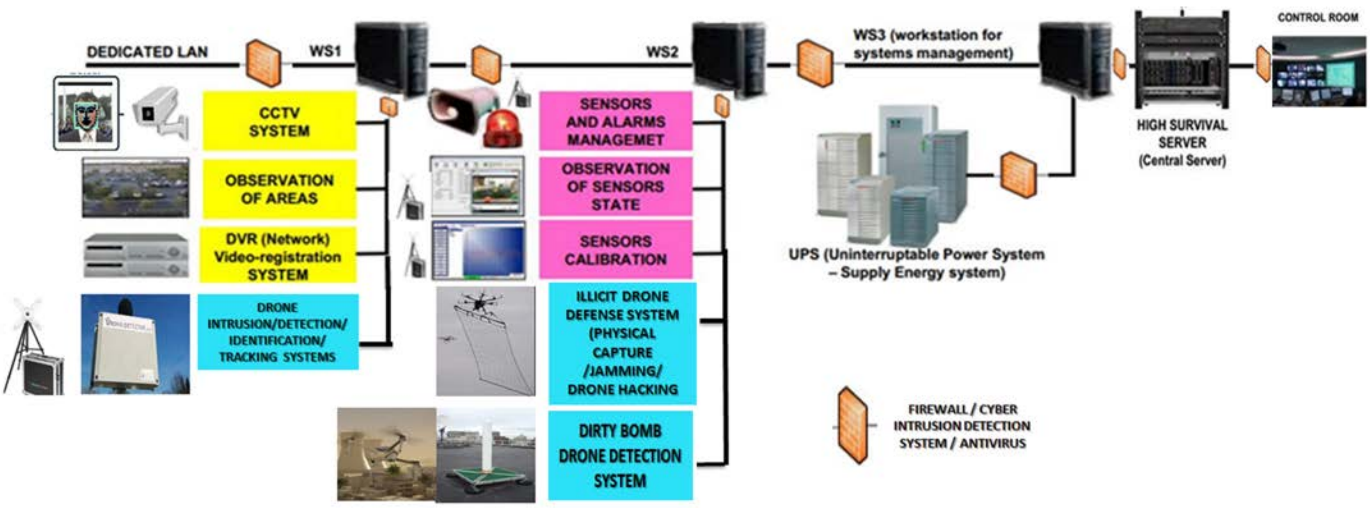

Figure 2. Hypothesis of Integrated Technological System Framework in integrated technological prevention/protection dirty bomb drone countermeasures.[24]

states, specially drones that payload, takeoff weight, autonomy are considered at risk. The comprehensive and integrated technological countermeasures such as the ITSF above mentioned, with the maximum level of flexibility, modularity and simplicity of utilization could counter an ongoing dirty bomb drones attack. It could make it possible through a fast and low-cost modification by using existing local and remote surveillance systems and commercial radiological and explosives detectors, integrated systems and new technologies, such as IoE, capable of connecting people, smart objects, data, information and processes.[23-25]

