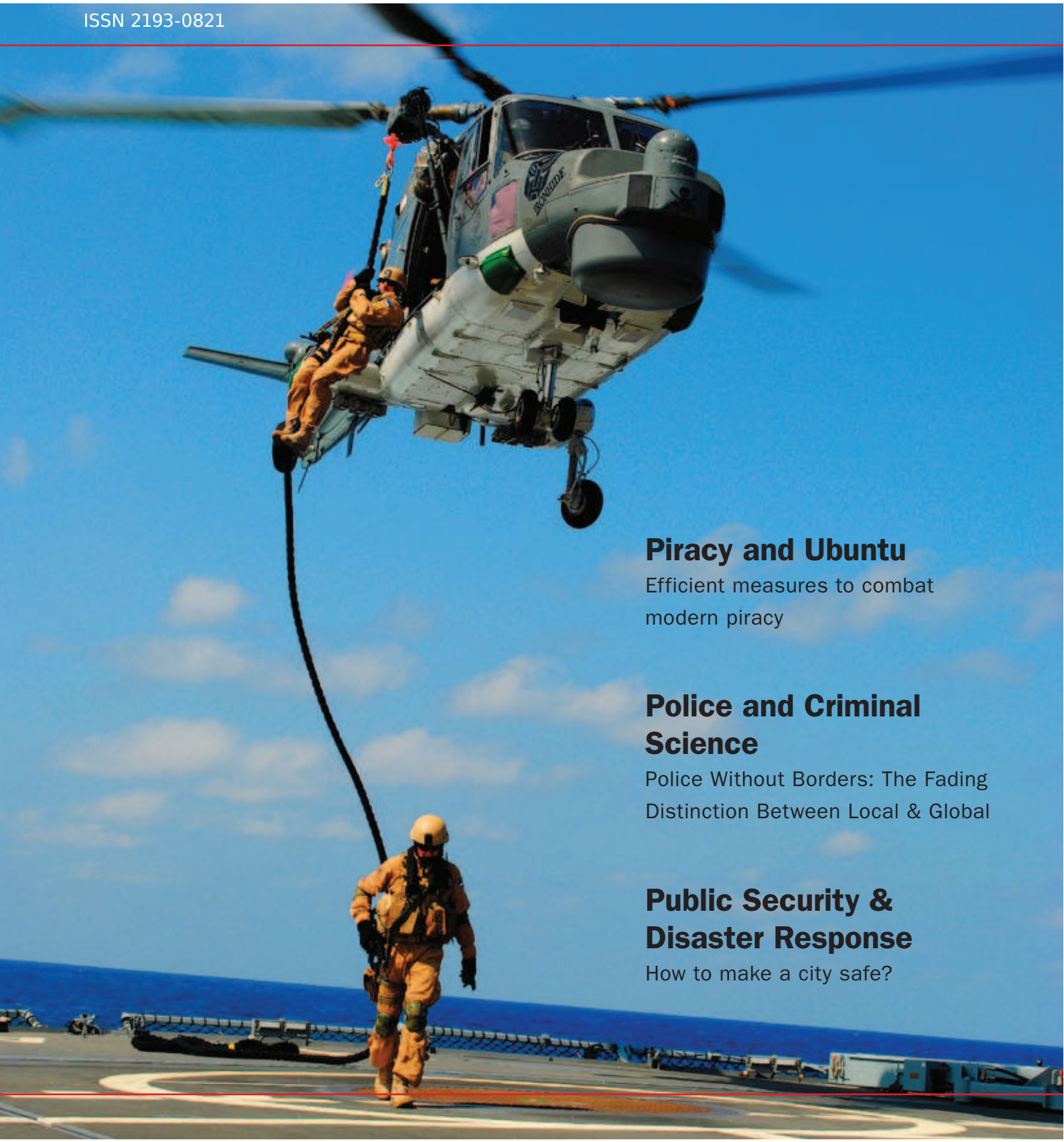
GLOBAL SECURITY

PUBLIC SECURITY AND DISASTER RESPONSE

2012

ISSN 2193-0821



Piracy and Ubuntu

Efficient measures to combat modern piracy

Police and Criminal Science

Police Without Borders: The Fading Distinction Between Local & Global

Public Security & Disaster Response

How to make a city safe?

www.homeland-sec.de

Public Security - Disaster Response - Comprehensive Approach

Piracy and Ubuntu

Efficient measures to combat modern piracy

Professor Dr. Cornelis Roelofse
Lukas Swart

The Horn of Africa actually exists of three different entities. Somaliland in the north is a stable area and for all intents is an autonomous state. This will probably be confirmed through a referendum and should lead to the establishment of an independent state. Puntland is a semi-autonomous region that forms the tip of the horn and then there is Somalia, a volatile and troubled region. This is the safe haven for Somalia pirates. The article presents an approach to piracy, perpetrated by Somali pirates from a practical point of view developed within specific theoretical perspectives in Criminology and the African culture of ubuntu.

