1540 COMPASS

FALL 2014 — ISSUE 7

Special Issue on Comprehensive CBRN Security Culture

Security Culture for Radioactive Sources — p. 40

Effective Implementation of UNSCR 1540 in Research and Academia — p. 25

Toward a Biosecurity Summit — p. 35

1540 Compass

http://cits.uga.edu/publications/compass

A journal of views, comments, and ideas for effective implementation of UN Security Council Resolution 1540 to prevent WMD proliferation and terrorism by non-state actors.

Published by the Center for International Trade & Security, University of Georgia in cooperation with the United Nations Office for Disarmament Affairs and using contributions from Kazakhstan, the Republic of Korea, Norway, the United States and the European Union. The views expressed within are those of the authors and do not necessarily reflect those of the Center for International Trade & Security, United Nations or those of the donors namely Kazakhstan, the Republic of Korea, Norway, the United States and the European Union.

CITS
THE UNIVERSITY OF GEORGIA
CENTER *for* INTERNATIONAL TRADE & SECURITY

UNODA
United Nations Office for Disarmament Affairs

The Compass welcomes letters and articles from all concerned with 1540 implementation. Articles should be 1,500-2,000 words in length and written in English. Digital photographs should be submitted in their native format, typically JPEG; scanned photographs should be saved in a lossless format like TIFF or BMP. Send submissions to compass@cits.uga.edu.

Table of Contents

From the Editor 2
Igor Khripunov
Op-Ed: Providing the Context for a Security Culture in the Life Sciences 3
Jo L. Husbands

DISCUSSION FORUM

Indonesia: Institutionalization of Security Culture 5
Djarot S. Wisnubroto
Law Enforcement and Security Culture 6
Antonio Vulas
What Does It Take to Perform a Self-Assessment of Nuclear Security Culture? Some Basic Considerations from a Regulator 7
Carsten Speicher
Vision and Objective of INSA 9
Hosik YOO
Ebola Outbreak: Stimulus for New Look on Biosecurity? 10
Lela Bakanidze
Working together to Strengthen CBRN Security Culture 11
Ambassador Bonnie Jenkins
Security Culture Self-Assessment at Bulgaria's Kozloduy NPP 12
Vladimir Yankov
Nuclear Security Culture at Poznan University of Technology in Poland 13
Jedrzej Lukasiewicz

ARTICLES

Effective Implementation of UNSCR 1540 in Research and Academia: the Role of CBRN Security Culture 14
Johannes Rath
Stakeholders Partnership for Nuclear Security: A Success Story 19
William Keller, Heru Umbara, Khairul Khairul
UNSCR 1540 and Export Control: How High-Tech Business Can Cope and Comply 24
Gary Bertsch
Realizing the Hybrid Control Concept 28
D.J. van Beek
Toward a Biosecurity Summit: The Nuclear Security Summit as a Model 37
Maurizio Martellini and Tatyana Novossiolova
Security Culture for Radioactive Sources: Assessment, Enhancement, and Sustainability 42
Igor Khripunov
Nuclear Forensics in the Context of UNSCR 1540 47
Benjamin C. Garrett and Klaus Mayor
Explosive combinations: Criminal Networks and WMD proliferation 52
Karl Lallerstedt
1540 Experts Column 55
Terence Taylor

From the Editor:

This *Compass* issue sends a clear message: CBRN security culture has not only become a buzzword but is also getting increasing traction among decision-makers, practitioners, and academics who contributed to it. Can that be a coincidence, or the result of a biased choice of authors? Rather, it stems from a growing recognition that the plethora of institutions and programs already in place to address CBRN security challenges is just the hardware—to use an analogy from information technology—or a global network of material preparations that risks staying idle without the cross-cutting interdisciplinary software furnished by CBRN security culture. Hardware is of no use without software.

Some contributors believe that a comprehensive approach to CBRN security culture must focus on human performance in several interrelated CBRN risk areas. These include security of relevant materials and associated facilities, strategic trade and trafficking control, and knowledge management, to name a few. Indeed, security-culture-empowered personnel respond to familiar and unfamiliar risks out of carefully nurtured professional qualities rather than improvisation. Security-culture promotion leads to enhanced vigilance; it can deter or even prevent malicious acts by insiders. When applied to strategic trade and illicit trafficking control, CBRN security culture can improve due diligence in issuing export licenses, verifying end-users, and preventing unauthorized transfers. Knowledge management requires that people involved in advanced dual-use research adopt a mindset that makes preventing CBRN proliferation a top priority. It also makes discretion in sharing sensitive information a professional standard of conduct.

CBRN security culture can be defined as an assembly of beliefs, attitudes, and patters of behavior of individuals and organizations that can support, complement or enhance operating procedures, rules, and practices as well as professional standards and ethics designed to secure CBRN materials, achieve nonproliferation goals and prevent their criminal use. Security culture exists in all CBRN domains. It is particularly advanced and widely practiced in the nuclear sector. Culture is shaped in each domain by the nature of that domain's unique operational requirements and how various audiences perceive risks. Unfortunately, efforts to promote and implement CBRN security culture remain largely isolated and uncoordinated because universal tools, horizontal communication, and a joint architecture have yet to be developed. Resolution 1540 offers a good framework to develop a truly comprehensive security culture, nationally and globally, through synergies of efforts of all stakeholders.

This subject matter is not new to the *1540 Compass*. *1540 Compass* will keep this subject matter on its radar screen, and your contributions are most welcome.

IGOR KHRIPUNOV
EDITOR, 1540 COMPASS
CENTER FOR INTERNATIONAL TRADE & SECURITY

Op-Ed: Providing the Context for a Security Culture in the Life Sciences

Jo L. Husbands
U.S. NATIONAL ACADEMY OF SCIENCES[1]

The discussions during the NATO Advanced Study Institute held in Yerevan, Armenia, June 9-13, 2014 underscored the contribution that education can make to creating a robust CBRN security culture. An engaged and committed workforce is essential to sustaining such a culture, but employees are not empty vessels into which leaders can pour values and ideas. People come to their jobs with experiences, attitudes, and values that will shape their performance. Introducing the core values necessary to a CBRN security culture as part of education and training helps provide the foundation on which a security culture can be more readily constructed.

What Yerevan also revealed is that fostering a "bio" security culture faces a number of significant challenges. Before one can think about the micro level challenges – in particular where it is reasonable and feasible to begin introducing a full, rigorous security culture and the accompanying self-assessment model – there are serious issues at the macro level. In particular, there is a relative lack of awareness of biosecurity issues within the wide and varied array of stakeholders who must be engaged. In addition, in contrast to the existing and relatively strong shared biosafety culture, there are continuing controversies over both the reality of security threats and the remedies for them.

This suggests that, as a starting point, it would be wise to frame the biological dimension of CBRN security culture in a way that can engage many stakeholders without expecting consensus at the outset. Many Yerevan participants were comfortable with using "biorisk management" rather than "biosecurity," and one can see this change appearing in a number of international discussions. But if a meaningful biological security culture should include facilities from different levels and sectors of government, industry, and academia (public health, basic and applied research, biodefense, etc.), then to me it makes sense to look for an even broader context through which to introduce the subject. This is not a substitute for addressing biorisk and security issues. This is how one opens the door, how one begins the conversation that leads to discussions of safety and security. Such a context should be compatible with security-focused education and training for more specialized, directly affected audiences. It should also complement legal and regulatory structures as well as voluntary measures, and provide a basis for discussing additional measures or changes in practices.

Introducing the core values necessary to a CBRN security culture as part of education and training helps provide the foundation on which a security culture can be more readily constructed.

For the last several years a number of organizations engaged in biosecurity education, including the U.S. National Academy of Sciences, have had substantial success in using concepts from the social responsibility of science to provide that context.[2] "Responsible Science" offers the opportunity to present security culture as a component of an existing culture of responsibility in the life sciences (and science more

1 Although this paper draws heavily upon reports and activities of the National Academy of Sciences, ultimately the product is the author's own, independent analysis and any opinions, findings, conclusions or recommendations expressed in this material are her own.

2 Examples of such activities were presented at a side event during the August 2014 Meeting of States Parties to the Biological Weapons Convention; copies of the presentations may be found under the "Side Events" heading at http://www.unog.ch/80256EE600585943/(httpPages)/ F837B6E7A401A21CC1257A150050C-B2A?OpenDocument.

generally). By building on something that can be presented as already part of the broader culture of science, it "makes scientists part of the solution, not part of the problem." This would be important under any circumstances, but is particularly so as the focus of threat reduction activities has shifted away from dismantling former weapons programs to the prevention of terrorism, an activity that requires the support of scientists and technical personnel who are not themselves considered potential security risks. Security can also become part of the discussions of responsible conduct of scienceandresearchintegrity that are accompanying the continuing global diffusion of research and industrial capacity in biotechnology. This recognizes the great hopes being invested in biotechnology while allowing a focus on how to ensure that the new capacity is developed and managed in ways that support safety and security.

"By building on something that can be presented as already part of the broader culture of science, it "makes scientists part of the solution, not part of the problem.""

There are encouraging signs that the Responsible Science framing is gaining acceptance in international discussions. One of five deliverables for Biological Security sub Working Group of the Global Partnership Program (GPP) is "Reduce proliferation risks through the advancement and promotion of safe and responsible conduct in the biological sciences," and "Responsible Science" was the theme for October 2013 GPP meeting under the United Kingdom's presidency. The report of 2013 Meeting of States Parties of the Biological Weapons Convention concluded that "In order to further efforts on education and awareness-raising about risks and benefits of life sciences and biotechnology, States Parties agreed on the value of using science responsibly as an overarching theme to enable parallel outreach efforts across inter-related scientific disciplines..." And the statement by Ahmet Üzümcü, the Director-General of the Organization for the Prohibition of Chemical Weapons (OPCW) during his Nobel Peace Prize lecture that "Our aim is to contribute to efforts towards fostering a culture of responsible science. This will ensure that current and future generations of scientists understand – and respect – the impact that their work can have on security" suggests that the increasing convergence of chemistry and biology could also extend to collaboration on the practical development of safety and security cultures.[3]

The argument to use the existing cultures of responsibility in the life sciences as entry points for introducing biorisk and biosecurity is not meant to suggest that these cultures are sufficiently strong at present. High profile cases of scientific misconduct are a major reason for the current global discussions of research integrity. Closer to CBRN, reports of accidents and serious lapses in biosafety practices with dangerous pathogens at U.S. laboratories raise questions about the state of the safety culture in even the finest facilities. But to end on an optimistic note, this may be precisely the time, when the life sciences community and those who oversee it are aware of the need for improvements, to strengthen the core values of safety and security.

3 The International Union of Pure and Applied Chemistry, with support from OPCW, has developed educational materials on the "multiple uses of chemicals" that fits well with a responsible science approach. The materials may be found at http://multiple.kcvs.ca/site/index.html.

1540 COMPASS

DISCUSSION FORUM

Please send letters for the Discussion Forum to Editor in Chief Igor Khripunov at i.khripunov@cits.uga.edu. Letters should not exceed 500 words.

INDONESIA: INSTITUTIONALIZATION OF SECURITY CULTURE

One of the previous issues of 1540 Compass carried an article on a pilot self-assessment project for security culture implemented in 2012-2013 at Indonesia's research reactors in Yogyakarta, Serpong and Bandung. Indeed, it was a pioneering project to put to test the emerging IAEA methodology for self-assessment of nuclear security culture. Our National Nuclear Energy Agency (BATAN) was happy to collaborate with the IAEA and contribute to a speedy development of this much needed technical guidance. This project also was made possible by cooperation with the Center for International Trade and Security at the University of Georgia, USA. When this draft guidance was endorsed in June 2014 by the IAEA Guidance Committee, we were all proud of having contributed to its successful development.

Interestingly, this experience has demonstrated to BATAN leadership and staff the value of culture as a major contributing factor to an effective nuclear security. As a result, BATAN started to accumulate unique expertise in effective management of the human factor at its facilities. In addition, a core group of BATAN staff was recognized as international experts and increasingly invited to share their skills with other countries. These and other realities motivated BATAN leadership to establish the Center for Security Culture and Assessment (CSCA).

Given common foundation of security, CSCA is designed to go beyond nuclear and apply the methodology to other domains, particularly chemical and biological. Our objective is to work together with other countries of the region in achieving comprehensive security culture. To this end, we are prepared to become a regional hub of expertise and collaborate with all stakeholders involved. It is recognized that a chain is as strong as its weakest link. It is our common resolve to address these weaknesses and make our security chain resistant to current and emerging threats.

Djarot S. Wisnubroto
CHAIRMAN, NATIONAL NUCLEAR POWER AGENCY, INDONESIA

LAW ENFORCEMENT AND SECURITY CULTURE

I am deeply convinced of the importance of cooperation between law enforcement agencies and "CBRN institutions". Cooperation can be seen as an essential prerequisite for developing CBRN Security Culture. Accordingly, CBRN Security Culture can be developed only through close cooperation between the CBRN experts and security experts.

Without any intent to monopolize the "security knowledge" for only the law-enforcement sector, I think that using the knowledge of security experts within law enforcement agencies can be a useful tool for the developers of CBRN Security Culture.

There are many reasons behind this way of thinking. First, the law enforcement agencies' staffs are security experts (in various fields). Second, sharing their knowledge with the "public" is a part of their jobs and duties. Third, it comes free of charge (important from a financial standpoint). Finally, it is their obligation to implement the laws, based on the UNSCR 1540(2004) and 1977(2011), with clear tasks, which should be performed daily by the same law-enforcement agencies.

However, despite all their willingness and professionalism they lack the necessary CBRN expertise. And there we come to the symbiosis point. In few words: we need each other.

The European Union has developed a system of such cooperation. Its aim is to fulfill the requirements placed by the Resolutions mentioned above. The European Union has designated the Directorate-General Home Affairs (part of the European Commission) as the body responsible for overall coordination of the implementation of the EU CBRN Action Plan (implementation period 2010-15). The **CBRN Advisory Body** is the main body which coordinates the work of the Member States and the EU bodies. It consists of the **C, B and RN subgroups**. Besides that, the DG Home has given a mandate to the Joint Research Centre, with its seats in Karlsruhe (Germany) and Ispra (Italy), for technical support in the implementation process of the Action Plan. Further development of the horizontal **(H)** actions within the Action Plan, among other things, envisages providing training and the exchange of good practices for all interested parties. One of the future steps could be establishing an EU Radiological-Nuclear Security Training Centre for Law Enforcement Community (EUSECTRA) located in Joint Research Centre facilities.

Such interagency cooperation could be a good example for the development and implementation of CBRN Security Culture worldwide.

Antonio Vulas
POLICE SUPERINTENDENT, CROATIA

WHAT DOES IT TAKE TO PERFORM A SELF-ASSESSMENT OF NUCLEAR SECURITY CULTURE? SOME BASIC CONSIDERATIONS FROM A REGULATOR

About the sense and benefit of a well-balanced security culture, everything has already been said. As a security inspector of several types of nuclear facilities, I have to state that indeed most security incidents are related to lax discipline, ignorance, knowing and willing rule-breaking rules, imprecise regulations, and, in general, an atmosphere in which few feel responsible for security. Security is supposed to be the guards' job, and a largely unnecessary one as the threat does not to be very serious. To sum up: weak spots in security awareness lead to low-level security events which may end up as severe security issues. To prevent such low-level events is not an easy task, as they are clearly related neither to holes in security regulations nor to weak physical protection. They only point to the staff's behavior. Like a hole in a mosquito net, the weakest element within a system decides whether it works out. When it comes to security, man is the weakest part.

A staff's behavior is the consequence of its members' specific cultural traits, so we should focus on the lived organizational culture within the security regime. How can a culture within an organization be evaluated? It is important, first of all, to understand the benefit from the results of such an evaluation. A self-assessment is wasted time if conducted only because it is expected or because it brings good marks ("good practices") from IAEA reviews. The second step is to draw up a workable plan for doing the self-assessment, and to define what the reviewers need to do it. This means developing a cogent plan, allocating resources such as expertise and manpower, and finally drawing up a concise roadmap. The latter is very important, because without a precise plan that is strictly followed, the self-assessment will be postponed forever. Managers tend not to like such projects because the benefit appears rather diffuse or unclear to them. They may consider it an unproductive gimmick rather than an useful organizational tool. And the third step is to involve external experts, not so much to supervise the self-assessment as to provide a broader, more dispassionate view from outside the facility. The final step is to start the project, taking the first step on the stairway to a successful self-assessment.

Now let us take a closer look at the first step: the willingness to perform a self-assessment. Here the regulator is able to actively support the operator by promoting the self-assessment. Regulators motivate the staff while helping the operator's security division overcome managers' prejudices. Evaluating the security culture within an organization is a serious task, not a game. Again, the second step is composing a concrete and concise plan. Where do reviewers get such a plan from? To my mind, the technical guidance compiled

by the IAEA offers a complete toolbox of everything needed to perform a rigorous self-assessment of nuclear security culture. Paying attention to the cultural background of the facility's home country, IAEA-supplied tools—surveys, interview techniques, inspection observations, document reviews, and so forth—may be adapted to the country's culture. If the staff feels unable to adapt these tools by itself, it can solicit help from external experts.

This leads us directly to the third step, seeking external support. External support may be provided by the IAEA, technical support organizations, or any other organization that has already performed such a self-assessment.

Whatever method the facility embraced, the assessment should be a self-assessment, initiated and fostered by the leadership's determination to improve the state of security within the site. In turn this will help to prevent not just major failures but low-level security events that tie up a lot of personal and financial resources.

Now you may ask if above-mentioned factors are primarily theoretical. I can reassure you that the process really works out like this. We have already performed self-assessments of nuclear security culture based on the draft IAEA technical guidance. I am quite sure the self-assessments help sharpen awareness of security issues while bolstering the state of security at these facilities. Nevertheless, it is hard to impress upon managers the importance of this endeavor. Security culture succeeds when nothing bad happens. It is hard to quantify security incidents prevented—and thus to prove the value of a security-conscious staff.