References

1. Art Levy: Drone Radiation Threat. Apogee Communication Group. http://apogeepreparedness.com/blog/, last accessed 2017/09/06.
2. Dark Horse News Homepage, http://darkhorsenews.com/isis-terrorists-plan-to-use-drones-for-horrific-dirty-bomb-attacks/, last accessed 2017/09/10.
3. Israel's Homeland Security Homepage, Weaponized Drones – Is It an ISIS Strategy? http://i-hls.com/archives/74387, last accessed 2017/09/10.
4. D. MacKenzie: Is Russia Building an Underwater Drone to Deliver a Dirty Bomb? https://www.newscientist.com/, last accessed 2017/09/10.
5. N. Genco: I Droni nel volo di terza generazione. Normativa, Istruzioni per l'uso, problemi e futuro. 1st edn. IBN Editore, Roma (2016).
6. Drones Globe Homepage, http://www.dronesglobe.com/affordable-list/, last accessed 2017/09/10.
7. S. Biancotto, A. Malizia, M. Pinto, G. M. Contessa, A. Coniglio and M. D'Arienzo: Analysis of a Dirty Bomb Attack in a Large Metropolitan Area: A Case Study, The European Physical Journal – Plus (in press, 2018).
8. F. Burton: Dirty Bombs: Weapons of Mass Disruption (https://www.stratfor.com/analysis/dirty-bombs-weapons-mass-disruption) last accessed 2017/09/10.
9. A. Malizia, V. Cusmai, V. Rossi, T. Labriola, E. Farrugia, F. Campopiano, F. Salerno, V. Trombadore, L. Cadoni, G. Rezza, R. Fantoni, S. Sandri, M. Chiappini, A. Gucciardino, F. D'Amico, C. Russo, D. Rothbacher, M. Carestia, D. Di Giovanni, O. Cenciarelli, C. Perrimezzi, I. Palombi, C. Bellecci, P. Gaudio: New Frontiers of Safety and Security: Chemical, Biological, Radiological, Nuclear, explosive events. EAI Speciale I-2014 ENEA technologies for security, 121-128 (2014).
10. G. E. Valori: Geopolitica dell'Incertezza. 1st edn. Rubbettino Editore, Soveria Mannelli (CZ) (2017).
11. N. Belmonte, C. Luetto, S. Staulo, P. Rizzi, M. Baricco: Case Studies of Energy Storage with Fuel Cells and Batteries for Stationary and Mobile Applications. Challenges vol. 8 (1) (2017).
12. U.S. Department of Homeland Security Homepage, https://www.dhs.gov/xlibrary/assets/prep_radiological_fact_sheet.pdf, last accessed 2017/09/10.
13. DJI Homepage, https://www.dji.com/, last accessed 2017/09/10.
14. F. Ferrella: Explosives and IED. International CBRNe Master Course – 2nd level, University of Roma "Tor Vergata" Lecture. (2015).
15. R. A. Meserve: Effective Regulatory Control of Radioactive Sources. US Nuclear Regulatory Commission (NRC), Washington D.C., United States of America.
16. R. Alexander Jr.: Human Behavior in the Social Environment: A Macro, National, and International Perspective. 1st edn. SAGE Publications, Thousand Oaks (2009).
17. Giovanni Calabresi: Security Management in Sogin S.p.A.. "Protection against CBRNe Events" International Master Courses – Rome Tor Vergata A.A. 2014/2015.
18. N. S. Genco: Drones: Civile Applications in Compliance with Current Legislation Conference. Trani, April 5th, 2017.
19. EASA – European Aviation Safety Agency Homepage, https://www.easa.europa.eu/easa-and-you/civil-drones-rpas, last accessed 2017/09/10.
20. EASA – European Aviation Safety Agency Homepage, https://www.easa.europa.eu/newsroom-and-events/news/overview-unmanned-aircraft-systems-uas-and-related-easa-activities, last accessed 2017/09/10.
21. Aviation S.J. Homepage, http://www.aviationspacejournal.com/2015/09/10/the-new-italian-regulation-on-uav-in-force-from-september-2015/, last accessed 2017/09/10.
22. Pietro Rossetti, G. Calabresi, F. Garzia, N. S. Genco: Operational Security Factors implementation in a Multidisciplinary Integrated Model for Security Management (MIMGS): Drones/Antidrones systems in Physical Protection of Nuclear Facilities. In: Book of Abstracts of 3rd International CBRNe Workshop - IW CBRNe 2016, Monte Porzio Catone (Roma), 25th November 2016, Texmat Ed. (2016).
23. F. Garzia: An Integrated Multidisciplinary Model for Security Management and Related Supporting Integrated Technological System. IEEE International Carnahan Conference on Security Technology (ICCST). IEEE (2016).
24. A. De Rosa: Come volano I droni della Polizia? Aeronautica n. 3, 8-9 (2017).
25. Centro Studi STASA Homepage. http://www.centrostudistasa.eu, last accessed 2017/09/10.