# @tomic 2012

## An Exercise in Perspective

# @tomic 2012:
# An Exercise in Perspective

# Table of Contents

# Introduction

Dear Sir/Madam,

From November 27 to November 29, 2012 the international tabletop exercise @tomic 2012 took place in The Hague. In this exercise new trusted networks were formed, lessons were learned, and points for improvement in the prevention of the threat of radiological or nuclear terrorism were identified. This independently written report contains information on these lessons learned, as well as the exercise's structure and content.

In February 2014 @tomic 2014, the successor to @tomic 2012, will be organized. This exercise will incorporate the lessons learned during @tomic 2012 and further expand the exercise's concept and scale. @tomic 2014 has been designated one of the three official side events to the Nuclear Security Summit 2014.

Organizing @tomic 2012 would not have been possible without the enthusiastic participation of the country delegations and the support of our (inter)national partners: INTERPOL, the IAEA, the European Commission, UNICRI and the EU CBRN Risk Mitigation Centres of Excellence, the Netherlands Forensic Institute and the Dutch ministries of Economic Affairs and Foreign Affairs. I would therefore like to extend my gratitude to them. Last but not least, I would like to thank the Netherlands Institute of International Relations Clingendael for writing this comprehensive report.

Yours sincerely,

**drs. H.W.M. Schoof**
*National Coordinator for Security and Counterterrorism*

# Executive Summary




The **@tomic 2012** exercise conducted in the Netherlands served as one of the first international attempts to envision a global incident conjoining radiological/nuclear terrorism with a "cyber" dimension. By giving form to a plausible scenario in which exercise participants and observers alike could be tested on their awareness of, preparedness for and ability to address the complex consequences resulting from a multifaceted threat, the organizing agencies behind it intended to further their efforts in establishing and maintaining effective nuclear security.

While risk reduction represents a key goal, capacity building, enhanced information exchange and networked human resource development are equally critical outcomes derived from the exercise. All four of these areas were identified at the conclusion of the Nuclear Security Summit (NSS) 2012 in South Korea as forward-planning objectives in aid of preventing illicit trafficking and smuggling of nuclear and radiological materials.

The exercise brought together 30 countries - 16 of which provided playing teams, and the rest which provided observers, with the total representing almost every continent. To guide both participants and observers for the duration of the exercise, subject matter expert (SME) groups were assembled in five key disciplines:

- Radiological/Nuclear
- Forensics
- Cyber Security
- Law Enforcement/Investigation
- Crisis Communications

The scenario was designed to fit a turn-based tabletop exercise, which enables participants to role-play in a facilitated and stress-free environment where information is gradually introduced. Four rounds, with four phases each, were spread out over two days, thus giving participants the opportunity to consider their actions (unlike simulations in which real-time continuous play emphasizes reactivity rather than deliberation). Five exercise objectives targeted learning through doing and evaluation; those objectives are:

- Increasing security awareness of radiological/nuclear and cyber security-related threats
- Strengthening coordination between sectors and connecting different fields of expertise

- Promoting awareness of procedures, coordination mechanisms, and operational cooperation
- Practicing procedures, information exchange and cooperation
- Building a trusted community

Each country's team was urged in advance preparations for the exercise to select players to fit what organizers identified as five roles corresponding to the aforementioned subject matter disciplines. Each team was led by a facilitator, whose responsibility lay in marshaling team members to hew to both the exercise objectives and rules.

Team structure was essential to the success in addressing the exercise's threat, which involved a fictional terrorist organization's effort to sow global panic and anarchy by harnessing cyber-attacks and digital communications to facilitate the dispersal of radiological material via aviation networks. The core of the exercise scenario is best characterized as "left of bang," but with sufficient opportunity to engage the use of nuclear forensics - one of @tomic 2012's primary learning objectives and a major factor in one of the points of agreement reached during NSS 2012.

There, participating countries acknowledged the need to further strengthen the protection and tracking of radiological materials used for industrial and medical purposes. While efforts towards nuclear disarmament and nonproliferation remain primary ambitions, preventing the devastating economic and psychological impact of radiological terrorism was identified as a vital aim given the greater probability of its occurrence. To that end, @tomic 2012 serves as the first step in developing a culture among technical experts to effectively address a radiological event and to build a multi-disciplined global community to provide expertise and assistance.

Despite its successes, the exercise revealed where need for improvement remains.
On the basis of the exercise's uncovering of core gaps, this evaluation puts forward four recommendations:

1. Media awareness must be built into community expertise at both the national and international levels
2. Emergency management as a cross-channel mechanism for information-sharing should be equally weighted with forensics and law enforcement



3. Expertise in few key areas - particularly in radioisotope activity, cyber security and crisis communications - and participation of international organizations as players should be increased
4. The next exercise should be explored as a timed simulation so that participants can understand more fully the impact of current technological trends on nuclear security

Follow-up on recommendations above should be an objective built into the upcoming NSS 2014 agenda so that lessons learned from @tomic 2012 are neither stovepiped nor left to languish.

Spearheaded by the Netherlands' National Coordinator for Security and Counter-terrorism (NCTV), @tomic 2012 represents an effort to bring together several Dutch government ministries (the Ministry of Economic Affairs and the Ministry of Foreign Affairs ), and the Netherlands Forensic Institute (NFI) with the International Atomic Energy Agency (IAEA); INTERPOL; the United Nations Interregional Crime and Justice Research Institute (UNICRI); and the European Commission and the European Union Centres of Excellence Initiative on Chemical, Biological, Radiological and Nuclear Risk Mitigation (CBRN CoE Initiative). With the upcoming Nuclear Security Summit 2014 (NSS 2014) to take place in The Hague, the Netherlands' hosting of @tomic 2012 embodies a measure to reach goals identified during NSS 2012.