Carsten Speicher
SENIOR NUCLEAR SECURITY OFFICER, MINISTRY OF THE ENVIRONMENT, CLIMATE PROTECTION & THE ENERGY SECTOR, BADEN-WÜRTTENBERG, GERMANY

VISION AND OBJECTIVE OF INSA (INTERNATIONAL NUCLEAR NONPROLIFERATION AND SECURITY ACADEMY)

With an increasing possibility of nuclear terrorism, countries have been required to strengthen their national nuclear security systems and there have been a lot of efforts to improve nuclear security worldwide. Effective nuclear security can be achieved through the provision of capabilities to prevent, detect and respond to malicious acts against nuclear facilities. These capabilities should be developed systematically and should be self-sustaining over a long-term period. This can be done by providing continuous and a high level of training and education in nuclear security. The ROK opened a new international training and R&D center in February, 2014. The establishment of an International Training Center called INSA (International Nuclear Nonproliferation and Security Academy) was pledged by the president of the ROK made during a nuclear security summit held in the Washington D.C. in 2010. There are three objectives of the center: provide customized and high quality nuclear security and non-proliferation training, as well as educational programs designed to meet the needs of both domestic and regional Asia-Pacific personnel, facilitate technical and scientific cooperation and assist to emerging countries, and promote R&D activities on physical protection systems. The INSA has several different features that set it apart from other training centers. The center can provide participants with more practical knowledge, rather than just providing classroom lectures. Compared with other centers that provide programs only for nuclear security or non-proliferation, the INSA provides a training program related to import & export control, which is essential for those who work in the business sector related to nuclear industry. One of the most distinguishing features of the INSA is its large scale test beds that

International Nuclear Nonproliferation and Security Academy, Daejeon, Republic of Korea

will be used both for training and R&D activities. Acquiring Data for evaluating the vulnerability of a nuclear facility is another important function of this facility. The test bed can also be used as a place where the performance of new equipment can be evaluated. The goal of the center is to not only to enhance the nuclear security culture, but to also be a leading hub for training and education in nuclear security and nuclear non-proliferation in the Asia-Pacific region. The INSA will also support the emerging countries that have plans to initiate their own nuclear industry by providing customized programs, as well as technical and scientific assistances. These activities have enabled the ROK to take the lead in non-proliferation and nuclear security.

Hosik YOO
VICE PRESIDENT, KOREA INSTITUTE OF NUCLEAR NONPROLIFERATION AND CONTROL

EBOLA OUTBREAK: STIMULUS FOR NEW LOOK ON BIOSECURITY?

The outbreak of Ebola in West Africa, in which the death toll has surpassed 1,000, serves as a reminder to global society that potential pathogens are circulating and evolving in the environment all the time, and that human action can have an immense impact on the emergence and spread of infectious disease.

A recent report issued by the Department of Homeland Security raises topics of possible inspiration for terrorist groups, specifically those based in West Africa, to weaponize the virus. Experts, however, doubt that West African terrorist groups have the scientific skills and ambition necessary to complete such an objective adding that Ebola is not airborne which limits the number of casualties a terror group could target.

As the report says, this fear by the West of Ebola weaponization dates back decades to the Soviet Union's VECTOR program. The program researched biotechnology and was thought to have conducted research aimed at weaponizing Ebola.

At the same time the Russian mass media, based on the Russian Federal Service on Customers' Rights Protection and Human Well-being Surveillance (RosPotrebNadzor), claimed that the United States had established laboratories on the borders of Russia, particularly in Georgia, Azerbaijan and Ukraine. They claimed that the functioning of these laboratories poses a deadly threat to the local population and neighboring countries.

In such situations it is very important to ensure countries are in compliance with the Biological Weapons Convention (BWC) and other international treaties. In this regard there are many challenges: the inherent dual-use nature, the widespread availability of the materials and technology, and the potential significance of even a small quantity of pathogenic material. These factors all combine to render traditional arms control approaches to enhancing assurance ineffectual.

Recent events once again illustrate the importance of researching vaccines and therapies. However, due to previously mentioned facts, it is often not possible to reach a definitive conclusion about whether or not countries are fully complying with their obligations under international treaties. Though it might not be easy, the global community should create a mechanism for substantially changing this situation. Of particular importance is engagement with civil society, particularly the scientific community and professional organizations, in order to promote awareness and a culture of responsibility and also to provide oversight of research and development.

Lela Bakanidze
GEORGIAN BIOSAFETY ASSOCIATION (GEBSA), REPUBLIC OF GEORGIA

WORKING TOGETHER TO STRENGTHEN CBRN SECURITY CULTURE

The United States and the international community have dedicated significant resources to chemical, biological, radiological and nuclear (CBRN) security. While a large portion of the funding has gone to the technical aspects of security, such as providing monitoring equipment to detect illicit nuclear materials, or enhancing physical security at sensitive facilities, a fundamental part of any successful effort to prevent CBRN terrorism is to focus on the human factor. Ultimately, it is the person working at the facility that has to make sure that the gates are closed,

the monitors are turned on, that pathogens and precursors are safe and secure, and that detectors are working. To ensure that personnel managing and working at facilities understand WHY it is important to take such measures, and to ingrain the importance of security into the culture of the facility, we need to devote resources and other efforts dedicated to enhancing security culture.

Regularly promoting a strong security culture within the four CBRN areas is critical to the immediate and long term success and sustainability of CBRN security programs and activities. Such training must involve everyone connected to relevant facilities, including CEOs. This requires engaging both governments and the private sector. In a time of constrained government funding, we need to ensure that the important work will endure.

A variety of entities, including international organizations, like the International Atomic Energy Agency (IAEA), and the United Nations Office for Disarmament Affairs (UNODA), and international initiatives, such as the Global Partnership, and non-governmental organizations, such as the University of Georgia and the Hungarian Institute for Foreign Affairs and Trade (IFAT), are increasingly focused on the importance of CBRN security culture. Collaboration between these groups will be necessary to help ensure CBRN security for the long term.

Ambassador Bonnie Jenkins
SPECIAL ENVOY AND COORDINATOR FOR THREAT REDUCTION PROGRAMS, U.S. DEPARTMENT OF STATE

SECURITY CULTURE SELF-ASSESSMENT AT BULGARIA'S KOZLODUY NPP

I want to draw the attention of the readers to something we started to perform in Kozloduy Nuclear Power Plant, Bulgaria together with CITS and IAEA – self-assessment on nuclear security culture. For the first time I heard about nuclear security culture was when I read the IAEA Nuclear Security Series No. 7 – Nuclear Security Culture. At this time I realized that a proper security culture can support a strong nuclear security but I did not have a clear picture in my mind of how to introduce the security culture in our nuclear power plant, nor how to enhance it later. And then an IAEA Technical Meeting came during April 2013 in Vienna, which purpose was to present and discuss a draft guide for nuclear security culture self-assessment based on a methodology applicable to diverse facilities and activity where nuclear security matters. At this meeting the pilot project of BATAN, Indonesia for testing the methodology at its three research reactors was presented and the need for testing the applicability of the methodology in a nuclear power plant was mentioned. I saw the opportunity to introduce the nuclear security culture as a part of the nuclear security regime and to estimate the strong and weak sides of the current security culture in our power plant in order to focus our efforts on improving our weaknesses and maintaining our strengths. I also wanted to raise the importance of the security culture at the level of safety culture, because there is a continuous process in our power plant for enhancement of safety culture since 2011. Now it is on its second self-assessment after introducing a three years action plan for improving the nuclear safety culture.

So after the IAEA Technical Meeting I proposed to our Safety & Security Director as well as to our Executive Director to conduct a self-assessment on nuclear security culture in the power plant. Both cultures, safety and security, being part of the organizational culture of the company, it was not difficult to convince them of need of as good security culture as the safety culture is, because of their understanding of the importance of the organizational culture. It seems that Bulgarian Nuclear Regulatory Agency (BNRA) also understands the importance of maintaining a proper nuclear security culture because we have their full support in this endeavor.

Further we proposed to IAEA through BNRA to conduct a self-assessment trial in Kozloduy NPP using the presented methodology to estimate its applicability in a nuclear power plant and this proposal was accepted. Most important role in this communication and in the further help from IAEA side was to Mr. Fumitaka Watanabe, who was in that time in charge of nuclear security culture at IAEA Office of Nuclear Security. In my opinion the leading role of IAEA had some influence on BNRA's decision to support the trial.

After finishing the self-assessment process by the end of the year, I will be glad to share the lessons learned and best practices with the readers and

referring to Resolution 1540 to share them among the CBRN domains. Currently only the nuclear domain has clear recommendations of how to maintain and enhance security culture but the fact that Kozloduy NPP is conducting the second self-assessment trial in the nuclear domain means that there is a lot to be done. In this regard it will be very helpful to interact with other domains and to learn from each other. We can conduct common workshops and can invite participants from other domains to the self-assessments which can help to develop a common CBRN security culture.

Vladimir Yankov
NPP SECURITY DEPARTMENT, BULGARIA

NUCLEAR SECURITY CULTURE AT POZNAŃ UNIVERSITY OF TECHNOLOGY IN POLAND

Poland is one of a few countries in Europe without a nuclear industry. Access to an independent source of energy and the need to reduce the emission of CO_2 were reason enough to make the decision to begin construction of the first Polish nuclear power plant. The development of Polish nuclear law and the development of the Polish nuclear industry have been underway for many years both at the government and investor level. The principle investor is PGE Polska Grupa Energetyczna SA and its subsidiary group PGE EJ1 (a special vehicle responsible for preparing investment processes and construction of the first NPP in Poland). At the beginning of July 2014 PGE EJ1 selected the Owner's Engineer. The winner of this selection is AMEC Nuclear UK Ltd. The Owner's Engineer will be responsible for technical support and guidance. According to PGE's work schedule related to the development of the first NPP in Poland, the first unit should start up at the end of 2023.

With respect to the Polish nuclear programmer, the Polish Ministry of Economy has established there a period program called ''Training for Trainers" directed at Polish teachers. Participants of this program were selected among teachers working at universities in Poland. The program commenced in 2009. Since that year all participants have been obligated to participate in three months of training in France in 2009, 2010, and 2011. Poznań University of Technology is one of a few universities in Poland that teaches nuclear engineering in the frame of an electrical engineering field of study.

Nuclear security at Poznań University of Technology is taught through lectures on security and safety of technical systems and in the frame of nuclear physics. Understanding the issues, such as terrorist attack on nuclear power plant is rather limited in Poland. Poland has never been attacked by terrorists, and attacks such as the 9/11 attacks or the attack on the London subway is only known from TV reports. Citizens of Poland are not aware of the continuously existing threat. Nevertheless, the number of people devoted to teaching security is enough to present the problems associated with nuclear security and nuclear security culture in a meaningful way.

Aspects of nuclear security culture are presented to the students during lectures but also through literature, such as Nuclear Security Culture NSS No.7 published by the IAEA as well as scientific papers from the library. It is crucial to point out that the best source of knowledge about security culture is always conversation, discussion or presentation. Given the special nature of security culture, my intention is to create and develop a portal specifically dedicated to security culture. The portal should be divided into chemical, biological and nuclear websites. The portal could be a good place to share experiences, articles, and information related to security culture. Teaching materials for students would be also welcomed. My second step would be to create a ring of colleagues working in nuclear labs, industries or universities who deal with teaching nuclear security to all cooperate in the education of students. It is absolutely important to share knowledge between experienced lecturers from industry with students of nuclear engineering. I believe that the collaboration between Poznań University of Technology in Poland and experienced lecturers from other countries will be possible.

Jędrzej Łukasiewicz
POZNAŃ UNIVERSITY OF TECHNOLOGY, POLAND

Effective Implementation of UNSCR 1540 in Research and Academia: the Role of CBRN Security Culture

Johannes Rath
UNIVERSITY OF VIENNA, AUSTRIA

Addressing the CBRN proliferation risks resulting from research and academia has been a continuous challenge. While building on classical non-proliferation instruments developed for State sponsored CBRN programs, many of the current instruments used in the implementation of UNSCR 1540 provide only unsatisfactory protection against the specific risks arising from the research sector.

Inclusion of research and academic institutions in classical non-proliferation regimes (e.g. export-control measures) and relevant conventions (e.g. BTWC, CWC) has proved to be a challenge for a variety of reasons. For example, a contributory factor in the failure to agree on an international verification protocol for biological weapons has been the substantial controversies over how to include biomedical research and development.

In the following sections, the relevance of including academic and research institutions in UNSCR 1540 implementation will first be established. Second, the specific challenges to effective UNSCR 1540 implementation at academic and research institutions will be outlined. Third, the concept of CBRN security culture will be briefly elaborated. Finally, the potential relevance of a CBRN Security Culture as an instrument in overcoming some of the challenges associated with UNSCR 1540 implementation in academia and research institutions will be discussed.

THE RELEVANCE OF ACADEMIC AND RESEARCH INSTITUTIONS IN EFFECTIVE UNSCR 1549 IMPLEMENTATION

Current and historical examples of incidents and threat scenarios indicate that research and academic institutions are key stakeholders in CBRN security. Thereby, academics and researchers do not act only as potential contributors of knowledge to large State-sponsored CBRN programs but also act as viable and standalone CBRN terrorism players (e.g. US Anthrax case). Therefore, a non-proliferation instrument, such as UNSCR 1540, with the mandate to mitigate CBRN risks arising from non-State actors will have to actively engage into the development and implementation of instruments that mitigate such risks effectively while at the same time protecting other legitimate interests of society and individuals.

Figure 1: The Challenges of Effective UNSCR 1540 Implementation at Academic and Research Institutions

THE CHALLENGES OF EFFECTIVE UNSCR 1540 IMPLEMENTATION AT ACADEMIC AND RESEARCH INSTITUTIONS (FIGURE 1)

Fundamental Rights Dimension

The regulatory complexity of introducing security measures in research, which has a strong foothold in fundamental rights such as academic freedom, freedom of speech or freedom of information, creates substantial challenges to any restrictive regulatory approach. The on-going controversy over how to handle biosecurity-sensitive research information obtained from gain-of-function studies on different influenza virus strains is one example of these difficulties. In practice, very little constructive work has been carried out on these issues. Effective implementation of UNSCR 1540 in research and academia will need to engage in the question over how balancing of fundamental rights with security can be accomplished. Legal principles that facilitate such balancing, such as the "Proportionality Principle" enshrined in Europe fundamental rights legislation, need to be addressed if effective and sustainable implementation of UNSCR 1540 at the research level is to be achieved.

Research dynamism and the Principle of Certainty

Criminalization in the use of CBRN weapons, a frequently used tool in national implementation of

international CBRN related legal instruments, has only limited preventative capacities. However, extending criminalization into preparatory acts and including, for example, the unlawful possession of dual use materials, technology and information quickly runs into legal limitations. The criminal law principle of "lex certa" requires lawmakers to provide unambiguous and clear definitions of criminal offenses. CBRN security sensitive research, however, unfolds in a constantly and often rapidly changing environment. Criminalization as a preventive measure would, therefore, require constant engagement in technology developments and updating of potential offenses. It is difficult to see how this could be achieved without referring to very generic "catch-all-clauses" that, in turn, would be incompatible with the Principle of "lex certa".

Research exemptions in export controls an ambiguous loophole

Export control legislation, another important instrument for the implementation of UNSCR 1540, also has difficulties when addressing research and academia. Dual Use export control legislation frequently applies exemptions for "fundamental" or "basic" research, undermining the effectiveness of such instruments in implementing UNSCR 1540 in relation to research and academia. In addition, inconsistent wording and definitions also raise challenging questions about the different remits of such exemptions. For example, inconsistent distinctions between "fundamental" and "non-fundamental" research, or between "basic" and "applied" research exist. Furthermore, in light of the lower thresholds for material and technology in which CBRN terrorism unfolds when compared to military CBRN programs, upholding such exemptions seriously undermines the value of export controls in the effective implementation of UNSCR 1540 in academic and research settings.

Political and economic interests

Effective implementation of UNSCR 1540 in research and academia also faces political headwinds due to substantial societal and economic interests in the promotion of research. Key areas of CBRN concern, such as biomedical research, synthetic biology, converging technologies, nuclear energy, new medical radiological equipment and therapies are also central in resolving current and future societal problems as well as ensuring prosperity. Regulating such technologies is usually equated with, at least, slowing down new developments and thereby contributing to a disadvantage for those affected by such regulations. These strong political interests have made the development of tools that mitigate the specific nature of CBRN risks in research and academia challenging.

> CBRN security sensitive research.....unfolds in a constantly and often rapidly changing environment.

Technical challenges

In addition to these general legal and political challenges, numerous technical challenges in the implementation of UNSCR 1540 in research also exist due to the lower material and technological thresholds at which such activities unfold.

For example, effective border control is frequently limited by the thresholds of the detection technology. For large shipments of chemicals and radioactive substances, a reasonable chance of being detected at borders can be assumed. Detection and identification of materials used in research is not only often complex but is challenging due to the small quantities and the need for low detection thresholds. Thus increasing the likelihood that smuggling will take place undetected.

Furthermore, sensitive CBRN security information can be transferred internationally by the Internet using modern encryption technologies, with little chance of detection by border control agents.

In the light of these weaknesses, it remains largely unresolved how "appropriate controls" can be developed (or put into place) in research and academic institutions.

CBRN SECURITY CULTURE

The concept of Nuclear Security Culture focused

on the human factor has been well established through the IAEA Nuclear Security Series No 7 [1]. This builds on similar approaches developed for nuclear safety. In the IAEA document, Nuclear Security Culture is defined as:

"The assembly of characteristics, attitudes and behavior of individuals, organizations and institutions, which serves as a means to support and enhance nuclear security."

At the June 2014 NATO sponsored Advanced Study Institute in Yerevan, Armenia[2], the possibility of extending this idea of security culture into the area of chemical, biological and radiological security was discussed. Specific questions regarding the role of professional ethics, fundamental rights such as academic freedoms or codes of conduct that relate to CBRN Security Culture were raised.

There was strong support among the experts from the varying disciplines that CBRN Security Culture is not only a viable concept to complement existing initiatives in CBRN security but that it could be especially valuable in mitigating risks arising from research and academia. Since it builds on organizational and management structures, the introduction of CBRN Security Culture in research and academia will, however, have to take into consideration the organizational and management structures at these types of institutions. This might differ from the organizational and management structures underlying the Nuclear Security Culture concept and, therefore, may warrant some amendments to the concept applied in the nuclear context. Nonetheless, CBRN Security Culture provides an important additional risk mitigation approach that complements other important measures in UNSCR 1540 implementation.