Background

Piracy is an ancient crime. Caribbean pirates are the most notorious and continuously harassed the Spanish galleons carrying valuable articles back to Spain in the 16th and 17th centuries. We are all familiar with the infamous names of pirates such as Blackbeard and Calico Jack. Pirates, always make use of safe havens. The Caribbean Pirates used Port Royal and Jamaica where they enjoyed protection against attack. Piracy is actually much older than the romantic period so aptly portrayed by Captain Sparrow in the movies. During the 1st century BC, there were pirate states along the Anatolian coast, threatening the commerce of the Roman Empire in the eastern Mediterranean. On one voyage across the Aegean Sea in 75 BC, Julius Caesar was kidnapped by Cilician pirates and held prisoner in the Dodecanese islet of Pharmacusa.[1] A ransom was claimed and paid but after the incident, Caesar's fleet pursued the pirates and killed them. Modern day piracy is a phenomenon that enjoys international focus and a large part of that focus is on Somalian pirates operating as far south as the Mozambique Channel and 1,000 nautical miles off the coast of Somalia. This article takes a look at modern day piracy and focuses on efficient ways to deal with this menace.

Definition

Piracy has been defined by international and national treaties and resolutions and/or law.

International Definition of Piracy[2] is taken from the 1982 "United Nations Convention on the Law of the Sea" or UNCLOS but for sake of space is not repeated here.

International statistics

According to NATO, there are 22,000 ships which travel in the Gulf of Aden. This makes heavy traffic and provides ample pry for pirates. The incidences of piracy in 2011 alone, around 1,000 hostages were in the hands of pirates and around US 126 million dollars were paid to their ravisseurs explaining also to what extent pirates and piracy may be a very profitable job.[3]

The International Maritime Bureau[4] reports that during the first six months of this year alone there were 196 confirmed pirate incidents globally. Of those incidents, 31 resulted in completed hijackings with 544 crew taken hostage. There still remain 360 crew members being held hostage as of June 30, 2010. Completed pirate hijackings in the first six months of 2012 represent 15.8% of all attempts.

Theoretical arguments

Although there are today no reliable statistical sources, the Somali population is estimated between 7.5 and 9.9 million people.[5] Of that figure, the entire Bantu population in southern Somalia is estimated at about 600,000, and those with strong east African identification are estimated at a fraction of that number. The Bantu people are ethnically and culturally distinct from the Somali nomads and the coastal people, who generally disdain agriculture and value a tribal lineage system that does not include the Bantu. A Security operator, and co-author of this article, who worked aboard a Russian vessel in the Gulf area and off the coast of Somalia states that from his experience, the pirates are primarily Somalia Bantu. There is speculation about the possible influence of Islamic elements in piracy but it is necessary to refer readers to the ethnic composition of Somalia of which only 40,000 are of Arab origin and some 600,000 Bantu. The rest are ethnic Somalis. One can also not fall trap of directly connecting ethnicity to religion as the Bantu belong to different religions. What is however not so commonly known is that they often practice or at least belong to more than one religion, unlike Muslims. A Bantu confessing Christ may still worship forefather spirits. However what runs through the Bantu culture and religious practices is the ubuntu culture.

The word 'Ubuntu' comes from one of the Bantu dialects of Africa. It is a traditional

[1] US Legal. Maritime Piracy Law & Definitions. Available at http://definitions.uslegal.com/m/maritime-piracy/ Accessed on 10 September 2012

[2] The United Nations Convention on the Law of the Sea (UNCLOS in article 101. Available at http://www.un.org/Depts/los/convention_agreements/texts/unclos/unclos_e.pdf

[3] Gunputh, R. Police and Military Response to Maritime Piracy in the Indian Ocean Organised crime: Mauritian Case Study. in Roelofse, CJ. Oliver CE. And Kgosimore, DL. (Eds) (2012) Organised Crime and Other Criminal Justice Issues in Africa. Mankweng. ACJUS. University of Limpopo.

