Crisis Management

5th Annual ISDP-AMS Conference
October 19-21, 2012

Edited by
David Mulrooney

CONFERENCE REPORT

Institute for Security &
Development Policy

Crisis Management

5th Annual ISDP-AMS Conference
October 19-21, 2012, Stockholm

Edited by

David Mulrooney

Contents

Foreword

It gives us great pleasure to introduce the proceedings of the fifth annual joint conference held by the PLA Academy of Military Science (China) and the Institute for Security and Development Policy (Sweden), which was held in Stockholm in October 2012. The joint conference is now a well-established tradition for both of our two institutions, and one that we hope to continue into the future. We believe that events such as this, which bring together Chinese military experts and scholars of international affairs together with their foreign counterparts, are important opportunities to build trust, enhance mutual understanding and gain deeper insight into each other's perspectives.

Crisis management, the subject of this year's conference, is a particularly important area for co-operation. One of the main trends in military affairs the world over is that the armed forces are increasingly being called upon to play a leading role in non-combat operations such as emergency rescue, disaster relief and contingency response. The People's Liberation Army has long played an important role in such operations in China, and in recent years has distinguished itself by its effective response to the earthquakes in Sichuan in 2008 and again this year, and in the Libya non-combatant evacuation operation in 2011.

This conference considered approaches to crisis management from a comprehensive point of view. In addition to looking at crisis management in the traditional security area—in the Middle East and on the Korean Peninsula—the presentations also covered areas such as counter-terrorism, cyber security and the use of social media in disaster emergency response.

We took away from this conference a conviction that responding effectively to a diverse set of threats requires both good advance planning and flexibility in execution. We also concluded that there is much to be gained by sharing lessons learned in responding to previous crisis situations, and that the possibilities for international co-operation in the area of crisis management are great.

Major General He Lei, PLA AMS
Dr. Niklas Swanström, ISDP

前 言

　　我们非常荣幸地推出 2012 年 10 月在瑞典斯德哥尔摩举行的第 5 届中国人民解放军军事科学院与瑞典安全和发展政策研究所联合研讨会论文集。联合研讨会是两家研究机构建立的一个机制良好的合作项目，我们希望能够在未来继续深入开展下去。我们相信，像联合研讨会一类的学术活动，即把中国军方的专家和国际问题学者与其他国家的专家学者聚集在一起，是建立信任、增进互信并深入了解双方观点的良好平台。

　　今年的会议主题"危机管理"，是一个特别重要的合作研究领域。世界范围内军事领域出现的一个主要趋势是，武装部队越来越多地在诸如紧急救援、救灾和紧急反应等非战争行动中发挥作用。中国人民解放军在该领域一向发挥着重要作用，特别是近年来在诸如应对 2008 年汶川地震、2011 年利比亚非战斗人员撤退等行动中，表现出色。

　　本届研讨会从综合的角度探讨了危机。除了探讨传统安全领域中的危机管理问题如中东地区和朝鲜半岛之外，会议发言也涉及到反恐、网络安全以及在灾难应急反应中社交媒体使用等内容。

　　通过本次研讨会我们更加坚信，要有效应对各类威胁，预先做好完善计划、在实施过程中保持灵活等十分重要。我们也认为，分享过去应对危机的经验让参会者受益良多，并且在危机管理领域的国际合作十分重要。

中国人民解放军军事科学院　何雷少将
安全和发展政策研究所所长　施万通

Acknowledgements

As we bring the proceedings of our fifth joint conference with the PLA Academy of Military Science to press, we would like to take the opportunity to acknowledge a number of individuals for their contribution to the success of this event. First, we would like to thank Lieutenant General Liu Chengjun, the President of AMS, and Major General He Lei, the Head of the Science Research Guidance Department at AMS, for their support. We also wish to express our appreciation for the work of Colonel Zhu Yuxing of the Foreign Affairs Office at AMS in helping us to plan and organize this event.

We are extremely grateful to the Swedish Ministry for Foreign Affairs for sponsoring this conference. We also wish to thank Mr. James Barker of the British Embassy in Beijing for his assistance with the arrangements for the speakers from the United Kingdom. Finally, we would like to extend our deep appreciation and thanks to all speakers and participants for their contributions.

The sixth annual ISDP-AMS joint conference with AMS will be held in Beijing in December 2013.

Dr. Niklas Swanström
Director, Institute for Security and Development Policy

Order of Events*

Saturday, October 20, 2012

Session 1: Responding To Natural Disasters
Moderator: Major General Karlis Neretnieks, Swedish Armed Forces (ret.)
- o Dr. Wang Dong, Peking University, "An Analysis of China's Military Operations other than War: the Policy and Academic Perspectives"
- o Dr. Jun Kurihara, Canon Institute for Global Studies, Japan, "Post-Fukushima Nuclear Safety Scheme: In Search of a Confluence of Nature and Science"
- o Dr. Cécile Wendling, Fondation nationale des sciences politiques, Paris, "The Use of Social Media in Disaster Emergency Response"

Session 2: Terrorism And Non-Traditional Security Threats
Moderator: Dr. Wang Dong, Peking University
- o Ambassador Tomas Rosander, Ministry of Foreign Affairs of Sweden, "To Prevent: Things we need to do better"
- o Colonel Wang Xiaobin, PLA Academy of Military Science, "Studies On The System And Mechanism Of Counter-Terrorism Emergency Command"
- o Prof. Akiko Yamanaka, former Vice-Foreign Minister of Japan, "Learning From The Past: Japan's Experience With Man-Made And Natural Disasters"

Sunday, October 21, 2012

Session 3: Cyber security And Emerging Technological Threats
Moderator: Mr. Olof Ehrenkrona, Ministry for Foreign Affairs of Sweden
- o Senior Colonel Fan Gaoyue, PLA Academy of Military Science, "Threats To Cyberspace And Responses"
- o Mr. Nick Haycock, Office of Cyber Security and Information Assurance, Cabinet Office, Whitehall (UK), "Prevention is Better than Cure"

Session 4: Dealing With Political Emergencies
Moderator: Senior Colonel Fan Gaoyue, PLA Academy of Military Science
- o Dr. Chang Kwoun Park, Senior Research Fellow, Center for Security and Strategy, Korea Institute for Defense Analyses (ROK), "Crisis Management in Relations between South and North Korea"
- o Lieutenant Colonel Simon Gray, Senior Military Advisor in the Security and Justice Group of the UK's Stabilisation Unit, "Building Stability Overseas, Crisis Prevention And Response"
- o Dr. Fredrik Bynander, Swedish National Defence College, "Political Crises: Spill-Over Effects And Vicarious Learning"
- o Dr. Liselotte Odgaard, Royal Danish Defense College, "China's UNSC Policy and Its Implications for Security Management in the Middle East"

---

* *Note: the papers delivered by Dr. Kurihara, Dr. Bynander and Lt. Col. Gray are not included in these conference proceedings*

Opening Remarks

Niklas Swanström, Director, ISDP

This year's conference will approach the topic of crisis management from a variety of perspectives in order to try to gain a better understanding of where we stand today and is an opportunity to consider ways in which we can cooperate more effectively in the future at a regional as well as at an international level. Cooperation is increasingly necessary, as many of the issues we face are transnational in nature and demand more cooperative and integrative solutions. The aim of this conference is to bring together policy makers and experts from the academic, military and government sectors to discuss the evolving art of responding effectively to crises in the twenty-first century.

Governments today are faced today by a range of eventualities that have little in common with one another beyond the need for rapid and effective responses, possibly involving coordination between multiple different civilian and military authorities. The past decade has seen incidents of terrorist attacks, natural disasters, industrial accidents and outbreaks of pandemic diseases in various countries around the world, all of which have presented challenges that governments have met with often mixed results. The coming decade may well see new kinds of crises emerge, e.g. if cyber-weapons are successfully deployed in an attack on critical infrastructure, disabling power and communications systems.

States also face crises beyond their borders, as when the security of citizens overseas is threatened by kidnappings, hijackings and piracy. Moreover, a political emergency in one state can represent a crisis for another, as when states need to respond to events such as civil wars, coups d'état and regime collapses in neighboring countries.

The approach taken to managing such crises is deeply informed by a country's political system, domestic situation and foreign policy orientation, all of which differ greatly from one state to another. However, the questions raised by thinking about issues of crisis response have a general relevance, e.g. how should responsibilities be distributed across civilian and military authorities in times of crisis? How should the chain of command be structured? In an era of social media and rapid electronic communications, how should accurate information be disseminated to the public without causing panic? How should information be shared within and between states in times of crisis? What can we learn from the handling of past crises to better prepare us to manage future ones?

This conference brings together leading experts from Sweden, China, the UK, Japan, Denmark, South Korea, France and several other countries for presentations on and an exchange of opinions about the topic of crisis management.

An Analysis of China's Military Operations Other than War (MOOTW): Academic and Policy Perspectives

Dr. Wang Dong, Associate Professor and Director of the Center for Northeast Asian Strategic Studies at the School of International Studies, Peking University (China)

I. The Evolution of the Discourse of MOOTW in China

The concept of Military Operations Other than War (MOOTW) was first proposed by the U.S. military in the early 1990s in the wake of the end of the Cold War. It first appeared in the 1993 document JP 03-0 *Doctrine for Joint Operations*, and later was expanded in JP3-07 *Joint Doctrine of Military Operations Other than War*, jointly released by the U.S Joint Chiefs of Staff, Department of Army, Department of Navy, Department of Air Force and U.S. Marine Corps in June 1995. JP3-07 lists 16 types of MOOTW, including arms control; combating terrorism; Department of Defense support to counterdrug operations; enforcement of sanctions/maritime interception operations; enforcing exclusion zones; ensuring freedom of navigation and overflight; humanitarian assistance; military support to civil authorities; nation assistance/support to counterinsurgency; noncombatant evacuation operations; peace operations; protection of shipping; recovery operations; show of force operations; strikes and raids; and support to insurgency.[1]

Historically, the People's Liberation Army (PLA) of the People's Republic of China (PRC) has engaged in a variety of MOOTW activities, such as industrial and agricultural production (*gongnongye shengchan*), infrastructure development (i.e. building roads, railways, bridges), and disaster relief, even without being informed by the concept of MOOTW. The concept of MOOTW was not introduced in China until 2000. An article published in the *PLA Daily* in August 2000 briefly introduced the U.S. military's concept of MOOTW. Another piece appeared two years later in a military journal, which also discussed MOOTW in a more general way.[2] Both essays were among the earliest literature that touched on the concept of MOOTW. The earliest academic article that introduced MOOTW was by Zhu Zhijiang, a military scholar at the PLA Nanjing Institute of Politics, an institution affiliated with the General Department of Politics of the Central Military Commission (CMC). Zhu's

---

[1] The Joint Chiefs of Staff, Department of Army, Department of Navy, Department of Air Force and US Marine Corps, ''Joint Doctrine of Military Operations Other than War,'' Joint-Pub 3-07, June 15, 1995.

[2] Teng Jianqun 滕建群, "Mei 'feizhanzheng junshi xingdong' touxi" 美'非战争军事行动'透析 [An Analysis of US Military Operations Other than War]. *Jiefangjun bao* 解放军报 (PLA Daily), April 2, 2008, 12; Zhu Yunwei 朱运伟，"21 shiji jundui de zhongyao zhineng—feizhanzheng junshi xingdong" 21 世纪军队的重要职能——非战争军事行动 [The Main Functions of the Army in the 21st Century—Military Operations Other than War (MOOTW)], *Guofang keji zazhi* 国防科技杂志 (Journal of National Defense and Technology), 2002, no. 12, 63-66.

analysis of MOOTW, however, was mostly based on American texts and the experience of the U.S. military.[3]

To their credit, the Chinese military analysts had, as early as the early 1990s, developed original concepts that were close to MOOTW, such as the "Military Struggle in Time of Peace" (*heping shiqi junshi douzheng*), the "Military Struggle Through Means Other Than War" (*feizhanzheng fangshi junshi douzheng*), the "Non War Use of Military power" (*junshi liliang de feizhanzheng yunyong*) and "Operations Other Than War" (*feizhanzheng xingdong*).[4] As these concepts appeared more and more frequently in newspapers, magazines and academic works, a debate over the role and importance of MOOTW began to rage.

Advocates of MOOTW believed that the execution of MOOTW should be an important mission of the military, and the PLA should carefully study and actively participate in MOOTW; that MOOTW's role in fulfilling political goals under certain conditions, independent of war should be recognized, and that MOOTW should be included in the field of military and strategic studies. Opponents held that that an over-emphasis on MOOTW might dilute the military's focus on preparations for combat readiness, leading to a decline in the military's fighting capabilities; that MOOTW can at best be regarded as supplementary and subsidiary to operations of war, and it might be dangerous to exaggerate its importance; and that military and strategic studies should focus on war, and to include MOOTW in the fields of the military and strategic studies might be detrimental to the fields in the long run.[5]

The debate and development of the academic discourse of MOOTW gradually caught the attention of policymakers. Through meetings, briefings and internal reports, the academic discourse of MOOTW was translated into the policy realm, and the concept was gradually recognized and accepted by the top leadership in the PLA. It is worth noting that when it was first adopted by policymakers around 2001-2002, the terms in use was actually Operations Other Than War (*feizhanzheng xingdong*). In July 2001, The Military Training & Service Arms Department under the General Staff Department (GSD) edited and published the first ever "Training Material on Operations Other than War for the Chinese PLA" (*Zhongguo renmin jiefangjun feizhanzheng xingdong jiaocai*). The training material covers disaster relief operational details for contingencies such as floods, fires, earthquakes, etc. It was distributed to all PLA troops and military academic institutions for use, and became the template for the PLA's training program on MOOTW.[6] In September 2002, the

---

[3] Zhu Zhijiang 朱之江, "Lun feizhanzheng junshi xingdong" 论非战争军事行动 [Theory of Military Operations Other than War], *Nanjing zhengzhi xueyuan xuebao* 南京政治学院学报 (Journal of the Nanjing Institute for Politics), 2003, no. 5, 83-86.

[4] Xiao Tianliang 肖天亮, *Junshi liliang de feizhanzheng yunyong* 军事力量的非战争运用 [The Non-War Use of Military Power] (Beijing: National Defense University Press, 2009), 7. Major General Xiao Tianliang is head of the Department of Strategic Teaching and Research at National Defense University.

[5] Ibid.

[6] Ibid.; Xu Zhuangzhi 徐壮志 and Ma Xiaochun 马晓春, "The PLA will Begin Training on Operations

CMC approved and issued an updated version of "Training Regulations for the Chinese People's Liberation Army" (*Zhongguo renmin jiefangjun xunlian tiaoli*), which stipulates that the PLA needs to conduct trainings on Operations Other Than War (*feizhanzheng xingdong*) and improve capacities for executing operations such as disaster relief, maintenance of social stability and peace-keeping.[7] The promulgation of training regulations on Operations Other Than War had an important impact on the PLA's concept and practices of military training, and training on Operations Other Than War soon became an important component of the PLA's military training. For instance, in November 2002, the Military Training Department of the Lanzhou Military Region Headquarters published an article in the *PLA Daily* summarizing its experiences and expounding its views on training methods for Operations Other Than War.[8]

The rise of the discourse of MOOTW in China was also closely related to the emergence of the discourse of non-traditional security (NTS) threats in China after the end of the Cold War. The discourse of non-traditional security threats first entered Chinese official policy discourse in 2002, as the 2002 *Defense White Paper* identified non-traditional threats such as terrorism, transnational crimes and drug-trafficking as increasingly prominent threats to China's security. In addition, the 2002 *Defense White Paper* also stressed the importance of establishing and practicing the "New Security Outlook," which places an emphasis on cooperative security and dealing with non-traditional security threats.

In December 2005, at an enlarged meeting of the CMC, Chinese president and CMC Chairman Hu Jintao emphasized that the PLA should improve its capabilities in dealing with diversified security threats and accomplish diversified military missions. The line was again enshrined in President Hu's report to the 17th Party Congress, thus making it an important guiding thinking and objective of China's military buildup.[9] It was also since 2005, following the CMC's instructions on strengthening research on MOOTW, that military academic institutions such as the

---

Other Than War such as Disaster Relief" (*Zhongguo renmin jiefangjun jiang kaizhan qiangxianjiuzai deng feizhanzheng xingdong xunlian*) 中国人民解放军将开展抢险救灾等非战争行动训练，Xinhua Net, Beijing, September 13, 2001.

[7] Xiao Tianliang, *op. cit.*, p. 8; Xu Zhuangzhi and Ma Xiaochun, *op. cit.*

[8] The Military Training Department of Lanzhou Military Region Headquarters, "Feizhanzheng xingdong xunlian" 非战争行动训练 [Training on Operations Other Than War], *Jiefangjun bao* 解放军报 (The PLA Daily), November 5, 2002,
http://www.chinamil.com.cn/gb/pladaily/2002/11/05/20021105001092_gdyl.html

[9] National Defense University Strategy Teaching and Research Unit: *Tuidong guofang he jundui jianshe kexue fazhan duben* 推动国防和军队建设科学发展读本 [Textbook on Promoting National Defense and Military Construction], Beijing: National Defense University Press, 2009, Chapter 5; Zhou Yifeng 周益峰, "Wancheng duoyanghua junshi renwu zhanlue sixiang de shidai jiazhi" 完成多样化军事任务战略思想的时代价值 [Contemporary Significance of Strategic Thinking for Achieving Diversified Military Tasks], *Xi'an zhengzhi xueyuan xuebao* 西安政治学院学报 (Journal of National University of Defense Technology), 2009, no. 1, 71-73. For the text of the report, see "Hu Jintao's Report at the 17th Party Congress," 人民日报 *Renmin Ribao* (The People's Daily), October 25, 2007.

National Defense University and the Academy of Military Science embarked on systemic and comprehensive studies of MOOTW. For example, since 2005, MOOTW has become an important research area for AMS, which has completed more than 50 projects related to MOOTW, such as *Studies on Counter-Terrorism Operations*, *Standards for Counter-Terrorism Exercises, Introduction to MOOTW*.[10]

It was in 2005 that the PLA Small Leading Group on Dealing with Unexpected Accidents (SLGDUA) (*jundui chuzhi tufa shijian lingdao xiaozu*) was established, headed by the Chief of General Staff. The permanent office of the SLGDUA, the Emergency Response Office, was housed in the Operations Department under the GSD (GSDERO, or *zongcan yingjiban*, in short), and was intended to be the key military leading agency for command, control, coordination and mobilization of military forces for MOOTW. Parallel Emergency Response Offices (EROs) were also instituted in four General Departments under the CMC, all Military Regions and Arms and Services of the PLA.

In September 2006, the General Office of the State Council and the General Office of the CMC jointly issued a document entitled "Concerning Further Strengthening the Mechanism Building of Military-Civilian Natural Disaster Information Sharing" (*Guanyu jinyibu jiaqiang ziran zaihai xinxi jundi gongxiang jizhi jianshe*). Following the issuance of the document, the GSDERO had established information sharing mechanisms with more than 20 ministries, including the Ministry of Foreign Affairs, the Ministry of Public Security, the Ministry of Transportation, the Ministry of Civil Affairs, the Ministry of Water Resources, the Ministry of Forestry, the State Bureau of Seismology, the State Bureau of Oceanic Affairs, the State Meteorological Administration, etc.[11]

Since 2008, the research on MOOTW has entered a period of fast track development, which was driven by ideational changes in policymakers' security concepts and strategic thinking, as well as important events. Barry Buzan, a leading security studies scholar, once noted that certain specific crises such as the 1962 Cuban Missile Crisis and the 2001 "9/11" terrorist attacks would not only make themselves objects of academic research, but also would change previous "understanding, relationships and practices" at a broader strategic level. In terms of the evolution of the discourse and practices of MOOTW in China, the 2008 earthquake in Wenchuan, Sichuan province, and China's dispatching of its naval fleet to patrol the Gulf of Aden are all such crucial events.[12] As one of the largest

---

[10] Tian Yiwei 田义伟, "Junshi Kexueyuan feizhanzheng yanjiu zhongxin chengli" 军事科学院非战争研究中心成立 [The Establishment of the Centre for Non-War Studies at the Academy of Military Science], December 12, 2011, http://chn.chinamil.com.cn/jdtp/2011-12/12/content_4739765.htm.

[11] Wu Tianmin 武天敏, Han Guoxian 韩国贤 and Li Yun 黎云, "Quanjun he wujing budui 2008 nian yilai suixing feizhanzheng junshi xingdong renwu zongshu" 全军和武警部队 2008 年以来随行非战争军事行动任务综述 [Summary of MOOTW Tasks Executed by the PLA and Armed Police since 2008], *Jiefangjun bao* 解放军报 (The PLA Daily), September 5, 2011.