# The Challenge:
# Background to @tomic 2012's Evolution


In the first quarter of 2012, the Netherlands' National Coordinator for Counterterrorism and Security (NCTV) began its planning for @tomic 2012, a tabletop exercise designed to test the international response to a conjoined nuclear and radiological terrorist threat with a cyber dimension. Having conducted such previous exercises as Cobalt 2009, Bioshield Global 2010 and Chemshield 2011 (designed to optimize international information exchange in order to avert nuclear/radiological, biological and chemical threats respectively), the NCTV sought to build upon these previous experiences by adding the layer of complexity that current technologies bring.

At the same time development of the @tomic 2012 exercise progressed, the Nuclear Security Summit in Seoul, South Korea (NSS 2012) concluded in March 2012 with certain key understandings: the repercussions of Japan's Fukushima nuclear power plant catastrophe demanded attention paid to both radiological security and the nexus between safety and nuclear security. Though the previous, inaugural Nuclear Security Summit (NSS 2010) held in Washington DC in 2010 focused on explosive nuclear devices as the primary threat, NSS 2012 identified prevention of radiological disasters and terrorism, with their devastating economic and psychological impact, as a vital aim given the greater probability of their occurrence. To that end, NSS 2012 recognized risk reduction, capacity building, enhanced information exchange and networked human resource development as four critical forward-planning objectives in aid of preventing incidents like the illicit trafficking and smuggling of nuclear and radiological materials.

These objectives and points of understanding established at NSS2012appeared as integral components of @tomic 2012. In its final form, @tomic 2012 took the shape of a radiological/nuclear exercise with a paired focus on forensics in a nuclear environment and cybersecurity. It is one of the earliest international exercises to test these conditions, and thus serves important aims, not least of which is building a trusted community of internationally networked, experienced individuals. The exercise's five objectives were:

1. **Increase security awareness**in the field of nuclear-, radiological- and cybersecurity-related risks and threats
2. **Strengthen coordination between sectors and connecting differentfields of expertise** (nuclear, radiological, forensic, communication and cybersecurity expertise)

3. **Raise awareness and improve knowledge of procedures and coordination mechanisms** of international organizations
4. **Practice procedures, information exchange and cooperation**between international organizations and individual countries
   a. Focus on timely and efficient use of available international expertise by individual countries
   b. Organize timely and effective international cooperation in (potential) R/N terrorism crises
   c. Undertake international coordination of crisis and risk communication
5. **Build a trusted community**

From the 27th to the 29th of November 2012, the @tomic 2012 exercise convened representatives from 30 countries at the Netherlands Forensic Institute (NFI) in The Hague. Sixteen countries provided teams of playing participants, and the rest provided observers, in total representing almost every continent. To guide both participants and observers for the duration of the exercise, subject matter expert (SME) groups were assembled in five key disciplines:

- Radiological/Nuclear
- Forensics
- Cyber Security
- Law Enforcement/Investigation
- Crisis Communications

Playing countries were urged in advance to assemble teams of up to five players whose skill sets would correspond to those disciplines and to @tomic 2012's radiological/nuclear forensic and cybersecurity emphasis; significantly, the advance tips for exercise participation to playing countries chiefly asserted the importance of including communications and media expertise within teams. Previous experience with the Bioshield and Chemshield exercises revealed difficulties in communications - both cultural and logistical - to be a consistent weak point in the course of such exercises. Thus some expectation was set with regards to how participants would engage with @tomic 2012. NCTV's @tomic 2012 exercise involved key international stakeholders including the International Atomic Energy Agency (IAEA) and INTERPOL; the European Commission and the European Union Centres of Excellence Initiative on Chemical, Biological,



Radiological and Nuclear Risk Mitigation (CBRN CoE Initiative); and the United Nations Interregional Crime and Justice Research Institute (UNICRI). At the national level, Dutch government stakeholders included the Ministry of Economic Affairs the Ministry of Foreign Affairs; and the Netherlands Forensic Institute (NFI) - the latter which is, like the NCTV, a division of the Netherlands' Ministry of Security and Justice.

# The Five Disciplines Tested


To guide players through @tomic 2012, subject matter experts (SMEs) were assembled for five key disciplines the exercise was designed to test. SMEs were charged with dispensing appropriate advice for players, as well as promoting and facilitating information sharing between countries. During the exercise, SMEs occasionally received information for certain rounds on an ad hoc basis that matched what players received on the second day of the exercise.

## 4.1 Radiological/Nuclear

Subject matter experts in this group addressed radiological and nuclear materials where theft, sabotage, unauthorized access (or other malicious attacks) or illegal transfer may compromise global security. The threats these materials pose include the use of a nuclear weapon; the use of nuclear material to make improvised nuclear devices; use of radiological/nuclear material to make radioactive dispersal devices (e.g. dirty bombs), radioactive exposure devices (e.g. contamination without explosives) or for use in radiation poisoning (e.g. material in the water supply, etc.); sabotage of nuclear facilities; and transport for nuclear/radioactive materials. Give the emphasis made during NSS 2012, @tomic 2012 served as a testing ground for reviewing the prevention, detection and response preparedness under the threat and event of a radiological emergency in which illicit trafficking of radiological material occurs. Made up of experts from the IAEA, the World Institute of Nuclear Security (WINS) and Lawrence Livermore National Laboratory, this group's representatives have both scientific and policy credentials.

## 4.2 Forensics

Led by a team of experts from the NFI, this SME group detailed the role of forensics in nuclear security. In the hope of creating new security protocols via information exchange and relationship-building between nuclear scientists and forensic scientists, @tomic 2012 highlighted forensics as one of the exercise's central concerns. Thus the SMEs exposed players to the importance of incident reconstruction and best practices, as well as the availability of databases (e.g. CODIS for DNA, AFIS for fingerprints and NFI's Nuclear Forensics Website and Knowledge Platform for nuclear material), lexicons and training curricula to constantly refine nuclear forensic skills - an area both technically complex and ever-evolving. Forensics SMEs also noted that traditional forensic skills (fingerprinting, DNA testing, etc.) still trump all others for essential investigative purposes, even under the threat of a nuclear/radiological incident.