[4] See http://www.lradx.com/site/content/view/286/110?utm_campaign=ppc&utm_medium=web&utm_source=google&utm_content=commercial_security&utm_term=commerical_maritime&gclid=CJ3XiIXlm7ICFWLHtAodxBUA2A

[5] See The Cultural Orientation Project at http://www.cal.org/co/bantu/sbpeop.html

Serious Concerns about Fukushima No. 1

The lack of information by TEPCO

Professor Dr. Minoru Yokoyama,
Faculty of Law,
Kokugakuin University,
Tokyo, Japan



The bloom of Japanese Cherry Blossoms in a park in Tokyo - photographed by Professor Dr. Minoru Yokoyama on April 10, 2011.

Tokyo Electric Power sought to construct more nuclear power plants under a plan to lift the supply of nuclear electric power from 30 % to 50 %. This was being promoted by the Japanese National Government. The Fukushima No 1 Nuclear Power Plant was hit by an unexpected large earthquake at 14:46 p.m. on March 11, 2011. Fortunately, three reactors stop generating electric power immediately after the earthquake by the emergency control system. Then, the uranium fuel rods were cooled for a while by water in their container vessels. It was hoped this would prevent explosions. However, after the Tsunami hit the plant at 15:27 p.m., they failed to continue supplying water under the Emergency Core Cooling System, as all electric power was lost in the plant. This caused uranium fuel rods to be exposed from their cooling water. These began to reheat and subsequently resulted in hydrogen explosions in the No. 1 reactor at 15:36 p.m. on March 12 and in the No. 3 reactor at 6:10 a.m. on March 15.

Despite this increasingly serious situation, Tokyo Electric Power provided the Japanese Government, media and the public with only fragmentary information from the optimistic standpoint. Later the company was blame by the estimation that many residents living near the plant might be bathed in radiation leaking at the time of the explosions owning to the lack of adequate information. It seemed that Tokyo Electric Power hesitated to offer the exact data in detail, because the company did not wish to de-commission the reactors at Fukushima No. 1 Nuclear Power Plant while seeking to construct two new reactors at the campus in the near future.

Given the exact information about the serious situation, the residents might change their supportive opinion about the plan to increase the nuclear reactors. Then, Tokyo Electric Power carefully avoided using words to express the serious situation. For example, at the press conference the company did not mention “the explosion of a nuclear reactor” soon after the hydrogen explosions at their No. 1 and No. 3 reactors occurred. If the company had wanted to prevent people’s safety from leaking

Executive Knowledge of White-Collar in Crime Business Organizations in Norway

Superintendent Professor Rune Glomseth
Professor Dr. Petter Gottschalk

Research Design for Empirical Study

The five hundred and seventeen largest business companies in terms of annual turnover were identified in Norway for our empirical study of white-collar crime. A letter was mailed to the chief financial officer asking him or her to fill in the questionnaire to be found on a web site using a password found in the letter. The research was carried out by a web-based questionnaire combined with a letter to the largest business organizations in Norway.

65 respondents filled in the questionnaire after the first letter, 45 responses were received after a reminder, and another 31 responses were received after a second reminder. Thus, a total of 141 complete responses were received. 141 complete responses out of 517 potential responses represent a response rate of 27 percent. In addition, 36 incomplete responses were received, creating a gross response rate of 34 percent. The survey web site was open to responses from January to April in 2010.

Separate analysis was conducted on the first set of responses, then the second set, and finally the third set included. This analysis shows few changes in results when moving from 65 via 110 to 141 responses. Thus, the analysis suggests that non-respondents might have provided similar responses to actual respondents.

The average number of employees in the 141 business organizations with complete answers was 1,719 persons. The largest responding firm in terms of employees had 30,000 persons in their staff.

Respondents were asked to type in their current position, even though the letter was specifically mailed to the top executive in charge of finance often called chief financial officer (CFO). Most of the respondents were indeed CFOs, but some were CEOs, corporate controllers, managers of finance, and chief group controllers.

The average age among respondents was 48 years among the first 65 responses, and they had 4.4 years of college and university education on average. The average age decreased to 46 years when the first reminder responses arrived, while the average education increased to 4.8 years. There were 91 men and 19 women responding after the first reminding letter.

The average age remained at 46 years after receipt of the final 31 responses, while average education continued to increase to 5.1 years. There were 117 men and 24 women among the total 141 respondents. The only change, therefore, seems to indicate that higher educated persons tend to respond more frequently after reminders.