[12] Barry Buzan and Lina Hansen, *The Evolution of International Security Studies* (Cambridge: Cambridge University Press, 2009).

disaster relief operations in China's history, the relief work of the 2008 Wenchuan earthquake had prompted Chinese policymakers, scholars, as well as the public to come to the recognition of the importance of MOOTW. Similarly, as one of the Chinese military's large-scale MOOTW abroad, the PLA Navy's mission to patrol the Gulf of Aden also provoked Chinese academic and policy circles to appreciate the necessity of building a strong capacity for power projection, and to contemplate ways to protect China's increasingly expanding global interests and to provide public goods such as security and freedom of navigation to the international community. Such a trajectory is also manifested in the evolution of the academic and policy discourses on MOOTW in China. For instance, a keyword search of China's largest dataset of academic works using the term "MOOTW" will yield altogether 1,204 pieces of work focusing on MOOTW, over the period from 2000 to now. Among the 1,204 pieces, 1,192 pieces, or about 99 percent, were produced after 2008, and only 12 pieces (or 1 percent) were written prior to 2008.

Since the 2008 Wenchuan earthquake, China's top leaders have come to further appreciate the importance of MOOTW. Chinese President and CMC Chairman Hu Jintao, in an important speech, noted: "MOOTW has increasingly become an important way of using national military strength. It plays an important and unique role for the military to achieve combat readiness and improve fighting capabilities."[13] The CMC took a series of measures to enhance capacity building for MOOTW.

Since the 2008 Wenchuan earthquake, the PLA has strengthened its disaster relief capabilities. By the end of 2010, the PLA had put together eight national level, professional emergency rescue troops with a total number of 50,000 soldiers. The GSD had beefed up the ERO with more staff and expanded responsibilities and roles. The coordination mechanism between the military and the civilian side of the government was also bolstered. The Ministry of Defense established Joint Meeting Systems (*lianxi huiyi zhidu*) with over 20 ministries and agencies of the State Council.[14]

In January 2009, the CMC issued "The Guidelines for Capacity Building of MOOTW for the Military" (*Jundui feizhanzheng junshi xingdong nengli jianshe guihua*). The guidelines laid down the goals of MOOTW capacity building as "having a smooth and highly efficient emergency command system, a professional force appropriate in scale; equipment and apparatus that are suitable and durable; solid and effective special training programs; comprehensive response and guarantee system that are basically in place; laws and regulations that are basically complete,

---

[13] Major General Peng Shuigen, Commander of the Jiangxi Provincial Military Region, "Nuli tigao junfenqu feizhanzheng junshi xingdong nengli" 努力提高军分区非战争军事行动能力 [Strive to Improve Provincial Military Regions' Capacity for MOOTW], *Guofang* 国防 (National Defense), No. 1, 2009, 39.

[14] Sun Yanxin, "Guofangbu: jundui niandi jiancheng 5 wanren yingji jiuyuan budui" 国防部：军队年底建成 5 万人应急救援部队 [The Ministry of Defense: the Military Will Establish 50,000 Emergency Rescue Troops by the End of Year], Xinhuanet, April 20, 2010.

all of which can suffice the need of executing tasks of MOOTW." The guidelines stipulate that the PLA will be tasked to fulfill six categories of MOOTW, namely "Counter-terrorism and stability maintenance" (*fankong weiwen*), "Rescue and relief work" (*qiangxian jiuzai*), "Defending rights and benefits" (*weihu quanyi*), "Security and guarding" (*anbao jingjie*), "International Peacekeeping" (*guoji weihe*), as well as "International Rescue" (*guoji jiuyuan*). It also stipulates the guiding principles and measures for MOOTW capacity building.[15]

More importantly, MOOTW became an integral component of China's "Military Strategic Guidelines for Active Defense in the New Period" (*xinshiji jiji fangyu de junshi zhanlue fangzhen*). The 2008 *Defense White Paper*, published in January 2009, spelled out that China's new military strategic guidelines "focus on enhancing the capabilities of the armed forces in countering various security threats and accomplishing diversified military tasks" and "work to increase the country's capabilities to maintain maritime, space and electromagnetic space security and to carry out the tasks of counter-terrorism, stability maintenance, emergency rescue and international peacekeeping." They would make MOOTW "an important form of applying national military forces," and "scientifically make and execute plans for the development of MOOTW capabilities." In addition, the 2008 *Defense White Paper* makes enhancing capacity to conduct MOOTW a priority on a par with increasing "core military capability of winning local wars in conditions of informationization."[16]

At a June 2010 working meeting on capacity building for MOOTW held by the National Mobilization Committee of the Beijing Military Region, Chinese Defense Minister General Liang Guanglie stressed that the key to dealing with non-traditional security threats was to improve the capabilities of joint military-civilian operations in fulfilling emergency tasks. General Liang stressed that emphasis should be placed on building "four systems" (*sige tixi*): namely, an information network system that incorporates military and civilian information resources; an emergency force system that incorporates troops on duty, civilian agencies and national mobilization system; an emergency response and guarantee system that integrates military and civilian logistics systems, and a comprehensive law and regulation system.[17]

Representative Research Works

There are a number of representative research works that are worth mentioning. For instance, in December 2012, the Nanjing Army Command College (NACC) edited

---

[15] Wu Tianmin et. al., op. cit.

[16] The Information Office of the State Council, *China's National Defense in 2008*, January 20, 2009, http://news.xinhuanet.com/english/2009-01/20/content_10688124_4.htm.

[17] Chen Hui 陈辉, "Liang Guanglie qiangdiao: dali jiaqiang feizhanzheng junshi xingdong nengli jianshe" 梁光烈强调：大力加强非战争军事行动能力建设 [Liang Guanglie Emphasizes Greatly Strengthening Capacity Building for MOOTW], Xinhua News Agency, Shijiazhuang, June 19, 2010.

and published an eight volume series of studies on MOOTW, covering eight special topics: basic theoretical study of MOOTW, counter-terrorism, peacekeeping operations (PKO), stability maintenance, rescue and disaster relief, dealing with border defense events, defending national rights and benefits, and foreign militaries' MOOTW. The NACC project is among the first comprehensive studies of MOOTW. The NACC project is distinct for its Army perspective, and its studies on counter-terrorism, stability maintenance and rescue and disaster relief are all based on the experiences and needs of the Army. The NACC book series is written in the format of teaching materials and can be used by PLA academic institutions and troops as textbooks.[18] Another representative work is *Political Work on MOOTW* (*Feizhanzheng junshi xingdong zhong de zhengzhi gongzuo*), a 2009 volume edited by Lt. Gen. Liu Yuan, Political Commissar of the Chinese Academy of Military Science. The book examines "political work," a tradition of the PLA, and studies the basic characteristics, guiding principles and main contents of political work, as well as issues such as capacity building of the political work in MOOTW.[19] In addition, Xiao Tianliang, professor of strategic studies at the National Defense University, published a book in April 2009, *The Non-War Use of Military Force* (*Junshi liliang feizhanzheng yunyong*), that examines the methods, characteristics and logistics of non-war use of military force.[20]

It is also worth noting that in February 2011 the CMAS established the Center for MOOTW Studies, the first of its kind in China. The establishment of the Center for MOOTW Studies at the CMAS signified that academic research of MOOTW has further come to maturity. As a research platform, it will be beneficial for research

---

[18] The series of books is as follows: 1) Li Chunli 李春立, ed., *Fei zhanzheng junshi xingdong jichu lilun yanjiu* 非战争军事行动基础理论研究 [Research on Non-War Military Operations] (Beijing: Military Science Press, 2008; 2) Wang Shuguang 王曙光 and Xu Lisheng 徐立生, ed., *Lujun fankong xingdong yanjiu* 陆军反恐怖行动研究 [Research on Army Anti-Terrorism Operations] (Beijing: Military Science Press, 2008; 3); Chen Yilai 陈贻来, ed., *Lujun weihu shehui wending xingdong yanjiu* 陆军维护社会稳定行动研究 [Research on the Army's Actions to Maintain Social Stability] (Beijing: Military Science Press, 2008; 4); Zhou Zhenduo 周振铎, ed., *Chuzhi bian (hai, kong) fang shijian xingdong yanjiu* 处置边（海、空）防事件行动研究 [Research on Operations to Manage Sea and Air Border Events], Beijing: Military Science Press, 2008; 5) Shang Zelian 商则连 and Wang Wenchen 王文臣, ed., *Lujun qiangxianjiuzai xingdong yanjiu* 陆军抢险救灾行动研究 [Research on Army Rescue and Disaster Relief Operations] (Beijing: Military Science Press, 2008; 6); Yang Hongjiang 杨洪江 and Qu Mingjun 屈明军, ed., *Weihu guojia quanyi yanjiu* 维护国家权益研究 [Research on Maintaining National Rights and Interests] (Beijing: Military Science Press, 2008; 7); Li Chunyuan 李春元, ed., *Lujun weihe xingdong yanjiu* 陆军维和行动研究 [Research on Army Peacekeeping Operations] (Beijing: Military Science Press, 2008; 8); Dong Aiguo 董爱国, Qu Guixi 曲贵喜, ed., *Waijun feizhanzheng junshi xingdong yanjiu* 外军非战争军事行动研究 [Research on Foreign Army's Military Operations Other than War] (Beijing: Military Science Press, 2008).

[19] Liu Yuan 刘源, ed., *Feizhanzheng junshi xingdong zhong de zhengzhi gongzuo* 非战争军事行动中的政治工作 [Political Works on Military Operations Other Than War] (Beijing: Military Science Press, 2009). General Liu Yuan currently holds the office of Political Commissar of the General Logistics Department.

[20] Xiao Tianliang, *op cit*.

and teaching on MOOTW in China, and will be conducive to the integration of policymaking and academic studies. [21] The Center for MOOTW Studies has assembled an impressive group of experts, including 28 specialists from state agencies, general departments of the CMC, local forces, the military academic institutions, armed police and public security units as steering experts or guest researchers. The research areas of these experts cover counter-terrorism operations, rescue and disaster relief work, and crisis and emergency management, etc. The Center for MOOTW Studies is expected to coordinate research activities concerning MOOTW, provide policy consultation to the central government, CMC, and general departments, build databases for MOOTW, as well as teaching and training of high-quality talented people to do research.[22]

Table 1. Policy and Academic Discourses on MOOTW in China, 2000-2012

# of articles / Issue Area	2000-2003	2004-2007	2008-Now
MOOTW	72	115	4031
Disaster Relief	18	32	2287
PKOs	14	39	767
Counter-Piracy	2	5	121
Escort Missions/Gulf of Aden	2	5	313
History	35	65	1536
Foreign Militaries	15	29	483

II. China's MOOTW Practices

Since the founding of the People's Republic of China, the PLA has engaged in a large number of MOOTW. Below I will examine China's practices of MOOTW in the areas of production and construction (*shengchan jianshe*), rescue and disaster relief, counter-terrorism, PKOs and counter-piracy.

1. Production and Construction (*shengchan jianshe*)

Historically, the PLA had actively participated in agricultural and industrial production in China. For instance, in the early period of the PRC, 35 divisions (altogether more than one million troops) were demobilized and sent to frontier

---

[21] http://www.chinanews.com/gn/2011/12-12/3526428.shtml.

[22] Tian Yiwei, op. cit.

regions to participate in production and construction.[23] In October 1954, the PLA's Xinjiang Production and Construction Corps (XJPCC) was established, consisting of 10 agricultural construction divisions and one engineering and construction division, which altogether made up 105,000 demobilized troops and 70,000 family members. The establishment of the CJPCC befitted a long tradition in China of having garrison troops to open wasteland and grow food grain in border regions (*tuntian shubian*) that can be traced back 2,000 years earlier to the Western Han Dynasty. The CJPCC directly reported to the CMC and was listed as a separate administrative unit on an equal footing with other provinces and autonomous regions in China. It was aimed at beefing up border defense in the Northwest Xinjiang region, helping develop the regional economy and maintaining ethnic unity in Xinjiang. Even to the present day, the CJPSS still remains a very important actor in the PLA and China. Amidst rising tensions in Sino-Soviet border regions, the Central Committee of the Communist Party of China (CC CPC) gave an order in June 1968 to establish the Heilongjiang Production and Construction Corps (HLJPCC) in the Northeastern region of China. Composed of six divisions and three independent regiments, the HLJPCC was aimed at fulfilling two tasks: 1) to have garrison troops open wasteland and grow food grain in border regions (*tuntuan shubian*); 2) meanwhile, the HLJPCC would be placed under the command of the Shenyang Military Region to carry out fire scouting operations, to disrupt and delay enemy forces' movements and to support the field army's combat operations once a Sino-Soviet war broke out. The HLJPCC was rescinded and turned into the General Bureau of the State Farm of Heilongjiang in February 1976, though certain para-military forces were retained until early 1980.[24]

In terms of industrial construction (*gongye jianshe*), in the period 1950-1984 PLA engineering troops had participated in the construction of more than 40 large- and medium-sized steel enterprises. The engineering troops also took part in the development of major oil fields such as Daqing Oilfield, Renqiu Oilfield, Dagang Oilfield and Shengli Oilfield, as well as pipelines across the country. The PLA engineering troops also played an important role in the development of water conservancy facilities across the nation.[25] For the development of transportation infrastructure, the PLA engineering troops had built major roads connecting Qinghai and Tibet as well as Sichuan and Tibet. The PLA Railway Engineering Corps had up to 1983 built seven major railways in China, namely the Chengdu-Kunming Railway, the Guiyang-Kunming Railway, the Xiang-Yu Railway, the Northeast Forest Area

---

[23] Jiang Tingyu 姜廷玉, ed., *Xinzhongguo guofang he jundui jianshe 60 nian* 新中国国防和军队建设 60 年 [60 Years of Building National Defense and the Armed Forces in New China] (Beijing: Party Building Books Publishing House, 200), preface 3.

[24] Ibid.

[25] Lin Jiangong 林建公, "Zai xinzhongguo de lishi fengbei shang—zhongguo renmin jiefangjun canjia shehuizhuyi jingji jianshe gongxun jianli (xiapian)" 在新中国的历史丰碑上—中国人民解放军参加社会主义经济建设功勋建立（下篇）[On Historical Monuments of New China: The PLA's Exploits in Building the Socialist Economy (Part Two)], *Dangshi wenhui* 党史文汇 [Journal of CPC History and Writings], 1999, no. 9, 7-11.

Railway, the Southern Xinjiang Railway, the Qinghai-Tibet Railway, as well as the Beijing Subways. Altogether, the PLA Railway Army has built around 13,000 kilometers of railway in peacetime.[26] Up to 2009, the PLA had altogether invested 500 million workdays and 30 million engineering vehicles and participated in a large number of major projects ranging from the industrial sector to transportation, water and electricity, telecommunication, etc.[27]

2. Rescue and Disaster Relief

The PLA has participated in virtually all rescue and disaster relief operations in the PRC. A prominent case of the PLA MOOTW was its deep involvement in the earthquake relief work during the massive earthquake in Wenchuan, Sichuan province, in May 2008.

At 14:28, on May 12, 2008, a massive (magnitude 8 on the Richter scale) earthquake occurred in Wenchuan County, Sichuan Province. The Wenchuan earthquake was the most devastating earthquake in the history of the PRC, with a death toll of 30,000 and causing the dislocation of more than 46 million people across 10 provinces in the Southwest and Northwest of China. The massive earthquake put the PLA's capacity for rescue and disaster relief under a severe test. Two minutes after the outbreak of the earthquake, Chief of General Staff General Chen Bingde received the first emergency telegram concerning the Wenchuan earthquake. Under the order of CMC Chairman Hu Jintao, General Chen activated the emergency command system. Ten minutes after the outbreak of the earthquake, Chengdu Military Region set up a headquarters for earthquake and disaster relief, and troops stationed near the quake-ridden areas, mostly from Chengdu Military Region and Lanzhou Military Region, were quickly dispatched for rescue and disaster relief work. By midnight on May 12, 34,000 troops from Jinan Military Region and Chengdu Military Region were mobilized and ready to be sent to the quake-stricken areas. By noon on May 14, another 30,000 troops were dispatched. Within only a few days, a total of 140,000 troops were dispatched to engage in rescue and disaster relief work.

On the morning of May 13, the CMC called an emergency executive meeting and decided to set up the Leading Small Group on Combating Earthquake and Disaster Relief Work (*kangzhen jiuzai gongzuo lingdao xiaozu*) or the Commanding Group of Combating Earthquake and Disaster Relief (*kangzhen jiuzai zhihui xiaozu*), which would be headed by Chief of General Staff General Chen Bingde. The LSGCEDR would follow the overall scheme of the State Council Combating Earthquake and Disaster Relief Headquarters and direct the PLA's rescue and

---

[26] The PLA Railway Engineering Corps was merged into the Ministry of Railway in 1983. See Chen Hui, "Renmin jiefangjun tiedaobing de jianli yu chexiao" 人民解放军铁道兵的建立与撤销 [The Establishment and Revocation of the PLA Railway Engineering Corps], *Dangshi bolan* 党史博览 (General Review of the Communist Party of China), No. 11, 2005, p. 19.

[27] Jiang Tingyu, *op. cit.*

disaster relief operations. On the afternoon of May 13, the LSG convened the first meeting and decided to put all troops under the unified command of the Chengdu Military Region. A Joint Command and Management System (JCMS, *lianhe zhihui guanli tizhi*) was established, and the distressed areas in Sichuan province were divided into five Areas of Responsibility (AOR), with the most senior commanders in an AOR to serve as the head of the JCMS in each AOR. Following the CMC instructions, a three-level response and guarantee system consisting of four General Departments, the Chengdu Military Region and the deployed troops, was established.[28] Under the direct command of the LSGCEDR, the GSD issued "Urgent Instructions on Carrying Out Work of Combating Earthquake and Disaster Relief" (*Kaizhan kangzhen jiuzai gongzuo de jinji zhishi*), and assembled troops to engage in rescue and disaster relief work; the General Political Department (GPD) issued "Instructions on the Political Work in the Operations of Combating Earthquake and Disaster Relief" (*kangzhen jiuzai zhong de zhengzhi gongzuo zhishi*), calling on the PLA to "carry forward a good tradition" and "play the role of storm troops" in the rescue and disaster relief work; the General Logistics Department (GLD) quickly assembled a great amount of disaster relief materials such as tents, foods and medicines, and organized 60 medical teams and sent them out to the distressed areas; and the General Equipment Department (GED) assembled a variety of heavy disaster relief equipment and sent them to the distressed areas.[29]

The rescue and disaster relief operations carried out by the PLA were impressive. Throughout the whole rescue and disaster relief period, the PLA dispatched 146,000 troops and 75,000 reserve militia, more than 4,700 sorties, 390,000 vehicles, and rescued 27,000 people, provided medical treatment to 630,000 injured and sick, and relocated 1.32 million people affected by the quake. The 2008 Wenchuan Rescue and Disaster Relief operations proved the PLA's pivotal role in and extraordinary capacity for carrying out MOOTW.

Lessons learned: 1) the 2008 Wenchuan rescue and disaster relief operations proved that a highly effective joint command and operations system was at the core of large-scale MOOTW, and yet the PLA capabilities of joint command and operations still needed to be improved; 2) in the future, the PLA's capacity building for MOOTW should put an emphasis on force projection capability.

Force projection capability would not only be crucial for domestic rescue and disaster relief operations, but also important for the PLA's involvement in international humanitarian assistance missions. Since 2001, the PLA has engaged in 20 international humanitarian assistance missions, including missions in

---

[28] Chen Bingde 陈炳德, "Zongcanmouzhang Chen Bingde zhuanwen yi Wenchuan dadizhen jiuzai de rizi" 中参谋长陈炳德撰文议汶川大地震救灾的日子 [Essay by Chief of General Staff Chen Bingde Recollecting the Days of Disaster Relief of the Great Wenchuan Earthquake], *Jiefangjun bao* 解放军报 (The PLA Daily), December 9, 2008, p. 7.

[29] "Wenchuan dizhen jiuzai rang shijie buzaigan qingshi jiefangjun" 汶川地震救灾让世界不再敢轻视解放军 [The World No Longer Dares to Look Down Upon the PLA since Its Role in Disaster Relief of the Wenchuan Earthquake], *Huanqiu shibao* 环球时报 *(*The Global Times*)*, June 10, 2008.

Afghanistan, Indonesia, Haiti and Pakistan. However, the PLA's ability to carry out MOOTW is also severely constrained by its limitations in overseas force projection capability. For instance, during the 2004 Indian Ocean tsunami, the PLA only dispatched a small group of engineering troops, while the United States sent the Lincoln aircraft carrier battle group to engage in rescue and disaster relief operations. During the 2010 flood in Pakistan, the PLA Army Air Force for the first time sent helicopters to engage in the rescue and disaster relief, but only four such helicopters were dispatched.

3. Counter-terrorism

Since the 1990s, China's armed forces, including the PLA and the People's Armed Police (PAP), have carried out a great number of counter-terrorism operations. At the domestic level, counter-terrorism is also closely related to the task of "stability maintenance" (*weiwen*).

At the international level, the PLA has conducted a considerable number of joint counter-terrorism exercises with foreign militaries since 2001. Within the framework of the Shanghai Cooperation Organization (SCO), the PLA has carried out 10 joint counter-terrorism drills since 2002. In addition, in recent years China has also carried out smaller-scale joint counter-terrorism training exercises with neighboring countries such as Thailand, India, Singapore and Indonesia.

Those joint exercises have improved the PLA's capabilities for joint operations and have deterred terrorists.

