COLLINS CENTER UPDATE

A Center for Strategic Leadership Newsletter

Volume 14, Issue 3 *April-June 2012*

INSIDE THIS ISSUE

This and other CSL publications can be obtained free of charge online at: http://www.csl.army.mil.

Countering Violent Extremism in East Africa

Professor Bert B. Tussing
Homeland Security and Issues Group

Before 9/11, the first awakening for many Americans surrounding the modern threat of terrorism came with a series of events in the region of East Africa. In August of 1998, al Qaeda-engineered attacks took place at United States embassies in Nairobi, Kenya and Dar es Salaam, Tanzania. Two years later, just across the Gulf of Aden, the USS Cole was attacked. Preceding both of these was our experience in Somalia in the final decade of the last century, seemingly forecasting the terrorist activity that has taken hold there, and which continues to be a source of concern for the rest of the region. Indeed, a general tone of terror seems to hang over the region, from Ethiopia to Tanzania and beyond. Concerns over the violent extremism that continues to nurture this prevailing and persistent threat to the region's security has captured the attention and concern of their governments, and the militaries that serve them.

In that spirit, the United States Africa Command and the countries of East Africa have convened a series of workshops focused on countering violent extremism in their region. This year's event will be held from 5-12 September in Arusha, Tanzania. Hosted by the Tanzanian People's Defense Force, the forum will bring in representatives from 7 countries; the African Union (AU), the South Africa Development Community (SADC); and the East African Community (EAC). Participating in support of AFRICOM in this event will be the Office of the Undersecretary of Defense for Intelligence, the U.S. Army War College and the Missouri National Guard.

The focus of the symposium/workshop, beyond "countering violent extremism (CVE)," will be to define CVE beyond a simple depiction of "terrorism." Specifically, the organizers are seeking to address the nexus between transnational criminal organizations, transnational terrorist organizations, and other illicit activities beneath and between the two. In that vein, the Center for Strategic Leadership has been asked to assist with speakers to address this nexus as it is being experienced in other areas of the world, and how those regions are attempting to counter the problem.

Following 3 days of presentations and discussion, the countries and regional organizations participating in the event will conduct a table top exercise designed to examine theory and practice against the region's requirements. Among the presenters at the event will be:

- Brigadier General Russ Howard USA (Ret.), former Director of the West Point Counterterrorism Center
- Dr. Nadav Morag of Colorado Technical University and the Naval Postgraduates School's Center for Homeland Defense and Security Affairs
- Brigadier General Meir Elran, Israeli Defense Forces (Ret.), currently of the Institute of National Security Studies, Tel Aviv, Israel

- Mr. Brett Lovegrove, London Police (RET), Gold Team Commander during the response to the July 7, 2005 London Bombings
- Professor Bert Tussing, Director of Homeland Defense and Security Issues, the United States Army War College's Center for Strategic Leadership

The table-top exercise will be guided and facilitated by the Missouri National Guard, teamed through the National Guard's State Partnership Program with the country of Tanzania. Other participating nations will include Uganda, Rwanda, Burundi, Kenya, Malawi and Djibouti. Looking past the immediate conference, the USAWC will use the initiative as an opportunity to provoke greater support to AFRICOM in its role in establishing and maintaining a regional initiative, devoted to the common end of countering violent extremism.

CSL

Strategic Leader Education Outreach and Engagement: Iraq War College and USAWC partnership

LTC Vince Lindemeyer
Operations and Gaming Division

As part of the United States Army War College and the Center for Strategic Leadership's strategic outreach mission, Lieutenant Colonel Vince Lindenmeyer (OGD, CSL) departed last August 2011 to assist the Government of Iraq as the Iraqi International Academy Advisor. Serving on the staff of United States Forces-Iraq and then the Office of Security Cooperation–Iraq, LTC Lindenmeyer was able to renew efforts in Iraqi strategic leader education that spanned the Iraqi Army to the National Security Council. The effort included finishing a $15 million campus, moving the Iraq National Defense University to the campus adjacent to the International Zone in Baghdad, standing up a new center for security studies, and planning a first-ever national security seminar for the new campus. A recent video teleconference (VTC) renewed the Iraq War College and U.S. Army War College partnership for mutual exchange and dialogue.