### 4.3 Cyber Security

The Director of the NCTV's Cyber Security Department addressed @tomic 2012 participants prior to the commencement of the exercise to stress the significance of expanding cyber understanding and detection skill. He asserted that an adjustment of government and business trends are required in light of three major rapidly moving trends: the rise of big data, global hyper-connectivity and disappearing borders (both physical and figurative). @tomic 2012 tested the latter two in particular, and the SME team assembled (led by NCTV cyber security directorate staff and other international experts) were charged with guiding players through an often unfamiliar set of circumstances in which hacking, social engineering, denial of service attacks and digital media usage combined to create chaos. Whereas physical society is based on a security concept, the cyber world lacks a security concept in its governance, and therefore poses great challenges when added to the already complex environment of nuclear/radiological security. In the hope of leveraging @tomic 2012 as an arena in which approaches towards a cyber security concept may be initiated, the SMEs of this group faced a significant opportunity to engage players in building cyber awareness and resilience.

### 4.4 Law Enforcement/Investigation

Although this topic was perhaps most familiar to @tomic 2012 participants, SMEs from this group attempted to ensure participants had up-to-date and complete knowledge of the scope of tools available to them in prevention, investigation and detection.
The Director of the CBRNE Terrorism Prevention Programme at INTERPOL led this SME group's focus on nuclear/radiological coordination within the framework of the exercise, which served as the fourth time NCTV and INTERPOL have collaborated in the effort to create a trusted international community around nuclear/radiological security. Bearing in mind that current global preparation structures for nuclear security are insufficient, SMEs from this group acquainted players with existing facilities like INTERPOL's secure information exchange database I24-7 and reflections from such previous experiences as Project Geiger (which provided analysis of radiological/nuclear trafficking) and Operation Failsafe (launched at NSS 2012 and designed to build upon existing INTERPOL capacity).

### 4.5 Crisis Communications

Consisting of experts from the IAEA and ministries from various countries, this SME group was responsible for exposing players to a wide range of vital skills that include emergency/crisis response, public relations and media outreach. To a cohort made up mostly from ranks within law enforcement, scientific and policy-making circles, this SME group's skills were the most essential in combating the civic chaos the scenario meant to unleash, at the same time they were perhaps the least understood. As a task, reassuring citizens and providing public safety information under conditions of uncertainty and risk eluded the professional competencies of most players; however, this SME group's presence undeniably asserted crisis communications' central role in the construction of any worthy global security action plan.

# The Exercise




## 5.1 The Exercise Format and Concept

The format of @tomic 2012 revolved around a turn-based tabletop exercise. Four two-hour rounds, with four phases each, were spread out over two days. The four phases of each round began with an information dissemination and discussion session, followed by a consultation and information exchange phase in which players could visit the five SME groups for advice and consult each other; the third phase required teams to harness the information acquired in the previous two phases to make decisions that would then be discussed in the fourth phase, a debrief. Thus the format was designed to give participants an opportunity to debate and consider their actions (unlike simulations in which real-time continuous play emphasizes reactivity rather than deliberation).

Apart from the assembled advisors for each SME group, @tomic 2012's participants consisted of active players, of which there could be up to a maximum of five per country team; facilitators, of which one was assigned per playing team by shared nationality and who served the key function of guiding the team; and observers, most of whom represented countries that did not supply playing teams to the exercise. The organizers of @tomic 2012 set out a clear mission for participants:

- Identify the impact of the cyber attack and its consequences for the nuclear/radiological domain
- Identify the people and the organizations involved
- Determine the targets and progress of the terrorist operation
- Focus on nuclear forensics
- Manage the media and the public to minimize the social impact
- Take measures to avert the threat and mitigate its potential impact

With the exception of a few outliers, most players in the exercise came from one of four major sectors of expertise: law enforcement (with strong representation in explosives expertise from police and fire departments); CBRN security and regulatory bodies; defense and intelligence services; and foreign affairs policy-making bodies. A few countries were notably able to comply with supplying communications professionals as observers and forensic and cyber-security experts as team-members, but countries with such capacity were in the minority.

Upon commencement of the exercise, teams received both country-specific and general "injects" of information, the central function of Phase 1 of each round. The injects took the form of news items and police reports that required teams to draft situation reports ("sit reps") consisting of preliminary threat assessments, a list of required actions and questions for the SME groups they would be allowed to visit during Phase 2. The information exchange function of Phase 2 also permitted players to establish bilateral contact among other teams. After collating the information received during the first two phases, teams were required in Phase 3 to alter or add to their earlier sit rep assessments; the decision-making function of Phase 3 required facilitators to help their teams come to their final choices of action, with particular emphasis on the areas of detection and interdiction, law enforcement, forensics, cyber security and public information. Finally, Phase 4 had each team evaluate the round with their facilitator and ponder whether they were sufficiently prepared at both the national and international levels, and what could be done to improve preparedness.

Split into two groups and kept separate from players, observers received the injects from every playing country during Phase 1 so that they could formulate their own version of an international threat assessment, as well as questions and actions they believed country teams should be contemplating. Observers were then allowed to independently roam through the SME and team areas during Phases 2 and 3. While they were not allowed to directly interact with players at any time, observers were allowed to ask questions of SMEs during Phase 3 and as long as players were not in proximity. Both observer groups returned to their separate rooms in Phase 4, during which they were guided by coordinators to evaluate the players' actions at every round.

A wrap-up plenary session at the conclusion of the exercise allowed both a facilitator representative and an observer representative to provide their final evaluation of the four rounds in total.



## 5.2 The Location

The exercise took place at the Netherlands Forensic Institute (NFI) and was spread out across three of the facility's floors. The opening and closing plenary sessions were held on the first floor (1 in Table 1), which was converted into the playing arena during the four rounds of the exercise. This area was sectioned off into cubicles for each team during play in such a way that teams did not have either visual or audio contact during deliberative phases.