4. PKOs

In 1988, China first applied to join the U.N. Special Committee on PKO, and in 1989 it first sent personnel to join the U.N. Transition Assistance Group to Namibia. In 1992, China sent its first PKO troops (200 engineering soldiers) to Cambodia.[30] Since then, PKOs have become an important component of China's practices of MOOTW. Since 2003, China has more actively participated in PKOs. Since 2007, China has maintained a large level of PKO personnel (more than 1,800). As of August 2012, China is participating in 11 PKOs, with 71 policemen and 1,853 military personnel on missions, putting it in the first rank among the five permanent members of the UN Security Council.[31]

So far, China has not dispatched combat troops to participate in UN PKOs. However, as China continues to rise and its global involvement deepens, China

---

[30] Tang Yongsheng 唐永胜, "Zhongguo yu lianheguo weihe xingdong" [China and United Nations Peacekeeping Operations] 中国与联合国维和行动, *Shijie jingji yu zhengzhi* 世界经济与政治 (World Economics and Politics), no. 9, 2002, 39-44.

[31] http://www.un.org/zh/peacekeeping/resources/statistics/contributors.shtml

might further appreciate the importance of maintaining regional security and stability for the sake of China's national interests and its great power status.

5. Counter-Piracy

On December 18, 2008, the Chinese government announced its decision to dispatch naval fleets to join foreign navies to patrol the Gulf of Aden and Coast of Somalia. By July 2012, China had dispatched 12 naval flotillas, conducted 474 escort missions, and escorted about 5,000 ships, involving about 10,000 person-time naval service men and women. China's escort mission to the Gulf Aden is the largest scale, longest-lasting MOOTW that the PLA has carried out abroad.

6. Defending Overseas Interests (*weihu haiwai liyi*)

As China's global interests continue to expand, defending overseas interests becomes an important component of the PLA's MOOTW. One prominent case was the evacuation of Chinese citizens from Libya. In early 2011, as the domestic conflict in Libya continued to escalate, the PLA, in close cooperation with the Ministry of Foreign Affairs, the Ministry of Transportation, Overseas Chinese Affairs Office and the Ministry of Public Security, played a major role in the unprecedented large-scale operations to evacuate 350,000 Chinese citizens as well as overseas Chinese from conflict-ridden Libya. The PLA Air Force dispatched 4 IL-76 transportation jets to join the evacuation operations. The PLA Navy's 7th flotilla, which had been carrying out escort missions in the Gulf of Aden, was also dispatched to Libya to assist in the evacuation operations. The evacuation operations were the largest in scale in Chinese history.

III. The Future of China's MOOTW

In the foreseeable future, as China continues to face diversified security challenges and threats, and as China's national interests continue to expand in multiple dimensions, the PLA will be facing the challenges of carrying out more diversified, complex MOOTW. And improving the PLA's capabilities to carry out MOOTW will help safeguard China's national interests, provide a strong and robust strategic pivot for maintaining the important period of strategic opportunity (*zhanlue jiyuqi*) for China's development, and help contribute to world peace and development.

Looking to the future, the following issues may be of importance:

1. Laws and rules.

To date, China has issued domestic laws concerning MOOTW such as the Flood Control Law (1998), Fire Protection Law (1998, 2008 revision), Emergency Response Law (2007), National Defense Law (2009), Law on Earthquake Prevention and

Disaster Relief (2009), and National Defense Mobilization Law (2010), as well as regulations such as the "Training Regulations for the Chinese People's Liberation Army" (2002), "The PLA General Emergency Response Plan for Dealing with Unexpected Accidents" (2006), "The Guidelines for Capacity Building of MOOTW for the PLA" (2009) and "The Regulations on PLA Emergency Command for Dealing with Unexpected Accidents" (*Jundui chuzhi tufa shijian yingji zhihui guiding*) (2010). However, it is also recognized that the current laws and regulations concerning MOOTW are not yet complete, specifically, the division of rights and responsibility are not clearly specified, the logistics system has not yet been completed, the command and control relationship has not been specified, thus restraining the efficiency of the PLA's participation in MOOTW. Therefore, scholars have called for the making of MOOTW Law that will further put China's MOOTW onto the track of legalization and institutionalization.

As China's interests continue to expand globally, China's MOOTW will inevitably involve the global commons, such as international air space and the high seas. As a great power, China is also expected to provide public goods such as international security and stability to the international community. Hence, China should actively participate in the international rule-making governing global commons, which will not only ensure efficiency in carrying out MOOTW, but also alleviate the outside concerns, anxieties and suspicions brought by China's rise, particularly its growth in military power, thereby helping to create a good external environment for China's continuous peaceful development.

2. Power Projection and Capacity Building

China's practices in MOOTW have also demonstrated the importance of strengthening the PLA's power projection capabilities. MOOTW practices are also conducive to innovation and growth in the PLA's core military capabilities, including power projection capabilities, and help improve fighting capabilities and combat readiness.[32] Meanwhile, China should learn from the lessons of foreign militaries, such as the U.S. military, and study carefully the question of how to avoid unnecessary or excessive involvement in MOOTW such as PKOs and counter-terrorism operations.

---

[32] Ma Yuezhou 马越舟, Tian Yiwei 田义伟, "Yangbing qianri, yongbing qianri—yu junshi kexueyuan feizhanzheng junshi xingdong yanjiu zhongxin zhuren Zheng Shouhua yanjiuyuan yi xi tan" 养兵千日，用兵千日——与军事科学院非战争军事行动研究中心主任郑守华研究员一席谈 [Training an Army for a Thousand Days to be Used for Thousand Days—A Conversation with Mr. Zheng Shouhua, a Research Fellow at the Centre for Military Operations Other than War at the Academy of Military Science], *Jiefangjun bao* 解放军报 (The PLA Daily), September 6, 2012, http://news.mod.gov.cn/headlines/2012-09/06/content_4397719.htm.

3. The Coordination between MOOTW and China's Overall Diplomacy

As China's global involvement deepens, China's overseas interests (*haiwai liyi*) such as personnel safety and investments are also increasingly exposed to growing risks. The damage to China's overseas interests caused by political turmoil in Iraq, Sudan and Libya are cases in point. As part of China's overall diplomacy, China's future MOOTW such as protecting overseas interests would need to be closely coordinated with other government agencies. In the Libya evacuation operations, the PLA had worked in close coordination and cooperation with MOFA, MOT, the Overseas Chinese Affairs Office and MOPS, and successfully completed the mission. In the future, China will need to build and improve the interaction mechanism between the PLA and various governmental agencies so as to improve China's efficiency in MOOTW.

The Use of Social Media in Disaster Emergency Response

Dr. Cécile Wendling, Research Fellow, Fondation nationale des sciences Politiques, Paris (France)

Introduction

Social media sites such as Facebook and Twitter are used more and more often during the full disaster life cycle of preparation, response and recovery. This paper focuses on the use of social media in disaster emergency response. Drawing on recent examples, this paper highlights the new spatial, temporal and social arrangements that emerge with the use of social media in emergency response. This paper analyses the consequences in terms of social practices, organizational structures and public policy adaptations.

1. Three different uses of social media in emergency response and the creation of new spatial, temporal and social arrangements

Social media have been used during emergencies to provide warnings and information, to conduct situational awareness, to identify survivors and victims. Using these three examples, this first part shows how these different uses of social media create new spatial, temporal and social arrangements.

First, social media are used to provide warnings and information in real time during emergencies. Several examples can illustrate this point.[1] This is done for instance in case of natural disasters like storms or tornadoes by the U.S. services in charge. The use of the Twitter sign-off "Please RT" (retweet) and the target of influential online individuals allow the dissemination of the warning message to be increased. Twitter and Facebook offer solutions because most of the users will receive the notification instantly and spread it in their network. During the earthquake in Indonesia in April 2012, 15 to 20 minutes after the earthquake, a Tweet from the U.S. Geological Survey said a tsunami was not likely, which was crucial information for the public and emergency services alike. During the Iceland volcanic eruption in Europe, people turned to Facebook and Twitter to get information. For instance, they used social media to know if they could fly, and also to get information on alternative travel plans in real time. Travellers asked for accommodation, which people living in the places where they were stranded offered. These examples show how new spatial arrangements emerge with the use of

---

[1] The examples come from the OECD report on the use of social media in risk and crisis communication: OECD (2013): "The Use of Social Media in Risk and Crisis Communication" GOV/PGC/HLRF(2012)4.

social media. The information can be provided by an institution located far away from the disaster scene. The receivers of the information can be located in a broad diversity of areas and still access the warnings as quickly as if they were on the scene. New time arrangements hence emerge as the provision of the warning or information is made instantly. The speed of the communication can accelerate the swiftness of adaptation of the population to the warning received. Finally, new social arrangements emerge as citizens can help themselves without relying on public authorities, as was the case with the travellers who were offered accommodation during the volcano eruption.

Second, social media can be used to conduct situational awareness during an emergency. Computer programs can be used to synthesize what types of content are being shared online on Twitter or Facebook and to provide meaning. The U.S. Federal Emergency Management Authority (FEMA) uses a new application called SAVER.[2] This application maps emergency declarations, and the progression of search operations. Similarly in Japan, in the aftermath of the March 2011 earthquake and tsunami, Georepublic Japan and OpenStreetMap Foundation Japan launched a crisis map that provided and visualized real-time information on news and official reports as well as information provided by the crisis-affected community (via SMS/text and Internet platforms) on evacuation centers, damage and requests for help.[3] Many crisis mapping application techniques exist to visualize crisis situational development in real time. Emergency services can also rely on content analysis tools, such as those provided by Google. In addition, emergency services can use network analysis to visualize who retweets what and be able to monitor rumors. The interactive mapping creates new spatial and time arrangements, as the emergency services can rely on a large aggregate of information to be visualized in real time for a given geographic area. A new social arrangement known as Volunteer Technology Communities (VTC) has emerged.[4] Volunteer technology communities are groups of people who voluntarily work on developing social media platforms or modules especially for risk and crisis communication during an emergency. A famous example is Ushahidi, which was used during the Haiti earthquake. The mapping done by this VTC was used by emergency services on the ground to best allocate resources.

Third, social media can be used to identify victims and survivors. Applications like the American Red Cross's safeandwell.org have been created for people in a

---

[2] http://idisaster.wordpress.com/2010/11/19/femas-s-a-v-e-r-platform

[3] http://georepublic.co.jp

[4] World Bank's Global facility for disaster reduction and recovery (2012): *Volunteer Technology Communities: Open development,* report available online:
https://www.gfdrr.org/gfdrr/sites/gfdrr.org/files/documents/Volunteer%20Technology%20Communit ies%20-%20Open%20Development.pdf

disaster area to register if they are safe so that their loved ones know they are OK.[5] It is possible to use this application to enter names during an emergency to check whether family members or friends are safe. Concerned family and friends can search the list of those who have registered themselves as "safe and well" by clicking on the "Search Registrants" button. The results of a successful search will display a loved one's first name, last name and a brief message. In Japan, during the earthquake and tsunami that occurred in 2011, people turned to Google Person Finder. 320,000 posts were made in one week. People also published photos of evacuation center name lists on Picasa. The social practice of identifying online to report on the status of victims or survivors diminishes the pressure on public authorities to provide this information. However, the information provided is to be related to a time and a space location, as the information might change very quickly, in the middle of an emergency. Someone can report themselves as safe and yet die in the next hour.

In its second part, this paper will stress the consequences of these new spatial, temporal and social arrangements on the adaptation of social practices, organizational structures and public policies.

2. New social practices, new organizational structures, new public policies?

In the context of new spatial, temporal and social arrangements, it is possible to trace new patterns of social practices, which raise the question of how the organizational structures in charge should adapt, and also more generally how public policy should respond.

The use of social media in emergency response is to be related to the emergence of new social practices. The first one is that of citizens to rely on multiple players to decide what to do in an emergency. Most of the citizens affected by a disaster turn not only to the official webpages but also to social media leaders providing information. A University of Georgia study shows that in the U.S. on May 22, 2011, during the Joplin tornado, less than two hours after the event a Facebook employee started to create a dedicated page from her iPhone called Joplin Tornado Info. She got 44,000 followers, which means that people searching for information on the situation were relying on her and other volunteers instead of on the direct official services.[6] This new social practice calls into question the role of trust but also the risk

---

[5] See: https://safeandwell.communityos.org/cms/index.php

[6] R. William, R., William G. Burton, D. (2012): *The Use of Social Media for Disaster Recovery: Lessons learned while creating and managing 'Joplin Tornado Info' (2011) on Facebook and further implemented with 'Branson Tornado Info' (2012), Missouri Flood Info (2011-2012) 'US Tornado Info (2012) and others,* University of Missouri, May 2012, available online:

of misinformation. If a multiple range of players can be followed through social media, what could happen if they spread misinformation, creating panic or endangering the lives of others? A solution used by officials in charge is to correct the information using the same social media. For instance, during the Fukushima disaster and nuclear accident, officials of the World Health Organization observed that some people were telling their friends to drink wound cleaning liquids, which contain iodine, because they thought this would help their body be prepared for a large amount of nuclear radiation. The WHO social media team warned people via Twitter and Facebook not to drink it because it could be harmful. The same day, the WHO noticed people rushing to take iodine pills and tweeted: "Consult your doctor before taking iodine pills. Do not self-medicate!"[7]

Another social practice is that of different segments of the population having different uses of social media and hence expecting different modes of communication from authorities in charge. A solution for authorities is to use multimodal warnings and alerts. In Japan during the 2011 earthquake and tsunami, they used both tweets and traditional paper fliers at the same time to make sure the information could circulate swiftly to all.

Finally, another new social practice is to turn to Facebook to volunteer on the ground. During the earthquake in Christchurch, New Zealand, a large group of volunteers gathered in response to a Facebook campaign organized by students to help those suffering from the disaster: "Supporting Christchurch Earthquake 22-02-2011." They worked closely with the civil defense units. These examples thus demonstrate that new organizational structures could be needed to face these new social practices that are emerging with the use of social media during emergencies.

New organizational structures are created inside administrations in charge to face the new challenges of social media. For instance, so-called online and social media divisions have emerged in risk and crisis communication departments. These units plan the social media strategy for each week in coordination with all the relevant services. These units can track misinformation and find ways to counterbalance it as quickly as possible. They can also track groups of volunteers mobilizing to coordinate their efforts with the official units in charge.

It is also possible to find examples of social media roundups with a daily or weekly presentation of the situation awareness through crowdsourcing of social media content. They can help detect digital smoke signals announcing an emergency. In addition, new virtual organizational structures have also emerged, as

---

http://extension.missouri.edu/greene/documents/PlansReports/using%20social%20media%20in%20disasters.pdf

[7] Amy Coopes, "Health experts sound warning over iodine rush," March 15, 2011, http://phys.org/news/2011-03-health-experts-iodine.html

shown by the examples of the VTC. The VTCs also raise the question of the interface between authorities in charge of the emergency response and the volunteers around the globe gathering online data they can use.

What could be the impact on public policies? First of all, education is needed. School programs could integrate the topic of the risk of misinformation and rumors in social media. Regulation could also be an option, as misuse can have vital consequences. In Mexico, Twitter has more than four million users in the country, 98 percent of citizens have a Facebook profile, and 30 million people are able to access the Internet. As these figures keep on increasing, a bill has been passed called the Veracruz Law.[8] This law prohibits citizens from spreading false rumors and information that may trigger panic. The difficulty lies in the definition of what constitutes false rumors. A risk is that these types of legislation or regulation may be used to censor social media.

Other public policies could be needed to preserve the openness of data, while maintaining confidentiality. Although most social media platforms do not have the in-house capacity to develop specific products for emergency managers, public policies could make sure they keep the platform open and adaptable so that third-party developers can build customized tools for platforms dealing with crisis situational awareness. However, a risk could arise from this openness in that the level of confidentiality of the data provided by users on their social media pages could be endangered. It is not clear whether bloggers or Facebook/Twitter users actually consent to the analysis of their data. According to a study of the ICT4Peace Foundation on the potential and challenges of open data for crisis informatics management, there is still a long way to go before all the actors will be convinced of the benefit of openness.[9] On the one hand, citizens may prefer to protect the privacy of their Internet exchanges; on the other hand, companies may wish to protect their competitiveness.

Finally the question of liability is important. Some citizens may believe that they should receive assistance if they have indicated via social media that they are in need of help. There is a risk that emergency services could be held liable if they don't answer an online request. Therefore the use of social media in risk and crisis management may require the adaptation of laws and current public policies to balance expectations from citizens when they turn to social media in times of disaster.

---

[8] Damien Cave, "Mexico Turns to Social Media for Information and Survival," *New York Times*, September 24, 2011, http://www.nytimes.com/2011/09/25/world/americas/mexico-turns-to-twitter-and-facebook-for-information-and-survival.html

[9] Stauffacher, D., Hattotuwa, S., Weekes, B., "The potential and challenges of open data for crisis information management and aid efficiency, a preliminary assessment," ICT4Peace Foundation, March 2012.

Conclusion

Social media have been used spontaneously by citizens to enhance resilience and solidarity in communities in times of crisis. There is a need to enhance collective intelligence in disasters and make sure the information provided is as reliable as possible. Different tools have been used for this purpose, such as the publication of rules and guidelines on the use of social media during a crisis, leaflets or other educational materials. Similarly, to develop government-led social media strategies in times of crisis, there is a need to introduce codes of practice at a government level, training of official servants in charge, etc.

However, it is still very difficult to evaluate the impact of social media in crisis communications and management and hence to demonstrate their efficiency or lack thereof. If metrics can be used (like Google Analytics) to know how many followers exist for a given social media, this does not indicate the extent to which people's practices are affected by their clicking on a social media page in a time of crisis. According to a study conducted by Booz Allen Hamilton and the American Public Health Association,[10] most of the emergency services use a combination of metrics, online comments and surveys to find ways to evaluate their use of social media in times of crisis. However, the rather recent emergence of new crowdsourced uses of social media makes it difficult to have enough data available to evaluate the impact of social media in risk and crisis management.

New fields of research are emerging, such as crisisinformatics, which has developed at the juncture between information technology and sociology. More specifically, there is a need to study the use of mobile technology to provide security in complex emergency management systems. Developers could work on the functionality of social media in times of crisis, with new applications and content enablers for smartphone holders. Pilot initiatives could lead the way to innovative use of social media in times of crisis (to estimate damage, conduct statistical analysis on victim locations, etc.). New methods are needed to discriminate between erroneous or misleading and awareness bringing information. In addition, depending on the nature of the disaster, people's emotions and people's behaviors could vary, making the use of social media very different from one crisis to another. There is a need to know for which types of disasters people will turn to social media, but also to discriminate between different practices of use of social media depending on the type of crisis faced (natural catastrophe, terrorist attacks, etc.). The type of social media used, the timing of use of social media, and so on, could vary depending on the nature of the disaster.

---

[10] Special Report, "Expert Roundtable on Social Media and Risk Communication During Times of Crisis: Strategic Challenges and Opportunities,"
http://www.boozallen.com/media/file/Risk_Communications_Times_of_Crisis.pdf

To Prevent: Things We Need to Do Better

Ambassador Tomas Rosander, Counter Terrorism Coordinator, MFA, Sweden

The focus of this conference is crisis management. I'll be focusing on prevention, but there is in fact no contradiction, as many of the measures that I consider preventive also come into play in crisis management. I'll make five brief points on countering terrorism and violence-oriented extremism, based on our experience in the national and international context. I will be focusing here on the "software" side, but this does not mean that we won't be also be paying attention to the importance of the "hardware" side, i.e. effective policing and security. These two sides must go hand in hand. Standardized physical security measures are a necessity, especially since profiling is very hard to do and even the best intelligence can be easily misinterpreted or simply not reach the right addressee.

My first point concerns the need for a comprehensive approach. It is a concept so often mentioned that it has become almost trivial. But it is worth repeating, as we still have a lot of implementation to do. Most of the terrorism and violence-oriented extremism is generated in societies plagued by war and conflict, and most of these countries are counted among the world's poorest; we need only look at Yemen, Somalia and the Sahel region. So we are ultimately fighting not only organizations and individuals, but even more so, certain social and economic and political deficiencies. That requires a broad outlook and approach.

We can learn from experiences gained in our development assistance work. We should explore potential synergies. I think we should continue to foster a more lively discussion about the links between security and development. That is why there is discussion in the EU on providing assistance to terrorist-ridden third countries and areas. This has in fact been a very important element for the relevant working groups in Brussels for the past few years.

Of course, we do not only find breeding grounds for violent extremism in zones of conflict, but also in our richest and most developed societies. We have seen the growth of enclaves of frustration generated by alienation and exclusion, by lack of identity, often, but not always with links to conflict areas. If you are a believer in the art of profiling, there is one large group that clearly stands out: one of our greatest challenges in the global countering of violent extremism and terrorism is the vulnerability of our young ones. You find them everywhere: youngsters caught between cultures and value systems, seeking easy solutions in frustration, becoming easy prey for extremist messages. We need to provide our young ones with the tools for critical thinking. This should also be reflected in our counter-terrorism strategies and action plans. This may sound far beyond the scope of everyday counter-

terrorism efforts. But it is in fact a core issue. Here we need to link up with our educational systems, with our social sciences, scholars and social field workers and with civil society.