The purpose of this text is to create insights into executives' knowledge of white-collar crime in Norwegian business organizations. That involves mapping their perceptions of magnitude, attitude, risks and offenders. In terms of risk, respondents suggest that probability of white-collar crime is low, while consequences when occurring are substantial. Most likely position category for white-collar crime is a purchasing manager in charge of procurement, followed by a marketing manager, and a person in executive management. It is argued that internal and external control authorities need to focus less on routines and regulations and more on persons in vulnerable positions.

Both descriptive statistics as well as correlation analysis in this text provide new insights into the extent of white-collar crime, as well as attitudes, risks and vulnerable positions for white-collar crime. Concerning executives own knowledge, they claim to be more competent in discovering white-collar crime than investigating such crime. They also claim an increased police competence in this field in Norway. Survey research was applied to find empirical answers to questions such as: The occupants of what roles and positions in the organizations are most likely to commit white-collar crime? What is the probability of various crime types being committed? What are the consequences of various crime types?

Magnitude and Executive Attitude

The first set of questions was concerned with the extent of and attitudes towards white-collar crime. Responses were measured on a scale from 1 (completely disagree) to 5 (completely agree). Average responses to all items are listed in Table 1.

Given an average score of 3 representing neither agreement nor disagreement, most statements achieve varying degrees of disagreement in the Table. The first

The American view of computer security

„The main objective of computer security is to ensure IT systems provide the availability, integrity and confidentiality necessary successfully supports their missions and businesses", Jim Litchko, CISSP-ISSEP, MBCI, MAS, said in an interview with Dr. Nadine Seumenicht from Homeland Security. Due to the growing impact of cyber crime users are more involved in the process of how to achieve computer security and they examine in more detail which resources should be implemented into existing systems.

Homeland: What is the main objective of computer security? What kind of influence has 9/11 on it?

Litchko: To me the main objective of computer security is to ensure IT systems provide the availability, integrity and confidentiality necessary successfully supports their missions and businesses. In my opinion, 9/11 did not have a big influence; it was more regulations, business losses (like Enron) and the privacy of personal information concerns before 9/11 that had the biggest impact on computer security. Government mandates had come out prior to 9/11 that required computer systems have to be secure. There are several federal cybersecurity regulations that focus on specific industries. A good example is the Health Insurance Portability and Accountability Act of 1996 (HIPAA), which establishes national requirements for organizations to protect individuals' personal health information. This regulation mandates that healthcare organizations protect their systems and patient information. Another one was Sarbanes–Oxley Act of 2002 (SOX) or the Public Company Accounting Reform and Investor Protection Act that was passed because of the major accounting scandals: Enron, Tyco International and WorldCom. The one that made the largest impact on government systems was the Federal Information Security Management Act (FISMA), which came out in December 2002, over a year after 9/11. FISMA applies to every government agency and their contractors.

Homeland: What was particularly important in the past as regards to the current development of computer security?

Litchko: When FISMA came out in 2002 it introduced several key concepts. First and most important, it put one person in charge of overseeing all government computer security, who was not only the responsibility, but also the authority over resources to deploy security solutions. I was a Navy Officer and one of the first things we learned was to never to accept the responsibility for something without having the authority to achieve success. If you do not have authority you do not have resources and you cannot enforce your decisions. FISMA put the Officer Management and Budget (OMB) in charge of the overseeing government security. That was important. Prior to FISMA, they tried telling government agencies to improve their security, but it did not work because there was no incentive for agencies to deploy a good security. With FISMA, they applied the "golden rule", which is "they with the gold rules". You see OMB oversees all of the agencies' budgets, in other words they control the funding that goes to the agencies. Additionally, OMB reports to Congress and the agencies were given individual grades, A through F, as to how good their security was.

Another key concept was they did not say in 2002 that all agencies will have all of their systems secured now. They took little steps initially to get the agencies to know what systems they had and what their security requirements were. The first things OMB asked the agencies:

- How many systems do you have, how many have approved security, and how many are left to be approved;
- How many systems do you have inventories for and what is your process for maintaining those inventories;
- How many employees have had computer security awareness training, etc.; and,
- Do you have programs for improving employee security awareness and key security personnel's security knowledge and skills?