CBRN Security Culture is not only a viable concept to complement existing initiatives in CBRN security but that it could be especially valuable in mitigating risks arising from research and academia.

CBRN SECURITY CULTURE AS A TOOL IN OVERCOMING CURRENT GAPS IN EFFECTIVE UNSCR 1540 IMPLEMENTATION IN ACADEMIC AND RESEARCH INSTITUTIONS

Criminalization, export and border controls, three key elements in UNSCR 1540 implementation, face substantial challenges in handling CBRN risks arising from research and complementary measures are urgently needed.

Over the last ten years numerous codes of conduct (CoC) have been developed by different institutional, national and international sponsors to address the issue of CBRN security in research. Many of these CoC have been purely aspirational, thereby often providing little operational guidance on how to accomplish the goal of CBRN security. As a consequence, professional security ethics equipped with practical tools to accomplish the goal of CBRN security in research and academia is still in its infancy.

In no other area of CBRN security is the human factor of such central importance in ensuring security

1 IAEA Nuclear Security Series No. 7: Nuclear Security Culture http://www-pub.iaea.org/MTCD/publications/PDF/Pub1347_web.pdf

2 The NATO sponsored Advanced Study Institute on CBRN security culture was a major international event in the series of workshops, training sessions and briefings organized by the Center for International Trade and Security at the University of Georgia, USA. Other partner organizations for the Yerevan event included UNODA, OSCE, STCU (Science and Technology Center in Ukraine), ICCSS (International Center for Chemical Safety and Security) and others. Over 50 international experts focused on developing a road map for CBRN culture promotion by synthesizing the experience accumulated by governments, industries and academia into comprehensive and universally applicable good practice tools and models that would be based on shared principles and approaches in these four domains. A major goal was not only to promote the CBRN security culture concept but also introduce compatible assessment and enhancement methodologies.

than in research and academia. Approaches, such as CBRN Security Culture, that focus on increasing security through enhancing attitudes and behaviors therefore provides a sensible approach to overcome some of the previously mentioned limitations. If embedded in collective self-governance, for example, CBRN Security Culture reduces fundamental rights concerns frequently associated with the introduction of prohibitive or restrictive legal measures on research. In addition, it provides a framework to include a new group of stakeholders into the governance of CBRN threats, by actively including civil society actors (e.g. researchers, academics, private enterprises) and take advantage of their individual and collective self-governance capacities and risk management know-how.

Nonetheless, future work is needed to transform CBRN Security Culture from the conceptual to the operational level. For research and academia this will require at the macro-level the development of practical mechanisms to resolve conflicts between security and other viable individual and societal interests. While at the micro-level it will require the development of tailored tools and monitoring concepts (e.g. for self-assessment) that take into account, not only the specific institutional setting of academia and research, but also the specific nature of the risks.

EXCELLENCE IN SCIENCE AND EXCELLENCE IN SECURITY

There is no good science without good ethics and if ethics is about reducing harm, security must be part of ethics. It follows that security considerations must therefore be integral elements in good science. To ensure that security considerations are integrated in research two elements are of key importance: training and education on the one-hand and oversight on the other-hand.

With regard to training, numerous initiatives have been launched in the last years to integrate security considerations into the training of researchers. For example, at the University of Vienna, for many years I have been teaching a course on laboratory safety and security. The course integrates chemical, biological and radiological safety and security in one training module. The development of such comprehensive training curricula is of special interest for the area of life sciences where chemical, biological and radiological risks often co-exist within one organizational unit.

Furthermore, security funding institutions have started to include CBRN security assessments into their funding scheme. As an example, the European Commission requires researchers in its research funding programs to take into account and carry out a self-assessment of CBRN security issues when writing up their research proposals. CBRN security (as well as safety) issues are also included into the proposal assessment during the so-called Ethics scrutiny process, in which independent experts (including security experts) participate.

Developing, operationalizing and implementing CBRN Security Culture as a practical tool to address the human factor in CBRN security sensitive research will not only support educational and training activities, but also provide funding institutions with clear behavioral and management standards in funding CBRN security sensitive research, thereby ensuring that excellence in science goes hand-in-hand with excellence in security.

CONCLUSIONS

Although UNSCR 1540 provides for a wide ranging set of tools to address CBRN threats by non-State actors, it contains serious gaps in managing the risks arising from research and academia. CBRN Security Culture, understood as a management and organizational system that focuses on the human factor, provides a new avenue to overcome current challenges and gaps in the implementation of UNSCR 1540 at academic and research institutions.

By focusing on the human factor and adding capacities of individual and collective self-governance of civil society and enterprises, CBRN Security Culture can provide a new and complementary element to the existing tool set of UNSCR 1540 implementation. Engaging in all available options to implement 1540 will be essential to effectively counter the complexity of the CBRN threat by non-State actors.

ACKNOWLEDGMENT

The author acknowledges the support provided by James H. Houghton, Dana Perkins, Malcolm Dando and Monique Ischi in the preparation of the manuscript.

Stakeholders Partnership for Nuclear Security: A Success Story

William W. Keller
DIRECTOR, CENTER FOR INTERNATIONAL TRADE AND SECURITY, UNIVERSITY OF GEORGIA, USA

Heru Umbara
HEAD OF THE CENTER FOR INFORMATICS AND NUCLEAR STRATEGIC ZONE UTILIZATION, NATIONAL NUCLEAR POWER AGENCY, INDONESIA

Khairul Khairul
DIRECTOR, CENTER FOR SECURITY CULTURE AND ASSESSMENT,
NATIONAL NUCLEAR POWER AGENCY, INDONESIA

This article outlines a successful trilateral cooperation between a non-governmental organization in the United States, a nuclear operating agency in Indonesia, and a UN institution in achieving their common goal of improving global nuclear security. In particular, it highlights how the Center for International Trade and Security (CITS) at the University of Georgia collaborated, in coordination with the International Atomic Energy Agency (IAEA), with Indonesia's National Nuclear Energy Agency (BATAN) in promoting good nuclear security culture practices nationally and internationally. As a result, Indonesia is now considered a success story and a role model for other countries to follow in this realm. Through a number of workshops, outreach events, and personal engagements within Indonesia and the Southeast Asian region from 2010 to 2012, the three stakeholders laid the groundwork for better nuclear security awareness and culture. The ultimate objective of Indonesia's program for security culture and assessment is to be a regional leader in the area of nuclear security culture promotion, assessment, and enhancement. It will require the improved skills of the core group of BATAN's experts and close cooperation with Gadjah Mada University, Indonesia's leading university for training nuclear professionals.

SECURITY CULTURE AND THREAT ENVIRONMENT

Both the human factor and security culture are critical components in ensuring the security of nuclear facilities, infrastructure and transport – their importance cannot be overestimated. To reflect that, the IAEA and the international experts have developed the concept of nuclear security culture and its implementing guide, which was published by the IAEA in 2008 under the Nuclear Security Series No. 7. The importance of nuclear security culture has also been recognized by the three nuclear security summits in 2010, 2012, and 2014, and included in the final communique and summit recommendations as one of the most important factors.

Indonesia operates three nuclear research centers for a wide variety of peaceful purposes. BATAN operates these three nuclear research reactors in addition to another radioactive source facility. BATAN's nuclear research centers are located in Bandung, Yogyakarta, and Serpong; the source facility is located at Pasar Jum'at Jakarta, SSDI, at BATAN Head Office in Jakarta. In 2001 and 2007, Indonesia invited IAEA-International Physical Protection Advisory Services (IPPAS) whose mission is to determine the security level at those nuclear research reactors. The IPPAS reports submitted to Indonesia's government emphasized that BATAN should promote nuclear security culture as a prerequisite of effective and sustainable physical protection.

Security conscious nuclear personnel were recognized by BATAN leadership as a priority course of action because of growing terrorist threats in the region. Terrorist incidents in East Asia and the Pacific have recently shifted from large-scale bombings of high-profile soft targets to smaller and more defuse attacks directed at domestic and foreign institutions as well as elements of industrial infrastructure. The list of past terrorist attacks includes a bombing outside the J.W. Marriott Hotel in Jakarta (August 2003); a car bomb detonated in front of the Australian Embassy (September 2004); a triple suicide bombing attack in Bali (October 2005) and others. The most recent incident happened in October 2012 when Indonesia's anti-terror unit uncovered a plot to attack the U.S. Embassy, a U.S. consular office, a mining company, and a site near the Australian Embassy.

Border security and the prevention of the illegal crossing of terrorists is especially challenging for Indonesia, given that the country is composed of more than 17,000 islands and has numerous points of entry by land, sea, and air. Monitoring remote locations among the thousands of islands in the Sulawesi Sea and Sulu Archipelago that spans the boundaries between Indonesia, Malaysia, and the Philippines is extremely difficult, which makes this tri-border area well-suited to terrorist activities, including movement of personnel, weapons, explosives, and funds.

A major input in recognition of the vital role of security culture came from the Center for International Trade and Security (CITS) at the University of Georgia (USA) which engaged, at that time, both BATAN and BAPETEN (Indonesia's nuclear regulatory authority) in a nonproliferation and security awareness raising program funded by the Carnegie Corporation of New York (CCNY). CITS staff demonstrated at BATAN hosted events a unique expertise, particularly in nuclear security culture, due to CITS fellows' participation in developing the IAEA Implementing Guide for Nuclear Security Culture, which was published in 2008 as its report No. 7 in the Nuclear Security Series.

SELF-ASSESSMENT PILOT PROJECT

In 2010, the Chairman of BATAN formally recognized the importance of nuclear security culture and demonstrated BATAN's commitment to its enhancement at the facility level. To support the dissemination of the IAEA Implementing Guide, BATAN, in cooperation with the IAEA, held the "Regional Workshop on Nuclear Security Culture" at PTAPB-BATAN, Yogyakarta in December 2011. CITS staff participated in this workshop and continued to strengthen its relationship with nuclear security practitioners in Indonesia.

In mid-2012, the IAEA developed the first draft of a guidance document for self-assessment of nuclear security culture. CITS Experts who were involved in drafting the guidelines offered BATAN to put to the test the draft self-assessment methodology at BATAN's three nuclear research reactors.

In the course of internal deliberation, BATAN experts identified several specific benefits that the self-assessment project could generate and recommended

A joint IAEA & CITS-UGA team visit to Yogyakarta reactor site in October 2012 to brief management on the self-assessment methodologies

the acceptance of the offer. It was becoming clear that such benefits would go well beyond the traditional scope of security. Results were expected to improve understanding of employees' concerns, needs, aspirations, and motivation; clarify employee opinions about key management issues; build a link to safety culture assessment and synergize mutual benefits, etc. In light of these diverse benefits, BATAN decided to invest its time and budgetary resources into the self-assessment project.

In the fall of 2012, BATAN leadership sent a letter to the IAEA Office of Nuclear Security announcing its decision to conduct nuclear security culture self-assessment using the IAEA draft guidance. Objectives included testing the draft and giving feedback to the IAEA about the results. BATAN viewed the assessment as a particularly useful contribution to better security due to Indonesia's threat environment and past incidences of terrorism. Testing the draft guidance offered the organization the opportunity to measure the improvement in the level of security culture in its facilities following the IAEA workshop and the BATAN culture outreach efforts of 2010. In October 2012, CITS experts briefed self-assessment teams at three nuclear research reactors in Serpong, Bandung, and Yogyakarta on the draft methodology for performing self-assessments. The IAEA was present and played a critically important role. Encouragement and support also came from the U.S. Partnership for Nuclear Security (PNS). BATAN agreed to follow the multi-stage self-assessment processs during the trial as recommended in the draft technical guidance.

BATAN employees fill in survey forms for the self-assessment project

BATAN's self-assessment of nuclear security culture at its three nuclear research reactors from October 2012 to March 2013 was the first attempt to test the emerging IAEA methodology. In this process, the self-assessment teams (composed of 41 people) surveyed 624 employees and interviewed 128. They developed and analyzed 87 histograms and accumulated more than 500 pages of data. In March 2013, IAEA and CITS experts visited Jakarta to assist BATAN in reviewing the results of the self-assessment pilot project.

MAINTAINING THE MOMENTUM

The preliminary results of the self-assessment pilot projects were presented by the Indonesian delegation in April 2013 at the IAEA Technical Meeting on Security Culture Self-Assessment Methodologies. This week-long event with the participation of about 30 member states focused on Indonesia's experience as a source for improving the IAEA existing drafts. A more detailed analysis included in the joint BATAN-CITS paper "Nuclear Security Culture in Practice" was presented at the IAEA Conference on Nuclear Security in July 2013 (Vienna, Austria). Widely publicized, Indonesia's pioneering experience served as an example followed by other countries. One of them is Bulgaria which volunteered in 2013 to conduct a project on self-assessment for security culture at its Kozloduy Nuclear Power Plant. This time, the briefing team in Bulgaria included IAEA, CITS and BATAN experts.

In the meantime, there are indications of increasing interest in security culture among Indonesia's practitioners and scholars. For example, several faculty members of the Gadja Mada University (GMU) visited CITS in 2013 for a two-day briefing on nuclear security culture as a major component of the nuclear security syllabus which is currently under development. GMU has recently joined the IAEA International Nuclear Security Education Network (INSEN) and established an INMM chapter for its students. As a result of at least two dedicated workshops organized in Jakarta by BATAN and CITS, security culture is increasingly recognized as a management tool by other Indonesian agencies outside of the nuclear community.

Collaboration is underway between BATAN and CITS to lay the groundwork to assess security culture for users of radioactive sources. In March 2014, BATAN and CITS released, under a grant from the Carnegie Corporation of New York, a report "Human Dimension of Security for Radioactive Sources: From Awareness to Culture." This report which was prepared prior to the 2014 Nuclear Security Summit in the Hague offers recommendations to adjust the IAEA security culture methodology to the specific needs for the safe and secure operation of radioactive sources.

A WAY FORWARD

After establishing the baseline for nuclear security culture assessment, BATAN leadership made an important decision to institutionalize this expertise by establishing a Center for Security Culture and Assessment (CSCA). Indonesia's Progress Report submitted in March 2014 to the Hague Nuclear Security Summit refers to the CSCA establishment as a joint initiative with the Center for International Trade and Security at the University of Georgia. CSCA goals are a) promoting through research, training and outreach events a better understanding of the important role that culture plays in shaping security; b) conducting, in collaboration with the IAEA, self-assessment projects of nuclear and radiological security culture at relevant facilities both in Indonesia and in neighboring countries; c) utilizing BATAN's expertise in self-assessment of nuclear security culture to share best practices with counterparts in the chemical and biological domains; d) supporting and enhancing the building of international and interdisciplinary relationships and initiatives with relevant stakeholders that can create new opportunities for combating global security concerns; and e) collaborating with established Nuclear Security Support Centers and EU Centers of Excellence to provide holistic expertise to stakeholders in the CBRN fields.

The formal inauguration event for the CSCA is scheduled at the conference "Promoting Security Culture in South East Asia" in Serpong (September 29-October 1). The CSCA Office will be located in building 90 at the Serpong Office of BATAN and operated under the Center for Utilization of Informatics and Strategic Nuclear Area (PPIKSN). Its programmatic activities in the next years will include:

1. A training workshop on nuclear security culture for nuclear professionals and academics from Indonesia, Malaysia, Thailand, Vietnam and other countries in the region.
2. Joint projects on security culture assessment for users of radioactive sources in ASEAN countries.
3. An intensive training course on nuclear security for faculty members and students of Gadja Mada University.
4. A new self-assessment project at one or two BATAN research reactors based on the lessons learned from the 2012-2013 pilot assessment project and on the updated IAEA methodology.
5. A train-the-trainer workshop on nuclear security culture assessment and enhancement.

CONCLUSIONS

As a result of carefully coordinated initiatives of the three stakeholders: a non-government organization in the United States (CITS), a nuclear operating agency in Indonesia (BATAN), and a UN specialized agency (IAEA), progress has been made not only in raising nuclear security awareness in a key regional country but also in contributing to this country becoming a hub of unique international expertise. The long-term goal of achieving sustainable nuclear security in Indonesia and the region will certainly require continued efforts and support from these and other stakeholders. The roots of this success story can be largely attributed to the dedication of the core group of BATAN leadership and experts, continuous IAEA engagement as well as the unique professional skills of CITS experts. Combined together they produced the desired result. Now that nuclear security culture has been recognized internationally as an important priority, this success story deserves to be closely scrutinized and perhaps reconstructed in other regions of the world where an acknowledged regional leader in nuclear security could be in a position to demonstrate the benefits of its expertise, collaborate with its neighbors and set higher standards of nuclear security.

UNSCR 1540 and Export Control:
How High-Tech Business Can Cope and Comply

Gary Bertsch
FOUNDER AND CHAIRMAN, TRADESECURE LLC, USA

In the global fight against the proliferation of weapons of mass destruction (WMD), high-technology firms pose significant challenges due to their products' applicability to WMD development. The next step in controlling WMD-related exports falls upon business leaders around the world. Business's commitment to trade and technology transfer compliance is essential in completing the process started by United Nations Security Council Resolution (UNSCR) 1540.

UNSCR 1540 demands that governments develop, establish, review and maintain effective national export and trans-shipment controls on items and technology that can contribute to WMD proliferation. States are required to take all appropriate measures to strengthen national export controls and to control access to intangible transfers of weapons-related technology and information that could be used for WMDs and their means of delivery.

The next step in controlling WMD-related exports falls upon business leaders around the world.

National governmental efforts and progress have been extensive in recent years. Yet governmental action cannot fully control the spread of dual-use items and technologies which contribute to WMD proliferation. While the actions of national governments are necessary, significant, and even critical, they are of limited value if their industries and businesses involved in dual-use trade and technology transfer do not comply. This article examines what is being and can be done regarding the critical role of businesses in high-tech trade and nonproliferation.

Most proliferation cases involve the selling and buying of dual-use items with both civil and military applications. National export control laws and regulations have now been set up in most states that require exporters to comply with national laws and international norms governing strategic trade. Most exporters do comply, but the minority that does not can cause considerable harm.