If you like, countering terrorism is ultimately about building society—with a view to establishing peace and security, rule of law and functioning democratic institutions, functioning market economies and social structures—or in other words, about eradicating an important part of the basis for violent extremism and terrorism, tendencies which are often generated by frustration. There are no easy, quick fixes; the enemy cannot be beaten once and for all in a one-time war, as it were; it is a continuous process, involving most parts of our societies.

Freedom and prosperity obviously require security, but we cannot achieve sustainable security without freedom. The red line that we must not cross in combating terrorism is giving up on safeguarding human rights and freedoms and respecting international law. The seriousness of the matter should not be an excuse for shortcuts. Apart from violating obvious fundamental values, taking shortcuts would in fact be highly counterproductive and in the long run undermine what we are trying to achieve. Truly effective policing and security building can only be based on the rule of law.

We have seen examples of terrorism cases of some magnitude where vital information has been available, but not forwarded to police authorities for lack of trust. Openness and transparency, building confidence, trust and credibility—these are all key factors in countering terrorism. We still have a way to go, within the European Union as well, when it comes to openness and transparency, not just in the field of counter-terrorism, even if this area is at the forefront of this discussion.

My second theme is very much related to the issue of openness. A good starting point for honoring openness and transparency is establishing a public national CT-strategy where all this is reflected. This would set standards and provide a platform for action. It would serve as a starting point for evaluation, and a point of reference for public scrutiny. And the process itself could be of great value, as various ministries, agencies and organizations could together, compare notes and cross cultural divides. It would facilitate constructive public debate.

For those countries that have not yet developed strategies, there is ample support and advice to be found, in this field, e.g. through the United Nations CT-agencies. The UN is at present developing a list of national experts on CT strategies to facilitate the sharing of experiences and best practices.

My third point, emanating from our own national experience, concerns the need for more knowledge, contacts with scholars and civil society and reaching out. When we recently revised our own Swedish CT-strategy we found not only that we needed

some more resources, some more coordination, but also deeper insight into the mechanisms behind terrorism and violence-oriented extremism.

At the beginning of this year we launched our first national action plan with a view to protecting democracy against violence-oriented extremism. It will run for three years and involve a number of NGOs, including religious organizations. It will cover a wide field—including the so-called "white power" groups, the autonomous left and religiously motivated violence. It will also look at ways to support defectors from these groups. There will be a clear focus on the younger generation, on the role of the schools and civil society.

Just to give a few concrete examples of projects we will carry out:

- a special study of the best methods of strengthening young people's democratic values

- a study of how xenophobia and related forms of intolerance can best be combated

- a study of how to enhance knowledge among youngsters to counter Islamophobia and anti-Semitism

- an action plan that includes support for civil society structures engaging in preventing the spread of violent extremism

We will of course be happy to share our findings with our international partners in due time.

Now to my fourth point, language and communication: how do we communicate about terrorism and extremism? It is an issue to which we need to devote more attention and an area where we have to be rather self-critical, also in the EU context. Communicating in the right way goes further than, as it were, countering the single narrative. We should try not to let the enemy set the tone. We should refrain from language that inflates the importance of the various extremist trends and organizations, which in fact can serve to glorify and mystify them and add to their attraction in certain quarters.

We should not underestimate the threat, and should also point out the intellectual and theological hollowness of the enemy's narrative and propaganda; we should illuminate the difficulties but also the progress made in combating terrorism. Also, we often use concepts like Islamism and jihadism rather haphazardly, sometimes estranging people who are not in the enemy group or susceptible to becoming part of that. We could stigmatize the innocent and create new enemies.

Finally, my last point concerns a very topical subject which is being portrayed as a new aspect of the terrorist threat and which in the discussion sometimes takes us

in the wrong direction: the use of the Internet. Yes, terrorists and extremists use the Internet for recruitment and propaganda, and sometimes for operational planning. And, yes, the use of the Internet for spreading propaganda promoting violent extremism and terrorism has increased since the relative weakening of al-Qa'ida's core and the increased fragmentation that has followed. And we must of course recognize that to its full extent. But we must not throw out the baby with the bathwater.

The Internet has given us tremendous new opportunities and has increased openness and transparency. There are few dark corners of the world anymore. If we believe that human development depends on individual expression of ideas, then we have a strong case for protecting a free Internet. Unfortunately, we see that the fear of terrorism is sometimes used as an excuse for regulating the free flow of information on the Internet, i.e. as an excuse for censorship. The problem of the Internet being abused as a channel for spreading messages advocating violence and terrorism should be duly recognized, but it has to be dealt with by means other than censorship. We find standards for freedom of speech and expression in international law that are also applicable to the Internet, so we don't need to re-invent the wheel. The same human rights that apply off-line should also apply on-line. In fact, a landmark resolution along these lines was unanimously adopted by the UN Human Rights Council in Geneva this summer.

Combating "hate speech" on the Internet should be carried out within the rule of law, while safeguarding human rights and freedoms and respecting international law. Propaganda promoting terrorism and violence on the Internet and elsewhere is a highly complex issue and again illuminates the educational task with which we are faced, i.e. of providing our young ones with the right tools for critical analysis.

Studies on the System and Mechanism of Counter-terrorism Emergency Command

Colonel Wang Xiaobin, Research Fellow at the War Theory and Strategic Studies Department, PLA AMS

In today's world, the non-traditional security crisis represented by terrorism has become increasingly prominent. This has had a significant impact on international relations and regional situations. Meanwhile, it is also a great challenge to global governance capability, to the crisis management level of countries and to their military functions. Many countries and international organizations are establishing and improving their systems and mechanisms of counter-terrorism emergency command and crisis management policies and mechanisms in order to deal with terrorist attacks in a timely, scientific and reliable manner. According to the experience of other countries in countering terrorism, the key to successfully dealing with incidents of terrorist attacks is the system and mechanism of counter-terrorism emergency command, which should be scientific, rational, responsive and effective.

I. The main characteristics and requirements of the system and mechanism of counter-terrorism emergency command

The mechanism of emergency command (crisis management mechanism) refers to forms of organization, modes of operation, technological systems and related laws and regulations of a nation and armed forces when preparing and dealing with emergency events in non-war conditions. Although different countries and armed forces have different conditions, there are some common characteristics and requirements.

A. Highly centralized and unified decision-making powers. Dealing with emergency events such as terrorist attacks is highly sensitive. It always consists of strategic decision-making, battle command and tactical operations. This requires highly authoritative and centralized command. Therefore, the top authority for crisis management is always in the hands of the top leaders of the state and their core decision-making organizations. In the U.S., this includes the president, the National Security Council and the special team for crisis decision-making. And in Russia, this includes the president, the core of the national security decision-making organizations and the Federal Security Service (FSB).

B. Active and flexible control of the whole process. Crisis management and emergency command of counter-terrorism mainly include the following: controlling terrorist attacks within a certain area instead of allowing them to spread; decreasing

the number of areas concerned and avoiding upgrade and transformation; recovering societal and security order and assessing the loss after the terrorist attacks in order to minimize the negative influences. Developed countries classify dealing with counter-terrorism emergency events as a branch of governmental crisis management. They emphasize early warning, prevention, control, resolving and soothing during the whole process. Various methods have been taken in order to realize dynamic and proactive management.

C. Strengthening coordination and integration of powers. Dealing with counter-terrorism emergency response requires unified deployment, overall planning and coordinative operation so as to use the various powers to their full advantage. We need to attach great importance to coordination between civilian and military powers, e.g. cooperation between the military, diplomatic services, intelligence services, the police, security forces, the transportation sector and the media. Forming a scientific and normal coordination mechanism can help various powers unify their thinking, allow their tasks to converge, share resources and synchronize their actions.

D. Emphasizing rapid response and efficient operation. We cannot see the portents of non-traditional security threats. It is difficult to forecast the time, place or damage. The time to respond and prepare is also short. According to statistics, more than 100 influential terrorist events have taken place since 1990. All of them were unanticipated. The initial response is quite important in dealing with terrorist attacks. A crisis management organization needs to be able to shift mode from its normal one to a crisis one and make right judgments and decisions as soon as possible.

E. Protected by laws and regulations. Many countries have emphasized the importance of drawing up laws and regulations to specify the responsibilities of crisis management organizations. For example, there are the *National Security Law, National Emergency Law* and *Anti-Terrorism Act, Federal Safety Act, Federal Emergency Law,* etc. in Russia and the *Non-military Emergency Law, Domestic Emergency Law*, etc. in the UK. These laws and regulations have defined functions, clarified responsibilities and supported mechanisms for emergency command work and have put non-traditional security crisis management on a standardized, institutionalized and legalized track.

II. Structure of systems of counter-terrorism emergency command

The organization of the emergency command mechanisms of major powers can be described in terms of system and mechanism. The emergency command mechanism of the armed forces is an important part of a government's crisis response capability. Being the most important aspect of a nation's power to counter terrorism, the armed

forces will quickly start emergency procedures to deal with terrorist attacks according to strategic decisions from heads of state and administrative and security decision-making organizations. On the basis of counter-terrorism experience, the world's major powers have established decision-making and decision-executing mechanisms of guidance, support and coordination. This has formed clear layers of responsibility in decision-making, command, coordination and action.

The first layer is the top decision-making layer, which consists of heads of state and administrative and security decision-making organizations. There are special organizations devoted to studying and solving the most serious national security problems in each of the major powers across the world. The heads of state administration are its core. The national security decision-making organizations are its main body and they implement unified emergency decision-making and strategic command. The heads of state administration (the president and the prime minister or premier) always serves as the chairman of the national security decision-making organization and the supreme commander of the military. He is the supreme commander and final decision-maker. Procedures with standardized mechanisms are conducive to realizing rational and efficient crisis management and can also improve response sensitivity. The National Security Councils established respectively by the U.S. and Israel, the Cabinet Committee on Security established by the UK and the Federal Security Conference established by Russia are all core decision-making organizations that can not only finish security advice work but can also deal with comprehensive security problems. After the "9/11" event, the U.S. created ministerial coordinating bodies and professional crisis management organizations. This has formed a comprehensive national security crisis management system with the president at the core, led by the National Security Council, which coordinates actions by the CIA, state council, Department of Defense, the White House Office, and the White House Information Office.

The second layer is the intermediate coordination layer, which consists of the higher level of the emergency command organization. This includes not only managing the special emergency organizations of the government in normal times, but also constructing temporary ones during emergencies. These organizations have various functions and independent status. They can improve the communications between different layers and departments with different functions. They are also tasked with configuration and mobilization of national strategic resources and emergency powers. Due to their independent status, they possess supra-sector power. The top national decision-making authority will directly order them to respond to emergency events. And this can decrease disputes over minor issues between different sectors. Examples of this kind of organization are: the Federal Emergency Management Agency (FEMA) under the Department of Homeland Security in the U.S., the Civil Contingencies Secretariat of the Cabinet Office in the

UK, the Joint Anti-terrorism Center in the UK and the Ministry of Emergency Situations in Russia.

The third layer is the front-line action layer, which consists of emergency command organizations in the places where events happened. They are always the organizations that first face emergency events and implement emergency actions. For instance, the government divisions, security divisions, war zone (military region) headquarters, etc. Their main responsibilities are to quickly respond to terrorist attacks, activate contingency plans and implement actions to deal with the situation. If the situation is really urgent, they can simplify decision-making procedures and decrease command layers in order to realize real-time command, which is face-to-face and point-to-point command from the strategic to the tactical level. In the U.S. armed forces, the joint command in war zones is responsible for dealing with counter-terrorist emergency events. During the hostage event in Russia on October 23, 2002, the president ordered a joint emergency command center to be established, to be headed by the Federal Security Secretary and appointed persons in charge from the Department of the Interior, MOD, Ministry of Emergency Situations and House Administration in Moscow.

III. Measures to strengthen the construction of the system and mechanism of counter-terrorism emergency command

In normal times, it is important to prepare to respond to terrorist attacks. Management of non-traditional security crises, such as counter-terrorism operations, involves many factors. Whether the response is timely, reliable and effective relates to the national security, the stability of the regime, social development and even international peace and security. Therefore, we must take comprehensive measures to strengthen the construction of the system and mechanism of emergency command.

A. Strengthening intelligence gathering and information sharing. Intelligence is the basis of counter-terrorism emergency command. It is important to expand access to intelligence and to establish a social information feedback network and comprehensive information database. We also need to perfect mechanisms of intelligence warning and risk assessment, establish mechanisms for military-civilian multi-intelligence sharing and systems for anti-terrorist intelligence warning in order to realize the exchange and sharing of intelligence and information resources. The armed forces should take advantage of technological measures and powers to establish integrated intelligence summary institutions and platforms for crisis management information combined with civilian intelligence forces. After the 9/11 event in the U.S. and the hostage event in Russia, both countries have considered improvements to their intelligence systems as an important step to perfect their

emergency management mechanisms. For instance, the U.S. government has established the position of National Intelligence Director who is in charge of national intelligence work, while the General Staff Headquarters in Russia has set up a position in the Intelligence Bureau in charge of military intelligence.

B. Perfecting the plan and the drill. It is important to perfect national counter-terrorist plans. According to the nature, type, scale, means and mode of the terrorist attacks, we should formulate various layers and kinds of emergency command plans to confirm the procedures, methods and occasions for taking action. We need to solidify the procedures and methods of non-traditional security management of armed forces through systematic planning. This means making sure of responsibilities for the mobilization of troops, means of dealing with situations, modes of support, ways of coordination and command relations, etc. A mechanism for amendments to the plan is also needed. The drill should be part of the routine work of anti-terrorism departments. Through regular drills, we can find problems and then amend, fulfill and perfect the plans.

C. Adopting expert advice. The international experience with counter-terrorism shows that counter-terrorist actions need professional knowledge and skills. Therefore, the main powers should pay attention to cultivating professional counter-terrorist forces in military and civilian units. The government should make sure that professional requirements, codes of conduct, standards of procedure and inter-departmental coordination guidelines are met. This not only means that an experts' group should be established, but also that think tanks are needed with strengths in policy studies, legal advice, media advertisement and psychological intervention.

D. Improving the legal system. Order, rather than disorder, is important to emergency command. Improving the legal system to perfect basic legal documents in the field of non-traditional security is an urgent task. Firstly, the operability of laws and regulations should be highlighted. The responsibilities, powers and interests should be unanimously decided upon, as should permissions and tasks. It is especially important to clarify the legal position and responsibility of the armed forces in counter-terrorism operations and to put counter-terrorism actions within the legal orbit. Secondly, there is a need to perfect the rules and regulations of emergency command procedures and clarify responsibility and coordination methods of every sector. Thirdly, under the premise of complying with the relevant international conventions, we need to perfect bilateral or multilateral protocols and mechanisms for briefing and consultation in order to provide legal support to further bilateral or multilateral cooperation. Currently, there are many counter-terrorist conventions, agreements and protocols. There are more than 20 counter-terrorist international laws.

E. Strengthening international collaboration and cooperation. Non-traditional security crises such as terrorist attacks are a challenge the whole world faces. Objectively, all countries need to strengthen international cooperation and military exchanges and work on the integration of mechanisms for international collaboration in the field of non-traditional security. With regard to the establishment of emergency command capabilities, we need to establish multi-layered mechanisms involving nations, regional organizations and the UN in order to cope with counter-terrorist or other non-traditional security crises. The relevant laws and regulations should be created to advance capacity for non-traditional security crisis management. The SCO is a good example. It has set up a mechanism for joint counter-terrorist operations and security cooperation. A mechanism for military drills among member countries is being set up. Security cooperation is deepening and plays a very important role in regional security stability. Furthermore, the UN should play a leading role in responding to non-traditional security crises. It should establish a fair, neutral, rational and highly efficient mechanism for international cooperation and emergency command within the UN framework. It should quickly coordinate between different countries if necessary in order to strengthen international collaboration and cooperation among countries to cope with non-traditional security threats together.

Learning From The Past: Japan's Experience with Human Induced and Natural Disasters

Akiko Yamanaka, Former Vice-Minister for Foreign Affairs of Japan & Senior Fellow, University Of Cambridge

I. Introduction

1. The International Situation

The political dynamics of the international arena have changed radically since the end of the Cold War. Both developed and developing countries need to establish a new security framework in order to fulfill their roles as leading members of a peaceful world community. After the Cold War, the international landscape has been extensively marked by increasing ethnic and religious conflicts, drugs, terrorism, the proliferation of weapons of mass destruction in certain countries and the prevalence of new diseases. In addition to these global issues, there are newly tangible phenomena such as piracy, oil spills, financial crashes and cyber terrorism, as well as natural disasters like tsunamis, earthquakes, droughts, floods, forest fires, volcanic eruptions, hurricanes, typhoons, tornados and the scramble for natural resources, any of which can jeopardize peace and stability at any time, anywhere on the earth.

The year 2011 made it apparent that the international community has to establish a new world order in order to seek prosperity based on peace and stability. Unexpected people's movements in Tunisia, Egypt, Libya and some other countries in Africa and the Middle East, and now in Syria, have not yet finished. In addition to these phenomena, the earthquakes and tsunami of March 11, 2011, with the accompanying nuclear power station accidents have been a cause of tremendous damage to Japan, and their economic and political effects are spreading to the world community. In particular, the Fukushima Daiichi event has caused serious problems of energy policy for each nation/state. The euro-zone crisis at this moment is still very serious, and may even change the EU itself.

The dawn of 2012 asked us to challenge the paradigm shift from traditional approaches to new ones. We have learned the importance of preventive diplomacy from the mistakes of the wars in Iraq and Afghanistan. Strained finances and budgetary deficits with an economic slowdown have brought a conceptual change from the traditional security framework, driven by a search for cost effectiveness. Even a rising China cannot continue her growth forever and in the future could suffer from shortages of water, food and energy. Moreover, North Korean nuclear problems may extend to Iran. Needless to say, the fundamental problem of the Middle East—the Israel-Palestine issue—is also getting worse.

In this environment of uncertainty, the challenge for all countries is to consolidate their own identities and influence. In order to do so, it is necessary to use a "two-handed policy": one hand is military preparation and the other is non-military diplomacy. This means a combination of traditional security measures employing military tools and perspectives, and non-traditional security measures such as conflict prevention and resolution efforts, regional confidence-building measures, and a range of economic, political and humanitarian security objectives.

2. *The Tide of History*

I would like to point out three elements that indicate where we are and in which direction we should go:

i) The first element is transition. We are in a transition period from traditional approaches to new ones across a range of issues, including conflict, war and peace.

ii) The second element is the changing nature of security. The nature of security has been evolving since the end of the Cold War from "against" to "with." During the Cold War, security meant being "against" certain countries. However, the concept of security now should mean being "with" every nation/state that is a part of each region. This means that we must make efforts to establish relations based on trust among countries so that peace and stability can be established in each region on the globe. We must also recognize that security is increasingly complex and multifaceted.

In addition, most of us would agree that the concept of security is being broadened considerably and continuously, to incorporate military, political, economic, societal and environmental dimensions, and the inter-linkages between them. The traditional model of security rests upon military defense of national territory. Yet for many people in the world—perhaps even most— the much greater threats to security come from internal conflicts, disease, hunger, environmental contamination, street crime, or even domestic violence. And for others, a greater threat may come from their own country itself, rather than from an "external" adversary. We are moving towards a concept of human security that revolves around individual and community welfare.

iii) The third element is cooperation. After the terrorist attacks of September 11, 2001, the need for international cooperation that crosses national borders has become more important than before. Even the United States, the sole superpower, cannot function without a coalition of nations/states. In international relations, this is recognized as the post post-Cold War phenomenon. As a result, it becomes important to examine where we are in the tide of history. If we are to change the past dependence upon war to resolve disputes, it becomes very important for us to

introduce the concept and value of "preventive diplomacy" for all regions of the world. In preventive diplomacy, a concept that was introduced by Dr. Boutros Boutros-Ghali, non-violent means of resolving international conflicts should be used whenever possible. However, if these don't work, it is important to have the capability and strength to step in and enforce peace where necessary.