The Iraqi International Academy $15 million construction program provided a western standard campus to enhance the prestige of strategic leader education in Iraq. The campus consisted of classroom buildings, a student center, dining facility and billeting lodge to provide the Government of Iraq a centerpiece to begin to build strategic leaders across all services and ministries. The Iraq National Defense University consisting of the Iraq War College and National Defense College moved into the campus in April 2012. The seminar in June marked a significant first event for the new campus and faculty supported by the United States Mission–Iraq, which includes the U.S. Embassy-Baghdad and the Office of Security Cooperation–Iraq.

The Iraq Regional National Security Seminar (IRNSS) occurred from June 17-19, 2012, and was hosted by Iraq's National Security Council (NSC). The inaugural event marked the ribbon-cutting of the new Al-Nahrain Center for strategic studies in Iraq International Academy campus in Baghdad. The Al-Nahrain Center was established by the NSC to serve as Iraq's first international/ regional strategic research institute, modeled after U.S. regional studies centers. The seminar focused on Iraq's emerging post-war role in the world – featured participation from senior Iraqi Officials and academics; U.S. and European academics and non-governmental officials; and members of the diplomatic community. Prime Minister Nouri al-Maliki opened the event, emphasizing that the Al-Nahrain Center will assume a central role in the country's ability to learn and adapt while developing and changing at the same time as the rest of the world.

Recently, the United States Army War College hosted a VTC with the Iraq War College faculty to begin developing a way ahead for regular

Pictured (from left to right) is BrigGen Hamame Mohammed (USAWC Class of 2010), MajGen Zeyad Shukry, Iraq War College Commandant, LTC Lindenmeyer (CSL and USAWC DDE Class 2011), LtCol Jonathan Downing and an IWC faculty member.

and continued dialogue and mutual exchange of ideas. The regular VTCs will be held quarterly and include presentations on curricula initiatives and insights on faculty development and future exchanges. LTC Lindenmeyer returned from deployment in May 2012 after hosting Lieutenant General Jasim Saleem Hussein on a U.S. visit to think tanks and academies. He is transitioning to U.S. Strategic Command at Offutt Air Force Base, Nebraska, this Summer. The lead for continued U.S. Army War College engagement with the Iraq War College will remain with the Deputy Dean, currently Colonel Rob Nye, at (717) 245-3349 or robert.k.nye.mil@mail.mil.

CSL

4th International Conference on Cyber Conflict (CyCon 2012)

Professor Jeffrey Caton
Science and Technology Division

Keeping in step with the June 2010 NATO Cyber Defence Policy tenets, the Cooperative Cyber Defence Center of Excellence (CCDCOE) sponsored the 4th International Conference on Cyber Conflict (CyCon 2012) at its home in Tallinn, Estonia from 5-8 June 2012. CyCon 2012 focused on "Military and Paramilitary Activities in Cyberspace," and it was designed to bring together over 400 security thinkers, strategists, political scientists, policy makers, lawyers, and technology experts interested in cyber defence at the international level; 39 countries had attendees there. The first day of the conference was a series of workshops on Computers and Networks; Malware Analysis; and Media. The next three days included plenary sessions as well as individual presentations given in three topic areas: Law and Policy; Technical; and Strategy.

The U.S. Army War College supported the conference by allowing Professor Jeffrey Caton to participate as an invited speaker and author. In his presentation, "Beyond Domains, Beyond Commons: Context and Theory of Conflict in Cyberspace," he argued that the view of cyberspace as a contested domain within a global commons is not sufficient to address the full range of conflict therein. He posited that deliberate examination of the ontology and evolution of cyberspace is essential to properly inform the management of resources, forces, and risk. Further, he examined potential influences of concepts such as complexity and emergence, self-organization and self-governance, human-machine integration, ethics and philosophy, and the blurring of distinction between the cognitive, content, and connectivity dimensions. His recommendations encouraged international cyberspace security planning to include a distinct effort to examine and characterize future manifestations of cyberspace.

The highlight of the conference was an address by the President of Estonia, H.E. Toomas Hendrik Ilves, who offered a very candid assessment of the global aspects of cyberspace. He felt that there is currently too much focus on technologies and not enough on the larger implications and trends. He summarized with five observations/needs for international cyberspace: (1) embrace the digital society; (2) learn from models that work; (3) embrace radical transparency; (4) develop effective international cooperation; and (5) develop a clear community ethic. Other speakers included Major General Jaap Willemse of NATO Allied Command Transformation, who provided an overview of what NATO is doing (and not doing) in cyberspace, and recommendations for the future. He reiterated the NATO policy of not pursuing offensive cyber capabilities and acknowledged that this needs to be clarified with respect to such areas as Red Teams. He also noted that NATO needs to develop a clear and full vision for cyberspace beyond 2015.