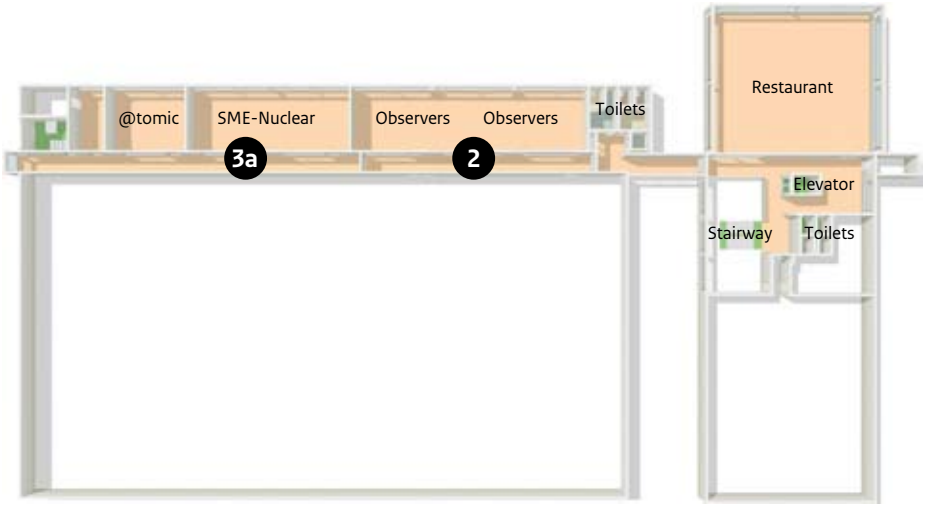
Observers were kept in two rooms on the second floor (2 in Table 1); this prevented direct visual contact with the playing arena, which was only accessible for observers during Phases 2 and 3.

The SMEs were housed in open areas on both the second and third floors of NFI (3a and 3b in Table 1). They were largely confined to their areas during the exercise and did not roam through the building, so that players and observers could find them easily. The physical configuration of the exercise required both observers and players to move quickly to and from their destinations within the phased time frame. Sometimes this resulted in logistical chokepoints: teams that were inclined to visit SMEs en masse - thereby leaving their playing cubicle empty - often missed out on bilateral opportunities when other teams made the rounds of the playing arena. While some teams managed to correct this by leaving a facilitator or single player to man the cubicle, some teams were unable to delegate roles to engage the terrain of the exercise more expediently. In addition, the constant rapid movement among players and observers throughout the maze of floors and rooms led to some confusion as to who was who - exacerbated by the lack of any identifying markers to distinguish players from observers. This occasionally led to unintended information sharing or worse, withholding of crucial information for fear of consequences, which gave rise to requests for color coded vests or similar visible identifiers to allow participants to distinguish roles more easily in future exercises.

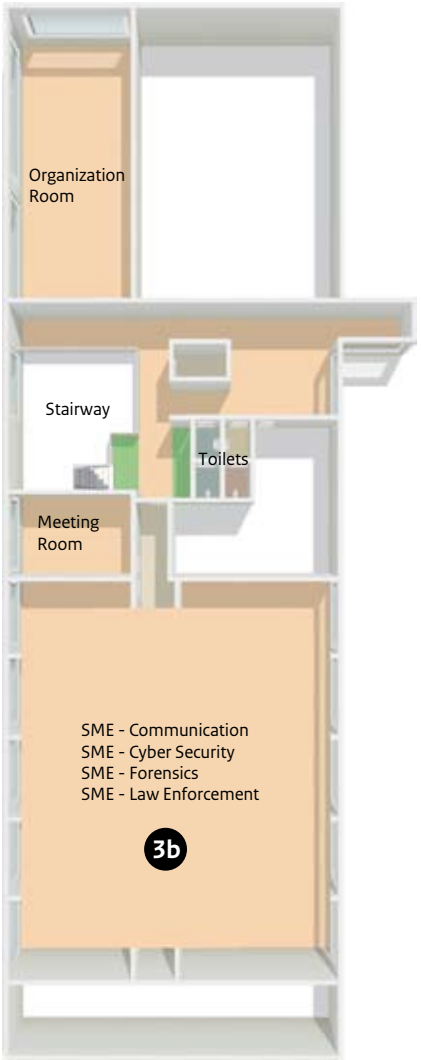
Thus the physical layout of the exercise added a dimension of complexity to which participants had to adapt.

## 5.3 Table 1: Diagram of Exercise Location & Chronology


**First floor**




**Second floor**




**Third floor**

**1** Location for opening and closing plenary sessions, which was converted into the playing arena during the four rounds of the exercise.

**2** Separate rooms for the observers preventing direct visual contact with the playing arena.

**3a** + **3b** Open areas for the SMEs. SMEs were largely confined to their areas during the exercise and did not roam through the building, so that players and observers could find them easily.

## 5.4 The Scenario

The purpose of @tomic 2012 was to produce a plausible exercise that featured a scenario as it was conceived by a fictional, multi-national terrorist group called the Brothers of Anarchy (BOA). With a timeline spread over a period of months in the recent past, the scenario was mainly "left of bang," and featured two clearly identifiable tracks: one that required nuclear/radiological forensics and one that was shaped by cyber activity.
In the scenario, the BOA plans a major international attack aimed at sowing mass panic and paralyzing global economic activity. The plan unfolds across two phases, Plan A and Plan B.

*Plan A - The HEU Attack:*

The first phase involves a series of cyber attacks in an effort to acquire highly enriched uranium (HEU) for the production of an improvised nuclear device. By subverting an employee of a company that produces HEU, BOA operatives hack into the company's security/information communication technology (ICT) system to facilitate a theft of the material. They are however foiled by the company's cyber security team, which consequently triggers BOA's attempt to buy HEU on the black market. BOA uses the black market HEU to create fear and panic. BOA triggers investigations by a number of national authorities.