OMB focused on making the agencies slowly grow their security capabilities. It was not until 2008 that the agencies had a good understanding of their systems' security requirements that is when OMB started to require the same reporting on the agencies' contractors' systems. At first, OMB focused on securing individual systems. Once they had all the systems documented that focus shifted to having the agencies look at IT security from an enterprise level and to deploy good monitoring and common controls. So, every year, OMB kept "raising the bar" on what the agencies needed to accomplish, so that the agencies would continue to improve their security. Additionally, this affected the security product vendors as they realized that if they automated there security products they would be

How to make a city safe?

Tillmann Schulze
Maurice Illi



Improved flood prevention and protection

The safety and security situation of cities changes constantly. What relevance for cities do incidents have that are relevant for civil protection? How the people in charge get the required basis for planning and decision-making is shown on the Safety and Security Reports of the City of Lucerne. From this approach all cities can benefit.

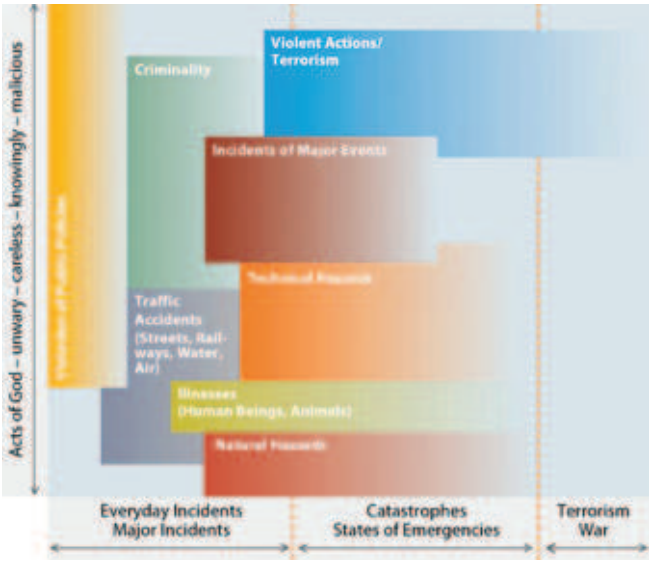
The last six month were affected by catastrophes: Extreme floods hit Eastern Australia while the Western part suffered from massive drought. Tornados of unknown power devastated parts of the U.S. Then Japan: earthquake, tsunami, nuclear power disaster. Looking at these incidents from a city's perspective it quickly becomes clear: Cities are unable to cope with such catastrophes and comparable states of emergencies. Even bigger communities like states with their crisis and emergency response organizations arrive at their limits. But it is the cities that are directly affected by such incidents. It is their population, it is their infrastructures and key assets which get damaged or even destroyed.

But looking at last month's local headlines, for cities other hazards seemed to be more important: Criminality for instance or violence in public spaces. Is it right to address primarily hazards that one will find in the local headlines in the newspaper? Wouldn`t it be necessary that a city also addresses hazards with a low feasibility of occurrence but that result in huge damage? That was a question the city of Lucerne was dealing with. They received their answers in two Safety and Security Reports.

Breaking new ground

Some years ago the safety and security department was convinced: A Risk Management was needed for the city of Lucerne. It would be the only way to get the city prepared for the relevant challenges in the context of safety and security. So the head of the department decided in 2005 to compile the first comprehensive Safety and Security Report for the city of Lucerne.

An integral, risk-based approach should be the basis for this report. Until now there is no other city that has chosen such an approach to assess their safety and



Overview of relevant hazards for Lucerne

modern technology, pervasive ideology, and radicalisation addressed the global threat in the wider geographical regions including the Arab Peninsula as well as Africa.

James Brokenshire MP



Former High Commissioner of India to Pakistan, Australia and Cyprus, Mr G Parthasarathy warned that another Mumbai style attack on India cannot be ruled out. He specifically tackled the 'Challenges of Terrorism in India,' and warned of the escalated risk from the Taliban and Haqqani networks, if they were to strengthen their hold in Afghanistan following the pull-out from the West. "India would like to cooperate with regional countries and the international community to ensure that Afghan soil does not become a haven for terrorists, who are determined to attack Indian soil and Indian interests abroad. Diplomatic processes to achieve this have to be inclusive and supportive of the democratically elected Government and Parliament in Afghanistan."

The summit featured record breaking attendance from foreign delegations from across Asia, including representatives from the Defence, Police, Military, and Para-military forces of Nepal, Myanmar, India, Georgia, Oman, Japan, Taiwan, Brunei, Myanmar, Saudi Arabia, Poland, UAE, Jordan, Somalia, and Bangladesh, among others.