Dr. Rain Ottis (CCDCOE) invited Dr. Sam Liles (National Defense University), Felix Lindner (Recurity Labs), and Professor Caton to participate in his panel discussion on "Military Operations in Cyberspace." Collectively, they addressed many cogent questions from the audience of 75 for about 1 hour. Professor Caton focused his insights on the strategy aspects; Dr. Liles focused on the operational and tactical; and Mr. Lindner provided the free-market perspective.

Officials of CCDCOE plan to post details of the 5th International Conference on Cyber Conflict on their website in early Fall 2012.

CSL

Cyber Ricochet: Risk Management and Cyberspace Operations

Mr. Ben Leitzel
Science and Technology Division, CSL

In 2010, the Center for Strategic Leadership conducted a Cyberspace Operations Workshop to identify critical areas for inclusion in senior leader education. Group members noted that "countering cyber threats is inherently all about risk management, as a network will always have cyber vulnerabilities and will be faced with constant cyber threats." This article provides a brief overview of the essay (http://www.csl.army.mil/) and is intended to expand on the efforts of the workgroup. Cyberspace operations offer options to accomplish objectives while reducing the potential of a direct military confrontation. However, senior

leaders must weigh the risks associated with these operations.

Recent media reports of the 'Duqu', 'Flame', and 'Stuxnet' malware highlight cyberspace operations capabilities as well as emphasize the vulnerabilities of computer networks and systems. Many computer security vulnerabilities go undetected for years and once discovered vendors can take months to correct the defects. Even after vendors release 'patches' to correct the problem, most users fail to update their systems immediately and completely. The result is a cyberspace environment plagued with undefended systems where seams and gaps are exposed to even the most novice cyber threat actor. Organizations might be tempted to isolate their networks from the internet to secure them from unauthorized intrusion. However, such physical barriers do not guarantee secure networks and systems.

Senior leaders should consider the benefits of employing cyber effects producing capabilities which have the potential to achieve objectives while risking fewer lives, saving money, and maintaining anonymity. Cyberspace operations can cause an array of effects to include intelligence collection and sabotage. The media classified the 'Stuxnet' malware as a cyberspace sabotage tool that infected Iran's centrifuges. Reports concluded that the cyberspace operation was dependent upon intelligence, provided by the 'Duqu' and 'Flame' malware, to identify specific systems in the Natanz uranium enrichment facility. Since the facility networks were isolated, the operation needed to bypass physical barriers to provide the desired effects.

Cyberspace operations can exploit vulnerabilities in adversary systems and networks to produce effects that can accomplish objectives with the promise of limited risk. However, malware can 'ricochet' and spread to unintended systems or adversaries can redirect the malware back against friendly systems. In addition, vendor patches can render malware programs ineffective. Leaders must consider the possibility of a 'cyber ricochet' striking friendly networks and systems that could not only adversely affect military capabilities and operations, but also place a nation's critical infrastructure and key resources at risk. Many critical infrastructure facilities use Siemens industrial control systems similar to those sabotaged at the Natanz facility. Once the malware 'ricochets' to computers around the globe, adversaries can reengineer and direct it against other systems. The expertise to reengineer malware is not always limited to the target of the malware but can be used by hackers, terrorists, and other nation-states. Senior leaders should also consider the limits on malware reuse after vendors and computer security companies discover and create patches for the compromised vulnerabilities.

When considering cyberspace operations for intelligence collection or sabotage, leaders need detailed information of the risks and benefits to make sound decisions. Before authorizing an intrusion into an adversary's network or system, a leader can identify and assess these critical factors by insisting on answers to the following questions:

- What is the cost and how long will it take for the cyberspace operation to accomplish objectives?
- What are the diplomatic ramifications if the identity of the source of the cyberspace operation is revealed?
- Are friendly systems vulnerable to the malware used against the adversary?
- What can be done to control the unintended spread of the malware?
- Will adversaries be able to reengineer the malware and use it against friendly systems?
- What can be done to protect friendly systems against reuse?

CSL