Rationale

The security expert community considers that the probability of terrorist attack using CBRN material is increasing.
Recent history shows that terrorists no longer hesitate to launch attacks that can lead to hundreds or even thousands of civilian casualties and that they are increasingly attracted to the usage of unconventional weapons - biological, chemical and radiological.

The difficulties of dealing effectively with CBRN crises are manifold:

- **Fragmentation:** The current approaches and systems are fragmented due to the multiplicity of players and organisational set-ups (often varying from one CBRN set-up to another one) as well as the lack of effective shared operational pictures and commonly shared information.
- **Legacy Systems:** The vast range of necessary equipments, the variety and distribution of data sources, the heterogeneity and distribution of the different stakeholders' legacy information systems as well as the lack of effective communication systems makes it very difficult to efficiently capture and interpret data to detect attacks and then to share information and support the command & control chains to coordinate a targeted response. Therefore CBRN should be seen as an additional "layer" which builds upon legacy systems.
- **Life Cycle Disconnect:** The insights that are produced at the planning stage from threat analysis and scenario development are not readily available during the operational crisis. In ICT terminology: the strategy and the tactics do not connect.
- **Information waste & fuzziness:** Much information is theoretically available, but not used.
- **Human factors:** Psychological and societal aspects – both at the levels of individual and population behaviour - are complicated to deal with. Current communication means are insufficient for creating awareness of the reality of threats and for "educating" responders, the general public and policy makers to both the appropriate preventive measures and behaviour in case of CBRN crises. As a result the fear is high and the overall preparedness low.
- **Holistic situation assessment:** The complexity of CBRN crisis makes it difficult to maintain an overall picture and assessment of the situation at hand, integrating in real-time the information coming from multiple heterogeneous sources.
- **Investment:** The rareness of CBRN crises makes it more difficult to convince political decision makers to commit to the necessary investments.
- **Training:** The scarcity of effective simulators and the lack of comprehensive awareness material for the different stakeholders.
- **Medical countermeasures:** Many treatments are theoretically available, but their efficiency is badly understood and they are often not easy to use.
- **Time dimension:** CBRN terrorist attacks are difficult to detect because in many scenarios they can take several hours or even days to show large scale effects.
- **Spatial dimension:** CBRN terrorism scenarios are characterized by the "spread" of agents and a potentially high mobility of victims in the aftermath of the attack. As well many terrorist attacks are "multi-scene" complicating the effective employment of emergency resources.

- **Frequency:** The relative rareness to-date of CBRN crisis makes it difficult to prepare against them. Hoaxes and false alarms make it even more difficult to detect the "real" events.
- **Openness:** Much information is classified and hence not shareable.
- **Ethical Aspects:** Some fundamental human rights and freedoms can never be suspended or derogated in a democratic society even in time of crisis. The main issue at stake concerns what values are non-negotiable even when in a state of crisis urgency.

CATO recognises that many elements for CBRN crisis management exist (detectors, decontamination methods, personal protective equipment, Standard Operating Procedures, emergency managements systems, training programmes, etc.). These different elements need to be pulled together in an **overall approach** to CBRN preparedness and resilience which:

- Addresses the overall effectiveness and performance of the response and not just of the individual agencies
- Can be adapted to different geopolitical, organisational and geographic settings
- Facilitates the multiple usage of the underlying technologies
- Creates an environment supporting progressive learning and enrichment, even beyond the scope of the project

CATO proposes a comprehensive holistic answer centred on an **integrated CBRN toolbox**. To achieve this objective the CATO consortium has pulled together stakeholders, technology providers and scientific experts. Thereby CATO will allow for a huge step in preparedness and resilience to CBRN crises. Furthermore by achieving this objective CATO will also

- Support effective collaboration and dialogue, as related to CBRN between EU, member states and beyond
- Define and develop tools which allow to prepare and respond to major disasters in general.