During these investigations, a critical forensic opportunity arises when the police discover a link to a Dutch resident suspected to be the one trying to acquire the HEU. A search warrant is obtained and the Dutch police, accompanied by NFI's hazmat team and the National Institute for Public Health and the Environment's (RIVM) Laboratory for Radiation Research team (LSO), execute the warrant. They seize a laptop and smart phone and confirm that the powder is radioactive. Details of the information contained in the electronic devices confirm that the powder was in fact a small quantity of natural uranium mixed with carbon steel shavings/powder. BOA's lack of success in achieving the HEU phase of their attack triggers Plan B.

*Plan B - The International Irradiation Attack:*

This phase of the attack is partially successful, resulting in the irradiation of civilians and causing global economic fall-out through the disruption of international air travel.



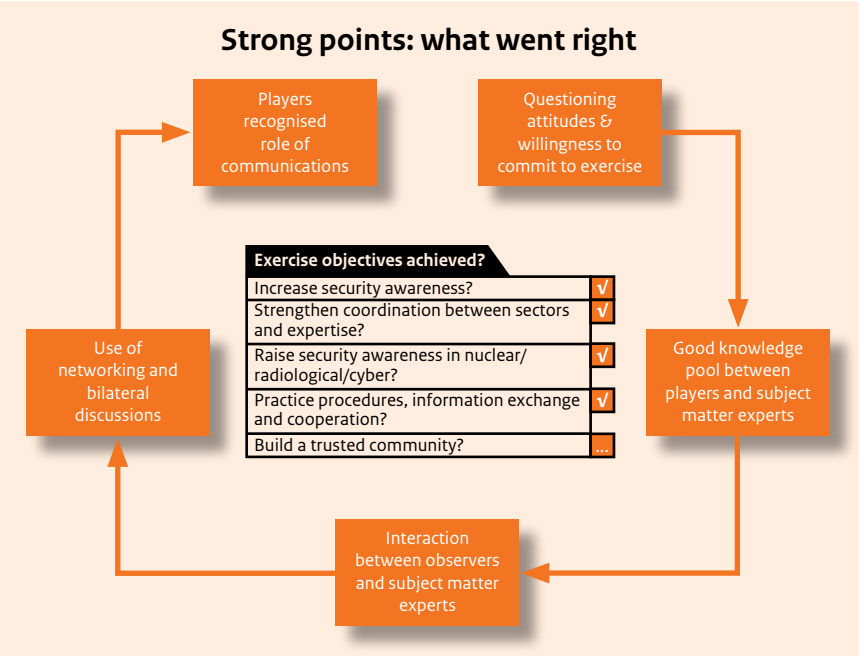
Plan B targets airlines and in this way disrupts international air travel. On the day of the actual attack BOA launches a denial of service attack on various government websites to distract the authorities.

While the attack itself is only partially successful and in the end all missing sources are ultimately detectedon arrival, the scenario ends with sickened air passengers, unanswered questions about the extent of radiological material in transit, global panic and damage to economic markets as a result of instability in the transport sector.
In the end, BOA makes good on their threat.

# The Players: Strong Points

6

## 6.1 Table 2: Diagram of Strengths




## 6.2 Point 1: Questioning Attitudes and Commitment to Exercise

Observers and facilitators alike noted the willingness among participants to fully commit to @tomic 2012. In the case of simulations and exercises such as these, a tendency for inattention to detail can arise among participants as a result of an "it's only just an exercise" outlook. But in this case, organizers asserted how impressed they were with the readiness teams and observers displayed in settling themselves fully into the scenario.

On occasion, some teams were observed questioning the scenario - not for lack of verisimilitude, but rather for what they deemed to be either red herrings or deliberate attempts on the part of organizers to confuse the players in a quest to test their skills. Indeed, several misleading points had been purposefully embedded within the various injects, designed to create "noise" that triggered more in-depth investigation by players; organizers strived to make the scenario sufficiently convoluted to engage the participants

in its complexity. However, rather than sapping players' willingness to spot patterns and question them, this technique appeared to motivate players to drill with greater granularity into the scenario - a good sign of participants' desire to thoroughly examine and question the information provided. Consequently, this tenacity led to successful identification of the detailed threat as early as Round 2, a particular achievement in light of organizers' expectations that this would most likely be reached during Round 3.

Overall, evaluators assessed participants positively for their devotion to the integrity of the exercise, their originality of thought and their open-mindedness about next steps as the exercise unspooled.

### 6.3 Point 2: Good Knowledge Pool Between Players and Subject Matter Experts

One outcome of commitment to the exercise manifested itself in the strong representation of nuclear expertise among team-members sent by participating countries. Law enforcement - particularly in the guise of first-responders, explosives and CBRN specialists - was also heavily weighted in team composition, which led to especially rapid interaction and progress with the Law Enforcement SMEs. While forensics was identified as a key component of @tomic 2012's concept, not all countries had managed to send forensic experts - a factor that is best attributable to different capacities at the national level, given the expense and experience necessary to support national forensic programs like the Netherlands' NFI, for example. The same could be said for cyber security expertise.

However, gaps in team skills were complemented by the SME groups. These clusters were critical to the performance of the teams, and many of the SMEs tried to improve ways to share knowledge and manage their interaction with players on the fly; for example, SME groups began to post signboards on the walls of their cubicles to alert participants and track what questions had been previously asked as the rounds progressed.

Not all SME groups were engaged by players equally: the most activity was observed in the Law Enforcement and Nuclear/Radiological SME areas. But then again, this was reflective of team structuring and expectations regarding an exercise like @tomic 2012. Within these groups, however, the quality of the discussion was elevated. For example,



an inflection point that hinged on identification of cesium chloride in the scenario demonstrated the players' multi-disciplined understanding and the well-defined questions they asked in these two specific areas.