Small, medium, and large businesses can all be sources of proliferation technology. However, large MNCs actively involved in international high-tech trade are generally well informed about the regulations and need for compliance. Small and medium sized businesses, and rapidly growing companies in the emerging economies, are often not. More must be done to inform and prepare these businesses for proliferation dangers and their responsibilities.

Fortunately, numerous governments are involved in industry outreach programs intended to promote awareness and best practices in strategic trade management and control. The U.S. Department of Commerce offers an annual Export Update conference in Washington, DC and regular regional conferences and seminars attended by many thousands of business representatives each year. The U.S. government also sponsors programs abroad intended to promote awareness and compliance in emergent and other economies. The European Union and European national governments sponsor similar programs, as do many OTHER governments such as China and Japan. These governmental efforts are critical, but they cannot stop proliferation alone. Governments lack the time and resources to build awareness and ensure strategic trade compliance in the millions of businesses across the globe.

Hence the need for business responsibility, and the responsibilities are considerable. Businesses must ensure their employees are aware of domestic nonproliferation-related laws and regulations, which are often exceedingly complicated. Given the nature of contemporary global trade and technology transfer, they must not only be conscious of their national regulations at home, but also the rules and regulations of those of countries abroad. Business leaders must make certain that their employees are informed, responsible and compliant with these regulations. If they are not, serious proliferation can result, and the responsible

individuals and companies will suffer severe penalties and loss of reputation.

What Do Governments Expect of Business?

Governments have outlined what businesses should do to promote strategic trade compliance. These requirements have coalesced into what are increasingly called global best practices. These internationally-held standards offer an archetype for which businesses should aspire to in their implementation of dual-use trade compliance.

First, they should implement internal compliance programs (ICP). Correct ICP implementation begins with a business's leadership. Upper management must make a written commitment to their business, enshrine best practices for operations, and allocate the necessary resources to achieve those standards. Leadership serves as the lynchpin for effective compliance.

As management establishes a "culture of compliance," continuous risk assessment for proliferation-related exports must follow. The business should create a manual of standard operating procedures against which corporate policies must be routinely compared. While this covers the business policy side of compliance, employees must also be kept updated on the constantly shifting regulatory environment. On-going training and awareness initiatives are essential in making sure all members of a business understand their role in maintaining compliance.

Merging Culture and Compliance

Businesses must be acutely aware of their trade-related operations. Export control demands careful vetting of employees, customers, end-users, and transactions. Businesses must take the initiative in minimizing their exposure to proliferation risks. Thorough record-keeping accompanies constant screening in order to verify a company's and its partners' insistence on fostering compliance.

Even in the most tightly-run compliance program, problems may arise regardless. To counteract these, routine internal and external audits are necessary. Businesses should always be monitoring their compliance. Audits examine operations in-depth and may uncover previously hidden or unnoticed violations.

UNSCR 1540 has motivated a large number of governments to enact laws and provide guidelines outlining exporters' nonproliferation responsibilities. But it is the responsibility of business to internalize these guidelines, and proactively hedge against violations within their own operations.

What Should Businesses Do?

First, they should build "cultures of compliance". The inherent difficulty of internal compliance and controlling exports stems from humans involved in business. Controlling the uncertainty of the "human factor" depends predominantly on the business's culture of compliance, a subset of greater organizational culture. A pervasive, non-complacent attitude must radiate from the upper management of a business. Leaders and management set the tone for the organization, and air-tight compliance requires every employee's attention and awareness. To set this tone, the management must codify a set of standards for the organization, along with an overall plan, standard operating procedures, and contingencies. By establishing a business's vigilant approach to compliance, creating an effective internal compliance program is more likely to succeed.

Second, high-tech businesses involved in strategic trade and technology transfer should build "internal compliance programs" (ICP). ICP is the framework through which a business mitigates the risks from potential proliferation-related exports. An ICP includes: a corporate policy statement regarding nonproliferation and management's commitment to this statement; organizational structure, policies and procedures concerning compliance; training; record keeping; auditing; and contingencies for reporting. As government punishment grows harsher due to the myriad dangerous applications of many modern technologies, businesses will find their investments in compliance producing long-term benefits.

Third, businesses involved in strategic trade should seek any available assistance to build their cultures of compliance and ICPs. Expert help allows businesses to stay abreast of the national and international rules and regulations related to their high-tech business. While industry struggles with regulations, governments do not have the time and resources to work directly with all the entrepreneurs and businesses needing assistance. Nevertheless, hundreds of nonprofits, NGOs, and for-profits specialize in providing such support.

For decades I directed a university-based center involved in this work. We found considerable demand for and interest in our work. Although not all businesses and governments were receptive, our dominant experience was that most countries and businesses wanted and appreciated our help. We organized, delivered, and participated in hundreds of industry outreach seminars and programs preparing companies for strategic trade compliance in dozens of countries around the globe. When our assistance was requested, we would work with individual companies to develop tailored solutions.

One of my most exemplary experiences was with a large state-owned enterprise (SOE) in China. The former Chinese leader Deng Xiaoping disbanded the Ministry of Ordinance, and in 1980, spun out an SOE called China North Industry Corporation (NORINCO). NORINCO grew and diversified rapidly, becoming a global marketing company. In the early 2000s, it ran afoul of the US government for allegedly exporting WMD related items to proscribed states. The US government sanctioned NORINCO, ordering it to cease conducting business in the United States. In response, NORINCO approached the University of Georgia (UGA) in 2006 for advice and assistance. The UGA Center for International Trade and Security (CITS/UGA) informed them about US extraterritorial and international laws and regulations. Further assistance included establishing internal compliance programs, building a corporate culture of compliance and keeping their relevant personnel informed of global regulatory developments and changes. Such fruitful relationship with NORINCO continues through the present day. NORINCO's ICP and commitment to compliance allowed the company to re-enter the US market and expand its business globally.

CITS/UGA has also worked with small and medium sized businesses. Their regulatory staff is more limited and their needs are often great. Smaller businesses often have no experience, and little to no staff and expertise, in dealing with government regulations. Many are involved in producing, selling and transferring dual-use items and technology of significant WMD application without sufficient safeguards. Ignorance is no defense if controlled technologies fall into the wrong hands; the punitive consequences can financially dismantle a business. NGOs, nonprofits, and for-profits can help companies avoid these costly mistakes.

Expertise is abundant for businesses cognizant of their compliance shortfalls. Later on, a group of retired faculty members created a service called TradeSecure, LLC. We work directly with companies to inform them of their nonproliferation responsibilities, build ICPs and cultures of compliance, and inform them of regulatory changes and challenges.

The nexus of TradeSecure's work has been in emerging economies. Many of these companies are quickly "going global" while having little experience with or knowledge of dual-use, nonproliferation trade regulations. Whether foreign or domestic, a major telecommunications firm or small microelectronics business, we have been pleased to work with their compliance officers to cultivate their cultures and programs in accordance with UNSCR 1540's mandate.

Even General Electric (GE), one of the world's most advanced and respected companies, came to TradeSecure seeking assistance in their efforts to stay ahead of the national regulations mandated by UNSCR 1540. TradeSecure worked with GE to develop a database giving

A view of the Port of Singapore

them and other companies 24/7 access to 34 fields of critical regulatory information—including controls lists, sanctions, licensing, etc. —for 60 of the world's major trading nations. Companies can access this database—*Accelerator by TradeSecure*— through a web portal around the globe. The database and TradeSecure assistance can help keep businesses up-to-date with regulations of strategic import.

Most crucially, TradeSecure and the companies we work with discovered that compliance efforts are ultimately an advantage for business. Creating compliance programs is seen by some, mistakenly, as a cost. In reality, a compliance program is a wise investment with considerable benefit. Companies "playing by the rules" engender the trust and respect that generate positive reputations and good business. Academic research and global experience shows that compliant companies get more business and make more money. GE and NORINCO are models of this reality.

CONCLUSIONS

UNSCR 1540 motivated governments to establish nonproliferation rules and regulations, yet proliferation's risk persists. Governments must mandate their high-tech, dual-use industries and trading companies to comply with these regulations, and they should give them all the help and guidance possible. But when their time and resources fall short, the relevant governmental authorities should encourage their strategic trade businesses to seek out NGOs, nonprofits, and for-profits that can help ensure compliance with UNSCR 1540 related laws and regulations. Such businesses involved in dual-use, WMD-related trade and technology transfer must recognize their responsibilities, seek outside help when necessary, and build strategic trade compliance programs. By complying, business will promote their commercial interests, restrict the spread of WMDs, and contribute to a safer, more prosperous world.

Realizing the Hybrid Control Concept

D. J. van Beek
CHIEF DIRECTOR, NON-PROLIFERATION, DEPARTMENT OF TRADE AND INDUSTRY, AND HEAD OF THE SECRETARIAT TO THE SOUTH AFRICAN COUNCIL FOR THE NON-PROLIFERATION OF WEAPONS OF MASS DESTRUCTION

Export control lists are essential components of global nonproliferation efforts, literally defining the materials, equipment, and technology that must be controlled. They are formulated with tremendous deliberation and technical precision in an effort to control the most essential goods while minimizing impact on legitimate trade. Control lists are the language of export control. Adopting control lists consistent with international norms has been recognized as an effective practice. The Hybrid Control Concept does not seek to supplant these control lists, but to facilitate their adoption and implementation by countries with very limited relevant trade flows.

Countries unfamiliar with export control lists will nevertheless be familiar with the Harmonized Commodity Description and Coding System (HS), the internationally standardized system of names and numbers for classifying traded products. It is used by almost all countries of the world. Many attempts have been made to develop so-called correlation tables mapping HS codes to export control list entries and vice versa, and those efforts have revealed fundamental challenges in relating the two systems. These challenges are summarized in this paper. Even if a useful correlation table could be made, it would not solve the language problem separating the export control community from the trade community. Giving a correlation table to a customs administration and expecting customs officials to control the items listed on export control lists would be like handing a Chinese-English dictionary to an English speaker and expecting him to speak Chinese.

Recognizing the problems inherent to devising and using correlation tables, many people who care about trade control have suggested that the HS should be reformed. But hoping for such reform is unrealistic. The hybrid control concept[1] proposed by van Beek is an attempt to adapt the control lists to the HS rather than expecting the HS to adapt to the control lists. However, several challenges associated with correlating export control lists and the HS could complicate implementing the hybrid approach.[2]

This article recaps the hybrid control concept, summarizes the major challenges encountered when developing correlation tables, and finally evaluates whether or how the hybrid approach could handle each of these challenges.

THE HYBRID CONTROL CONCEPT

The hybrid control concept, first proposed at a Workshop on the Implementation of UNSCR 1540 for African States in 2012, tries to accomplish two fundamental objectives: to simplify implementation of control lists by focusing effort on those controls relevant to the trade flows a country actually sees, and to express those controls in the context of the HS that the trade community actually uses.

Implementing the hybrid control concept would require two related efforts:

- **Trade analysis** to determine which HS codes are frequently used and which are seldom or never used. This could be done at the national level or with finer resolution for particular border crossings, ports, or routes.

- **Control list analysis** to determine which HS codes potentially cover items subject to export control, understanding that those HS codes would also inevitably encompass non-controlled items as well.

1 D. J. van Beek, "A Practical Way to Implement Export Control Lists in Developing Countries," *1540 Compass* Issue 4, University of Georgia Center for International Trade and Security.

2 See, for example, the World Customs Organization's Strategic Trade Control Enforcement Implementation Guide, <http://www.wcoomd.org/en/topics/enforcement-and-compliance/instruments-and-tools/wco-strategic-trade-control-enforcement-implementation-guide.aspx≥. Annex IV of this guide identifies several specific correlation problems.

For heavily used HS codes, indicating extensive trade in the goods classified under those codes, control lists entries associated with those HS codes would be implemented verbatim. For rarely used HS codes, however, there would be no need to expend the effort[3] associated with implementing the full technical precision of the control lists, and instead *all* trade in those goods (which would be minimal) would be subject to control.

	Frequently used HS codes	Rarely used HS codes
HS codes covering items subject to export control	CONTROL LIST Implement control lists precisely under these HS codes. Trade falling under these HS codes needs to be evaluated in relation to the control lists to distinguish the controlled items from the uncontrolled items that will also be caught by these HS codes.	CONTROL ALL Subject *all* trade falling under these HS codes (which is minimal) to export control.
HS codes not associated with export control	EXPEDITE Expedite trade falling under these HS codes since they are high volume but not of concern.	NO ACTION No action required. These goods are not traded and they are not subject to control.

The end product of the hybrid approach would be a list of HS codes, some calling for control of all trade falling under those codes and some calling for control according to regime control lists. It is important to note that all regime-listed items would still be under control using this approach, but control would be applied more simply where trade is minimal.

CORRELATION CHALLENGES

The control-list analysis mentioned above may encounter many of the same problems that have plagued correlation efforts. The HS is organized into 21 sections and 97 chapters, accompanied by general rules of interpretation and explanatory notes. The system comprises a set of six-digit codes, with the first two digits designating chapters, starting with crude and natural products and then moving on to manufactured products of increasing complexity. The first four digits are referred to as headings, with the final two digits defining subheadings. Subheadings must be interpreted in the context of the heading and chapter under which they fall.

By comparison, control lists are not designed as a system of classifying goods. They define controls on goods rather than goods themselves, and are often organized according to the function of the goods. Some controls are open-ended or specific based on function, while others are highly specific, making distinctions based on multiple technical variables.

Since the HS is based on the state of processing or value added while strategic goods are identified by their use and technical specifications, efforts to correlate the HS with strategic-goods control lists have not been completely successful. A brief examination of any of the existing correlation tables indicates a many-to-many relationship. Investigating these many-to-many relationships reveals several specific correlation problems:

3 One of the principal reasons behind the technical precision of the control lists is to minimize impact on legitimate trade. Where there is minimal trade anyway, this impact is moot.

- **Some controls do not identify specific goods.** For example, some controls are based on function, or they may use terms like "usable in" or "specially designed for." It is not always clear what specific commodities are covered by such a control.

- **Some controls identify several kinds or multiple forms of goods**. For example, many of the controls on metals specify not only the metal but also alloys, compounds, manufactures, waste, and scrap forms of those metals, corresponding to many different HS codes.

- **Some controls are narrowly defined based on technical specifications** not used in the HS. The HS code corresponding to these controlled items will generally also encompass many uncontrolled items that don't meet the control specifications.

- **Some controls overlap** such that a commodity falling under a certain HS code could fall under various controls depending on technical specifications or intended use. For example, titanium tubes fall under HS 8108 ("Titanium and articles thereof..."), but, depending on their purpose and technical specifications, those tubes may be controlled as titanium alloys, as centrifuge rotor tubes, as heat-exchanger tubes, or not at all.

- **Some controls apply to goods not explicitly included in the HS**. Many strategic items get classified as "Other" under the most suitable HS heading or subheading. As a result, these "Other" classifications often encompass multiple strategic items as well as many non-strategic items.

- **Structural incompatibilities between the two systems.** In some cases, the organizing approach of the HS fundamentally differs from the basis for control. For example, miraging steels are defined by their production process and composition, and their control specifications are based primarily on strength. But HS Chapters 72 and 73 do not distinguish steels based on their physical properties, but on their chemical composition and form. There is no way, using the HS codes, to distinguish miraging steels from other alloy steels.

- **Technology controls.** Export controls generally apply to technology required for the development, production, or use of controlled items. Tangible exports of technology are classified under HS according to the physical media (e.g., printed material, magnetic tape, etc.), while intangible transfers of technology are not classified under the HS at all.

HOW THE HYBRID APPROACH WOULD ADDRESS THE CORRELATION CHALLENGES

Before attempting to implement the hybrid control concept, it makes sense to consider how it will handle the challenges encountered in the development of correlation tables.

- **Some controls do not identify specific goods.**

Controls on control lists are sometimes based on the item's function, or the control language could contain regime language like "usable in" or "specially designed for." The following example, 1C101 from the European Union's dual-use list[4], illustrates this point:

It is not obvious what materials and devices might meet this control specification. According to the European Union's official correlation table, 1C101, correlates to the following HS codes: 282110, 320649, and 392099, defined by the HS as follows:

- 282110: Iron oxides and hydroxides
- 320649: ...putty and other mastics... — Other

4 EU 388/2012, <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2012:129:0012:0280:En:PDF>. <http://trade.ec.europa.eu/doclib/docs/2006/december/tradoc_131339.pdf>.

1C101 Materials and devices for reduced observables such as radar reflectivity, ultraviolet/infrared signatures and acoustic signatures, other than those specified in 1C001, usable in "missiles" and their subsystems.

Notes:
1. 1C101 includes:
   a. Structural materials and coatings specially designed for reduced radar reflectivity;
   b. Coatings, including paints, specially designed for reduced or tailored reflectivity or emissivity in the microwave, infra red or ultra violet regions of the electromagnetic spectrum.
2. 1C101 does not include coatings when specially used for the thermal control of satellites.

- 392099: Plastics and articles thereof ... Other plates, sheets, film, foil and strip, of plastics, non-cellular and not reinforced, laminated, supported or similarly combined with other materials ... —Of other plastics

These HS codes mainly include non-controlled items, but also the controlled ones.

After investigation of the various HS codes, it is possible that a most likely code emerges. However, this code would still contain many uncontrolled items. To assist decision-making it may help to assign a probability that this HS code may contain a controlled item as part of a decision-making model. A further factor to consider is whether these HS codes are frequently traded or not. This could simplify the problem again. If these codes are frequently traded, the actual regime control text should be used in the second part of the list under each identified HS code.

- **Some controls identify several kinds or multiple forms of goods.**

These items would correlate with many HS codes because the HS code structure separates different forms or processes. The following example illustrates this clearly:

This control correlates to many HS codes, including:

- Zirconium and articles thereof, including waste and scrap
- Germanium oxides and zirconium dioxide
- Other metal oxides
- Other fluorides
- Other chloride oxides and chloride hydroxides
- Hydrides, nitrides, azides, silicides, and borides, whether or not chemically defined
- Ceramic wares
- Ferro-alloys—Other

In this case zirconium, in various forms, with less than the naturally occurring amount of hafnium,

1C234 Zirconium with a hafnium content of less than 1 part hafnium to 500 parts zirconium by weight, in the form of metal, alloys containing more than 50% zirconium by weight, or compounds, or manufactures wholly thereof, waste or scrap of any of the foregoing.