II. Preventive Diplomacy & Preventive State Theory

1. Traditional Security

The Japanese Self Defense Force (SDF) in Iraq was referred to as a "non combat force" by the Western media. It is true that the SDF is not allowed to fight with arms, according to the constitution issued in 1947 just after World War II under the U.S. occupation. The reason for the restriction is to avoid Japan becoming militarized again. However, as I mentioned, the world community has changed and is changing even now to seek a new world order. Therefore, even NATO's mission is being reviewed. The non-combat force has contributed and is contributing in different ways as an active member of the world community.

i) Anti-Terrorism

The Japanese Government passed the Anti-Terrorism bill in November 2001, soon after the September 11 attacks in New York. The Japanese Maritime Self-Defense Force was sent to the Indian Ocean to supply fuel to the warships of various countries that were actively involved in the Afghanistan War until November 2007, as rear support to the anti-terrorism war.

ii) Anti-Piracy

We passed the "Anti-Piracy Measures Law" on July 24, 2009, when I was serving as an Acting Director of the Defense Committee of the Liberal Democratic Party (LDP), the ruling party at that time. This law enables Japan's naval vessels to protect any ship from pirates, regardless of her flag. Japan has deployed two Japan Maritime Self Defense Force (JMSDF) destroyers with Japan Coast Guards on board. As of October 12, 2011, when I visited, Japan's vessels have escorted 2,256 ships on 291 escort missions. Japan is also very active in participating in discussions in the Contact Group on Piracy off the Coast of Somalia, established pursuant to UNSC resolution 1851, and even chaired the group in 2009. At this moment about 120 MSDF and 60 GSDF staff are working at the base in Djibouti Airbase and at a new facility called the Japanese Facility for Counter-Piracy Missions in Djibouti. However, we have to seriously consider the provisions concerning the use of weapons against pirate vessels.

iii) Peace Keeping Operations (PKO)

That the Japanese SDF serves for peace and stability with other nations/states and cooperates with the UN as a member of the world community is in accordance with the spirit of the Constitution. Therefore Japan passed the "PKO Bill" in 1992, at the same time as China. Since then, we have dispatched missions to the following conflict areas: Cambodia (1992), Mozambique (1993), Rwanda (1994), Pakistan (for Afghan refugees, in 2001), East Timor (2002, when seven females were included for the first time) and Iraq (2004). At this moment, Japanese PKO of SDF are in the Golan Heights, Haiti, East Timor and the decision has been made by the Government to send SDF to Sudan.

2. Non-Traditional Security

i) Human security

I would like to propose to review the definition of human security to include responsibility to protect not only from violence but also to secure the basic rights of human beings as follows:

ii) Food security

Food security should not be looked at as an issue affecting a country in isolation, but considered from a regional perspective. Japan should work together with its Asian neighbors with a bird's eye view. Japan's agricultural technology, high productivity, irrigation and distribution systems can help to construct an Asian food security network to provide mutual support in times of need. I believe this model can also be applied to Africa.

iii) Water security

Japan's compact water purification systems, desalination facilities and water treatment systems can be used in any place where water exists. At the same time, Japan can promote afforestation and reforestation, which can prevent desertification in the Middle East, South America and Africa, and even in China.

iv) Energy security

The spread of solar and wind power is gaining momentum; however wave power generation, tidal power generation, geothermal generation and the development of methane from the sea can also be accelerated by Japan. In addition to the above, Japan's technology can contribute to upgrading nuclear power stations and risk management, if we can learn the lessons from the accident at Fukushima Daiichi.

3. Preventive Diplomacy

In its simplest form, preventive diplomacy can be divided into, and explained by, four stages:

i)   Creation of an environment of trust in the region

ii) Prevention of violent conflict from breaking out

iii) Prevention of conflict from expanding

iv) Prevention of the resumption of hostilities

From conflict prevention to the final phases where financial aid is required, Japan should aim to implement a comprehensive approach. Japan should also consider to what degree it could effectively link: i) military conflicts; ii) confrontation; iii) peace negotiations and ceasefires; iv) peacekeeping; v) peace building; vi) reconstruction; and vii) preventing conflicts from restarting, as part of a framework that encompasses PKO and prevention activities.

4. Human development through the Peace-building Preventive Diplomacy Training Centre

As Vice-Minister for Foreign Affairs in Japan in 2007, after five years of research I launched a program called "Human Resource Development in Asia for Peace-building." Half of the participants in this program are Japanese and the other half are from other Asian nations/states. The program features three months of lectures at Hiroshima University, a six-month internship in UN-related organizations in conflict zones and wraps up in Tokyo. In 2009 we expanded to the Middle East (which is West Asia, according to Prince Hassan of Jordan). Taking a slightly long-term perspective, within 15 years or so, those who have been trained at the Centre could conceivably be working in positions of influence throughout the region. This human network, with its seeds sown by Japan, would surely prove a useful and effective tool to prevent conflict from breaking out and be a base for peace and stability in Asia. I remember the previous Labour Government in the UK appointing the Prime Minister's Special Representative for Peace Building and sending him to Japan. And at the end of the Bush administration, the Institute for Peace was established in Washington D.C., with a Norwegian Director and carried out its first training course in 2010.

III. Japan's Experience

I believe that disaster prevention is based on the same concept of preventive diplomacy, whether it is based on natural or human induced disaster. In that sense, I would like to refer to the tragic events of March 11 in Japan, especially Fukushima

Daiichi, because I had warned against them at the Committee of Science and Technology of the Japanese Diet. When the Donen accident happened in 1999, I flew to the U.S. in order to do research on crisis preparation, risk management and defusing crises regarding nuclear power, because one's most fundamental and important duty as a statesperson is to protect and save one's people and land/territory. The U.S. government was kind enough to help me to be able to get all the necessary information from Siemens Power Corporation, Pacific Gas & Electric Company and Lawrence Livermore National Laboratory, saying "Akiko, if you yourself would like to learn about the bitter experience of the U.S. in the Three Mile Island accident, we will help you." At that time, the Government LDP members said to me, "Yamanaka-san, don't worry too much, because Japanese technology is a world leader. Therefore, there will be no accidents at the nuclear power stations." And no one in the DPJ, the current government, showed any interest in it. At the end of the day, there was no progress made regarding the issue of crisis management at nuclear power stations. I believe in the Japanese saying "Be prepared and you'll have no regrets." Therefore, I wrote a book in 2003 entitled *Think or Sink,* making the case for crisis preparation and risk management at nuclear power stations drawing on Preventive State Theory, which is why Mr. Katsumata, the chairman of TEPCO, sought my advice at the beginning of April last year.

Every year Japan is seriously affected by typhoons. Japan has also suffered many times from earthquakes. Moreover, tornados have been very visible in Japan this year. These have made preparing for natural disasters part of the Japanese mindset. Practical preparations include keeping a fire extinguisher, emergency provisions and an air-raid hood, etc., ready at each house. At the same time, there are active fire brigades in local areas whose members are young volunteers ready to protect the local people and the area in cooperation with the fire station and are very active when any kind of natural disaster occurs.

In June of this year, a question was raised at an international conference at the University of Cambridge: "Why, out of a population of 10 million, did only three people die in Tokyo as of five weeks after March 11? If there was an earthquake of the same level in another country in a city with the same population, presumably tens of thousands of people would die." Because of their experience every year, each citizen has been prepared for natural disasters, starting with their schooling at elementary school. Everyone is ready to put out fires and to decide whether to immediately shelter under the table/desk or leave for the emergency evacuation site. However, Japan is not as well prepared for either terrorist attacks or accidents at nuclear generators.

The year 1995 was a year of disasters for Japan. On January 17, we had the Great Hanshin earthquake (Kobe Earthquake), a magnitude 7 and seismic intensity 7 earthquake in which 6,434 died, 43,792 were injured, 104,900 houses collapsed

completely and 639,686 houses half-collapsed. The fires that occurred at the same time made the damage even greater. During this crisis, we learned a number of things about urban natural disasters. For example:

- The damage to high-rise buildings was worst on the first floor, not the ground floor;

- The Road Traffic Law did not allow for stopping individual cars, which prevented fire engines from neighboring prefectures coming into the fire site of the city center;

- International rescue from the UK came within 24 hours, but could not fully act because of the six-month quarantine inspection requirement for dogs;

- Foreign doctors from neighboring countries could not act because of the domestic-oriented Medical Practitioners Law;

- Complicated procedures for requesting the mobilization of the SDF, etc.

Since then, we policy makers have made reforms of various laws, which enabled the response to March 11 to be much better.

On March 20, 1995, the Sarin attack on the Tokyo subway by Aum Shinrikyo happened in the center of Tokyo. I see this as a kind of terrorist incident, because the members of Aum Shinrikyo collectively planned and prepared for the attack and intended to cause the downfall of the government. Thirteen people died and more than 6,300 were injured by sarin poisoning. The scale of this event inside the underground was beyond expectation. There was a delay in identifying the antidotes that were needed, and the slow reaction of police and station employees due to their lack of understanding what to do increased the number of victims.

As already mentioned, in 1999 the Donen accident happened. But in 2007 we had the Shin Niigata Chuetsu Earthquake. At that time, a seismic intensity of 7 was measured under the Kashiwazaki-Kariwa Nuclear Power Plant but no radiation was measured. Even the International Atomic Energy Agency (IAEA) praised the technology. However, this confidence saw the Tokyo Electric Power Company (TEPCO) extend the use of Fukushima Daiichi for another 10 years, even though it had already been in use for 40 years, having been the first generator imported from the U.S. As an older design, the technology used was not as advanced as more recent models.

Regarding tsunamis, we have two warning systems: the WCATWC (West Coast and Alaska Tsunami Warning Centre) and the PTWCP (Pacific Tsunami Warning Centre). The WCATWC has 11 areas based on coastal topography and one or two levels of Tsunami Information Statements, and one to three levels of warning systems are applied depending on the area. Japan has contributed heavily to the PTWCP, which was organized by UNESCO with 26 nations/states, such as Japan, the

U.S., China, Australia, Chile, Russia, Korea, etc. after the severe damage caused by the 1960 Valdivia earthquake (Great Chilean Earthquake) and tsunami. The wide gathering of data made it possible to forecast tsunamis.

However, the problems pointed out long before March 11 were as follows:

i)   The dreadfulness of tsunamis is forgotten year by year by people;

ii) People get used to the warnings and do not want to escape;

iii) The strong and huge breakwater seawall established on the coast of areas frequently affected by tsunamis makes residents feel safe, causing them not to react immediately to warnings.

Indeed, we have forgotten the experiences of the Teikan earthquake and subsequent tsunami of 1869, which was 20 meters high, the 1703 Genroku earthquake and 38.2 meter high tsunami, and the 1896 Meiji-Sanriku earthquake and tsunami. Other notable events include the 90m high tsunami following the earthquake in Greece in BC 1628, which is known as Noah's flood; the Lisbon earthquake and tsunami of 1955, which left 10,000 dead; the 30m high Aleutian earthquake tsunami; the Chile earthquake tsunami in 1960, which reached Japan 22 hours later; and the 2004 Sumatra earthquake resulting in a 34m high tsunami, which left 250,000 people dead.

One village in Japan had an old wooden board on a hillside saying "Do not build a house below this point," which prevented villagers from building houses in places of low elevation that could be reached by a tsunami, thus saving a lot of lives on March 11.

Lessons Learned

What we have learned from the March 11 disaster is very simple. Everyone in a position of responsibility can and should do more to develop criteria for decision-making, gather necessary information and provide guidance based on facts and forecasts. These include:

i)   Systematic preparation, management and practice for a crisis based on a "fail-safe" spirit, in other words, understanding that the worst *can* happen;

ii) Immediate decision-making and taking of responsibility by leaders, especially in politics and in the relevant companies;

iii) Human development of expertise and specialists at all levels.

In order to prepare for and respond to natural and human induced disasters, a solid philosophy is needed. In this regard, preventive diplomacy theory can be applied to the nation's development as preventive state theory in order to minimize damages.

IV. Prevention & Response

These are the steps that are immediately required:

1. Immediately establish a Tohoku Recovery/Development Agency with all ministries involved led by a minister and create a new model for the development of the affected region;

2. Recovery of industrial capability of producing products in Japan and trading power, such as a Free Trade Agreement (FTA) with the EU, Trans-Pacific Strategic Economic Partnership (TPP), etc.;

3. A future-oriented energy policy, as well as setting up regulations for safer usage of existing power resources.

In order to follow through on these, Japan still needs *gaiatsu* (foreign pressure), because the people of Japan would not believe in their political leadership or in agencies such as TEPCO, etc.

V. Challenging Issues

The challenges for each region will be as follows:

1. Disaster Prevention and Peace-building Network Establishment;

2. Joint Studies on the combination of technological/scientific perspectives and policy-relevant perspectives of preparation, management and recovery activities, in other words, "hard and soft power collaboration in preventive diplomacy";

3. Human development, as expertise and specialists of crisis preparation and management should be considered in each region of the globe.

VI. Conclusion – an age of balance

The twenty-first century is the age of balance. This struggle for balance is being waged on an international, state and individual level, between dichotomies of competing values. These are:

1. Development vs. Environmental Protection;

2. Globalization vs. Regionalization;

3. High Tech Information vs. Individual Privacy;

4. Group Orientation vs. Individualism;

5. Work vs. Leisure;

6.   Materialism vs. Spiritualism;

7.   Male vs. Female;

8.   Military Solutions vs. Non-Military Alternatives;

And even

9.   National interests vs. International interests = common interests

In closing, I would like to end with a quote from the Greek philosopher Aristotle, who said 2,000 years ago: "It is more difficult to organize peace than to win a war; but the fruits of victory will be lost if the peace is not well organized."

Threats To Cyberspace And Responses

Senior Colonel Fan Gaoyue, Research Fellow at the World Military Studies Department, PLA AMS

Note: The views expressed here are solely those of the author and do not stand for the views of the PLA Academy of Military Science.

Summary: With the advent of the information age, the Internet has become more and more popularized and the number of Internet users has increased rapidly to more than 2 billion. On the Internet, people control traffic and transportation, distribute energy and power, do their shopping and pay their bills, enjoy music, exchange sentiments and know the world by sending and receiving information. The Internet has become a tool for crossing national borders, communicating global information and exerting influence upon international and domestic affairs. However, because cyberspace exists across the world, transcends geopolitical borders and is readily accessible in varying degrees to anyone and subject to the availability of the electromagnetic spectrum, it is seriously threatened by cyber-invasions, cybercrimes, computer viruses and worms, network attacks, etc. To deal with these threats, people must raise their consciousness of cyberspace security and strengthen the protection of cyberspace, strengthen the innovation of network technology to reduce the vulnerabilities of network systems, establish national cyberspace security watches and warning systems to detect and prevent cyber attacks in a timely and effective manner, perfect laws and regulations for cyberspace security to consolidate the management of cyberspace and strengthen international cooperation to promote cyberspace security together.

I.   The roles and characteristics of cyberspace

Cyberspace is composed of hundreds and thousands of interconnected computers, servers, routers, switches and fiber-optic cables and is the nervous system of critical infrastructures such as transportation, energy, telecommunications, public health, banking and finance. With the advent of the information age, the Internet has become more and more popularized and the number of Internet users has increased rapidly. From 2000 to 2010, the number of Internet users in the world increased from 360 million to more than 2 billion.[1] Towards the end of 2012, the number of Chinese

---

[1] Department of Defense, "Department Of Defense Strategy For Operating In Cyberspace," July 2011.

netizens reached 538 million and the Internet popularization rate reached 39.9 %; the number of mobile phone netizens reached 388 million, the number of network shoppers reached 210 million, the number of network bank users reached 191 million, representing increases of about 9.2%, 8.2% and 14.8% respectively compared with the previous year; the total number of domain names in China is 8.73 million (including 3.98 million .CN domain names) and the total number of network stations has increased to 2.5 million. [2] Every day countless netizens obtain or send information on the Internet all the time all over the world. The Internet has become an effective tool to cross national borders, communicate global information and exert influence on international and domestic affairs. The wide application of various networks has greatly raised the efficiency of social labor and production, reduced costs and changed the approaches of activities and decisions by enterprises, governments and social entities. The public and specialized information flowing rapidly on international networks, regional networks and city networks has already become a motivating force to promote the rapid development of politics, economy, military affairs and diplomacy throughout the world.

Networks now develop very fast and are becoming increasingly popular. It is of great importance to recognize the basic characteristics of cyberspace in running and applying networks. According to the development and application of networks, cyberspace is mainly characterized as follows: (1) it is created, maintained, owned and operated by public, private and government stakeholders and exists across the globe; (2) it changes as technologies, architectures, processes and expertise co-evolve to produce new capabilities and operating constructs; (3) it is subject to the availability of the electromagnetic spectrum; (4) it allows high rates of operational maneuver that capitalize on decision-quality information moving at speeds that approach the speed of light; (5) it enables operations across the domains of air, land, sea and space; (6) it transcends commonly defined geopolitical borders; (7) it is formed by its supporting critical infrastructure, devices that store, process and transmit data, the use of software and hardware applications; (8) it includes data, voice and video "at rest" and "in motion"; (9) it is readily accessible to varying degrees to other nations, organizations, partners, the private sector and to adversaries.[3]Besides, there are vulnerabilities in cyberspace architecture, network technology, physical protection, open source information, personnel training and cyberspace policy.

---

[2] China Internet Information Center, "China Internet Development Posture Report," July 2012.

[3] Chairman of the Joint Chiefs of Staff, "The National Military Strategy For Cyberspace Operations," December 2006, p. 3.

II.   Serious threats to cyberspace

Owing to the basic characteristics and vulnerabilities described above, cyberspace is facing a variety of complicated and dangerous threats. Some threats come from abroad, some from home, some from national governments, some from non-state actors, and still others from the vulnerabilities of computer systems. Technology that is small can have a large impact. A potential adversary who cannot make complicated and expensive weapon systems may be able to produce an obvious impact on a big country's security through its networks. Ninety percent of the participants in the 2003 Computer Security Institute survey reported using antivirus software on their network systems, yet 85 percent of their systems had been damaged by computer viruses. In the same survey, 89 percent of the respondents had installed computer firewalls, and 60 percent had intrusion detection systems. Nevertheless, 90 percent reported that security breaches had taken place, and 40 percent of their systems had been penetrated from outside their networks.[4] The threats to cyberspace can be classified into five categories:

1. Cyber invasion. Cyber invasion refers to an intrusion into networks to collect information, while neither adding nor modifying data or undermining and interfering with the networks. Both government intelligence departments and non-state actors are prioritizing their efforts to obtain information from networks because it is much easier and cheaper than human intelligence. Hence cyber invasions increase rapidly. In August 2005, IBM Global Services issued the *IBM Security Report: Government, Financial Services and Manufacturing Sector Top Targets of Security Attacks in First Half of 2005*, saying that in the first half of that year, the reported number of invasions throughout the world reached 237 million, among which governmental organizations suffered most, recording 54 million cyber invasions; manufacturing sectors ranked second with 36 million invasions; financial services and health services ranked third and fourth, with 34 million and 17 million respectively. By country, the United States government and private sectors concerned suffered most, recording 12 million cyber invasions; New Zealand ranked second with 1.2 million; and China ranked third with 1 million.[5] *China Internet Security Posture 2011* shows that about 47,000 overseas IP addresses participated in controlling about 8.9 million main servers within China (22.8% in Japan, 20.4% in the United States, 7.1% in South Korea), 11,851 overseas IP addresses remotely controlled 10,593 network stations within China using Trojan programs.[6] From January to March 2012, IP addresses revealed that both

---

[4] The White House, "The National Strategy To Secure Cyberspace," February 2003, p. 8.

[5] IBM Global Services, "IBM Security Report: Government, Financial Services And Manufacturing Sectors Top Targets Of Security Attacks In First Half Of 2005," August 2, 2005.

[6] Yang Tintin and Wu Duoke, "Network Attacks On China Increase Enormously," *Global Times*, March 21, 2012.

the website of the Defense Ministry of the People's Republic of China and China Military website suffered 80,000 invasions from abroad monthly.[7] These cyber invasions, either for getting money, obtaining intellectual property rights or undermining important defense systems, constitute complicated and grave challenges to a country's political system, economy, military affairs and diplomacy.

2. Cybercrime. Cybercrime refers to the use of networks to carry out criminal activities such as running pornographic websites, engaging in computer-related fraud and selling illegal products over the Internet. The Federal Bureau of Investigation of the United States investigated 547 criminal cases and ended 399 of them in 1998, and investigated 1,154 criminal cases and ended 912 of them in 1999, with the quantity of criminal cases doubled in a year. Since 2006 the total number of cybercrimes on China's networks has also run to an all-time high, with an annual average of about 4.7 million. In fact, the actual occurrence of cybercrime is double this number, according to the most conservative estimates of some professionals. Among cybercrimes, the most prominent problem is pornographic materials, which gravely endanger the health and mentality of the under-aged. Copyrights on software, video works and records are seriously infringed on by pirate activities, which have caused enormous losses to the owners. Cyber businesses are often harassed by fraudsters: some credit cards are embezzled, some never see the merchandise they bought, some delivered goods but never received the payment. According to statistics from Japan and Taiwan, pornography cases occupy 30-35 percent of cybercrimes, while cyber-fraud, sale of illegal products, intimidation and blackmail, insult and slander also account for a large percentage compared with other criminal offences.