In the SME areas with which players had less familiarity, Cyber Security in particular, participants still showed strong interest which deepened as the exercise progressed. Despite the organizers' requests for teams to place an emphasis on Forensics and Crisis Communications, these two SMEs were the least "busy;" however, experts from these groups attempted to turn the tide by setting up whiteboards prompting players to ask certain questions. These SME actions were integral in augmenting the understanding and experience of participants. On the positive side, they successfully raised awareness of relevant technical disciplines supporting nuclear security; they also served for many participants as their first exposure to the necessity of cross-training in media (across digital and traditional) and technical forensic (across cyber, nuclear/radiological and traditional) expertise.

### 6.4 Point 3: Good Interaction among Observers and Subject Matter Experts

For observers, @tomic 2012 provided non-playing countries and agencies with useful feedback on how to address nuclear/radiological security in the face of changing technologies. Due to the exercise's turn-based construction, observers were able to maximize their opportunities to learn from not only watching the players, but especially from also being given the freedom to discuss observations with SMEs.

Contact with SMEs did not begin smoothly: in the first round, observers in SME areas asked questions and engaged in discussion with players present. This was due to an inability to distinguish between observers and players. In subsequent phases and rounds, once this flaw had been identified and observers developed more familiarity among themselves and players, this problem dissipated - although not without recommendations as to how visible identifiers (such as the aforementioned vests or pins) could be used to circumvent this logistical problem.

Because SMEs were free to comment on not only the exercise with the observers, but also how the players were navigating the subject matter, observers received an especially broad perspective on strengths and weaknesses that was beyond the reach of players.

Moreover, several observers were adept at quickly grasping the nuances of each SME group's insights on the scenario and the behavior of the players. By the second round, this alacrity created an interesting feedback loop between observers and the SMEs in which a running dialogue on the efficacy of the exercise was achieved through the duration of all four rounds. As a result, observers were able to glean a wider top-down view of how playing countries actually fared in @tomic 2012, and SMEs were able to use the information garnered from interaction with the observers as the basis for taking active measures to draw in players more effectively in the latter rounds. Consequently, this interaction between observers and SMEs served to enhance the players' experience and knowledge.

### 6.5 Point 4: Use of Networking and Bilateral Discussions

As observers made the most of their unfettered interaction with SMEs, players subsequently delved deeper into areas with which they were less familiar like media, forensics and cyber security, enabling better networking and bilateral information sharing.

At the start of @tomic 2012, certain facilitators expressed interest in seeing how countries would cooperate on information exchange. Would playing countries mostly follow established relationships and share only with longstanding allies, or would the demands of the exercise encourage collaboration that transcended typical national behavior?

While knowledge sharing tended to mostly follow traditional national patterns, observers were surprised to see players extend their teamwork once they realized that SMEs were not the only source of information. Towards the second half of the exercise, coordination and information-networking, especially in law enforcement, exceeded the expectations of @tomic 2012's organizers. The eagerness to share built up successively over the 4 rounds to the extent that by the end of the exercise almost all teams had managed at least two or three bilateral discussions - albeit mostly with countries with the largest footprints.

Such mutual interaction can serve as an initial step towards building a trusted community. The importance of creating effective and real partnerships to avert nuclear/radiological crises cannot be emphasized strongly enough: countries have certain habits of sharing, but the global nature of such threats requires breaking free of these patterns. While the



launch of a global network of expertise and specialists requires much more work on a consistent and iterative basis to truly establish a recognizable community, these early gestures should offer reassurance that such a structure is indeed possible.

### 6.6 Point 5: Recognition of Media's Importance

Proactive crisis communications was not, in sum, an area of strength among players. Rather, as explained in the next chapter, it is the exercise's most distinct area for improvement. However, the combined efforts of observers, SMEs and facilitators helped to magnify a focus on media's central importance by the last round, once the inject narrative had accelerated to a point where unrest over lack of communication became impossible to ignore.

That recognition, late as it was, should still be viewed as a positive in light of the general lack of team experience with cyber security, digital media and public information response. The pace of the exercise allowed enough time for teams to learn by talking with SMEs, which confirms the necessity of conducting table-top exercises (as opposed to simulations) to promote learning in nascent, complex multi-disciplinary topics. Participants had to get up to speed relatively quickly, and several teams were able towards the end to incorporate public information campaigns into their final sit reps.

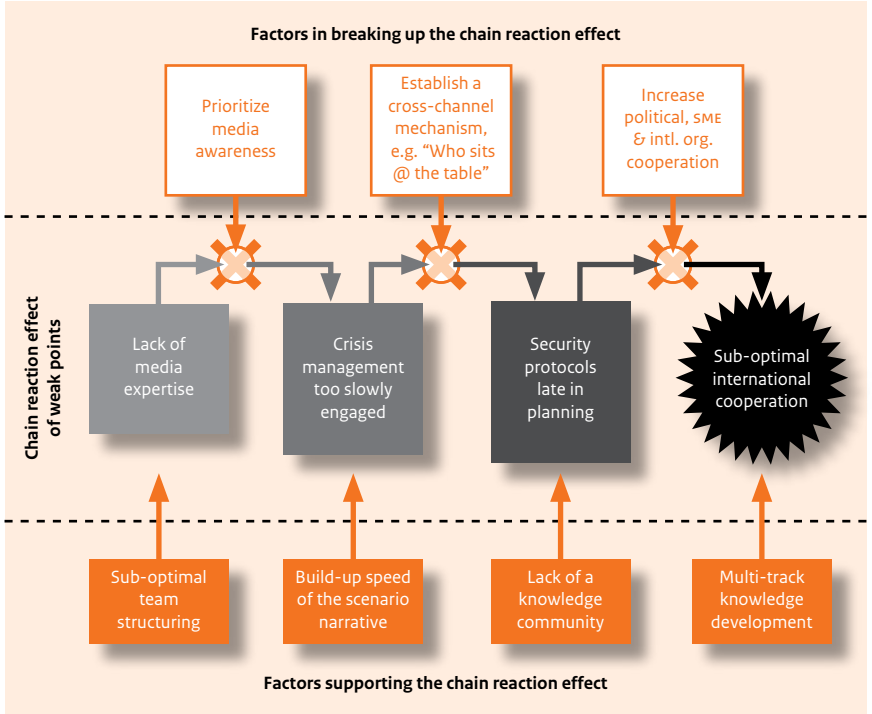
### 6.7 Exercise Objectives Met (Mostly)

The aggregative effect of these five points of success, as imperfect as some may be, amounts to most of the objectives set out by @tomic 2012's organizers as having been met. Certainly, it created greater awareness of nuclear/radiological/cyber security, as well as strengthened global cooperation through the practice of procedures. Whether a trusted community with longevity could be considered built is too early to tell. However, it would be fair to say that @tomic 2012 has facilitated a fledgling acquaintance among experts, which with time and further testing, may become more entrenched.