Note: Item 1C234 does not control zirconium in the form of foil having a thickness of 0.10 mm or less.

is controlled. It is unlikely that common, naturally occurring zirconium compounds would be formulated using low-hafnium zirconium. Large-scale production of items made of zirconium sand, such as ceramics for domestic purposes, could also be excluded because they would not be produced from refined zirconium metal—zirconium from which the hafnium content had been removed. In this case the HS code covering zirconium and articles thereof, while still including uncontrolled zirconium, would be much more likely to correspond to controlled zirconium than would the other codes, which may not indicate zirconium at all. The uncertainty would be drastically reduced.

- **Some controls are narrowly defined based on technical specifications not used in the HS code system.**

The HS code corresponding to these controlled items will generally also encompass many uncontrolled items that don't meet the control specifications. The case of high-energy storage capacitors is a good example:

The best correlation to use in the HS system would be: 85322x–Other fixed capacitors. It should be noted that the vast majority of capacitors falling under this correlated subheading will not meet the control specifications of 3A001.

In the hybrid approach, if this HS code is not frequently traded, then all trade under this HS code would be flagged as abnormal. However, if this HS code is frequently traded, then the precise export control language would be used to specify which capacitors would be controlled and subjected to a risk-based procedure to prevent unnecessary delays through customs.

- **Some controls overlap, such that a commodity falling under a certain HS code could also fall under various other controls depending on technical specifications.**

Commodities that may fall under multiple controls result in multiple correlations. For example, titanium tubes falling under HS heading 8108 (titanium and articles thereof) could be controlled under 1C002.b.3 (titanium alloys), 1C202 (titanium-alloy cylinders and tubes meeting certain strength and dimensional specifications), or 2B350.d (heat exchangers ... and tubes ... designed for such heat exchangers ... made from any of the following materials: ... 7. titanium or titanium alloys).

Under the hybrid approach, if HS 8108 is frequently used, all of these controls would need to be included in the precise export control language to clearly specify what titanium articles must be subjected to controls. But if titanium is not commonly traded, and HS 8108 is infrequently used, then all such trade would be subjected to control.

- **Some controls apply to goods not specifically included in the HS.**

Many controlled items do not specifically or explicitly appear in the HS, so they get classified as "Other" under the most suitable heading or subheading. This results in some of these "Other" classifications' encompassing many strategic items and many non-strategic items. A good example is HS heading 8479 (Machines and mechanical appliances having individual functions, not specified or included elsewhere ...), which encompasses a significant number of strategic goods.

3A001 a. Capacitors with a repetition rate of less than 10 Hz (single shot capacitors) having all of the following:

1. A voltage rating equal to or more than 5 kV;
2. An energy density equal to or more than 250 J/kg; and
3. A total energy equal to or more 25 kJ;

b. Capacitors with a repetition rate of 10 Hz or more (repetition rated capacitors) having all of the following:

1. A voltage rating equal to or more than 5 kV;
2. An energy density equal to or more than 50 J/kg;
3. A total energy equal to or more than 100 J; and
4. A charge/discharge cycle life equal to or more than 10,000;

In general, frequently traded commodities do get specific HS codes, and these "Other" codes tend to relate to infrequently traded goods. Hence, customs may be generally more interested in scrutinizing such shipments. Under the hybrid approach, where these "Other" codes are frequently used, all relevant controls would need to be included in the precise export control language. If trade under these codes is low or nonexistent, the HS heading could be subjected to control, with the understanding that many uncontrolled commodities may also fall under those codes.

- **Structural incompatibilities exist between the two systems.**

In some cases, the organizing approach of the HS fundamentally differs from the basis used for the export control lists. This can result in excessive correlations or an absence of suitable correlations. The case of miraging steels demonstrates this case well. Miraging steels are defined by their production process and composition, while their control specifications are based primarily on strength. According the correlation tables, these controls correspond to dozens of HS codes in Chapters 72 (Iron and steel) and 73 (Articles of iron and steel).

These chapters are organized according to the physical forms of the material (flat-rolled products, bars and rods, wire, ingots, sheet, tubes, structures, tanks, chain, cables, etc.) rather than according to composition, physical properties, or method of production. Thus, many of the individual codes in these chapters could correspond to miraging steel or to very common alloy steels. There is no way using the HS codes to distinguish miraging steels from the rest.

In this case, it may be most helpful to apply the hybrid approach at the HS chapter level, and include all specialty steel controls if steel trade (i.e., trade under HS Chapters 72 and 73) is common, and to control all steel in cases where such trade is uncommon.

- **Errors linger in existing correlation tables.**

Beyond the fundamental and structural challenges which make correlations imperfect, in many cases the existing correlation tables simply contain errors. This may also be a result of an attempt not to leave any loopholes. As an example, TARIC correlates the following commodities to HS 8508 (Vacuum Cleaners):

- Filament winding machines
- Equipment ... for the production of propellant and propellant constituents
- Batch and continuous mixers
- Multi-stage light gas guns
- Chemical reaction vessels
- Heat exchangers
- Biological containment facilities
- Fermenters
- Automatic loading, multi-chamber, central wafer handling systems
- "Information security" test, inspection, and "production" equipment
- Equipment to produce, align, and calibrate land-based gravity meters
- "Robots" specially designed for underwater use

These errors already plague users of correlation tables and are not specific to the hybrid concept. These errors should be fixed, or at least identified, with the assistance of the various regime experts in conjunction with the correlation-list compilers. It is sometimes more helpful to identify the main correlation rather than all possible correlations.

- **Technology controls apply.**

Export controls generally apply to technology required for the development, production, or use of the controlled items. Tangible exports of technology are classified under HS according to the physical media (e.g., 4906 for plans and drawings and 8523 for discs, tapes, solid-state storage devices, smart cards, and other media). As a result, correlation tables relate these media-related HS codes to virtually all controlled items. Even worse, intangible transfers of technology are not classified under HS at all.

In developing countries where the hybrid approach may be more applicable, technology exports are unlikely to occur in any case.

CONCLUSIONS

The hybrid approach, even taking into account the various correlation problems, may be beneficial to a developing economy. Even where a normal control-list approach is used, some of the ideas expressed here may improve the current utility of correlation tables.

The following table summarizes how the correlation challenges could be addressed to ensure that the full intent of the original control list is implemented as far as possible.

The hybrid concept can greatly simplify adoption and implementation of strategic trade controls by countries with limited relevant trade, and also help to form a stronger basis upon which the licensing and customs authorities can discuss and facilitate export enforcement activities.

Correlation Challenge	Treatment under the Hybrid Approach	Assessment of the Implementation of the Hybrid Approach
Some controls do not identify specific goods.	Make use of the possible HS codes provided in the cross-reference lists.	No worse than the status quo. The problem is control-list based. The hybrid approach will not solve the problem posed by these ambiguous controls, which will require dedicated awareness-raising efforts if they are to be successfully implemented.
Some controls identify several kinds or multiple forms of goods.	These controls correlate to many HS codes. In the hybrid approach, that would potentially require repeating a control entry many times. It would be beneficial to differentiate strong/primary correlations from weaker/secondary ones.	No worse than status quo, but if this condition is common, it could weigh down the hybrid approach.
Some controls are narrowly defined based on technical specifications.	These controls tend to correlate to HS codes that also cover many uncontrolled items. If the HS code were associated with high trade volumes, the control would be implemented. If the HS code is not traded, the whole HS code would be subjected to control.	Not a problem.
Some controls are overlapping. Items falling under an HS code may correlate to many different controls.	The HS code in question would have multiple controls under it. If the HS code were associated with high trade volumes, all those controls would be implemented. If the HS code is not traded, the whole HS code would be subjected to control.	Not a problem.
Some controls apply to goods not explicitly included in the HS.	These controls will tend to accumulate under HS codes for goods not elsewhere specified. These HS codes would have multiple controls under them. If the HS codes were associated with high trade volumes, all those controls would be implemented. If the HS code is not traded, the whole HS code would be subjected to control.	Not a problem.
Structural incompatibilities remain.	In these situations, the control may need to be repeated under many different HS codes. In the worst case, the controls may need to be expressed at the HS chapter level rather than at the heading or subheading level.	No worse than the status quo.
Technology controls apply.	Technology controls, and particularly control of intangible technology transfers, are difficult for customs. Because the HS does not address intangible technology, the hybrid approach would not improve the situation.	No worse than the status quo.

Toward a Biosecurity Summit: The Nuclear Security Summit as a Model

Maurizio Martellini and Tatyana Novossiolova,
ICIS, STATE UNIVERSITY OF INSUBRIA AND LNCV, COMO, ITALY

The Nuclear Security Summit (NSS) contributed to devising concrete measures to ensure security of nuclear materials worldwide and strengthening the existing international nuclear regime. If replicated in the area of biosecurity, a similar mechanism could contribute to the security of biological materials and expertise and to the norm against the hostile misuse of biological science and technology. A Biosecurity Summit (BSS) could offer an occasion to present and consolidate initiatives in bio and health security. By dint of being underpinned by state leadership, long-term political commitment and international cooperation, a BSS could be considered a crucial step towards fostering a culture of biosecurity worldwide.

CHANGING INTERNATIONAL SECURITY LANDSCAPE: NOVEL BIOSECURITY CHALLENGES

Increasing globalization and changing face of conflict after the end of the Cold War have given rise to novel security challenges and concerns that require flexible approaches and systematic action at multiple levels. Against this backdrop, potential increased spread of disease and the rapid advancement of science and technology in life sciences merit specific attention, not least because of the enormous dual-use potential whereby the same developments that promise tremendous health, social and economic benefits could also facilitate the emergence of sophisticated biological weapons and enable bioterrorism. Fascinating breakthroughs in biotechnology offer significant prospects for social and economic betterment in the form of new therapeutics, effective prevention and treatment methods, and food security. Yet at the same time they also pose an array of multifaceted security, ethical and legal concerns. The global diffusion of modern biotechnology capabilities, the close integration of the life sciences with other disciplines and the rapid pace of progress make the dual use potential of biotechnology particularly acute.[1] At the same time, while we have improved methods of response to infectious disease outbreaks, international travel and interconnectedness are making the spread of outbreaks, as well as access to potentially dangerous agents by malevolent actors, easier. Hence a very complex process of continuous checks and increasing professional responsibility among all the stakeholders is necessary.

Still worse, unlike the international legal architecture pertaining to other types of weapons of mass destruction (WMD), the biological non-proliferation regime remains weak and pervaded by severe limitations. Efforts to promote both chemical and nuclear disarmament are underpinned by explicit state leadership, international coordination and cooperation, adequate financial support and multi-stakeholder engagement. By contrast, the Biological and Toxin Weapons Convention (BTWC), the cornerstone treaty prohibiting the development, use, and possession of biological weapons has neither a verification system nor an adequate international infrastructure to coordinate and monitor its national implementation. The development of these systems within the BTWC that binds all States is improbably in the foreseeable future, so that a high-level political initiative is impracticable within the BTWC today, but may be fostered with a voluntary initiative in the BSS. There is also an urgent need for consolidating global efforts to promote biosecurity and build confidence among states with regard to their obligations enshrined in BTWC and Security Council Resolution 1540.

The launch of a Biosecurity Summit (BSS) patterned on the Nuclear Security Summit (NSS) could be an effective step in this direction. A BSS could serve as a comprehensive framework for promoting policies, initiatives and measures with the goal of strengthening the international prohibition against

1 NRC, *Life Sciences and Related Fields: Trends Relevant to the Biological Weapons Convention* (Washington, DC: National Academies Press, 2011), available at http://www.nap.edu/catalog.php?record_id=13130.

biological weapons; fostering culture of responsibility and security in the life sciences; and preventing non-state actors from developing or otherwise acquiring bioweapon capability.

NUCLEAR SECURITY SUMMIT: AIMS, FORMAT AND SUPPORT INITIATIVES

First launched in 2010 in Washington by the United States President Obama, the Nuclear Security Summit (NSS) was conceived as a high-level political initiative to address, inter alia, the issue of security of nuclear materials against potential non-state actors and complement the existing international nuclear nonproliferation and convention regimes. As outlined in President Obama's Prague speech delivered the previous year, the chief objective of the NSS was to tackle the risk of nuclear terrorism by:

- Promoting concrete nuclear security measures, including the reduction of the amount of dangerous nuclear material in the world by shifting from a national approach to a voluntary multilateral system;
- Strengthening the nuclear security architecture (not limited to the Non-Proliferation Treaty - NPT) and the role of the International Atomic Energy Agency (IAEA) conventions through the endorsement of a process steaming at the level of State heads;
- Fostering a holistic approach to the nuclear security culture; and
- Adopting an overall inclusive approach that allows the participation of Non NPT States, International Organizations and non-governmental organizations (NGOs).

The NSS is a biannual event and so far three NSSs have been held – Washington (2010), Seoul (2012) and The Hague (2014). Each Summit concludes with a Communiqué that reflects the commitment of participating states to the overall goal of enhancing nuclear security worldwide. The Washington Work Plan adopted at the end of the first NSS has largely set the agenda and work priorities for the subsequent Summits. It has also provided an incentive for many countries to make pledges to take specific actions to support and promote the Summit's objectives. More than half of the states represented at the 2010 NSS expressed commitment to implement 67 measures in total. Prior to the Seoul Summit in 2012, over 80 per cent of those commitments were fulfilled.[2] Among the areas noted in the Washington Work Plan were:

- ratification and implementation of international treaties;
- support for Security Council Resolution 1540;
- conversion of civilian facilities from highly enriched uranium to non-weapons-useable materials;
- research on new nuclear fuels;
- detection methods and forensic technologies;
- development of corporate and institutional cultures that prioritize nuclear security;
- education and training; and
- joint exercises among law enforcement and customs officials to enhance nuclear detection opportunities.[3]

Underpinning the NSS ambitious agenda are a range of key international agreements, initiatives and mechanisms of support. With regard to treaties, it is worth noting the UN Security Council Resolution 1540 the Non-Proliferation Treaty (NPT) and the Convention on Nuclear Safety. Security Council Resolution 1540 specifically calls upon states to 'to take cooperative action to prevent illicit trafficking in nuclear [...] weapons, their means of delivery, and related materials'. While the NPT does not make an explicit reference to non-state actors, the 2010 Review Conference seems to signal that the illicit trafficking issue must be addressed irrespectively from the nature of the cause. The Convention on Nuclear Safety is relevant for a holistic extension of the NSS scope to the issue of safety as hinted at the Seoul 2012 NSS.

The multilateral initiatives discussed in the NSS contribute to the international nuclear safety and security in concert with other instruments. The following list of international and multilateral organizations, initiatives and mechanisms dedicated to strengthening global nuclear security and promoting

2 'Nuclear Security Summit at a Glance', *Arms Control Association Factsheet,* available at https://www.armscontrol.org/factsheets/NuclearSecuritySummit.

3 Ibid.

nuclear non-proliferation and disarmament is indicative rather than exhaustive:

- International Atomic Energy Agency (IAEA)
- The Global Partnership Against the Spread of Weapons and Materials of Mass Destruction (GP)
- The EU CBRN Risk Mitigation Centers of Excellence initiative (CoEs)
- Convention on the Physical Protection of Nuclear Material(CPPNM)
- Code of Conduct on the Safety and Security of Radioactive Sources
- International Convention for the Suppression of Acts of Nuclear Terrorism
- Global Initiative to Combat Nuclear Terrorism (GICNT)
- INTERPOL
- 1540 Committee
- World Institute for Nuclear Security(WINS)
- International Nuclear Security Education Network (INSEN)
- IAEA Nuclear Security Support Centers (NSSCs)

What immediately stands out is the wide range of actors spanning government and non-government entities, particularly industry and academia. The IAEA is the principal international organization tasked with coordinating and consolidating the efforts in fostering nuclear security worldwide. Since 2002, the IAEA Board of Governors prepares and approves 3-year Nuclear Security Plans outlining milestones and objectives to be met at global level to 'protect both nuclear and other radioactive materials from malicious acts.' Despite not being directly related, given the similarities in their scope and goals, the Nuclear Security Plans and the NSS mandate are mutually reinforcing. Nuclear Security Plans outline milestones and objectives to be met at global level for the purpose of ensuring that nuclear and radioactive materials are only used for peaceful purposes. The implementation of the Plans is financed through a Nuclear Security Fund to which Member States can contribute on a volunteer basis. The World Institute for Nuclear Security (WINS) plays a crucial role in engaging the private sector with nuclear security issues by focusing on capacity building, outreach and developing sustainable professional competency. The EU CBRN CoEs, the International Network for Nuclear Security Training and Support Centers (NSSC Network), and the International Nuclear Security Education Network (INSEN) constitute other key mechanisms for promoting nuclear security awareness, training and education at several levels by supporting institutions in developing courses, exchanging training materials and sharing best practices, codes of conduct and lessons learned.

TOWARD A BIOSECURITY SUMMIT

A BSS, possibly proposed and hosted by a country interested in leading the discussion on biological security, would invite world leaders, representatives of international governmental mechanisms and of scientific and non-governmental organizations, to gather on a voluntary basis and discuss multilateral approaches to the security of biological materials and expertise.

The BSS could serve as an important international mechanism to complement the efforts to prevent the hostile misuse of the life sciences. In particular, it could facilitate effective action in support of the BTWC and UNSC Resolution 1540 by promoting dialogue on specific issues such as national implementation, cooperation and assistance and voluntary peer-review of compliance; it could work in collaboration with the BTWC-Implementation Support Unit (ISU) and the UNSC 1540 Committee and thus enhance their role and function; and it could provide a platform for multi-stakeholder engagement to foster biosecurity culture globally. By dint of being a high-level, multilateral platform, the BSS could could aid in furthering the objectives of the BTWC, for example, by inviting and assisting countries to join and ratify the Convention; and it could coordinate, review and evaluate new and already existing biosecurity initiatives, so as to avoid the duplication of effort and facilitate the development and exchange of best practice.