3. Malware. Malware usually includes computer viruses and worms, Trojan horses and logic bombs, spam and phishing attacks. Computer viruses and worms refers to the use of illegal channels in a network to transmit programs to undermine a computer and its systems. Computer viruses and worms emerged and spread widely in the 1980s. The most noted worms and viruses include: the *Morris Worm*, which resulted in more than 6,000 infected systems, accounting for one-tenth of the computers on the Internet at that time; the *Melissa Virus*, which infected more than 100,000 main servers within 4 days; the *Code Red Virus*, which influenced 150,000 computers within 14 hours; *Nimda*, which spread to the whole country within one hour and attacked 86,000 computers in a few days by combining computer worms and viruses together; *Stuxnet*, which was employed to attack Iran's nuclear facilities and was regarded as marking a new chapter in the use of cyberspace because of its complicated techniques and excellent

---

[7] Liu Yang, "Department Of National Defense: China's Military Network Station Suffered Eighty Thousand Attacks From Abroad," *Global Times*, March 30, 2012.

pertinence.[8] Trojan horses and logic bombs are subversive codes attached to programs or systems that begin to conduct sabotage under given conditions. Spam refers to the junk mail sent to computer users by businessmen to promote sales, which can only cause minor problems. Phishing is tricking computer users into giving their account numbers and passwords by inducing them to enter seemingly legal homepages and has become one of the most prevalent methods of cheating in networks. This kind of malware usually undermines computer systems by way of leak invasion, backdoor embedding, hardware infusion or input-path introduction.

4. Cyber attack. So far a real "cyber war" has not occurred, but cyber attacks have taken place several times and have achieved brilliant victories. In March 2003, the U.S. forces intruded into the Iraqi military's classified network and sent emails to thousands of Iraqi officers persuading them to line up their tanks and armored vehicles outside of their military bases and leave to save their lives, which resulted in the disappearance of the Iraqi troops without a fight. Deep in the night of September 6, 2007, Israeli fighters fooled Syria's air defense system by using a cyber-attack and destroyed the "nuclear facilities" within Syria without incurring any loss. During the Russia-Georgia conflict that broke out on August 7, 2008, Russia launched continuous, complicated and intensive cyber attacks upon Georgia, resulting in Georgia losing control of its country code top-level domain ".ge" and being obliged to transfer its governmental websites to foreign servers, but Russia changed its attack paths, pretending that the cyber-attacks were from Georgia, which triggered the automatic protection system of most foreign banks to cut their connections with Georgian banks, causing the Georgian banks' business to collapse on account of being unable to visit the European balancing systems. As a result, the Georgian credit card system ceased working and mobile phone systems broke down as well.[9] Although to date there has not yet been a cyberwar, the threat of a cyberwar is real. Some countries began to train cyberwarriors in the 1990s and have now built large cyberspace operation forces, cyberspace service commands and joint cyberspace commands, which often conduct cyberspace operation exercises and can wage a cyberwar once there is a need.

5. Cyber vulnerabilities. The fragility of computer system security, or the capability of software and hardware to enter a network without authorization, increased evidently from 2000 to 2002, with the number of vulnerabilities increasing from 1,090 to 4,129. Even if the software and hardware are integrated into a set of

---

[8] Paul Cornish, David Livingstone, Dave Clemente and Claire Yorke, "On Cyber Warfare, A Chatham House Report," 2010, p. 7.

[9] Richard A. Clarke and Robert K. Knake, "Cyber War: The Next Threat to National Security and What To Do About It," Harper Collins Publishers, 2010.

application systems, they are still in danger of being interfered with. Most of the information technology products used by countries around the world are manufactured and assembled by foreign countries. There is a question as to whether using these products represents an unpredictable risk.[10] China is short of core computer technology (chips) with its own property rights and most of its computers adopt foreign core technology, which buries hidden trouble for its cyber security. Therefore, new weaknesses in the security of computer systems will appear all the time. To guarantee the security of networks and systems, we must persistently upgrade protection measures instead of relying on the security protection means available.

Besides these manmade threats, cyberspace still faces some natural and accidental threats. Natural threats that can damage and disrupt cyberspace include acts of nature such as floods, hurricanes, solar flares, lightning and tornados. Accidental threats are unpredictable and can take many forms, including a backhoe cutting a fiber optic cable of a key cyberspace node, inadvertent introduction of viruses, etc.

III.   Responses to the threats

In the information age, cyberspace has already become the basis of all kinds of social activities and has provided important support for national politics, economic affairs, military affairs, diplomacy, civil infrastructure and national security. If a country's cyberspace suffers heavy attacks, its energy and power, traffic and transportation, finance and other sectors will suffer enormously, which in turn will greatly affect social stability and national security. Hence practical and effective measures must be taken to ensure national cyberspace security.

First, launch a national cybersecurity education movement to raise consciousness of cybersecurity protection. Cyber threats cannot be seen or touched, they come and go without leaving footprints and it is hard to feel their existence. Therefore, the cybersecurity awareness of most netizens is rather weak. At present, most countries are eager to build networks on a large scale and with high speed, neglecting related security support measures. A lot of application systems are actually in a state of being non-defensive, leaving enormous hidden trouble for cyberspace security. Government and the sectors concerned should finance national cyberspace security education using radio, television, Internet, newspapers and magazines to make all netizens understand the grave threats they face and the enormous damage they might suffer. Thus the cyberspace security awareness of

---

[10] The White House, "The National Strategy to Secure Cyberspace," February 2003, p. 8.

netizens can be strengthened and the protection of networked systems can be consolidated.

Second, strengthen network technology innovation to reduce vulnerabilities of networked systems. Cyber attacks can burst onto a nation's networks with little or no warning and spread so fast that many victims never have a chance to hear the alarms. Even with forewarning, they likely would not have had the time, knowledge or tools needed to protect themselves. Therefore organizations that rely on networked systems must take the following proactive steps to identify and remedy their vulnerabilities, rather than waiting for an attacker to be stopped or until alerted of an impending attack: (1) Persistently assess the vulnerabilities of networked systems and adopt timely remediation measures; (2) Create a multilayered defense and a resilient network to remedy the most serious vulnerabilities; (3) Invest in research and development of new network protection products to reduce the vulnerabilities of networked systems; (4) Regularly conduct cybersecurity protection exercises to ensure networks against being attacked or to be able to restore functions in a short time after being attacked so as to minimize the potential damage caused by cyber attacks.

Third, establish a national cyberspace security response system to detect and prevent cyber attacks in a timely manner. The vast majority of a country's cyberspace is usually not owned by any public or private group and there is thus no panoramic vantage point from which we can see attacks coming or spreading. To mitigate the impact of cyber attacks, information about them must be disseminated widely and quickly. Analytical and incident response capabilities that exist in numerous organizations should be coordinated to determine how best to defend against an attack, mitigate its effects and restore service. Therefore, a national cyberspace security response system should be set up by governmental and nongovernmental entities to be responsible for analyzing, warning against and managing incidents of national significance; promoting continuity in government systems and private sector infrastructures, and increasing information sharing across and between organizations to improve cyberspace security. The system should include organizations such as information sharing and analysis centers, incident operations centers, incident management centers, response contingency centers and coordinate with governmental organizations such as national communication systems, national infrastructure protection centers and national energy support departments to bring national cyberspace security watch-and-warning work into full play. Thus, we can detect potentially damaging activity in cyberspace in a timely manner, analyze harm and warn potential victims, coordinate incident responses and restore essential services that have been damaged.

Fourth, perfect cyberspace laws and regulations to strengthen cyberspace management. Nowadays there are more than 4 billion wireless digital devices in the

world; one-third of the world's population uses the Internet; countless people also have contact with the Internet in their daily lives. Many countries have made cyberspace laws and regulations to strengthen cyberspace management and safeguard cyberspace security. For example, China has successively established laws and regulations such as *Regulations of the People's Republic of China for Computer and Information Systems Security Protection*; *Provisional Rules of the People's Republic of China for Management of Computer and Information Network and International Internet* and *Measures for Computer and Information Network and International Internet Security Protection Management*. Besides, 30 countries including 26 member States of the Council of Europe, the United States, Canada, Japan and South Africa signed the *Convention on Cybercrime* in Budapest in November 2001, hoping to work together to promote cyberspace security. These international and domestic laws and regulations have played important roles in strengthening cyberspace management and safeguarding cyberspace security. However, these laws and regulations can no longer entirely satisfy the requirements of the rapid development of various networks. They need to be perfected on the one hand and new laws and regulations need to be made on the other. To manage networks more effectively to assure cyberspace security, we need to do the following: (1) Revise out-of-date cyberspace security laws and regulations to enrich their contents and make them more practical; (2) Make new cyberspace security laws and regulations to cover the domains that have not yet been addressed such as the establishment of identity management (identity management is not just about authenticating people, authentication mechanisms can also help ensure that online transactions only involve trustworthy data, hardware and software for networks and devices); and (3) strengthen law enforcement to raise the level of cyberspace security management.

Fourth, strengthen international cooperation to promote cyberspace security. As the cyberspace of one country is closely interconnected with international cyberspace and is dissimilar to the traditional domains of land, sea and air, which have definite national boundaries, it is far from sufficient to rely on one's own efforts to safeguard one's own cyberspace security. Therefore we should do the following to strengthen international cooperation and promote cyberspace security together: (1) Enlarge the signatories to the *Convention on Cybercrime* so as to deal together with cybercrimes such as illegal access, illegal interception, data interference, system interference, misuse of devices, computer-related forgery, computer-related fraud, offences related to child pornography, and offences related to infringements of copyright and related rights; (2) Promote the establishment of an international "watch-and-warning" network system to detect and prevent cyber attacks that are coming and spreading in time; (3) Build international law enforcement cooperation mechanisms to strike cybercrimes together and enhance the intensity of striking transnational cybercrimes; (4) Hold international conferences on cybersecurity

regularly or irregularly to discuss the ways and methods to cope with threats and challenges to cyberspace security; (5) Establish international norms of behavior to safeguard cyberspace security as soon as possible and follow these norms together to contribute to the realization of international cyberspace security; (6) Negotiate and sign an agreement or treaty to prevent cyberwar as soon as possible to draw a clear line for cyberwar and forbid attacks on national economies and network systems essential to people's livelihoods such as power and water supplies, financial, medical and educational systems, and prevent the escalation of ordinary cyber attacks into a cyber war to ensure that the information environment upon which people are relying to live will not suffer ruinous strikes.

Practical Measures to Avoid Crises in Cyber Space

Nick Haycock, Office of Cyber Security and Information Assurance, UK Cabinet Office; and UK representative on the UN Group of Government Experts on Developments in the Field of Information and Communications Technologies in the Context of International Security

Abstract

As cyber space is the result of collective human endeavour, improved collaboration can make significant advances in the field of both crisis avoidance and crisis management. Paradigms of conventional arms control may be used as a starting point for this work, although the unique characteristics of cyber space will require innovative approaches. Ideological differences should not be a bar to intensified international discussion on agreed practical measures. An affirmation that all aspects of existing international law apply to cyber space, and a commitment to work on its practical challenges is the necessary starting point for this work. There is a need for a sustainable and institutionalised multi-stakeholder dialogue to complement ad hoc initiatives, and the growing sophistication and extent of cyber threats provides a clear imperative to make early progress. Some first steps towards enhanced international dialogue are suggested.

Context

In considering approaches to crisis management in cyber space, it is important firstly to recognise that it is a man-made phenomenon. There can be no "natural disasters" in cyber space: any crisis will have as its root cause a failure of human endeavour, interaction, or communication. It follows therefore that a cyber crisis should be at best avoidable, or at least predictable and manageable, provided those same human qualities can harnessed into greater international cooperation on this issue, focusing concurrently both on crisis avoidance and management.

It is equally important to recognise that although cyber space is a virtual, man-made world, the effects of any crisis would be felt in the real world. The dependence of many developed and developing nations on cyber space in general and the internet in particular, especially in the area of critical national infrastructure, means that operations of the financial, energy or transport sectors for example could be significantly threatened, with potential widespread economic and societal consequences, including injury and loss of life. It cannot be in the interests of any responsible state to precipitate these effects, and so it immediately becomes apparent that there is a significant area of common interest uniting those states, despite some

underlying ideological differences and tensions around other aspects of international cyber security.

The Ideological Gap

Discussions within the international community on threats in cyber space are relatively immature and often handicapped by significant ideological differences. These revolve around the role of the nation state in a domain which is largely owned and operated by commercial interests; the desirability of comprehensive multilateral instruments on the topic; the extent to which information itself may be seen as a threat and thus in need of greater control; and the challenge of reconciling traditional notions of state sovereignty with the dynamic, borderless environment of cyber space. These differences even extend to the use of specific taxonomies: China and fellow members of the Shanghai Cooperation Organisation favour the use of terms such as "information security" and "information space" to denote a doctrine that includes the *content* of messages transmitted, broadcast, or stored as a potential threat that needs to be tackled. Other countries, including the UK, reject this notion on the grounds that this approach could be used to legitimise restrictions on freedom of expression that would violate existing obligations under the UN Charter and the International Convention on Civil and Political Rights, among others. For this reason the terms "cyber security" and "cyber space" are preferred, as this terminology is limited to the physical infrastructure of servers, routers and communications paths, excluding the information they store, process, or transmit.

In September 2011, China, Russia, Uzbekistan and Tajikistan tabled a draft proposal for a Code of Conduct for Information Security at the United Nations. This initiative would create a politically binding framework for international cooperation in this field, and might serve as the basis for an eventual legally-binding treaty. Criticism of this initiative centres on its premature nature; the inclusion of notions of content control; the undermining of the current model of multi-stakeholder internet governance by shifting the balance to nation states under a UN-led structure; and excessive emphasis on notions of state sovereignty.

Although the UK is fundamentally critical of the initiative, the nature of its objections needs to be clearly understood. The UK is not opposed to the principle of a multilateral instrument *per se*: after all, it supports the Budapest Convention on Cyber Crime as an effective means of harmonising international approaches and cooperation in this specific field. However, the complex and comprehensive nature of any binding agreement across the entirety of a cyber space that constantly evolves at "net speed" means that it could not be effective or command widespread support without many years, possibly decades, of painstaking work on norms of behaviour and confidence building measures to build up the necessary understanding and trust among signatories. To the extent that paradigms of conventional warfare may be

applied in cyber space—a subject discussed in more detail below—their lessons clearly show that meaningful and effective multi-lateral instruments are the *culmination* of diplomatic attempts to develop shared understandings and approaches, not their starting-point. The UK therefore sees no merit in attempts to pursue a top-down approach to this complex issue: this would only lead to the partial and premature imposition of an approach to a domain too immature to support it.

Equally, although the UK rejects much of the content of the proposed Code outright for reasons noted above, some of its concepts such as improved efforts on capacity building for developing countries, certainly merit further discussion. Such discussions should however take place in the context of a different and evolving normative framework, not as an exercise in refining a Code of Conduct, which cannot currently be an effective contribution to the international debate on these issues.

The Specific Challenges

In tackling issues of state-to-state behaviour in cyber space, the experience of developing arms control regimes for conventional weapons may be a helpful starting point. These approaches have shown that states, cooperating either bilaterally or multilaterally, can over time identify common threats and embark on practical measures to address them. The initial benefits of this cooperation will be to increase the transparency and predictability of state action, thus reducing tension and the prospects of unintended or unnecessary escalation of incidents. This initial focus can build sufficient confidence among the parties to move to the next stage and engage in more difficult discussions. This next stage essentially involves the voluntary relinquishing of elements of state sovereignty in return for wider international benefits.

This comparison is useful up to a point, but cyber space presents some unique challenges not present in conventional domains. For example:

- States do not own, operate or manage cyber space. Although they must take responsibility for their own behaviour and lead international discussions on the topic, the environment in which they are operating is essentially commercially-run. Commercial operators and civil society representatives therefore have a legitimate stake in these topics and care must be taken to ensure they are given a voice.

- Unlike conventional weapons, cyber malware is inherently dual use: an apparently useful and benign function can quickly be transformed into something damaging.

- The issue of non-state actors is an acute issue in cyber space. Whether operating under the direction of states, with their connivance, or entirely independently, non-state actors have the potential to cause real-world effects comparable to those that historically would have been the preserve only of sovereign states.

- Issues of attribution and verification are much more difficult. It is possible for those possessing sophisticated capabilities to hide the provenance of their actions, or to plausibly attribute them to another party.

These are not hypothetical challenges: they exist today, and the growing interest among some countries in developing sophisticated cyber capabilities makes it even more imperative that the international community pick up the pace of discussion about how best to tackle them.

A Starting Point for Cooperation

States face common threats and challenges in cyber space. The interconnected nature of cyber space means that it is impossible for one state to insulate itself from these threats without also insulating itself from its enormous economic and social benefits. This is a further imperative to international cooperation, should one be needed. Given sufficient goodwill from all parties, the existence of differing ideological approaches need not be a bar to this cooperation. Again, the lessons of conventional arms control may be helpful here: the greater the degree of doubt, suspicion or distrust in a domain, the more that initial approaches to cooperation have to be founded on modest, achievable and pragmatic steps that avoid any ideological conflict. Such approaches can lay the foundations for the more difficult conversations that have to follow.

Cyber space is not the Wild West: the existing framework of international law applies with equal force there as anywhere else. There are challenges in reaching agreement among states on exactly *how* it should apply, but a recognition of its applicability is a necessary pre-condition for meaningful discussions on practical next steps.

These next steps might include:

- A clear affirmation of the applicability of existing international law to cyber space. This would include International Humanitarian Law (IHL) as well as other elements of customary international law. There has been some apparent hesitancy in some quarters about affirming the applicability of IHL on the grounds that this could be mis-interpreted as preparing a battlefield for future conflict. This is a dangerous argument: while discussions should of course take place on *preventing* a situation where the equivalent of armed conflict

may arise in cyber space, any reluctance to accept that IHL would apply should an armed conflict occur sends an escalatory signal. In essence, a refusal to accept IHL on the part of any state risks sending a message that its activities may be undertaken in an indiscriminate, disproportionate and gratuitous manner. Other states will inevitably be alarmed at such a signal, and may tailor their own strategies and potential responses accordingly, thus increasing levels of tension and unpredictability. The importance of correct signalling in respect of adherence to all elements of international law is therefore difficult to overstate.

• Affirmation of international law would provide the basis for the detailed discussions among policy makers and legal experts about *how* it applies to the specific challenges mentioned above. This will be a complex and doubtless protracted task, but one that will yield substantial benefit.

• In parallel, work needs to continue to develop agreed norms of behaviour among states. While these will include questions of international law, they may also cover state responsibility in respect of its own infrastructure, and the need for greater cooperation on cyber crime, and capacity building in less developed countries. This is a major focus of the UNGGE discussions currently under way.

• Work has begun in the Organisation for Security and Cooperation in Europe (OSCE) and the ASEAN Regional Forum (ARF) on an initial set of CBMs for cyber space. This provides an excellent illustration of the point above that progress can be made despite differing ideological approaches: current work is likely to focus on exchanges of points of contact, terminologies, strategies and doctrine. Such transparency and communications CBMs can not only yield useful results in their own right, they can also help build up confidence in the process and the personal relations among representatives that will allow for more challenging work subsequently to be undertaken.

• As noted above, developed countries should consider collaborative capacity building initiatives towards others: this will help raise basic levels of security and help protect the overall eco-system of cyber space.

• States should develop a sustainable, multi-stakeholder process for continuing discussions on these issues. The UNGGE, the London and Budapest Conferences, and other one-off events make important contributions in this area; but there needs to be a more institutionalised approach to these issues that will match the pace of development in cyber space.

Conclusion

The imperative to act in order to avert or manage a potential international crisis, starting in cyber space but quickly becoming a "real" phenomenon, becomes increasingly acute as sophisticated invasive cyber techniques are developed and deployed. States possessing such capabilities have a duty to act proportionately and responsibly in their own operations by acting in accordance with existing norms of behaviour applicable in more traditional domains. Beyond that, however, they have a duty to recognise the need for enhanced international cooperation to improve transparency, predictability and stability in cyber space. Will the international community see the same levels of human endeavour and collaboration deployed in the creation of cyber space used to prevent it becoming the cause of an avoidable crisis? Only time will tell, but time is not on our side.

Crisis Management in Relations Between South and North Korea

Chang Kwoun Park, Senior Research Fellow at the Korea Institute for Defense Analyses

There is still a high possibility of a crisis on the Korean Peninsula, either triggered by North Korean domestic instability or by the strained South-North Korean relations. North Korea has made several local military provocations against South Korea and it has also endured severe famines, causing the deaths of more than several hundred thousand people from 1995 to 1997. Contrary to some experts' predictions, Kim Jung Un (KJU), the new young leader of the North, seemed to have very skillfully managed the third-generation power succession after Kim Jong Il's death and has stabilized the closed society. Nevertheless, as long as the North Korean regime cannot alleviate its chronic economic problems and its young leader does not give up military options and change the game on the peninsula, a crisis can always recur and inflict severe damage on the peninsula and Northeast Asia.

Against this background, this paper attempts to present two major possible scenarios for a North Korean crisis: local armed clashes between the two Koreas on the Northern Limit Line (NLL) in the West Sea (Yellow Sea) and humanitarian disasters precipitated by North Korean political instability and economic hardship. It's largely uncertain how stable the North Korean regime is and which directions it will take in relations with the South and the world. It has not yet revealed any significant signs of change in terms of denuclearization and opening up, even though it announced partial economic reform measures to introduce privatization in the agricultural and industrial sectors. The North Korean regime faces a structural dilemma in deciding its future directions, as it is in need both of strengthening the political power base of KJU as well as his advocates and resolving harsh economic problems. In order to get over difficulties in the transitional process, North Korea may feel tempted to breed military tensions between the two Koreas. The regime may fail to provide much-needed food and services to the people if its economic situation deteriorates further or political instability gets worse. South Korea and the international community need to recognize possible crisis scenarios and develop proper strategies and cooperative policies in advance to prevent the outbreak of such terrifying situations.

