



Topic: **In Search of Sustainable Approaches to CBRN Security Culture<sup>1</sup>**

Event: The Center for International Trade and Security (CITS) at the University of Georgia is organizing, in partnership with the United Nations Office of Disarmament Affairs and Stanley Foundation, a workshop on universal and sustainable approaches to CBRN security culture to be held in Athens, GA (USA) on February 6-8, 2012.

*Objective:* The workshop is expected to synthesize the expertise accumulated by governments, industries and academia into comprehensive and universally applicable best practice tools and models that would be based on shared principles and approaches in these four areas. A major goal is to enable countries that are lacking this experience to optimize the role of the human factor in dealing with CBRN risks and complying with their international obligations, including those under UNSCR 1540.

*Background:* The human factor plays a key role in ensuring the security and safety of the nuclear, chemical and biological industries from outside as well as inside threats. Most security lapses at critical facilities result from human failings such as inadequate skills, negligence, miscalculation, or malice. Security systems, procedures, and practices are designed to stop an adversary whose goal is to defeat the system itself. For the purpose of this workshop, we tentatively define CBRN security as the prevention and detection of, and response to, theft, sabotage, unauthorized access, illegal transfer or other malicious acts involving CBRN materials and substances, or their associated facilities.

Continuous evaluation of a security system, and the ability to predict the performance of the system against changing scenarios, is a function that can be performed only by personnel imbued with security culture. In this sense, security culture connotes not only the technical proficiency of the people directly and indirectly involved in security, but also their willingness and motivation to follow established procedures, comply with regulations, and take the initiative when unforeseen circumstances arise—as they will, given the limits on human foresight and the inventiveness of the adversaries we face today. Security culture enables a person to respond to known and indefinite security risks out of carefully tuned and proactive habit rather than improvised effort.

1. *Chemical.* Among the risks to the chemical industry and to chemical-weapons storage/destruction facilities are deliberate attempts to release toxic materials while they are in transit to or from points of storage or use; theft or diversion of chemical weapons or toxic materials for terrorist acts; and sabotage that releases toxic contaminants. A multitude of industrial chemicals, though not as deadly as chemical warfare agents, could be released in massive quantities, inflicting lethal effects despite

---

<sup>1</sup> We have selected a commonly-used term CBRN (chemical, biological, radiological and nuclear). WMD generally include nuclear, biological, chemical and sometimes radiological weapons. The terms ABC (atomic, biological, chemical), NBC (nuclear, biological, chemical) and CBRN have often been used synonymously. UNSCR 1540, mandating efforts to prevent WMD proliferation with special emphasis on non-state actors, does not explicitly cover radiological weapons, but the 1540 Committee recognizes the need to address this risk.

their lower toxicity. As new challenges to chemical security are widely recognized, the Organization for the Prohibition of Chemical Weapons (OPCW) is initiating a comprehensive program to promote a more effective protection of chemical materials and facilities throughout the entire production and supply chain.

2. *Biological.* At biotechnology labs and pharmaceutical plants, the role of the human factor is especially important because of the ease with which an unscrupulous staff member could divert pathogen samples from their proper uses. Preventing bioterrorism requires innovative solutions specific to the nature of the threat. A minute amount of pathogens can be used to create a sizable stock of weapons-usable material. The approach to fighting the abuse of biotechnology for terrorist purposes will have more in common with measures against cyber-crime than with our work to control nuclear proliferation. Although biosecurity culture is structurally different from security culture in the nuclear and chemical complexes, there are principles and approaches common to all of them.
3. *Radiological.* Almost all radioactive material can be used to commit acts of radiological terrorism, including fission products, spent fuel from nuclear reactors, commercial radioactive sources, and relatively low-level materials such as medical, industrial, or research waste. Radiological terrorism represents perhaps the most effective and easily available tool for terrorist groups. Such acts can contaminate vast territories and structures, cause panic, disrupt vital institutions, and inflict psychological damage on the public, both in the immediate vicinity of an attack and well beyond. Of particular concern are radioactive sources, which number in millions worldwide and currently are used for cancer treatment, oil exploration, food irradiation and other purposes. Given the diversity of users representing structurally different organizations, efforts to promote a healthy security culture from cradle to grave is a challenge.
4. *Nuclear.* Emerging security challenges have led to extending the scope of nuclear security and the associated culture beyond the traditional task of protecting weapons-usable material. The 2010 Nuclear Security Summit in Washington DC recognized culture as a critical element to prevent terrorists, criminals and other unauthorized actors from acquiring nuclear materials.. The International Atomic Energy Agency (IAEA) adopted this concept in 2008, launched a training program, and intends to work towards a new, more comprehensive security culture, which would cover transportation, radioactive sources, and spent nuclear fuel, among other hazardous radiological substances, while encompassing a wide variety of installations and activities. It would account not only for power and research reactors and related fuel-cycle facilities, but also for waste storage sites related to research, academic, agricultural, and industrial installations.

*Mission:* The CBRN threat environment makes it imperative to explore and shape an appropriate culture-based response in support of the global efforts against WMD proliferation and terrorism. Security cultures do exist in respective areas to safeguard sensitive materials, protect assets, and prevent acts of sabotage but their promotion and implementation are largely isolated from each other in the absence of sufficient horizontal communication and best practice sharing. What the workshop needs to accomplish—in addition to reinforcing sustainable security culture in each CBRN sector—is to identify their synergies and build a common architecture which would lead to a shared vision of CBRN security culture to deal with current and future risks. This common architecture is to become a valuable tool for many countries to enhance their CBRN security regimes.

*Issues for Panel Discussion:*

- Organizational culture and applicability of its models to CBRN risks
- Security-safety conflict and confluence
- Legal and regulatory framework for CBRN culture
  
- Security culture imperatives for Category 3 and 4 biological laboratories
- Cradle-to-grave protection for radioactive sources and associated security culture
- Insider threat: characteristics, motivation, and potential for malicious acts
- Contributing factors for CBRN security culture and the role of stakeholders
- CBRN security culture and professional ethics
- Evaluation methodologies for CBRN security culture
- CBRN culture for law enforcement agencies
- Cross-cutting principles of security culture applicable to all CBRN sectors

*Deliverables:*

- A brief report on developing a comprehensive and sustainable nuclear security culture to be released prior to the Seoul Nuclear Security Summit (March 26-27, 2012)
- A full report with concrete recommendations for promoting better CBRN security culture to be compiled by the workshop core group before the end of 2012

*Who Should Attend?*

- Participation is by invitation only. Government agencies, international organizations, business and academic communities, and independent experts are expected to participate.

*For further information contact:*

- Dr. Igor Khripunov (Workshop Chair) – [i.khripunov@cits.uga.edu](mailto:i.khripunov@cits.uga.edu)
- Mr. Christopher Tucker – [c.tucker@cits.uga.edu](mailto:c.tucker@cits.uga.edu)