The BTWC, while remaining the cornerstone of the prohibition of the whole class of biological and toxin WMD, controlling those weapons is challenging especially when compared to nuclear and chemical weapons. Also, the BTWC does not have the same formal verification requirements of the Chemical Weapons Convention (CWC). The Confidence Building Measures (CBMs) introduced at the BTWC Second Review Conference in 1986 are not compulsory and underutilized, and the treaty has no mechanism

for the verification of compliance or an implementing organization. A further challenge to the effective functioning of the BTWC is the lack of universality. To date, sixteen states remain outside the Convention and another ten are still to ratify it. These figures are staggering given that the NPT membership counts 189 states and that of the CWC 190. However, like to the NSS process, a BSS mechanism could facilitate the engagement of the States not parties to the BTWC to the sharing of common responsibilities and measures, even standing out of the BTWC.

Against this backdrop, a BSS could tremendously contribute to strengthening the BTWC processes and consolidate global efforts to ensure that the life sciences are used only for peaceful, prophylactic and protective purposes. For example, it could support the work of the ISU and foster linkages with the UNSC 1540 Committee to promote state adherence to the provisions outlined in Resolution 1540 and its subsequent extensions. Other international organizations, such as the World Health Organization (WHO), World Organization for Animal Health (OIE) and the UN Food and Agriculture Organization (FAO) could further inform the workings of the BSS by attending its meetings and sharing relevant experience and expertise. Other important international instruments designed to prevent the hostile misuse of the life sciences, and promote biosecurity awareness and culture, include 2005 WHO International Health Regulations (IHR) and CWA 15793:2011 Laboratory Biorisk Management. It is essential that the implementation of those agreements is well-coordinated so as to avoid stifling innovation. To this end, a multilateral cross-sectorial comprehensive approach is required underpinned by collaborative action, multi-stakeholder engagement and adequate financial support. Best practices and lessons learned from existing projects and initiatives need to be utilized as that would help avoid duplication of efforts and enhance sustainability. Table 1 further illustrates a number of existing multilateral mechanisms with relevance to the goals of a BSS.

Civil society featuring professional associations, academia, think-tanks and industry could make a significant contribution to the work of a BSS. The International Federation of Biosafety Associations (IFBA), Biotechnology Industry Organization (BIO), universities, funding bodies (e.g. charities, foundations, research councils) and publishers of life science research constitute key players in the biotechnology enterprise with the potential to initiate, foster and sustain the development of a global biosecurity culture.

One way to facilitate effective action through a BSS would be to adopt a 'gift basket' approach patterned on the practice of the NSS. Therein, by design, a 'gift basket' is an extra ad-hoc initiative offered by a group of the participating countries, which could serve as a model for a specific collective nuclear security aspect. This "gift basket diplomacy" is considered a key tool of the NSS process, since it allows to their participants to share available resources, assistance, technologies and opportunities that can be shopped and exchanged among partners. Moreover, more important, these initiatives are essential to the diffusion of a global nuclear security culture beyond the frameworks of the internationally legally binding mechanisms. Therefore, the BSS could establish a similar "gift basket diplomacy" and "incubator" approach in parallel to the voluntary measures implemented in the framework of the technological assistance Art. X of the BTWC, by allowing some participating countries and organizations to offer extra initiatives that can function as role models for specific biosecurity objectives. Therefore the BSS could be a mechanism to rationalize and present in a consistent "forum" opportunities that now are in part scattered among the several independent initiatives of bio and health security listed above. Again, like to the NSS process, the BSS could help all the stakeholders to design a "global bio security architecture" standing against the potential misuses by non-state actors of the needed life science developments and achievements.

The NSS has set an important model for promoting multifaceted and effective action to enhance nuclear security globally. If replicated in the area of biosecurity, this mechanism could have an enormous positive impact on the efforts to uphold the international norm against biological weapons and thus avert the hostile misuse of modern biotechnology. As the nuclear security experience clearly demonstrates, state leadership, international cooperation and long-term unequivocal commitment are essential building blocks of developing a robust system against the proliferation of WMD. The launch of a BSS could therefore be seen as a useful step toward fostering a sustainable biosecurity culture worldwide.

TABLE 1: MULTILATERAL INITIATIVES IN THE AREA OF BIOSECURITY

Initiative	Description
The Global Partnership Against the Spread of Weapons and Materials of Mass Destruction (GP)	• A voluntary multilateral group established at the Kananaskis Summit in 2002 currently comprising 26 members • Focused on countering the proliferation of WMD • The GP has a Biological Security sub-Working Group whose expertise the BSS could leverage http://www.nti.org/treaties-and-regimes/global-partnership-against-spread-weapons-and-materials-mass-destruction-10-plus-10-over-10-program/
The EU CBRN Risk Mitigation Centres of Excellence (CoEs)	• An EU initiative implemented by UNICRI and the European Commission's Joint Research Council • Addresses regional CBRN needs through specific tailored projects in fields of concerns • Seeks to strengthen a regional culture of safety and security by increasing local ownership, local expertise and long-term sustainability • A key feature is the integration of safety and security within a risk mitigation framework • The BSS could benefit of utilizing the expertise, best practice, and lessons learned developed as over the past few years http://www.unicri.it/topics/cbrn/coe/
The Global Health Security Agenda (GHSA)	• An informal, international partnership among like-minded countries to strengthen health preparedness and response globally to naturally-occurring outbreaks and intentional or accidental releases of dangerous pathogens • Launched in November 2001 PLEASE CHECK THE DATE • Supports the World Health Organization's disease surveillance network and WHO's efforts to develop a coordinated strategy for disease outbreak containment http://www.ghsi.ca/english/index.asp

Security Culture for Radioactive Sources: Assessment, Enhancement, and Sustainability

Dr. Igor Khripunov,
DISTINGUISHED FELLOW, CENTER FOR INTERNATIONAL TRADE AND SECURITY, UNIVERSITY OF GEORGIA, USA

The current emphasis on the need to protect radioactive sources from being used for malicious purposes makes it imperative to explore and shape an appropriate culture-based response in support of the global effort against WMD proliferation and terrorism. This paper proposes a roadmap for security management of radioactive sources with an emphasis on a security culture model, including self-assessment tools and a series of indicators as benchmarks to help take a culture's measure and identify practical ways for improvements in security. It adjusts the existing International Atomic Energy Agency (IAEA) concept and methodology for nuclear security culture to specific requirements for and mode of operation of radioactive sources. Though this IAEA security culture model in Nuclear Series Report #7 is designed as generic to be applicable to a wide range of operations involving nuclear and radiological materials, the modifications proposed in this paper are needed to make it user friendly and more focused on the security requirements of radioactive sources. This toolset can facilitate a more robust and sustainable security regime for radioactive sources throughout their life cycle, i.e. from cradle to grave.

GLOBAL RISKS

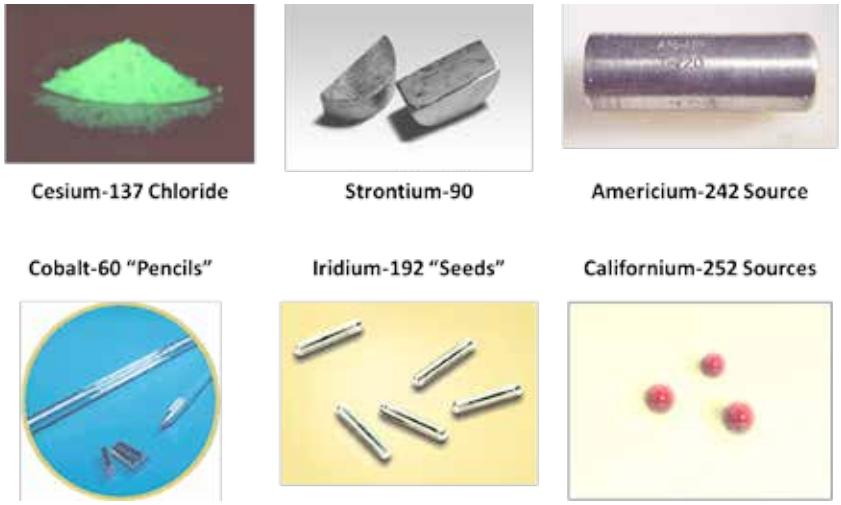
Despite extensive efforts by the world community to place radioactive sources and material under effective control, this goal remains largely elusive and may benefit from human based innovative approaches. The International Atomic Energy Agency (IAEA) Incident and Trafficking Database (ITDB) contains a total of 2,331 confirmed incidents (as of 31 December 2012) reported by participating states, but this could be just the tip of the iceberg. The database is clear evidence of porous security, easy accessibility, human complacency and inadequate regulatory control. The majority of thefts and losses reported to ITDB involve radioactive sources that are used in industrial or medical applications. Industrial sources are mostly those used for non-destructive testing and for applications in construction and mining. Most devices use relatively long-lived isotopes such as iridium-192, caesium-137, cobalt-60, and americium-241, which constitute an attractive target for groups and individuals with malicious intent.

Millions of sources have been distributed worldwide over the past 50 years, with hundreds of thousands currently being used, stored, and produced. The IAEA has tabulated over 20,000 operators of significant radioactive sources globally. In many countries, as regulatory control of radioactive sources is weak, the inventories are not well known. These "orphan sources" include sources that have been abandoned, lost, or misplaced as well as sources that were stolen or removed without proper authorization. Exactly how many orphan sources there are in the world is not known, but the numbers are thought to be in the thousands. Orphan sources expose society to the risk of radiological accidents and terrorism.

There have been many incidents all over the world in which radioactive sources have been smuggled, lost, stolen, and abandoned. The most recent case took place in Mexico in December 2013 when thieves stole a truck containing a decommissioned teletherapy unit that was once used for cancer treatment and contained a small capsule of highly radioactive material. It was reported that the capsule's content – 3,000 curies of cobalt 60 – made it a "category 1" radiation source which is the most dangerous of the five categories. Luckily, there were no immediate reports of serious injuries and no contamination found in the area nearby, but had the stolen Mexican capsule ended up in the hands of terrorists, they could have used it to build a "dirty bomb", causing very few radiation-related deaths, but, nonetheless a disastrous economic, psychological, and to some extent, political, impact.

CULTURE-BASED APPROACH

An effective security for radioactive sources depends not only on proper planning, training, operations, and maintenance, but also on the thoughts and actions of people who plan, operate, and maintain security systems. Radioactive source users may be technically competent, but are still vulnerable if they discount the role of the human factor. One of the IAEA security recommendations for radioactive sources emphasizes the importance of promoting a security culture: "All organizations and individuals involved in implementing nuclear security would give priority to the nuclear security culture with regard to radioactive material, to its development and maintenance necessary to ensure its effective implementation in the entire organization." The entire security regime stands or falls based on the people involved.



Radioactive Isotopes and Sources

The IAEA defines nuclear security culture as "the assembly of characteristics, attitudes and behavior of individuals, organizations and institutions which serve as a means to support and enhance nuclear security." In 2008, the IAEA published an Implementing Guide on Nuclear Security Culture in its Nuclear Security Series. The Implementing Guide defines the concept and characteristics of nuclear security culture while delineating the roles and responsibilities of institutions and individuals entrusted with this function.

The Implementing Guide is the only IAEA publication released so far on nuclear security culture and is intended to serve as an introduction to the subject for its potential users. The Model, its characteristics, and its indicators are generic enough to be used by regulatory bodies and other organizations involved in activities utilizing nuclear and other radioactive material including transportation. Its generic nature has both advantages and disadvantages. On one hand, the Model can be utilized throughout the entire nuclear industry and lay the groundwork for shared values and practices. On the other, it lacks specificity and comprehensiveness when applied in each special domain requiring adjustments and additions to gauge the status of security culture. The Implementing Guide recognized these limitations and explains that the objective is to encourage self-examination by organizations and individuals, i.e. to stimulate further thought rather than to be prescriptive. Accordingly, given the lack of expertise and experience among some users of radioactive sources, it would be helpful to adjust its generic approach to the specific needs of their facilities and facilitate the process of self-examination.

There are several features of radioactive source security that make it distinct from nuclear security and have a substantive effect on its culture design. These distinct features can be summarized as follows:

CONTINUED PREVALENCE OF SAFETY ORIENTATION

The Code of Conduct for the Safety and Security of Radioactive Sources was originally oriented largely to safety and radiation protection rather than security. Most organizations using radioactive sources are characterized by other, larger operational units where no radioactive sources are utilized and where security mentality is not well developed or popular. As a result, managers tend to delegate security to their lower-tiered staff and are less involved personally. For those in charge of or operating sources the priority is still to protect people from sources rather than to protect sources from people.

DIVERSE APPLICATIONS

Radioactive sources are utilized across a wide range of industrial, construction, research, medical, and other applications. The diversity of security regimes and its impact on organizational culture is much more extensive than throughout the more uniformly structured nuclear sector. Dispersed throughout numerous industrial units and medical institutions, security culture poses a serious challenge to efforts towards formulating a uniform approach.

MOBILE AND PORTABLE OPERATION

Industrial radiography sources, a wide range of gauges and others are routinely moved around and often located off-site where traditional approaches to physical protection cannot be effectively applied in practice. For this category of sources, a timely detection, delay and response are not easy to accomplish. The difficulty in controlling with the use of traditional methods amplifies the importance of human reliability, vigilance, and improvisation as key traits of security culture. The mobile and portable modes of operation impose a burden on users of radioactive sources to continuously improve security arrangements in coordination with local law enforcement personnel across the country.

LIMITED RESOURCES AND AWARENESS

In less-developed countries, financial, technical, and human resources are still lacking to address the risk of diversion of radioactive material and its malicious use. Most of these countries do not have an established nuclear power infrastructure which, given its scale and significance for the national economy, often serves as a source of advanced security methodology and best practices to share with users of radioactive sources in other countries.

DISPOSITION CHALLENGES

End-of-life source management is another challenge due to a lack of uniform practices that often leave sources without regulation. Options open to users include return to manufacturers, recycling or disposal and storage but financial constraints frequently prevent them from following these procedures in a consistent manner. As a result, some disused sources become vulnerable to weak control and may fall into the category of "orphan sources."

Hence, the security culture model proposed in this article for radioactive sources cannot be an exact replica of the IAEA model described in the 2008 Implementing Guide. Based on the same organization culture approach, the proposed model and its characteristics and indicators must reflect features specific to the operation of radioactive sources (safety-security integration, diverse organizational applications, mobile and portable mode of operation, limited security awareness and disposition challenges.

The security culture model for radioactive sources may take some time to get accepted, refined and implemented as a tool for human capacity building in support of effective security. Though not a panacea, it can enhance the security regime and contribute to its major objectives throughout the entire life cycle of radioactive sources, i.e. from cradle-to-grave. Whilst a security regime for radioactive sources has been traditionally built on existing radiation regulatory and safety measures, there are factors in the use, storage and transport of radioactive sources that make security distinctly different and challenging. In addressing these challenges, an integrated approach is required to ensure that all responsible organizations have adequate and compatible security culture to establish, strengthen, implement and sustain security regimes for radioactive sources from their production to disposition.

BUILDING AND ASSESSING A SECURITY CULTURE

Special security requirements for radioactive sources may justify a more differentiated approach toward security culture. More frequent and intense efforts are expected to focus on a select group which has a direct or indirect relationship with radioactive sources (management teams, security personnel, operations, technicians, and others). The general policy is that security awareness and culture development is applicable to all employees as a core value through several techniques. However, given limited resources, it would be reasonable to place more emphasis on the security commitments for this select group. In other words, the differentiation is a targeted

approach and makes time and resource investment in awareness and culture development commensurate with the roles and responsibilities of individuals.

Topics to be covered during security awareness sessions should explain (1) why radioactive sources may be targeted, by whom and why, (2) how adversaries including insiders can endanger them, (3) their motivation and possible consequences of their actions, (4) the limitations of security regimes and concurrent vulnerabilities, and (5) what can be done to prevent their loss or damage. Emergency drills and exercises would complement these sessions.

The ability to assess the status of security culture is a prerequisite of its successful development and maintenance. Applying assessment methodology demands a multidisciplinary approach since culture is composed of intangible human characteristics such as beliefs, values, and ethics. Security awareness and culture assessment plays a key role in developing and maintaining an awareness of strength and weaknesses in protecting radioactive sources. The purpose of a security culture assessment is to provide a clear picture of the influence of the human factor on an organization's security regime.

The ability to assess the status of security culture is a prerequisite of its successful development and maintenance.

Self-Assessment is a multi-stage process comprising both non-interactive and interactive assessment tools focusing on management and behavior characteristics of the Radiological Security Culture Model. These characteristics are evaluated by comparing what the culture is at present to their optimal parameters specified by culture indicators assigned to each characteristic. Due to the heavy focus on perceptions, views and behavior, regularly held comprehensive assessment help one understand the reasons for an organization's patterns of behavior in certain circumstances.

Surveys are important to self-assessment because they establish a baseline for tracking changes over time. Survey statements are derived from culture indicators. It is up to the management to determine the scoring scheme for the survey. The present article suggests a scoring system employing a 7-point scale from 1 ("Strongly Disagree") to 7 ("Strongly Agree"). This scheme indicates that a particular indicator in either fully observed or present, completely unobserved and absent, or somewhere in between. Respondents to a survey are requested to offer comments if they have something else to say.

Interviews play a significant role in cultural assessment because they allow for flexible questioning and follow-up clarifications from interviewees. This eases the task of getting at the deeper tenets of an organization's culture. Interviewees, who need to be carefully selected by their experience, work positions, and skills, can give specific examples of past practices that they have seen done or heard about and even supply explanations that would provide insight into people's beliefs and attitudes. Compared to individual face-to-face interviews, focus-group sessions have the advantage that interactions within a group setting often prompt and sustain discussions. Group members share over a relatively short period their experiences, views and attitudes about the topic in question, eliciting responses from one another.

Document reviews and observations can take place prior to assessment to familiarize evaluators with past security incidents, their root causes, and corrective measures taken, or used as a tool during the process of assessment. Document review can supply insight into how management sets its priorities and how it intends for its policies, programs, and processes to operate in practice. Combined with surveys and interviews, a document review helps evaluators appraise differences between stated policies and procedures and actual behavior. The purpose of conducting observations is to record actual performance and behavior in real time and under different circumstances, especially at general meetings, training sessions and emergency drills. Observations are well-established, time-tested, commonplace tool for managing security.