North Korean Political and Economic Situations: Seeds of Crisis

As of today, the third-generation power succession in the North seems to be progressing in a stable manner. The North appointed Kim Jung Un as the Commander-in-Chief on December 30, 2011, right after Kim Jung Il's funeral. Then it revised its constitution and raised the late Kim Jung Il to the position of "Eternal

General Secretary." Kim Jung Un was appointed the first Secretary of the Korean Workers' Party (KWP) and the first Chair of the National Defense Commission during the Party conference held in April. Hereby, he assumed all the official positions needed to be the supreme leader of the North.

In order to demonstrate his leadership and to consolidate power, KJU has undertaken various efforts. Above all, he tries to portray himself as an affectionate, active and attractive leader, compared with the late Kim Jong Il, and eventually making him look more like his grandfather Kim Il Sung. For instance, he is making physical and friendly contacts with the people, visiting several construction sites, enjoying culture tours in an amusement park and wearing stylish clothes. In particular, he inspected the Army nuclear and missile unit, visited the DMZ, and went to the coastal battery unit located on remote islands, which bombarded South Korea's Yeonpyeong Island in November 2010. He also gave an impressive first public speech at the 100th anniversary of the birthday of Kim Il Sung. North Korean propaganda has been very successful in imprinting the perception that their young leader is capable of leading the country, cares for the improvement of peoples' living standards and regards the military as the backbone of the regime and the society.

The North has been successfully filling the powerful positions of the Party and the military with his close confidants over the last nine months. This can be seen as a military-dominated power structure to keep the balance between the Party and military powers. KJU's uncle, Jang Sung Taek, was promoted to the second man in power. With his support, Choi Ryong Hai assumed the key power positions, such as Director of the Korean People's Army (KPA) General Political Bureau, member of the National Defense Commission, and vice chairman of the KWP Central Military Commission. Also, Kim Jong Gak became minister of the Armed Forces, replacing Kim Jong Il's man, Kim Yong Chun. Meanwhile, Ri Yong Ho, Chief of the Army's General Staff and vice chairman of the powerful Central Military Commission, was suddenly dismissed from all his posts without any disturbance. His main mission was to check Jang Sung Taek. So far, the change in the members of power elites has been progressing smoothly and the power structure is assessed to be relatively stable.

KJU has shown his intention to carry out economic reform to fix rampant economic poverty. During his first public speech on June 28, he announced that he would make sure that his people "[would] never have to tighten their belts again." On the same day, it was reported that the North had adopted new economic management measures, characterized by giving factories and collective farm incentives to increase their productivity. Under the new proposed economic measures, North Korea will allow farmers to take 30 percent of their harvests home and to decide what items they would produce and their prices, amounts and marketing methods. The removal of Ri Yong Ho is presumed to have been caused by

his opposition to plans to seize control of economic policy from the military, especially foreign currency-income business conducted by the military. But, contrary to general expectations, the North might have determined and announced economic management measures during its supreme Party conference held in late September, even though specific reform measures have not yet been officially revealed. Therefore, it is too early to forecast the future direction and scope of North Korean economic reform. Nevertheless, this paper supposes that considering the nature of KJU's authoritarian regime, North Korean economic reform is likely to face great difficulties in the process of implementation.

In spite of the successful power transition, the Kim Jung Un regime still has some weaknesses in governing the state. Compared with his father, KJU rose to power in a very short time and did not have sufficient time to consolidate his own power base and develop his charisma. It is hard to rule out the possibility of a power struggle between the party and the military elites, as revealed in the process of Ri Yong Ho's dismissal. KJU reshuffled the power arrangement that Kim Jung Il had structured for him. It is questionable whether the system of checks and balances among the power groups is working. It seems that party elites centering around Jang Sung Taek have more political weight than military groups, who once enjoyed the greatest influence under the "military-first" policy. All told, the leader's young age and the third-generation succession may work against developing his strong control of society. In order to consolidate his legitimate authority, KJU needs to demonstrate his forte and bring about successful policy implementation for the people and the country. Even though he has made continuing efforts, it will take more time for him to gain recognition as a "true," "competent" leader.

In the near future, harsh economic conditions will be a mounting challenge to KJU. North Korea made an official request for international food assistance in January 2011, for the first time since 2004. Moreover, after the pouring rain and floods in July, it asked the UN and the international community for emergency aid. The UN Resident Coordinator in Pyongyang, Jerome Sauvage, said that about 16 million out of the total population of 24 million North Korean people suffer from chronic food insecurity, high malnutrition rates and deep-rooted economic challenges. He added that as a result, about 2 million people have starved to death since the mid-1990s.[1] The 2011 report of the World Food Programme estimated that there was an uncovered food deficit of 414,000 tons for the 2011/12 marketing year.[2] KJU is now attempting to take bold economic measures to resolve the food shortage

---

[1] Bloomberg BusinessWeek, "North Korea requests Emergency Flood Aid from United Nations," August 3, 2012, http://www.bloomberg.com/news/2012-08-03/north-korea-requests-emergency-flood-aid-from-united-nations.html

[2] World Food Program, "Special Report: FAO/WFP Crop and Food Security Assessment to the Democratic People's Republic of Korea," November 25, 2011.

problems within the next three years. Nevertheless, there are many factors that hinder successful implementation of the economic reforms, such as frequent natural disasters, a malfunctioning and closed social and economic system, and finally poor agricultural infrastructure.

Unless the North shows us that it is taking genuine actions towards its denuclearization, international sanctions will continue to be imposed. The North breached the February 29 agreement with the U.S., which had been intended to forge a favorable environment towards resuming denuclearization dialogues, by testing long-range rockets despite strong opposition from the U.S. and the international community. The international community is greatly concerned about North Korea's uranium enrichment program (UEP), which was revealed in November 2011. The North declared itself a nuclear-armed nation in its revised constitution. As the years go by, North Korea will strengthen its nuclear capability in terms of both quantity and quality. In order to keep North Korea from developing its nuclear programs, the international community would be well advised to take a stronger carrot and stick approach. It would be very difficult for the North to escape international isolation unless it shows a sincere attitude towards denuclearization. The North is trying to deepen its economic cooperative relations with China and the next South Korean administration may adopt some engagement policy toward the North. Yet international sanctions will continue to greatly restrain its economic reform efforts. Also, the continued North Korean nuclear development and deadlock of the multilateral nuclear negotiation can create some unexpected situations, which may bring about a deterioration in North Korean problems.

With the social and economic reforms, an increasing inflow of information into North Korea will affect the thinking and behavior of North Korean people. Currently, North Korea tightly controls the inflow of outside information. Nevertheless, there are more than 1 million mobile phone users and the number of phone users will increase. Also, North Korean people are likely to have more opportunities to contact foreigners as a result of various economic activities. The Special Economic Zones that North Korea has created in cooperation with China can serve as a gateway for this type of contact. It is not hard to predict the impact of information inflow to North Korea. If the regime fails to properly manage the social and economic problems, discontent among people will make itself felt. Nowadays we witness many North Korean defectors raising concern over humanitarian issues in North Korea. Most recently, some soldiers defected to South Korea by crossing the DMZ.

Local Armed Clashes and Crisis Escalation

It is not guaranteed that North Korea will not conduct another military provocation. The North has frequently resorted to the use of military force around the military boundary line, especially the NLL in the West Sea (Yellow Sea) for its political objectives. It attempts to change the *de facto* maritime boundary line in the West Area, the NLL, which has been maintained for almost the past 60 years. There were three direct naval clashes between the two Koreas. The first and second Yeonpyeong (YP) naval battles in 1999 and 2002, respectively, damaged and sunk our patrol ships, taking the lives of many sailors. After the battles, the two Koreas reached an agreement during the South-North summit in 2004, promising to make a favorable environment to prevent accidental clashes. But in November 2009, the naval clash reoccurred when a North Korean gunship crossed the NLL and disregarded the warning announcement of the South Korean naval vessels, issuing an order to retreat. Moreover, in 2010, a North Korean mini-submarine attacked a South Korean naval corvette, the Cheonan, and bombarded South Korea's YP Island with artillery shelling, marking the first direct attack on South Korean territory.

Why does North Korea continuously attempt to make military provocations, especially on the NLL? The history of past North Korean provocations indicates that there are many complicated background factors behind North Korea's decisions. Considering the tight centralized control system, it is not conceivable that North Korean naval vessels accidentally crossed the NLL or that coastal military units even fired gunshots against the South without any planned intention. Many observers claim that North Korea's military adventurism should be attributed to the strained inter-Korean relations. But such arguments cannot explain the naval battles in 1999 and 2002, when the South actively pursued a Sunshine Policy towards North Korea. The first nuclear test of the North in 2006 occurred when South Korea's progressive administration actively carried out an engagement policy towards Pyongyang. The lessons of the past show that North Korea utilizes military provocations for its various political purposes. Above all, internal political needs and a coercive strategy against the South have been the main reasons behind the provocations.

All of South Korea's leading presidential candidates revealed the future direction of their North Korea policy, characterized by easing military tensions and developing good relations with the North. Therefore, whoever becomes the next president, South Korea will pursue bilateral dialogues to improve the strained inter-Korean relations. Nevertheless, the engagement policy cannot guarantee that it will prevent another North Korean provocation. There is a high possibility that the North can face many challenges and risks while consolidating KJU's power base and carrying out social and economic reforms. In addition, in order to solidify its status as a nuclear power, North Korea always feels tempted to conduct a nuclear test and

to launch long-range rockets. This implies that the North has various motives for further provocations, regardless of the condition of inter-Korean relations.

Even though KJU appears to be pragmatic and progressive, he has yet to show clear attitudes on military and security issues. North Korea has long pursued strategic superiority over the South as its main priority. It launched a series of long-range rockets and undertook preparations for its third nuclear test. Recently, several North Korean fishing ships repeatedly crossed the NLL and the South Korean navy fired warning shots against them on September 21. It is reasonable to predict that as a young leader, KJU will be lured into using his military forces if the internal and external situations are not favorable to his regime. In fact, in his first public speech, KJU emphasized that he would maintain the "military-first" policy. During his visit to military units, he stressed a strong readiness posture to counter South Korea and the U.S. In addition, there is a likelihood that North Korean military elites will intentionally plan further military provocations to win recognition from KJU during a possible power struggle.

In the wake of the Cheonan incident and the shelling of Yeonpyeong Island, the South Korean government adopted a new doctrine of "proactive deterrence," which will eventually change the rules of the military tit-for-tat game between the two Koreas. Under the "proactive deterrence" guidelines, the South Korean military is empowered to promptly retaliate against North Korea's possible military provocations; it will attack not just the origin-of-attack units, but also their supporting forces and command structures in the North. The South Korean defense minister has repeatedly affirmed his firm resolve to retaliate against North Korea's further provocations. South Korea is operating a modern surveillance system around the frontline Northwest Islands and long-range artillery, MLRS, and helicopters are already deployed on those Northwest Islands. Plans to further strengthen our military strength to counter North Korean provocations are also being developed. In addition, the South Korean navy is strengthening its patrol units stationed in the West Sea and is improving its Anti-Submarine Warfare (ASW) capabilities. The JCS is now developing joint military plans to prepare for a possible local clash between the two Koreas. Considering the strong military posture of the two sides, once a military clash occurs, it can easily escalate into a serious crisis.

The most typical scenario for a North Korean crisis would be one triggered by North Korea's provocation. Naturally, the South Korean military will immediately retaliate against the origin of the attack and its supporting forces under the "proactive deterrence" guidelines. South Korea's modernized military forces are believed to be capable of intercepting and effectively countering another incoming hostile attack from North Korea. KJU, as a new leader, will not want to lose face, so he may attempt to take more risks by resorting to a strategy of brinkmanship. However, he has critical limitations when he relies on military instruments, in that

North Korea's forces are relatively weak and obsolete. So, North Korea may try to explore new ways to which the South cannot properly respond with its modernized conventional forces. It may include applying new asymmetrical means, expanding the geographical scope of the conflict, and using WMD threats. Because the two sides will try to dominate the escalation process, there is a high likelihood that a crisis will end up escalating, out of the hands of the two Koreas.

In order to prevent the occurrence of such a crisis and to manage it effectively, domestic and international defense policymakers and other all players in the defense/security field should make progressive efforts. If North Korea makes a reasonable choice, as expected by the international community, it is most desirable. If not, all surrounding countries need to watch closely and assess the risks of a crisis on the peninsula. They should make active efforts to persuade and coerce North Korea to change its hostile behavior. South Korea's constructive engagement policy, coupled with its strong deterrence capabilities, can help ease military tensions on the peninsula and prevent a miscalculation of North Korean intentions. The U.S. can effectively utilize its comprehensive international resources and take the lead in dealing with North Korea. China is a major power, with a critical role to play in prevention and management of crises. However, China always insists that it cannot intervene in North Korea's domestic matters and that it has limited influence to restrain North Korea's aggressive behavior. However, it is high time for China to recognize the serious impact of a possible crisis on the peninsula and to wield its political and economic leverage to prevent potential provocations. After the Cheonan incident and the shelling of Yeonpyeong Island, South Korea and the U.S. navy conducted large-scale combined exercises in the East and West seas. At that moment, the Chinese navy conducted a counter naval exercise in the West Sea. China would do well to remember that if armed clashes occur on the peninsula, the regional powers may face unwanted military confrontations in the spiral of crisis escalation.

Humanitarian Disaster in North Korea and Security Risks

A humanitarian crisis in North could be precipitated by KJU's weakening governing power and any unexpected natural disasters. North Korea has demonstrated its effective governing capability, showing few signs of instability after the death of former leader Kim Jong Il. North Korea seeks to resolve the chronic food shortage and to improve its economic conditions mainly through expanding its economic cooperation and exchange with China and increasing incoming international aid. Nevertheless, it is uncertain whether North Korea can continue to properly handle significant challenges ahead. KJU's governing power and performance have not yet been verified. Considering his young age and political inexperience, it seems not to

be an easy task for him to build his own solid power base. And it is still questionable how faithful the military and political elites are to KJU. In this sense, the possibility of a power struggle in North Korea cannot be ruled out. Meanwhile, the history of communist authoritarian regimes shows that economic reform measures may accelerate social disturbances, regardless of their success or failure. There is also a possibility that unexpected natural disasters may hit North Korea and cause its economic situation to deteriorate.

North Korean problems have been a cause of great concern to the international community. Millions of North Korean people have endured chronic famine and poverty since the mid-1990s. After the severe flooding in July, which resulted in more than a hundred casualties and damaged homes and public facilities, North Korea requested immediate food aid from the international community. Deforestation and conversion of forest land over the past 20 years has accelerated the risk of damages and costs caused by floods and landslides. The North Korean regime is assessed as lacking the capability to prevent and respond effectively to natural disasters. Even though the North Korean economy is slowly improving, it will take a long time to fix its inherent systemic problems. In fact, we witness notable signs from North Korea that it is going to take bolder economic reform measures. In particular, KJU places the improvement of economic conditions as his first policy priority. North Korea is trying to deepen its economic relations with China by expanding the volume of border trade, attracting Chinese investment to its mining projects and establishing Special Economic Zones. Trade with China, which accounts for up to 89% of North Korea's total external trade, is becoming an economic savior for North Korea, which otherwise suffers from international isolation and sanctions. However, North Korea cannot take dramatic reform measures because it is largely concerned about the impact of the reforms on regime security. Thus, reforms have inherent limitations in improving the impoverished social and economic conditions. Also, such difficult conditions may bring about humanitarian disasters at any time.

Even worse, a food shortage may be coupled with a power struggle that damages the governing function of the regime. In other words, a crisis may occur when natural disasters hit North Korea and KJU's regime is incapable of responding effectively. Of course, such a complicated scenario is far less likely to occur. It is not far-fetched to suggest that under such a difficult situation, with food shortages in North Korea every single year, a political upheaval could take place. If KJU fails to consolidate his power and suppress a power struggle, this could be a realistic possibility.

In the case of humanitarian disasters, the necessary proper measures and responses should be carried out as early as possible to prevent them from escalating. The North Korean regime does not appear to have the capacity to take proper actions no matter how hard it tries. Moreover, possible political instability may

hinder proper response, which is necessary to minimize the costs of natural disasters. The deep-rooted poverty and starvation in North Korea can be exacerbated by natural disasters and political inability, which may lead to a large-scale humanitarian disaster.

Furthermore, there is the possibility of a terrifying nuclear disaster. The Fukushima nuclear accident in 2010 shows how serious the impact of a man-made nuclear accident can be to a country and the region. If a nuclear accident occurs in North Korea, it can cause massive casualties and damage to not only the two Koreas but also to the regional countries. Compared to those of other countries, North Korean nuclear facilities lack transparency and credibility in terms of safety measures. Even though the 5MW nuclear reactor in Yongbyon was disabled in 2007, it is not certain that the nuclear materials are safely stored and managed. North Korea is now making great efforts to build a new light water reactor in Yongbyon. Satellite pictures reveal that the reactor containment building is close to completion. Furthermore, North Korea is operating an UEP, as disclosed in November 2010. There is speculation that North Korea may have undiscovered nuclear facilities. However, it is better to hope that North Korea is well aware of the importance of safety measures in dealing with nuclear materials.

Nevertheless, it should be remembered that nuclear accidents can take place in any country, even in a quite developed country like Japan. Like natural disasters, a nuclear accident can happen by mistake or due to other uncontrolled causes. North Korea may lack safety management technology for preventing the leakage of nuclear radiation. It may also have difficulties in acquiring sufficient safety equipment due to cost problems. That is, the North Korean nuclear facilities may not have the capacity to satisfy the international rules of redundancy and diversity necessary for the safety of nuclear facilities. As mentioned in the food shortage crisis scenario, it is hard to avoid the possibility that a nuclear accident can occur in a very complex crisis situation.

If a humanitarian disaster occurs in North Korea, an improper response could exacerbate the crisis situation. North Korea is a highly closed and controlled society and has very limited exposure to the outside world. Information on disasters may not be conveyed either properly or in a timely manner to the concerned countries and actors. If the North Korean authorities try to control the information, the international community may have limited information about the severity of the situation in North Korea. As a result, this will delay the evaluation of the situation and hinder the prompt supply of needed emergency aid to the affected areas. Additionally, North Korea has poor social infrastructure for transportation and communication. Mountainous terrain and rough road conditions will hinder fast access to the damaged areas. Even though North Korea is a small country, access to the disaster area can take several days. Poor communication infrastructure may

cause difficulties in information exchange and coordination among aid suppliers. Furthermore, the regime may not allow international aid groups to directly contact affected residents and conduct relief activities. As an authoritarian regime, North Korea will consider not only the disaster relief activities but also the possible political impact of the disaster and international support on its regime. In this respect, North Korea's political concerns may well prove a great challenge to effectively responding to a disaster in North Korea.

A humanitarian disaster in North Korea could affect the security of South Korea and the surrounding countries. So far, many North Koreans have crossed the Chinese border since the crisis caused by the severe famine of the mid-1990s. A food crisis and political instability could accelerate a massive migration of North Korean people flowing into China. Also, a nuclear accident could cause not only massive loss of human life but also irreparable damage to the environment. The most effective approach to dealing with the aforementioned crises is first to change North Korea's behavior and thus to make North Korea strengthen its preventive and response capability. However, because there is little expectation that North Korea will change its hardline policy, the neighboring countries and the international community need to take actions in advance. Currently, there are not many open discussions regarding humanitarian disasters in North Korea. In order to properly prevent and respond to crises, neighboring countries and the international community should openly handle this issue, recognize the potential security risks involved, and continue to persuade, or push, North Korea to take economic and social reforms and also to follow the international norms on nuclear issues, no matter how strongly North Korea resists. Finally, it is imperative to develop a cooperative mechanism for effective response to and management of a potential crisis.

Desirable Cooperative Mechanism to Prevent and Manage the Possible Crises

South Korea and other neighboring countries have a common interest in that they want to effectively prevent and mange possible crises in North Korea. Nevertheless, practical actions have not ensued from their interests and concerns. There is no actual cooperative mechanism for mitigating the possible crises that could occur in relations between South and North Korea. All the regional countries are concerned about the high level of military tension between the two Koreas and the possible humanitarian disasters in North Korea. They do talk about relieving the problems and trying to develop some cooperation to counter them. But efforts have been limited to the recognition of risks and mutual consent for partial cooperation on the related crises. Now they need to move forward beyond the basic cooperation level and construct more concrete mechanisms to counter these crises.

First of all, the regional countries need to establish crisis management on the Korean Peninsula as a major topic on their agenda for bilateral and trilateral cooperation. China and North Korea maintain a very close relationship. Accordingly, China can convey its concerns to North Korea and induce North Korea to change its belligerent behavior as well as to improve its vulnerable infrastructures. All Northeast Asian countries maintain bilateral talks and cooperative mechanisms, even though the level of cooperation is different based on the nature of their relations. South Korea holds a trilateral meeting with the U.S. and Japan and tries to develop cooperative mechanisms on nontraditional threats and North Korean issues. South Korea also holds an annual meeting with China and Japan together to improve their cooperation. I am convinced that these cooperative mechanisms can offer an opportunity for drawing public attention and lead to practical cooperative efforts.