For a full list of speakers, foreign delegations, exhibitors, and subject information go to http://www.securing-asia2012.com

Following on from the resounding success of the Securing Asia 2012 Homeland Security and Counter Terror Summit, Securing Asia 2013 will be held next on 18th - 19th June 2013, with the ultimate goal to bring to the western corridor a host of Asian government buyers and influencers looking to source the latest information and solutions on counter terror and homeland security.

Imprint

Editorship: Dr. Nadine Seumenicht
Publisher: Dr. Nadine Seumenicht

Advisory Team
Comprehensive Approach: Harald Kujat, General a. D.
Net Centric Operation: Dr.-Ing. Andreas Groth; Ralph. D. Thiele, Oberst i. G.

International Editorial Team
Comprehensive Approach: Dr. Stefan Queisser, Fregattenkapitän d. R.; Michael Hartung, Oberleutnant d. R.
Civil-Military Cooperation: Hauke Muck, Oberstleutnant d. R.; Michael Zacher, Major d. R.
IT-Security: Georg Wenner, EDS-CSO Germ. Gov. a. D.; Jim Litchko, CISSP-ISSEP, MBCI, MAS
Robotics Unstructured Environments: Prof. Dr.-Ing./Univ. Tokio Thomas Bock
International Criminology: Robert F. J. Harnischmacher
Safety and Security Training in Economic Matters: Klaus- Dieter Jörn; Robert F. J. Harnischmacher
Austria: Hofrat Mag. Maximilian Edelbacher
Canada: Prof. Dr. Darryl Plecas
China: Prof. Dr. Gu Minkang
Japan, Korea: Prof. Dr. Minoru Yokoyama; Prof. Dr. Dr. h.c. mult. Haruo Nishihara; Prof. Dr.-Ing./Univ. Tokio Thomas Bock
Mexico: Walter M. McKay, M.A.
Norway: Superintendent Prof. Rune Glomseth; Prof. Dr. Petter Gottschalk
Poland: Prof. Dr. Dr. h.c. Brunon Holyst
South Africa: Prof. Dr. Cornelis Roelofse
USA: Prof. Dr. Dilip K. Das; Prof. Dr. Otwin Marenin; Prof. Dr. Linda Keena
Capital City Office in Berlin: Heike Barnitzke
History: M. A. Volker Hollmann
Politics: Dipl. Verw. Joachim Zacher
Science: Prof. Dr.-Ing. Michael Gerke; Dr. Nadine Seumenicht
Design and Layout: Christian Prünte

Publishing House:
HOMELAND SECURITY UG
(haftungsbeschränkt)
Deilinghofer Straße 2, D-58675 Hemer, Germany
Tel.: +49 (0)2372-9 35 26 10
Fax: +49 (0)2372-9 35 26 19
redaktion@homeland-sec.de
www.homeland-sec.de

Single price:
10,- EURO (incl. 7% VAT and delivery within Germany)

Annual subscription:
18,- EURO (2 issues a year)
Aktion Deutschland Hilft e. V. benefits with 1, - EURO per subscription.

Circulation:
16,000
ISSN 2193-0821
Issue 1

Picture credits:
Cover: Bundeswehr/PIZ Marine

Aktion Deutschland Hilft e. V., Bayer MaterialScience LLC, O a. D. Ruthard Berberich, Bundeswehr, Bundeswehr/Laudan, Bundeswehr/PIZ Djibouti, Bundeswehr/PIZ Marine, Bundeswehr/PIZ Marine Djibouti, Curzon Public Relations, Ernst Basler + Partner, Superintendent Prof. Rune Glomseth, Prof. Dr. Petter Gottschalk, Robert F. J. Harnischmacher, Homeland Security, ISL - Institute of Shipping Economics and Logistic, Japanese Red Cross, JENOPTIK AG, Dr. Hans-Joachim Kolb, Jim Litchko, MEDAV, Dr. Nils Meyer-Larsen, MILIPOL Qatar, Prof. Dr. Cornelis Roelofse, Prof. Klaus-Ehrenfried Schmidt, Arne Schönbohm, Smiths Heimann, Stadt Luzern, Lukas Swart, UNIFIRE AB, Vetter, WEW Westerwälder Eisenwerk, Prof. Dr. Minoru Yokoyama

If we refer to the Internet pages of third parties, HOMELAND SECURITY UG (haftungsbeschränkt) assume no responsibility or liability for the content of the pages.
The views of the contributors are not necessarily the views of the publisher and editor.