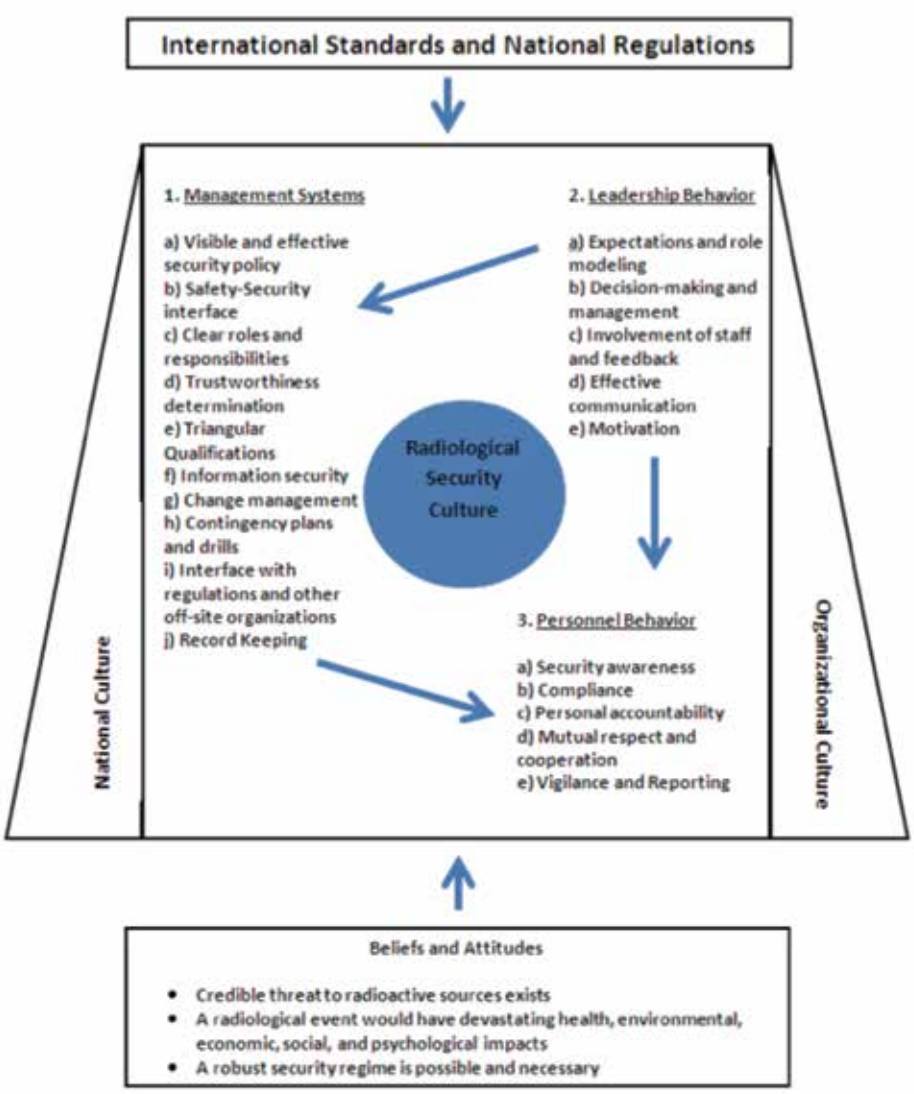
The analysis stage is critical for comparing and integrating the findings of assessment tools. Without conducting an analysis evaluators are at risk of merely reporting what they have learned and presenting a factual summary. The significant value that evaluators

can bring is their interpretation of the findings, their analysis of underlying root causes, and their informed opinion about what problems might exist and what should be done. Upon receipt of the assessment report senior managers expect to be able to draw upon the insight of evaluators to address the identified cultural deficiencies.

CONCLUSIONS

Against the background of the increasing use of radioactive sources in areas characterized by a lack of stability, inadequate operational experience, and low security priority, a cultural approach to protection of high-risk radioactive sources is becoming indispensable. In this context, however, seldom will a security culture self-assessment yield clear-cut or easily actionable results. Instead, it helps move the organization along its learning curve by determining what attitudes and beliefs need to be established in an organization. In this sense, assessment of security culture should complement the currently used evaluation methodology for gauging vulnerability and physical protection, thus helping refine the overall security arrangements for radioactive sources. A realistic, rational, risk-based approach will become possible under the assessment methodology advanced in this article.

Figure 1: Security Culture Model for Radioactive Source



Nuclear Forensics in the Context of UNSCR 1540

Benjamin C. Garrett (USA) and
Klaus Mayer (Germany),
CO-CHAIRMEN OF THE INTERNATIONAL TECHNICAL WORKING GROUP (ITWG)

SHARED INTERESTS: UNSCR 1540 AND FORENSICS

United Nations Security Council resolution 1540 (UNSCR 1540) establishes obligations for all States to enact and to enforce domestic legislation criminalizing non-state actor involvement in weapons of mass destruction (WMD). One potential aspect to non-state actor involvement in WMD involves use or attempted use of nuclear and other radioactive materials as a WMD. Forensic science is a vital component to a State's regime for combating such use or attempted use. Results from forensic examinations can aid in identifying the origin of such materials, the pathway taken in diverting these materials from legitimate activities, and the parties involved in loss of regulatory control over the materials.

THE CHALLENGE

In the mid-1990s, law enforcement operations in several nations led to the successful seizure of nuclear or other radioactive (RN) material. These operations demonstrated that such material was the object of black market trafficking. The intent of this trafficking appeared to be financial, where the traffickers imagined that these RN materials might command a high price. But the seizures fed concerns that RN materials might be inadequately protected against loss of regulatory control and, thus, might be diverted for use by terrorists – for example, as an element in a radiological dispersal device (RDD) or as the fuel in an improvised nuclear device (IND).

In 1995, the International Atomic Energy Agency (IAEA) established what is now called the Incident and Trafficking Database (ITDB), a voluntary program to report incidents of illicit trafficking and other unauthorized activities and events involving

Crime scene personnel prepare an item of evidence contaminated with radionuclides for shipping to a forensic laboratory

RN materials outside of regulatory control. The ITDB provides a tool for estimating the frequency, distribution and magnitude of seizures. Between January 1993 and December 2012, a total of 2,331 incidents were reported to the ITDB, including 419 that involved unauthorized possession, attempted sales, or other criminal activities involving RN material. Sixteen reported incidents in this category involved so-called weapons-grade uranium or plutonium – that is, nuclear material that is suitable for use in an IND. Some of these incidents dealt with kilogram quantities, adding to the concerns over diversion for terrorist purposes.

Recent cases demonstrate the continued availability of RN material on the black market despite significant progress made in securing such materials. These incidents have motivated the international law enforcement, policy, regulatory, and scientific communities to enhance capacities to deter, detect, prevent, and investigate loss of regulatory control over RN materials, thereby lessening the prospect that such materials might be diverted to criminal or other illicit purposes. One example of an effort to develop enhanced capacities is the Nuclear Forensics International Technical Working Group (ITWG).

THE ORGANIZATION

ITWG is a multinational, informal association of official practitioners of nuclear forensics - laboratory scientists, law enforcement personnel, and regulatory officials - who share a common task in responding to nuclear security events involving RN materials out of regulatory control. ITWG was established in 1995-1996 as a result of an initiative of the G-8 (both the 1995 Ottawa Summit and the 1996 Moscow Nuclear Security Summit), largely through the efforts of concerned scientists from the national laboratories of the US Department of Energy and from the Institute for Transuranium Elements representing the European Commission, with the encouragement of government officials. Its establishment reflected heightened concerns over the threat posed by the diversion of RN materials, as witnessed by the open-reporting of black market-related seizures of these materials.

Known originally as the "Nuclear Smuggling International Technical Working Group," ITWG changed its name in 2010 to reflect the increasing importance attached internationally to nuclear forensics. It also reflects the emphasis ITWG is devoting to best practices for forensics - both those forensic analyses directed toward the RN material itself as well as traditional forensic procedures conducted on evidence contaminated with radionuclides.

ITWG conducts its work primarily through a combination of task group activities, convening meetings, and the conduct of exercises. There are five task groups: Evidence, Exercises, Guidelines, National Nuclear Forensics Libraries (NNFLs), and Training and Outreach. Participants in each group are encouraged to engage in activities on a continuous basis, and the ITWG website, www.nf-itwg.org, facilitates such engagement. ITWG seeks to convene a formal meeting on an annual basis and has held twenty such meetings since its founding in 1995. ITWG also holds less formal meetings on special topics where appropriate.

Exercises have been of two types: table top exercises (TTXs), where participants explore certain topics but which typically require minimal or no laboratory resources, and material-based exercises, where participants collaborate on the analysis and characterization of RN materials. Additional details on these exercises are offered below.

A Questioned Documents examiner prepares evidence from a radiological crime scene to determine whether there is any indented writing or other hidden impressions

THE SCIENCE

The participants in ITWG define nuclear forensic science, often referred to as simply nuclear forensics, as "the examination of nuclear or other radioactive material, or of other evidence that is contaminated with radionuclides, in the context of legal proceedings, including national or international law or nuclear security." In the view of ITWG, nuclear forensics is an essential component of national and international nuclear security response to events involving RN material out of regulatory control. The abilities to collect and preserve seized RN material as evidence and to examine this evidence may provide information about the history and origin of the material, the point at which regulatory control was lost, and identity of those responsible for this loss of regulatory control.

Nuclear forensics is a technical capability that will also inform the investigatory process. The goal of nuclear forensics is identical to the goal of any other forensic examination: to determine whether linkages

Table I. Collaborative Material Exercises of the ITWG

Years	Material	Participating Laboratories[a]
1999-2000	Plutonium oxide powder	Austrian Research Centre, Seibersdorf, Austria; Commissariat a l'Energie Atomique (CEA), Valduc, France; Institute for Transuranium Elements (ITU), Karlsruhe, Germany, European Commission; Institute of Nuclear Chemistry and Technology, Warsaw, Poland; Institute of Physics, Vilnius, Lithuania; and Lawrence Livermore National Laboratory (LLNL), Livermore, California, USA
2000-2002	Highly enriched uranium (HEU) (uranium oxide powder)[b]	Austrian Research Centre; AWE; CEA; Cekmece Nuclear Research and Training Center, Istanbul, Turkey; ITU; Institut für Radiochemie, Munich, Germany; Institute of Isotope and Surface Chemistry, Hungarian Academy of Sciences, Budapest, Hungary; LLNL; and Nuclear Research Institute Řež (NRI Řež) , Czech Republic[c]
2009-2010	HEU (uranium metal)[d]	Australian Nuclear Science and Technology Organization (ANSTO), Menai, Australia; AWE; Comissao Nacional de Energia Nuclear (CNEN), Pocos de Caldas, Brazil; CEA; Defence R&D Canada, Ottawa, Canada; Institute of Isotopes, Hungarian Academy of Sciences, Budapest, Hungary; ITU; LLNL; and NRI Řež

[a] The name of the laboratory shown in the table is the one that was in use at the time of the exercise.
[b] 90+% ^{235}U, provided by Nuclear Research Institute Řež, Czech Republic.
[c] In addition, Defense R&D Canada, Ottawa, Canada, participated on a delayed basis, submitting its report separately.
[d] 90+% ^{235}U, provided by a US government facility, Oak Ridge, Tennessee.

– that is, associations – exist among people, places and things. And, as with all forensic examinations, both inclusion results and exclusion results are important in terms of the forensic inquiry being conducted. Inclusion results in nuclear forensics demonstrate a linkage or an association of some sort, much as a match for a fingerprint or a DNA profile might do in traditional forensics. Similarly, exclusion results yield no linkage or association and might allow certain people, places or things to be excluded from further investigation.

EXERCISES TO ADVANCE CAPACITIES

Collaborative Materials Exercises

ITWG provides a distinctive forum for exercises in which laboratories that elect to participate can test their ability to analyze RN material, comparing their results with those of other participating laboratories. One feature of these exercises is that results are coded to afford participants a measure of anonymity as well as to avoid having results misused, such as grading the performance of any one laboratory or any group of laboratories.

Additionally, while exercise results are anonymous, they can be used to inform requirements for research and development, such as enhancements in analysis techniques, availability of reference materials and improvements in instrumentation. Such exercises have proved useful in enhancing capacities to analyze and characterize RN material.

Through 2014, ITWG has overseen development, conduct, comparative data analysis, and reporting

for three collaborative material exercises, dubbed "Round Robins". The years, the materials used and the participating laboratories of Round Robin 1, 2 and 3 are given in Table I.

Important lessons have been gleaned from these exercises, including:

(a) Participating laboratories have demonstrated their technical competence for performing analyses critical to nuclear forensic investigations.

(b) Guidance documents such as the IAEA Nuclear Security Series publications as well as the ITWG Best Practices guidelines have proven useful. Conversely, the results of the exercises have aided in identifying areas within these guidance documents where changes are desired or where greater clarity must be sought.

(c) Databases, historical records, and archived materials are valuable in identifying similarities and dissimilarities between materials of known provenance and samples associated with nuclear security events. Both types of results – that is, "inclusion" and "exclusion" in the terms used in forensic science – can be valuable in determining the origin of a material.

(d) Ensuring availability of personnel, instrumentation, and equipment is challenging, perhaps reflecting the voluntary nature of these collaborative exercises.

(e) Few participating laboratories have developed robust methods for the safe and effective conduct of traditional forensic examinations on samples contaminated with radionuclides. Consequently, results from such traditional forensic examinations have under-exploited.

The results of and lessons learned from the most recent exercise, Round Robin 3, have been published, and a copy is available from the ITWG website.

A Trace Evidence examiner uses oblique light to aid in finding hairs, fibers, or similar small material that might be deposited on an item of evidence from a radiological crime scene

A fourth collaborative material exercise (CMX-4), involving low enriched uranium (LEU), is in progress. Laboratories from 14 nations and one international organization are expected to participate. Shipment of the samples will occur in the third quarter of calendar year 2014. Laboratory analysis and characterization are to be completed within two months of the exercise start date.

Galaxy Serpent

ITWG executed the table top exercise *Galaxy Serpent* during 2013 and 2014. *Galaxy Serpent* was a first-of-its-kind, virtual, web-based international TTX where individual teams of scientists from various countries and organizations used provided public-domain spent-fuel compositions to formulate their own NNFL, and then used these data to determine whether a hypothetically seized spent nuclear fuel is or is not consistent with their national nuclear forensics library. The TTX promoted best practices by providing a vehicle for participants to gather key technical expertise to create an NNFL using guidelines in draft IAEA documents. It also illustrated the potential probative benefits offered by creating such a library.

Galaxy Serpent involved nuclear forensic practitioners from approximately 24 countries, and the active participation of teams from 17 nations

and one international organization. During the play of *Galaxy Serpent*, many teams recognized a need to involve other areas of expertise outside of their immediate domain, such as nuclear reactor engineers and fuel experts. The involvement of such additional experts helped to mature the range of expertise of the nuclear forensics international community.

Teams also found that different technical approaches yielded similar analytical conclusions, a finding that analogous to what obtains in traditional forensic science disciplines and an important finding relative to strengthening the scientific basis on which nuclear forensics rests. Teams noted that the original purpose, history, and limitations of the provided spent-fuel data sets could limit the confidence levels attached to their findings. The exercise has yielded insightful lessons regarding the efficacy of NNFLs.

The unique nature of *Galaxy Serpent* as well as the importance of its results prompted the Institute of Nuclear Materials Management (INMM) to devote a special publication to its conduct and results. This publication, *Journal of Nuclear Materials Management*, Summer 2014, Vol. XLII (4), was released in the July 2014 and is available electronically through the INMM website, www.inmm.org. The publication provides an overview of the exercise and technical reports from nine teams that completed the exercise.

Despite certain artificialities, the exercise proved valuable in engaging and expanding the existing nuclear forensics community of experts. Participants found the exercise beneficial, instructive and insightful, and many requested a follow-on "*Galaxy Serpent 2.0*" exercise based upon a different class of nuclear material. Consequently, ITWG plans to host *Galaxy Serpent 2.0* beginning in early 2015.

CONCLUSION

ITWG contributes to fulfilling goals of UNSCR 1540. In particular, ITWG assists States to advance their capabilities and capacities in nuclear forensics. This assistance is provided through the task group activities, meetings, and exercises conducted by ITWG and covers aspects of nuclear forensics ranging from evidence collection through laboratory analysis and characterization. Such assistance is open to all parties having an interest in nuclear forensics and a willingness to participate in ITWG. Participation in ITWG is open to competent and qualified individuals affiliated with national response organizations from states having, or wishing to have, a nuclear forensics capability. The voluntary, informal nature of ITWG fosters cooperation and collaboration among scientists and allows focusing on scientific and technical issues in order to advance the discipline of nuclear forensic science.

"The voluntary, informal nature of ITWG fosters cooperation and collaboration among scientists and allows focusing on scientific and technical issues in order to advance the discipline of nuclear forensic science."

Explosive combinations: Criminal Networks and WMD proliferation

Karl Lallerstedt
BLACK MARKET WATCH, SWITZERLAND

The US National Security Strategy spells out that "The American people face no greater or more urgent danger than a terrorist attack with a nuclear weapon". The threat of a terrorist attack using Weapons of Mass Destruction (WMDs) attack is not limited to any one country. Enormous efforts have been invested in measures around the World to reduce the vulnerability of key sites, safeguarding expertise, and enforcing dual-use export restrictions. However, such efforts will only be successful if complemented by a broader fight against the criminal infrastructure serving organized crime more generally, which can also be leveraged for WMD proliferation.

The objective of UN Resolution 1540 is to ensure that all States develop and enforce appropriate legal and regulatory measures against the proliferation of chemical, biological, radiological, and nuclear weapons and their means of delivery, in particular, to non-state actors. In order to make this a reality a number of very targeted and specific actions have been, and still need to be, taken. For example improved security routines can be implemented at research facilities where sensitive material is stored, or export control legislation relating to dual-use technologies can be enacted.

> "The ambitions of Resolution 1540 can only hope to succeed when overall border control and law enforcement capacities are effective."