Secondly, the scope of the six-party talks, a multilateral nuclear negotiation forum for North Korean denuclearization, needs to be expanded to include crisis management issues. There would be concerns that an expansion of the scope of the six-party talks may lead to a dilution of their original objective. Also, regional countries may not be willing to participate in the meeting to talk about sensitive crisis management issues. Nevertheless, it is the right time to advance a regional multilateral security instrument for the prevention and management of crises. Because of the devastating effects of potential crises on the peninsula, all regional countries must play a constructive role. In particular, South Korea, as well as China, needs to push forward with the agenda of crisis management for the six-party talks.

Thirdly, South and North Korea and the regional countries should accelerate their efforts to build a peace regime on the peninsula. There are many obstacles to a peace regime on the peninsula, particularly North Korea's nuclear activities. The two Koreas demand specific conditions for achieving a peace regime on the peninsula that are not acceptable to the other side. For example, South Korea demands that North Korea take practical denuclearization measures. On the other hand, North Korea demands that South Korea break the ROK-U.S. alliance. As both demands are considered as imperatives necessity for their security, it is impossible to meet their conflicting demands.

As a result, the role of regional countries is very important in this process to overcome the situation of deadlock. China's position is critical because it provides North Korea with a security umbrella as an ally. As China is located right next to North Korea, upon its decision, it can deploy massive military forces in a contingency in a short time. It means that North Korea's efforts at denuclearization will not harm its security, as it is still protected under the framework of its alliance with China. China, in cooperation with regional countries, needs to persuade and push North Korea to change its position in this peace-regime building process. And

finally, South Korea should pursue a constructive engagement policy toward North Korea backed by proactive deterrence capabilities in order to relieve the military tensions and create a peaceful environment for facilitating peace regime building on the peninsula.

China's UNSC Policy and its Implications for Security Management in the Middle East[1]

Liselotte Odgaard, Royal Danish Defence College

This paper argues that China has used the UN Security Council as a means of applying an alternative to the Western interpretation of the UN principles for global security management. China uses the UNSC as a platform for making within-system adjustments to world order. These include decoupling regime issues from issues of creating peace and stability, prioritizing dialogue as a means of influencing other states, the non-use of force in conflict management and increasing reliance on regional organizations in the pursuit of international security management. In the Middle East, the choice between Western and Chinese views on world order is giving rise to a dividing line both within and outside the region between those states that predominantly join the Chinese interest-driven concept of international relations and those that prefer the Western value-based concept of international relations. In the case of Syria, this entails rejecting the Western proposal for endorsement of the Arab League's peace plan by means of a UNSC resolution, arguing that the peace plan's calls for Syrian President Assad's resignation constitute a breach with absolute sovereignty. As such, the resolution would set a precedent for intervention without consent, which is unacceptable to China.

There is no longer one vision of world order, based on the established Western powers and their liberal aspirations for international integration on the basis of common values. Two visions exist alongside one another. The coexistence alternative is promoted by China. In part, it arises from dissatisfaction with pressures to adopt the political democratic and human rights structures of liberalism. In part, it arises from China's need to revise the existing world order in a direction that better serves Chinese interests. First, China is concerned with pursuing its global overseas economic interests without needing to make a prior political assessment of the legitimacy of the governments with which it is economically engaged. Second, Beijing insists on international political pluralism. China argues that common interests rather than common values best form the basis of world order, allowing states to pursue domestic politics according to their specific historical characteristics, national identity and level of development. Third, China insists that the non-use of force should prevail in global security management, instead pleading for diplomatic instruments and governmental consent as the way forward. Fourth, China promotes the role of regional and functional institutions in

---

[1] The views on China's UNSC policy in this paper are based on Liselotte Odgaard, *China and Coexistence: Beijing's National Security Strategy for the Twenty-First Century*, Washington, DC: Woodrow Wilson Center Press/Johns Hopkins University Press, 2012.

identifying threats to international peace and security and in managing issues that involve such threats.

The UN Security Council plays a central role in China's attempt to promote its vision of world order. As a permanent member, China is confronted with Western attempts to revise the existing world order. These involve demands for using the UN system to promote the idea that grave breaches of civil and political rights should be defined as threats towards international peace and security, allowing for intervention without governmental consent from the target state. By contrast, China supports the view that absolute sovereignty and non-intervention remain central to the UN and must not be compromised as fundamental principles of international law. In addition, Beijing's version of world order is suitable for being coupled to the UN due to its emphasis on regional and functional institutions under the UN system and on the UN Covenant's principles of absolute sovereignty and non-intervention. As the weaker economic and military power compared with the U.S., China does not have an alliance system that gives Beijing access to stable partners on the basis of security guarantees. Instead, China relies on political and diplomatic power. This approach implies persuading other states that China's version of world order serves their interests better than the Western liberal integrationist approach. China has used the UN Security Council as a means of applying its vision of world order to issues of global security management and to demonstrate to other states that China's international relations practice is in line with the principles that make up its vision of international order.

One thing to note about the UNSC is that China is not agenda setting, in the sense that Beijing does not refer cases to the Council. An obvious explanation is that China does not expect to have an easy time getting support for its strategy in the UNSC because Russia is the only veto-wielding power that tends to be sympathetic to Chinese policies. By contrast, the U.S., the U.K. and France often vote together on UNSC issues. China's relatively weak position in the group of permanent UNSC members with veto powers reflects the fact that China's power is still not that of a full-blown great power. As such, it does not have the means to be agenda setting in the main forum for global security management. As a consequence, China's actions in the UNSC tend to be reactions to the demands of the Western majority, rather than proactive attempts to set an agenda instigated by Beijing.

China uses the UNSC as a platform for making within-system adjustments. These adjustments are pursued by advocating a framework for international order consisting of three key principles that are the means to implement China's peaceful coexistence strategy in the UNSC. First, Beijing advocates the idea that UN authorization of the use of force requires consent from the host government unless proof exists of a threat towards international peace and security. Beijing's approach to the use of force also implies a broader role for regional and functional institutions of the UN system in global security management. China's program for the use of

force encompasses respect for legal, individual foreign policy choices taken by the target governments and for multilateral efforts at conflict settlement that have obtained consent from the target government. This approach involves full or partial delegation of implementation of UNSC decisions to a functionally or regionally specialized institution within the UN system, such as the IAEA, the AU or the UN special envoy. China's advocacy of non-military means of persuasion and negotiation appears, at least in part, to be a defensive policy designed to slow down demands for punitive actions against governments that are seen by Western UNSC members as threats to international peace and security. The proactive element of the program appears to be China's concern to ensure that some kind of conflict management dialog takes place that is led by UN bodies or institutions based on the principles of the UN Charter, in the event that some kind of UNSC intervention cannot be avoided.

Second, Beijing adheres to effective control as a requirement for political authority, and prioritizes the legal equality of states so as to allow for socio-economic development objectives to encourage state stability. China's restrictive definition of effective control as the criterion for sovereign political authority implies that governments are recognized as representatives of their peoples, irrespective of regime type, and are treated as the equals of other governments. This is a conservative effort designed to preserve the old UN system as the foundation of international order. Through this effort, China has become the principal defender of the Westphalian model of state-society relations, as argued by liberal analysts. A proactive new effort is Beijing's promotion of top-down support for socio-economic development, which is said to be fundamental to enhance human welfare.

Third, Beijing defends the fundamental status of absolute sovereignty in international law. China's concern to strengthen the rule of law in international relations is a conservative effort mainly designed to preserve the existing foundations of international law. China focuses on preventing calls for allowing civil and political rights to have equal status with the principle of absolute sovereignty. China's promotion of the rule of law in international relations constitutes an effective barrier against demands for taking collective action against governments that refrain from adapting their domestic political structures to the rule of law.

China's UNSC policy on Libya has confirmed that China pursues a mixture of a conservative defensive and a coexistence-style offensive form of diplomacy based on old and new elements of the UN system. China voted for UNSC resolution 1970, which in February 2011 imposed sanctions on the Libyan government in response to the use of force against civilians, stressing that the special circumstances in Libya called for an endorsement of the resolution. Beijing's decision reflected its concern to consolidate the regionalization of UNSC security management, prompting China to support Chapter VII measures following the condemnation by the Arab League, the African Union and the Organization of the Islamic Conference of the serious

violations of human rights and international humanitarian law that were being committed in Libya.[2] In March 2011, China abstained from voting on UNSC resolution 1973 which, acting under Chapter VII, approved a no-fly zone over Libya. The resolution authorized all necessary measures to protect civilians by a vote of ten in favor with five abstentions. China's abstention was determined by Beijing's preference for peaceful means of conflict settlement and its concern not to block measures approved by the Arab League and the AU.[3]

China's UNSC policy on Syria is to a large extent a response to the Libya intervention, in which NATO acted on the basis of a very wide interpretation of the mandate. This interpretation has made China reluctant to accept that similar UNSC resolutions are endorsed in future, as demonstrated with China's veto of a proposal for a UNSC resolution endorsing an Arab League peace plan calling for Syrian President Assad to resign. By contrast, the West supported the Arab League's peace plan for Syria, trying to use China's calls for regionalization of UNSC security management against Beijing. While China has endorsed the Arab League's peace plan as a useful way forward, China is not willing to risk a rerun of what happened in Libya. In China's view, NATO abused the UNSC mandate for purposes of regime change instead of limiting the intervention to putting a halt to violence that threatened to derail peace and stability in the Arab world. Indeed, the Libyan intervention is considered to have had quite the opposite effect by encouraging regime opposition in neighboring states following the successful ouster from power of Libya's ruler Muammar Qadhafi in 2011. According to China's interpretation, the UN's security management responsibilities are strictly for purposes of promoting international peace and stability and not for influencing domestic political situations. In view of the alleged domino effect from Libya on neighboring states such as Syria, China argues that it is concerned to limit peace-making activities to regional organizations whose governments have vested interests in preserving their own power. The potential threats to regime survival in neighboring states means that these will be concerned to concentrate efforts on reestablishing regional peace and stability rather than risking instigating changes of regime that could backfire.

China takes the view that the Arab League should work for the implementation of its peace plan at the regional level without the involvement of the UNSC. Although the resolution was approved by a majority, China voted against a non-binding UN General Assembly Resolution condemning human rights violations in Syria in February 2012. Following the vote, Chinese Vice Foreign Minister Zhai Jun stated that China supports the mediation efforts of the Arab League to find a political solution to the Syrian crisis. These efforts involve the initiation of an inclusive Syrian-led political process in an environment free from violence. China

---

[2] UNSC Meeting 6491, SC/10187/Rev.1.

[3] UNSC Meeting 6498.

calls upon the relevant parties to increase communication and negotiations to find a peaceful and appropriate solution to the Syrian crisis within the framework of the Arab League and on the basis of the Arab League's relevant proposals for a political solution.[4] Similarly, together with Russia in February 2012 China vetoed a UNSC draft resolution on Syria supporting the Arab League's proposed peace plan. Thirteen other member states, Morocco, France, Germany, the U.S., Portugal, the UK, Columbia, Guatemala, India, Pakistan, South Africa, Azerbaijan and Togo, voted for the draft resolution. On this occasion, China supported Russian efforts to conduct further negotiations with the Syrian government and argued that the Arab League's "good office" efforts to restore stability in Syria should be constructively assisted with respect for Syria's sovereignty, independence and territorial integrity.[5] However, a concern for China was a rerun of the regime change scenario implemented in Libya in view of the fact that the Arab League's peace plan would require President Bashar al-Assad to hand over power to a deputy and start negotiations within two weeks.[6] This in-built regime change provision without prior consent from the Syrian president is not in line with China's insistence that absolute sovereignty and non-intervention must be upheld and that UNSC resolutions must not set a precedent for breaching this principle by ignoring the requirement of governmental consent.[7]

Together with Russia, in July 2012 China vetoed a second draft resolution that would have extended the mandate of the United Nations Supervision Mission in Syria (UNSMIS), which had been deployed in April 2012, and that threatened to endorse Chapter VII peacemaking sanctions. Two other members, Pakistan and South Africa, abstained, while the remaining eleven members voted in favor of the draft resolution. On this occasion, China argued that regrettably the good work of UNSMIS had been coupled to the threat of Chapter VII sanctions in the draft resolution, prompting Beijing to veto the UNSC resolution. China urged support for the extension of UNSMIS, for example through a technical rollover. Pakistan, India, Russia and South Africa similarly expressed regret that the efforts of UNSMIS had been coupled to threats of Chapter VII sanctions in the draft resolution. [8]

---

[4] Chinese Vice Foreign Minister Zhai Jun is quoted in CBS News, "China supports Arab League's proposal for Syria," *CBS News*, February 18, 2012, http://www.cbsnews.com/8301-202_162-57380952/china-supports-arab-leagues-proposals-for-syria

[5] Security Council 6711th Meeting, "Security Council Fails to Adopt Draft Resolution on Syria as Russian Federation, China Veto Text Supporting Arab League's Proposed Peace Plan," SC/10536, February 4, 2012, http://www.un.org/News/Press/docs/2012/sc10536.doc.htm.

[6] Kareem Fahim, "Arab League Floats Ambitious New Peace Plan for Syria," *The New York Times*, January 22, 2012.

[7] Qu Xing, "Why Has China Vetoed the Security Council Syria Resolution," *China-US Focus*, February 29, 2012, http://www.chinausfocus.com/foreign-policy/why-has-china-vetoed-the-security-council-syria-resolution

[8] Security Council 6810th Meeting, "Security Council Fails to Adopt Draft Resolution on Syria that Would Have Threatened Sanctions, Due to Negative Votes of China, Russian Federation," SC/10714,

Subsequently, in August 2012 China together with a number of other states, including Russia, North Korea, Belarus, Zimbabwe, Iran, Myanmar and Cuba, voted against a UN General Assembly non-binding resolution that was approved, condemning the Syrian government of President Bashar al-Assad for its human rights violations against opposing rebels. In China's view, the UNSC draft resolutions on Syria proposes to set a precedent that absolute sovereignty can be compromised with reference to the domestic illegitimacy of the incumbent regime. Travelling down this route is not compatible with Chinese demands for security management.

The message sent by China is that regional organizations—rather than the UN—should play a leading role in deciding when there is a threat towards international peace and stability and in implementing conflict management. The UN may monitor and assist the region in its efforts to secure peace and stability, but it should be in a supportive rather than a leading role in relation to the regional organizations of the UN system. In this way, countries with a stake in creating a lasting settlement that is conducive to the priorities of neighboring states are invested with primary responsibility for regional security management. However, the regional organizations must work on the basis of the old UN system and its principles of absolute sovereignty and non-intervention, which in the Chinese view requires governmental consent before the political set-up of state-society relations can be questioned. The inherent requirement for regime change inherent in the proposed UNSC endorsement of the Arab League's peace plan constitutes a breach with this fundamental principle which would set a precedent that is not acceptable to China.

A fundamental problem with the Arab League as regional peacemaker is that it does not include Israel and Iran, despite the fact that both states are central to international peace and security in the Middle East. A peace plan put together by the Arab League does not hold much credibility in terms of creating regional peace and stability insofar as the long-term strategic partner of the U.S., Israel, and China's strategic partner, Iran, are not part of the equation. China is concerned with preserving a precarious balance in the Middle East that sees Iran as a strategic partner of China and an opponent of Israel, thereby consolidating the position of core supporters for China's version of world order in the Middle East. The fall of Assad's Syrian government is also likely to mean the loss of a central Iranian ally and a weakening of China's influence in the Middle East. China's unwillingness to support UNSC endorsement of the Arab League's peace plan allows China's regional strategic partners time to support the Syrian government in its efforts to preserve its hold on power.

China's UNSC policy aims at decoupling regime issues from the need to establish peace and stability, on dialogue with the incumbent with a view to

July 19, 2012, http://www.un.org/News/Press/docs/2012/sc10714.doc.htm

exercising political influence, on the non-use of force in conflict settlements, and on increasing reliance on regional organizations in the pursuit of international security management. China's policy is at odds with U.S. and European preferences for coupling regime characteristics with conflict settlement, for using UNSC endorsement of political reforms to exercise political influence, for using punitive measures against regimes that are seen to violate fundamental UN principles, and for increasing reliance on the UNSC to implement these policies.

The implications for security management in the Middle East are that China steps up strategic cooperation with those countries that are pronounced pariahs by the West. This stance is founded on the view that the common interest in peace and stability should form the basis for security management rather than alleged value-based assessments of regime characteristics. China promotes the view that moral and ethical issues are founded in parochial values that are not universal and are unlikely to be translated into universal political doctrines. This point of view is founded in the interest-driven Chinese definition of coexistence as a concept defining China's external relations. This interest-driven focus stems from a tradition of inward-looking policies since the People's Republic of China emerged in 1949 as a power that sought to carve out an independent alliance-free existence at a time when most of the world belonged to the U.S. liberal partial world order or the Soviet communist partial world order. In this environment, China concentrated most of its resources on developing its own form of communist development with few attempts to merge with the ideological and political values of other states. This inward-looking tendency in terms of political and ideological values remains relevant for China at a time when it is in a transition phase, as it moves away from the state-society relations of the Cold War towards a political set-up that has yet to be thoroughly defined. China's market economic reforms have not yet been combined with political reforms that match the growing demands from the population for getting a share of the increase in China's overall wealth. China's Communist Party is in the process of defining and implementing legal and political reforms that meet popular demands without compromising the authoritarian political set-up of the Chinese state. This work centers on finding a Chinese approach to these political reforms that ensures that feedback mechanisms and accountability are constructed in a way that preserves top-down political processes and the Communist Party's control of all sectors of society. China's leaders are as yet unable to saw where this process will end, and as long as this is the case, China will continue to base its external relations on interests principally defined by economic and security needs rather than on political-ideological values.

This entails fundamentally different demands for world order compared to the U.S. and Europe and their insistence that liberal values are fundamental to the extent to which other forms of exchange and cooperation can be established. In view of China's growing role in the Middle East, this appears to give rise to a dividing line

between those states that predominantly join the Chinese interest-driven concept of international relations and those that prefer the Western value-based concept of international relations. Since there is no universal concept for world order that allows for the establishment of a permanent conflict settlement and security management mechanism, these will have to be negotiated on a case-by-case basis and on the basis of trial-and-error policy coordination. In addition, in the absence of agreement between the U.S. and China on at least a minimal order, such as that which defined right and wrong conduct during the Cold War on the basis of absolute sovereignty and a liberal and a communist sphere of interest, secondary and small powers do not have to choose sides. Instead, they will side with the U.S. on some issue areas and with China on other issue areas, maximizing their national interests by not choosing sides. This implies an unpredictable world order that requires high expenditure of resources and high levels of flexibility from states who cannot be sure of the strategic choices of their neighbors.

Speakers (in Alphabetical Order)

Dr. Fredrik Bynander, Research Director at CRISMART at the Swedish National Defence College and chairman of the Center for Natural Disaster Science at Uppsala University

Dr. Wang Dong, Associate Professor and Director of the Center for Northeast Asian Strategic Studies at the School of International Studies, Peking University (China)

Senior Colonel Fan Gaoyue, Research Fellow at the World Military Studies Department, PLA AMS

Lieutenant Colonel Simon Gray, Senior Military Advisor in the Security and Justice Group of the UK's Stabilisation Unit (a joint MOD, FCO and DFID body)

Mr. Nick Haycock, Assistant Director, Office of Cyber Security and Information Assurance, Cabinet Office (UK)

Dr. Jun Kurihara, Research Director, Canon Institute for Global Studies (Japan)

Dr. Liselotte Odgaard, Associate Professor, Institute for Strategy, Royal Danish Defence College

Dr. Chang Kwoun Park, Senior Research Fellow, Center for Security and Strategy, Korea Institute for Defense Analyses (ROK)

Ambassador Tomas Rosander, Counter-terrorism Coordinator, Ministry of Foreign Affairs of Sweden

Dr. Cécile Wendling, Research Fellow, Fondation nationale des sciences politiques, Paris (France)

Colonel Wang Xiaobin, Research Fellow at the War Theory and Strategic Studies Department, PLA AMS

Prof. Akiko Yamanaka, Former Vice-Minister for Foreign Affairs of Japan

Participants

Swedish Foreign Ministry and Armed Forces

Mr. Olof Ehrenkrona, Political Adviser to the Minister of Foreign Affairs, Ministry of Foreign Affairs of Sweden

Major General Karlis Neretnieks, Swedish Armed Forces (ret.)

AMS Delegation

Major General He Lei, Chief of Scientific Research Guidance Department, PLA AMS

Senior Colonel Ma Weifang, Chief of Comprehensive Planning Department, Scientific Research Guidance Department, PLA AMS

Colonel Zhu Yuxing, Director of Foreign Affairs Office, PLA AMS Dr. Niklas Swanström, Director, ISDP

ISDP Team

Dr. Niklas Swanström, Director

Mr. David Mulrooney, Research Fellow

Mr. Magnus Hilding, Intern