# The Players: Points for Improvement

7

## 7.1 Table 3: Diagram of Points for Improvement - "The Chain Reaction Effect"




## 7.2 The Chain Reaction Effect and Its Supporting Factors

### *7.2a Factor 1: Sub-optimal Team Structuring*

Gaps in knowledge, combined with the novelty of the topic and the complexity of the scenario, created a "chain reaction effect" as the exercise progressed. Critical deficiencies that were built into exercise pre-planning choices were not easily overcome as the scenario unfolded and teams became more pressured. Some teams found themselves struggling and falling behind in their responses as the narrative elapsed through the four rounds.

While the exercise revealed several factors worthy of scrutiny, perhaps the most serious of these - unsurprisingly, given previous experience with Bioshield Global 2010 and Chemshield 2011 - was a lack of familiarity with media, how it works, and how to use it.

This report uses the term "media" in its widest sense: it encompasses public relations and crisis communications; social media and other digital and traditional/analog forms of communication; and even the cyber methods by which antagonists may choose to construct their attack.

As stated earlier, @tomic 2012 organizers clearly conveyed to potential teams in the pre-planning stages that they wanted countries to place a specific emphasis in having media skills represented. From a structural standpoint, this was imperative due to the media-driven nature of the exercise. Not only were the scenario's terrorists actively using social media, chat forums, video services and traditional media outlets to convey their message, they were fully aware of the instantaneous nature of modern media and the consequent global chaos and mob mentality it can generate. In short, the BOA had a very strong and strategic media plan as part of their attack.

By comparison, teams were unable to counter this because none had included media/crisis communications experts as part of their team-member composition. Thus no country developed a strategic information campaign at the outset of the first round. Even as late as Round 3, an expert within the Crisis Communications group remarked that the attitude of the players was "the crisis has not yet happened." Ultimately, crisis management had to be undertaken as a result of team inaction, rather than as a response to the scenario. Players failed to take into account the very real possibility of panic and civil unrest - and the consequent requirement of proactive public-safety counter-measures - triggered by a real-world situation in which civilians would receive information (whether via social media or other means) at the same time as first responders. They could not see the necessity of the state's responsibility in providing information and reassurance.

At one point, SMEs within Crisis Communications conveyed to observers during the exercise that they had a few encounters with players who expressed frustration that they could not fathom the necessity of media work because they were scientists and engineers. This cultural mind-set - that somehow media is considered a lesser or secondary subject when dealing with technical incidents like nuclear or cyber threats - was in strong evidence during @tomic 2012. Unfortunately for country teams, this disregard for the power of media and the necessity of knowing how to use it created a drag effect on their ability to craft credible responses to the attack.



### *7.2b Factor 2: Build-up Speed of the Scenario Narrative*

When the encumbrance of media inexperience combined with the second supporting factor in the chain reaction effect - the acceleration of the scenario narrative - centrifugal forces made it even harder for teams to keep up. Consequences from the BOA's actions began to pile up quickly starting in Round 1: scenario injects made clear that the public response to BOA's threats was immediate and growing with every passing round. Injects featuring Twitter feeds and man-in-the-street interviews with news services showed teams that the public was aware of the threat and frightened of the potential for catastrophe, with some interview subjects even pleading for information from their governments. However, few teams had noted the need for emergency public information responses on their sit reps even well into Round 3.

Apart from the effects of lacking media savvy within teams, the consequences of sub-optimal team structuring also slowed things down once the attack took the form of a radiological incident: while the majority of teams were well-equipped to deal with the HEU phase of the attack, far fewer had sufficient background to consider the forensic signatures of radiological material. The lack of uniformly strong radiological, forensic, cyber and media skills among teams required extra time with corresponding SMEs to understand how best to proceed.

As a result, teams could not establish comprehensive crisis management strategies that effectively dealt with the escalating emergency, the public hysteria and its consequences. Teams were behaving reactively for the most part, rather than proactively.

To be fair, some smaller logistical factors made this difficult. For example, the purpose of the sit rep was not entirely clear to all teams: some used it as a to-do sheet for exercise actions, while others viewed it in its correct form as an operational to-do list. This confusion could, in future iterations, be resolved by perhaps granting more time in Round 1 or providing pre-exercise booklets with more information on documentation. One consideration for future documentation could be an alteration of the sit rep so that it becomes more like an impact assessment and action list, with appropriate intake sections on intelligence and analysis feeds. Doing this would enhance the dialogue within teams, thus supporting the external dialogues being held with SMEs or within bilaterals. In addition to the paperwork issues, the relatively small size of the SME

groups made it difficult to ensure whether players' questions were fully addressed and whether the full range of expertise required for guiding players was actually available. For example, relevant expertise in source security and detection at the Nuclear/ Radiological and Forensic SME groups was not as accessible as some players required.

### *7.2c Factor 3: Lack of a Knowledge Community*

While a few teams managed by Round 3 to fast-track security protocols once they stepped up their bilateral dialogues, uncertainty still seemed to cloud the decision-making of others. Not only were many players' national action plans short of completion, a lack of consensus on protocols became evident early in the exercise. For example, discussions with some players indicated a lack of familiarity with the Joint Radiation Emergency Management Plan of the International Organizations (JPLAN); others appeared less clear on the vectors where typical crisis first-responders like police and fire departments would intersect with the policy and law enforcement bodies heavily represented by teams; several teams could also be observed questioning to what degree political and legal concerns would determine actions (a result of the scenario's dispersal of radiological sources through an aviation network, which invoked thorny questions involving the cross-border legal implications of flights carrying radiation sources).

