Implicazioni Operative degli scenari non tradizionali

L'IMPATTO DELLA MINACCIA IBRIDA NEL DOMINIO AEREO (E SPAZIALE)

Roma, 23 maggio 2017

Gen. B.A. Alberto BIAVATI
AGENDA

✓ Definitions
✓ The «military problem»
✓ Conceptual framework
✓ Legal framework
✓ Consequence management
✓ Deterrence
✓ Technological challenge and gaps
✓ Hybrid Threats’ effects on the Air Domain
✓ Conclusion
DEFINITIONS

✓ Hybrid Warfare

✓ Strategy on NATO’s role in countering Hybrid Warfare

✓ Paradigm shift
THE «MILITARY PROBLEM»

- A broad range of flying devices are emerging as disruptive means to potentially cause significant damage to human life and critical infrastructure.

- COTS technologies have greatly improved non-state actors aerial warfare capabilities, broadening the aerial threat spectrum with the so-called low, slow, small (LSS).

- The proliferation of Weapon of Mass Destruction in Cyberspace represents another transversal “enabler” of the hybrid threat evolution.

- An adaptive and faceless adversary, whose asymmetric aerial/digital capabilities may allow him to conduct undetected violations of airspace, threatening Homeland Security and national interests, therefore represents the actual military problem.

The solution must consider the integration of key capabilities necessary to effectively defend National territory, domestic population, and critical infrastructure from aerial asymmetric threats improving Homeland Air Defense (HAD) in contribution to the Homeland Security (HLS).
CONCEPTUAL DEVELOPMENT

- The NATO Military Committee is beginning to work on a redraft of MC400 in lieu of a new Strategic Concept.
- The strategic environment has changed fundamentally since 2010 so to require a major update;
- The new US Administration will need to buy into NATO policies and NATO may need to realign itself somewhat with the new Administration.
- Undoubtedly, the invasive effects on the Homeland Security and the National Defense system, generated by hybrid threats in the Air Domain, require an increased coordination and harmonization at a multinational level (NATO/ EU cooperation) to achieve political, industrial/technological and procedural common results.
- EU Member States and NATO Allies alike expect their respective organizations to support them, acting swiftly, decisively and in a coordinated manner in the event of a crisis, or ideally to prevent the crisis from happening.
- Hybrid threats represent a challenge not only for NATO but also for other major partner organizations. An effective response calls for dialogue and coordination both at political and operational level between organizations.
LEGAL FRAMEWORK

✓ NATO Integrated Defense System currently represents an effective reactive and defensive posture to traditional threats.

✓ Hybrid threat, potentially also through civilian aerial platforms (e.g. Renegade) requires necessary shared political agreements among European Nations to counteract and regulate these unique scenarios.

✓ A new shared regulatory framework across the EU would represent a more coordinated approach that would allow to overcome current restrictions imposed by NATO Air Policing Rules of Engagement for air intervention against civilian aircrafts.

✓ The traditional posture of the Air Policing can no longer be a viable solution to counter the hybrid threat.

✓ This gap is even more evident in the case of use of small remotely piloted technologies: the “non-coincidence” between the technology platform and the human element implementing the attack (attribution problem)

✓ The future air spaces management should always consider the potential hybrid threats coming from the third dimension.
Another important aspect is posed by the consequence management, following the reaction engagement stages and abatement (kinetic or non-kinetic) of a hybrid attack.

Safeguards those who “hold the responsibility to decide and engage a LSS” in relation to the damage of properties and people that such action might entail.

The lack of a consolidated approach and a dedicated legal protection indirectly represents a significant gap that weakens the concept of deterrence of a nation.

New policies and juridical frameworks to broaden its responsibilities and improve his cooperation/integration with the joint and interagency communities.

The solution addresses the requirement for policy changes by highlighting the need for an overarching legal framework, to legitimate the ADC for the protection of domestic population, critical infrastructure and national interests, against all terrorist, illegal, hazardous and dangerous acts in the air domain.
NATO recognizes that national resilience creates a more effective deterrent

The gap today perceived regarding hybrid consists in the urgent need to draw inspiration from the approach deployed in the nuclear and IAMD, aware that the national ownership of forms of resilience does not solve the problem in its complexity and totality.

NATO should gradually take on a role as coordinator and actuator for basic skills, rewriting a new paradigm that transforms the traditional concept of DA by introducing a suitable level of flexibility in managing the spectrum of new hybrid threats.
One of the most noticeable gap is inherent with technologies.

The availability of technologies to deal with the hybrid threat must not ignore the preliminary definition of a model that takes into account:

- the political perception of the problem;
- an industrial cooperation at an international level;
- the development of concepts of employment and specific procedures.

It seems clear that the complexity of the topic requiring, even at a national level, a synergy to a multi-sectorial and inter-ministerial, needs a procedural maturity that today has not yet been set.
HYBRID THREATS’ EFFECTS ON THE AIR DOMAIN

- Effects on space enablers
- Effects on critical infrastructures (network/services) to support Air Domain
- Effects on the responsibility of ensuring the national airspace since the peacetime
CONCLUSION

✓ New small, low and slow threats coming from the aerial dimension
✓ Modern cyberspace threats require a major change in the concept of traditional homeland security
✓ Special attention will need to be addressed in regards of the consequence management stemming as a result of an hybrid attack
✓ The issue of hybrid warfare has been addressed by NATO through the conceptualization of a strategy aimed at providing Nations with an improved level of resilience to contrast hybrid hostile activities
✓ Areas of cooperation between NATO and EU have been identified in order to ensure a successful implementation of aforementioned strategy.
✓ Hybrid threats are considered a complex, adaptive and rapidly changing problem, and in order to address it, a comprehensive, multi-dimensional and broad approach is needed.
✓ Today's means available to the Alliance are still limited: this situation can be both a challenge and an opportunity
Implicazioni Operative degli scenari non tradizionali

QUESTIONS?
Traditional Warfare

- Desired effect: Influence or topple government
- Government
- Population
- Military
- Focus
- Desired effect: Defeat military

Irregular Warfare

- Desired effect: Influence
- Government
- Population
- Military
- Focus
- Desired effect: Gain or erode support
- Desired effect: Render irrelevant
«Un giorno senza lo SPAZIO...»

difesa cibernetica