Yet even fulfilling requirements in the legal sense, ticking the boxes and implementing every single piece of appropriate legislation is no guarantee that the letter of the law is observed in practice. And even when procedures are observed in practice, e.g. security routines at a particular facility, it can never protect against all forms of corruption, or in even more extreme circumstances if the state were to lose control of that particular facility.

To truly ensure safety, and prevent the proliferation of WMD related items, the sensitive facilities in question need to be surrounded by a secure environment where the rule of law is firmly applied. Unfortunately the real world is never free from corruption, organized crime, terrorism and conflict. This does not make the focus on specific issues, like safety routines at research reactors, any less important, but it does mean that we also need to take a broader and more holistic security perspective into consideration when we are considering proliferation.

If state officials are corrupted, and the general security environment is unstable, how can the other actions mandated by Resolution 1540 be effective? In fact Resolution 1540 spells out the need for states to "develop and maintain effective border controls and law enforcement efforts to detect, deter, prevent and combat, including through international cooperation when necessary, the illicit trafficking and brokering in such items…." One way of interpreting this is that border controls and law enforcement efforts can only be effective if corruption and one of its key causes, illicit trade, are addressed.

Since the inception of the World Trade Organization (WTO) in 1995 cross border trade has more than trebled. In 2013 merchandise exports alone were estimated at 18.8 trillion US dollars. Over a hundred million twenty foot containers of goods are shipped per year. An enormous volume that is clearly very difficult to exercise effective control over, and this does not even include volumes imported/exported by rail, road and air.

The underside of this boom in legitimate trade has been an explosion in illicit trade. The International Chamber of Commerce estimates that the value of

the market in pirated and counterfeited goods alone could reach 1.8 trillion US dollars by 2015. Irrespective of the accuracy of this estimate, it is clearly a problem of enormous magnitude. Counterfeiting affects all categories of products, from sophisticated items such as airplane components, to ordinary consumer products such as washing powder, to items essential for survival, such as the food we eat or medications we take. In addition to counterfeiting the smuggling of other contraband, such as excise goods, drugs, arms, and people brings the total negative economic and social impact of illicit trade far higher.

The general difficulty in controlling trade flows is pointedly illustrated by a report by Global Financial Integrity released earlier this year. It estimates that over the past decade 25 percent of the value of all goods imported to the Philippines went unreported to customs officials. It is probable that large numbers of developing countries suffer problems of comparable proportions.

While often considered a "victimless crime", mass scale illicit trade in relatively "harmless" products such as contraband consumer goods nonetheless has serious consequences. It provides the underlying economic turnover to develop the necessary "criminal infrastructures" and networks, which facilitate the trafficking of other low turnover but more dangerous items. Beyond such direct smuggling synergies, the profits generated from smuggling can also finance the expansion of completely separate, and potentially much more violent, criminal activities. Illicit trade in "normally legal goods" not only deprives the government of tax revenues, but the corruption associated with it undermines the integrity and effectiveness of the state.

We must not be under any illusion that the border security issues only poses challenges in a limited number of developing countries. The case of the EU clearly illustrates that developed countries are also under pressure.

A study carried out by the Centre for the Study of Democracy illustrates how corruption enhances the vulnerability of the EU's borders. Over a three year period thirteen member states confirmed border guard involvement in smuggling of consumer goods. An equal number of states experienced problems with border guard personnel providing information to criminal groups. Nine states indicated border guard complicity in the contraband weapons trade, and in eight states individuals connected to organized crime were known to be infiltrating border guard organizations.

Europol estimates that there are 3600 international criminal organizations operating in the EU, and over a thousand are so called poly-crime groups. This would suggest synergies between different forms of smuggling, and criminal "support services" catering to those wishing to smuggle. The potential smuggler of dual use items can leverage pre-existing criminal knowledge of certain border weaknesses, clever methodologies for transporting products across borders, fraudulent supplies of documentation (IDs and transportation documentation), and corrupted border guards and other officials — all supplied by organized crime.

> Illicit trade networks have been leveraged by states seeking to enhance their WMD capacities.

Illicit trade networks have been leveraged by states seeking to enhance their WMD capacities. Brian Finlay, managing director at the Stimson Center explains:

"Although we have yet to see the widespread evidence of a common clientele between WMD items and other contraband, increasing participation of criminal actors in proliferation networks demonstrates that the supply chain connecting dual use producers to dual-use recipients does share common pathways with other illicit items. North Korea, for instance, has developed a significant non-nuclear covert smuggling capability that has also aided in the transfer of sensitive items into and out of the country. Similarly, despite significant economic sanctions, the Government of Iran has managed to rely upon similar networks to obtain critical technologies for their uranium enrichment program. And while drug smugglers are never likely to become nuclear terrorists, the illicit transportation networks that they have built have been unwittingly leveraged in support of state-based proliferation programs."

Illicit transportation networks are also useful to non-state actors seeking WMDs. If a state wanted to supply a non-state actor with WMD-related capacity, it would likely want to do so in a way that enabled plausible deniability. Hence the use of criminal smuggling networks may be an attractive option. Non-state actors operating without state support would have little other choice.

In July 2014 it was reported that the terrorist group known as the Islamic State (IS, formerly known as ISIS) had seized nearly 40 kgs of uranium compounds, at Mosul University. In a letter to the UN Secretary-General Ban Ki-Moon Iraq's UN Ambassador wrote "Terrorist groups have seized control of nuclear material at the sites that came out of the control of the state," adding that such materials "can be used in manufacturing weapons of mass destruction." He went on to warn that they could also be smuggled out of Iraq.

Two years earlier Interpol's Secretary General had warned that there had been almost 3,000 reported cases in 119 countries concerning radioactive material.[1] This indicates that the risk of terrorists smuggling components for a "dirty bomb" or other potential weapons of mass destruction are not remote theoretical possibilities. And if a container of consumer goods can be smuggled, so can anything. A local weakness in one particular country hence becomes a global concern.

The ambitions of Resolution 1540 can can only hope to succeed when overall border control and law-enforcement capacities are effective. Consequently, measures that address illicit trade and organized crime more broadly are prerequisites to counter the proliferation threat.

This requires a higher political prioritization of the fight against organized crime. For such a transformation to take place a more holistic understanding of illicit trade is key. In several countries, in the developing world in particular, illicit trade constitutes a significant proportion of overall economic activity. It deprives governments of tax revenues, undermines the rule of law and weakens border security. This whilst it boosts corruption, empowers organized crime, and in some cases provides significant income for insurgents or terrorists (which further diverts much needed resources from the state).

A prerequisite to setting an appropriate level of prioritization against the broader problem of illicit trade — to the benefit of the broader security environment and counter-proliferation efforts — is to enhance our understanding of the broader impact of illicit trade. As illicit trade is an underground activity public data is not readily available. A challenge the OECD has responded to by establishing the Task Force on Charting Illicit Trade. Individual states should support this effort and need to do much more to understand the risks and vulnerabilities in their regulatory environment and trade infrastructure. They must become better at mapping the illicit trade within their own national territories, and within those countries to which they provide development assistance; they should also assess how illicit trade affects their commercial self-interests abroad.

Armed with such data governments will see their self-interest in prioritizing the fight against illicit trade more clearly. This will, in turn, facilitate the required political mobilization. The pay-off will boost trade, job creation, the effectiveness of development assistance and enhance national as well as international security. Of course gathering data is only a first step. But without this first step of "mapping the problem" the high-level political prioritization necessary to dismantle broader criminal infrastructures will not become reality until it is too late.

The clock is ticking. Unless we change our approach to organized crime and criminal networks it is not a matter of if, but when, major WMD attacks will occur.

1 REMARKS by Ronald K. Noble INTERPOL Secretary General, Nuclear Security Summit 2012, 27 March

1540 Experts Column

Terence Taylor
COORDINATOR OF THE 1540 GROUP OF EXPERTS,
UNITED NATIONS

In terms of outreach events in 2014 the 1540 Committee and its experts had, by the end of August participated in [45] outreach events in various parts of the world. Due to demands on resources and availability of Committee members and experts it has not been possible to attend all events for which invitations have been received. Demand appears to be increasing. The events outlined below are a selection to give a flavour of the trend in outreach events engaged in by the Committee and its experts.

There are a number of reasons for this increase. In addition to dedicated tenth anniversary events, it is due in part to the Committee's effort to encourage the States that have yet to report the measures that they have taken to implement resolution 1540 (2004) to do so. While the overall reporting record is impressive, nearly 90% of UN Member States have made such reports – most of them several times with updates. At the time of writing 20 States had yet to report. In its Program of Work (S/ 2013/327 of 31 May 2013 and S/2014/369 of 23 May 2014) the 1540 Committee included achieving universal reporting among its priorities. In addition to individual visits to certain non-reporting States, a series of meetings to engage them was held with the support of the UN Regional Centre for Peace and Disarmament in Africa (UNREC). These meetings were intended to bring together all the non-reporting States in three linguistic groups -- English, French and Portuguese. Representatives from 16 of the then 21 non-reporting States participated in these meetings[1]. The meetings focused on the obligations under resolution 1540 (2004) and gave assistance in the drafting of national reports.

This priority task converges with another in the Committee's Program of Work which is to take opportunities for direct interaction with States to enhance the implementation of resolution 1540 (2004). In this regard, visits to States by invitation are, perhaps, of the highest order of importance. These visits involve meetings with the key national stakeholders involved in 1540 implementation, and usually engage high level participation. In addition to comprehensive discussions on current implementation and future plans they also typically include site visits to demonstrate and discuss practical issues related to 1540 implementation. Such site visits have included nuclear research reactors, biological laboratories, container ports and border posts. Visits to three States have taken place so far in 2014 to Niger, Malawi [Photograph available – site visit] and Bangladesh [Photograph available – Bangladeshi Foreign Minister]. Invitations for the Committee to visit have also been received from China and the United Kingdom; they will take place later this year in October and November respectively.

In 2014, there has also been a welcome increase in outreach events in collaboration with international organizations. These have involved the experts in a joint country visit to Mongolia with the Counter-Terrorism Executive Directorate (CTED), participation in INTERPOL events in Poland, Tajikistan and Thailand, with the Organization for the Prohibition of Chemical Weapons (OPCW) at their headquarters in The Hague, Netherlands and in Argentina and Australia (for a meeting with a group of Pacific Island States). The Secretary-General of the World Customs Organization (WCO) shared the podium at UN headquarters in New York with the Chair of the 1540 Committee for an open debate on 1540 implementation. Members of the Group of Experts participated as speakers in two WCO meetings in Brussels on enforcement of controls in relation to strategic trade.

The Organization for Security and Cooperation (OSCE) in Europe has also helped to extend the Committee's reach in organizing meetings, with support from UNODA, with a particular focus on developing voluntary National Implementation Action Plans (NAPs). These activities have involved meetings in Vienna with representatives from Armenia,

1 The meetings included representatives from the following non-reporting States: Cabo Verde, Central African Republic, Chad, Comoros, Equatorial Guinea, The Gambia, Guinea, Guinea Bissau, Haiti, Malawi, Mali, Mauritania, Sao Tome and Principe, Swaziland, Zambia and Zimbabwe. Representatives from Brazil, Republic of the Congo, Gabon, Lesotho and South Africa also participated.

Briefing at the Dedza border post, during the 1540 Committee visit to Malawi, at the invitation of its Government, 8 August 2014

Uzbekistan and, in Ashgabat, from Turkmenistan. An important event in June, in cooperation with the OSCE, was an address by the Chair of the 1540 Committee, Ambassador Oh Joon, to the Dialogue Meeting of the OSCE's Forum for Security Cooperation.

Another important event involving representatives of international and regional organizations was the convening of a meeting by UNODA in Vienna to share experiences with technical assistance programs and to share effective practices.

Looking ahead, in other regions of the world, we are looking forward to an Asian regional 1540 tenth anniversary event in Seoul in October, sponsored by the Government of the Republic of Korea. In Latin America and the Caribbean, UNODA's regional office in Lima, Peru, is embarking on a series of events to enhance implementation of resolution 1540(2004) through an assistance package on strengthening the implementation of the resolution in the Caribbean States, in this regard, a national round table took place in Grenada in June 2014.

The participation by the experts has been constrained somewhat by the departure earlier this year of three members of the Group of Experts, Nicolas Kasprzyk (France), Petr Litavrin (Russia) and Dana Perkins (USA). We wish them well in their future endeavors. Their replacements were selected by the 1540 Committee last May but they have yet to take up their posts. They are Gennady Lutay (Russia), Rafaël Prenat (France) and Michael Rosenthal (USA). We look forward to their arrival in early autumn.

Promotion of CBRN Security Culture: Background Information Sheet

Date	Select Events, Products, Deliverables	Comments
	2012	
February	International Workshop "In Search of Sustainable CBRN Security Culture," Athens, GA, USA	Organized by the Center for International Trade and Security at the University of Georgia (CITS/UGA) in cooperation and partnership with UNODA, Nuclear Threat Initiative and Stanley Foundation
March	Release of the CITS/UGA report "Nuclear and Radiological Security Culture: A Post-Seoul Summit Agenda" and distribution on the margin of the 2012 Nuclear Security Summit in Seoul, Republic of Korea	
April	Meeting "Towards a CBN Security Culture: developing a holistic approach", Vienna, Austria	The event was hosted by the Permanent Mission of Hungary to the United Nations in Vienna and organized in cooperation with UNODA
May	Workshop on CBRN Security Culture for Indonesia's counterterrorism task force, Jakarta, Indonesia	Organized by CITS/UGA and supported by the Carnegie Corporation of New York (CCNY)
November	Conference on the Establishment of the International Center for Chemical Safety and Security (ICCSS), Tarnow, Poland	CITS/UGA joined as a partner and contributed chemical security culture content to the proceedings
November	A series of briefings on the methodologies for self-assessment of nuclear security culture for the management of Indonesia's nuclear research reactors in Serpong, Yogyakarta and Bandung.	CITS/UGA helped Indonesia's National Nuclear Power Agency (BATAN) implement the self-assessment pioneering project in cooperation with the IAEA and with support from CCNY
	2013	
March	Review of the results from the pilot project for self-assessment of nuclear security culture at BATAN's three research reactors, Jakarta, Indonesia	CITS/UGA continued to support the self-assessment project in collaboration with the IAEA
July	Presentation of the paper "Nuclear Security Culture in Practice" at the IAEA International Conference on Nuclear Security, Vienna, Austria	The paper was jointly developed by CITS/UGA and BATAN for the conference and presented at a plenary meeting
October	Meeting "Developing a Comprehensive Security Culture Chemical, Biological, Radiological and Nuclear (CBRN): Threats and Responses", Vienna, Austria	The event was hosted by the Permanent Mission of Hungary to the United Nations in Vienna and organized in cooperation with UNODA and VCDNP
November	Roundtable on Building CBRN Security Culture for GUAM Countries (Georgia, Ukraine, Azerbaijan and Moldova), Baku, Azerbaijan	The event was organized by the Science and Technology Center in Ukraine (STCU) and UNODA in partnership with CITS/UGA which provided training material and exercises

	2014	
January	Briefing for the management team of the Kozloduy NPP on the IAEA draft methodology to self-assess nuclear security culture, Kozloduy, Bulgaria	CITS/UGA participated in the IAEA mission as lead drafter of the self-assessment methodology
March	Release of the report "Human Dimension of Security for Radioactive Sources: From Awareness to Culture" and distribution on the margin of the 2014 Nuclear Security Summit in the Hague	The report was jointly developed by CITS/UGA and Indonesia's BATAN
April	Open Briefing for International and Regional Organizations on Comprehensive CBRN Security Culture, Vienna, Austria	The event was co-organized by UNODA and OSCE Conflict Prevention Center and CITS/UGA made a keynote presentation at this event
April	Workshop on CBRN Security Culture for Indonesia's Armed Forces and Law Enforcement agencies, Jakarta, Indonesia	The workshop was organized by CITS/UGA in partnership with Indonesia's BATAN and funded by CCNY
June	Comprehensive (CBRN) Security Culture Seminar, Budapest, Hungary	The Seminar was organized by the Hungarian Institute of International Affairs together with the Ministry of Foreign Affairs of Hungary and UNODA
June	NATO Advanced Study Institute "CBRN Security Culture in Practice," Yerevan, Armenia	CITS/UGA organized the week long ASI with support from UNODA, OSCE, Swedish Radiation Protection Agency, DOW Chemical and other partners.
September (pending)	Publication of a special issue of the "1540 Compass" devoted to the Comprehensive (CBRN) Security Culture	CITS/UGA in cooperation with UNODA
September (pending)	International Conference "Promoting Security Culture in South East Asia," Serpong, Indonesia	CITS/UGA is organizing this event jointly with Indonesia's BATAN to inaugurate its newly established Center for Nuclear Security and Assessment as well as discuss its programmatic activity for the next two years. The scope of work will cover CBRN security culture and its promotion. The conference is supported by UNODA, the Partnership for Nuclear Security (PNS) and CCNY
November (pending)	Side event on CBRN security culture for the Global Partnership (GP) Meeting, Berlin, Germany	It is designed as a one day event for GP donors to discuss the benefits and dimensions of comprehensive CBRN security culture, particularly as applicable to the Centers of Excellence. CITS/UGA was requested to provide substantive context, develop the agenda and select speakers.

The 1540 Compass
Center for International Trade & Security
120 Holmes/Hunter Academic Building
Athens, GA 30602
USA


Holmes/Hunter Academic Building, University of Georgia

The 1540 Compass is a publication of the Center for International Trade & Security at the University of Georgia

The Center for International Trade & Security's mission is to mitigate the global spread of nuclear, biological, and chemical weapons. The Center carries out this mission by researching the dynamics of arms trade control, training government and industry representatives to implement policies that limit the spread of these weapons, and educating students in the discipline of nonproliferation and international security. With offices on the University of Georgia campus and in the U.S. capital, CITS bridges the worlds of research and policy, bringing the best of each to the other.

706-542-2985 http://cits.uga.edu

Contact the Compass:

http://cits.uga.edu/publications/compass

Editor in Chief: Igor Khripunov
i.khripunov@cits.uga.edu

Managing Editor: Christopher Tucker
c.tucker@cits.uga.edu