The lack of an existing knowledge community - with representative experts in not only the subject matter @tomic 2012 identified but also from the political, legal and private sector communities - was an unavoidable factor in support of the snowball effect. Naturally, exercises like these help initiate the development of such communities. However, the repercussions of not having a community where people know and trust one another and can harmonize approaches to emergency situations at an international level became manifest in the procedural and planning gaps observed during @tomic 2012 - thus reinforcing the critical need for its creation.

### *7.2d Factor 4: Multi-track Knowledge Development*

The end-point of the chain reaction effect, sub-optimal international cooperation, was the result of all the supporting factors reinforcing a build-up of inefficiencies. Perhaps the most difficult factor to resolve, however, is the multi-track nature of knowledge development at the international level.



Wealthier countries have the capital resources, educational systems and governance structures to permit nuclear/radiological/cyber security expertise to flourish. But what of countries that do not have either the capital or the infrastructure to tackle the installment of a comprehensive emergency response network? Countries with weak rule of law, and insubstantial skill in areas represented by the SMEs pose a hazard for the creation of an international, trusted community of expertise. A two-track - or even multi-track - environment in global emergency response training ensures difficulty in dealing with threats that require countries to work with each other to prevent disaster. Lack of infrastructure and experience may also be compounded by cultural issues, such as face-saving, that make this challenge especially acute.

Interaction and cooperation to jointly resolve cross-cutting issues remains paramount among SMEs within a burgeoning global network of expertise - with a particular obligation among the more experienced to understand the needs of the less seasoned. To create an international "culture" among technical disciplines requires actually delving, and in some cases overcoming, the cultural obstacles that can serve as practical impediments.

Consequently, reducing the impact of this particularly sensitive issue requires viewing it not only via a prism of expertise, but also through a political lens. Cooperation in dealing with transnational emergencies needs statecraft and diplomacy, which must be incorporated into any trusted community framework if it is to succeed. This may be done via international organizations and agencies, and/or multi-laterals among states; but without inclusion of international institutions and political bodies in future iterations of such exercises to determine how best to grapple with inequality at the response level, the viability of a trusted community will diminish.

# Recommendations

8

As a coordinated training event, @tomic 2012 was successful in exercising the skills of international experts and country representatives. The lessons learned have re-affirmed its value while identifying areas of improvement. Future exercises that further expand upon the areas of cyber security, forensics, and media as components of a nuclear security exercise are already in the planning stages.

Lessons learned upon the conclusion of @tomic 2012 may be expressed through four general recommendations. To address the weak points observed through the course of the exercise and to strengthen the foundation of a nascent international culture around nuclear/radiological security, the following four options - which are oriented to both future exercise and policy options - should be considered:


**EXERCISE-RELATED**

**Recommendation 1: Future Iterations as Simulations**

The deliberative pace of @tomic 2012 served its purpose in helping participants understand the complexity of merged radiological/nuclear and cyber incidents. It gave players room to make mistakes and engage each other collaboratively in the learning process. However, what the exercise did not provide was the verisimilitude of real-time events. While it may be true that radiological/nuclear events may elapse over days, weeks or months, news now travels in seconds. Consequently, successful emergency response planning must factor in the immediacy of the existing global media landscape. The development of a comprehensive knowledge culture and public information strategies focused on clarity, reassurance and safety are best tested by the instantaneous pace and pressures of current circumstances. Thus the next exercise should be explored as a timed simulation so that participants can more fully understand the impact of technological trends on nuclear/radiological security. Only by experiencing the demanding tempo of a simulation can participants learn the skills of maintaining calm and methodical application of a rehearsed strategy - or at least develop enough practical experience to shape and improve future test exercise iterations.

EXERCISE- AND POLICY- RELATED

**Recommendation 2: Media Awareness**

If the scenario narrative occurred under real conditions, governments represented by @tomic 2012's players would be barraged by public and media alike for ineffective, opaque communication. Media awareness must be built into community expertise at both the national and international levels; this consists not only of facility with social media, but also an integrated, comprehensive crisis communication strategy as part of a national/global emergency action plan.

**Recommendation 3: Need for Greater Expertise**

Expertise in a few key areas must continue to grow in sophistication and readiness. Apart from the aforementioned need to emphasize greater media proficiency, radiological expertise, as opposed to strictly nuclear, should be a key focus for improvement. Moreover, cyber security and how it can be expanded must now constitute a central component of any emergency response strategy. Forensic knowledge of radioisotope behavior, while notably ripe for improvement, may be secondary to guaranteeing high standards for knowledge of traditional forensic expertise. One way to facilitate increased expertise within a global knowledge community is to include the participation of such international organizations as the IAEA, INTERPOL and even NATO and the EU as players in future exercise iterations.

POLICY-RELATED

**Recommendation 4: Emergency Management as a Mechanism**

An emergency management strategy that can be harmonized via a global, networked community of experts should be formulated. Built through exercises like @tomic 2012 in which potential members may consistently and repeatedly gather to practice procedures and create trust via experience, this community can function as a back-channel mechanism through which politically sensitive situations (such as legal jurisdiction over threats using aviation networks or other cross-border, transnational methods) may be addressed. The existence of an international command and control mechanism may also serve as a cross-channel pathway for information-sharing among experts, especially in cases where training inequalities may arise.



Publication

**National Coordinator for Counterterrorism and Security**

*Postal address*

P.O.Box 20301, 2500 EH Den Haag

*Address*

Turfmarkt 147, 2511 DP Den Haag

Telephone 070 751 50 50

E-mail info@nctv.minvenj.nl

Twitter @nctv_nl

Website www.nctv.nl

*Publication*
National Coordinator for Security
and Counterterrorism (NCTV)

June 2013