USAF COUNTERPROLIFERATION CENTER

CPC OUTREACH JOURNAL

Maxwell AFB, Alabama

Issue No. 674, 19 December 2008

Articles & Other Documents:

Welcome to the CPC Outreach Journal. As part of USAF Counterproliferation Center's mission to counter weapons of mass destruction through education and research, we're providing our government and civilian community a source for timely counterproliferation information. This information includes articles, papers and other documents addressing issues pertinent to US military response options for dealing with nuclear, biological and chemical threats and attacks. It's our hope this information resource will help enhance your counterproliferation issue awareness.
Established in 1998, the USAF/CPC provides education and research to present and future leaders of the Air Force, as well as to members of other branches of the armed services and Department of Defense. Our purpose is to help those agencies better prepare to counter the threat from weapons of mass destruction. Please feel free to visit our web site at http://cpc.au.af.mil/ for in-depth information and specific points of contact. The following articles, papers or documents do not necessarily reflect official endorsement of the United States Air Force, Department of Defense, or other US government agencies.

Times of London
December 9, 2008

Russia and China Accused of harbouring Cybercriminals

Murad Ahmed, Technology Reporter, and Laura Dixon

Russia and China are protecting gangs of criminals engaged in cybercrimes such as internet fraud, blackmail and money laundering, a study says today.

The annual Virtual Criminology Report, which draws on interviews with senior staff at organisations such as the Serious Organised Crime Agency, the United Nations and the FBI, found that a number of countries were providing "political cover" for criminals against attempts at prosecution by other nations.

The report said: "The cyber-kingpins remain at large while minor mules are caught and brought to rights. Some governments are guilty of protecting their in-country offenders."

The study found that Russia and China were among those harbouring internet criminal networks, and that they are "especially reluctant to co-operate with foreign law enforcement bodies for reputation and intelligence reasons".

"A lot of it is corruption," said Dr Ian Brown, of the University of Oxford, one of the report's authors. "In Russia, it is in regional governments and police agencies, there are connections between the cyber-criminals in those areas."

The report also sounded a warning about the growing threat of cyberterrorism, saying internet hackers will soon become "powerful enough to launch attacks that will damage and destroy critical national infrastructure", including the National Grid, gas and water supplies, and bank payment systems.

The British Government said earlier this year that key national utilities were under attack thousands of times a day from web criminals and terrorists. Dr Brown said that without significant improvements to the security in the next five years, these attempts to shut down vital systems like the National Grid could succeed.

Security experts say that any successful attack would be likely to result from a hacker exploiting the part of a computer system that was connected to the internet - known as a port - and are concerned that British companies were not doing enough to protect their networks.

The Virtual Criminology Report, commissioned by McAfee, the computer security firm, found that the volume of internet viruses, one of the web criminal's weapons of choice, had almost tripled in the last year, the vast majority of them attributed to attempts at soliciting or stealing money from victims.

Dave De Walt, Chief Executive at McAfee, said: "We've seen a clear evolution from basement teenagers who were written about for many years to sophisticated cybercrime groups."

The report found that there was growing evidence of "cyberespionage", with states responsible for co-ordinating internet attacks on other countries. India and Belgium are the latest countries to have complained that they had come under web attacks believed to have originated in China.

Researchers said that they had uncovered evidence of Russia having carried out state-sponsored cyberwarfare against Georgia by attacking government computer networks during the recent conflict.

The study found that the current economic downturn is exacerbating the problem, pointing to an increase in the number of fake e-mails purporting be from banks, and the likelihood that more people are being tempted by "get rich quick" schemes.

"Recession is fertile ground for criminal activity as fraudsters clamour to capitalise on rising use of the internet and the climate of fear and anxiety," the report said.

Security experts said that the trade in bank information and personal identities over the web continued to thrive. Credit card numbers can currently be bought in internet forums for as little as 30p.

Matthew Bevan, a reformed hacker who now works as a computer consultant, told researchers: “The credit crunch is also hitting the cybercriminals – they’ll be working even harder to make money.”

The Chinese Embassy in London said: “These kinds of allegations are not new, China has been accused on different occasions in the past, but every time they have failed to produce the evidence. China is also a victim of these virtual attacks, and we hope to work with other countries other countries to fight against it.”

http://technology.timesonline.co.uk/tol/news/tech_and_web/article5312323.ece

(Return to Articles and Documents List)

Arkansas Democrat Gazette

U.S. Irked, Wary of Chinese Cyber-security Rules

BY JOE MCDONALD THE ASSOCIATED PRESS
Posted on Monday, December 15, 2008

BEIJING - The Chinese government is stirring trade tensions with Washington with a plan to require foreign computer security technology to be submitted for government approval, in a move that might require suppliers to disclose business secrets.

Rules due to take effect May 1 require official certification of technology widely used to keep e-mail and company data networks secure. Beijing has yet to say how many secrets companies must disclose about such sensitive matters as how dataencryption systems work. But Washington officials complain the requirement might hinder imports in a market dominated by U.S. companies, and is pressing Beijing to scrap it.

"There are still opportunities to defuse this, but it is getting down to the wire," said Duncan Clark, managing director of BDA China Ltd., a Beijing technology consulting firm. "It affects trade. It's potentially really widescale."

Beijing tried earlier to force foreign companies to reveal how encryption systems work, and has promoted its own standards for mobile phones and wireless encryption.

Those attempts and the new demand reflect Beijing's unease about letting the public keep secrets, and the government's efforts to use its regulatory system to help fledgling Chinese high-tech companies compete with global high-tech rivals. Yin Changlai, the head of a Chinese business group sanctioned by the government, has acknowledged that the rules are meant to help develop China's infant computer security industry by shielding companies from foreign rivals that he said control 70 percent of the market.

The computer security rules cover 13 types of hardware and software, including database and network security systems, secure routers, data backup and recovery systems and anti-spam and anti-hacking software. Such technology is enmeshed in products sold by Microsoft Corp., Cisco Systems Inc. and other industry giants.

Giving regulators the power to reject foreign technologies could help to promote sales of Chinese alternatives. But that might disrupt foreign manufac- turing, research or data processing in China if companies have to switch technologies or move operations to other countries to avoid the controls. Requiring disclosure of technical details also might help Beijing read encrypted e-mail or create competing products.

"I think there's both a national security goal and an industrial policy goal to this," said Scott Kennedy, an Indiana University professor who studies government-business relations in China. "I'm sure before they came out with this, there was a discussion with industry and industry probably was giving them lots of requests about what should be included."

American officials objected to the rules in August at a regular meeting of the U.S.-China Joint Commission on Commerce and Trade.

"We don't believe China imposing these regulations is consistent with its trade commitments," said a U.S. Embassy spokesman, who spoke on condition of anonymity in line with official policy. "If there is an international standard that has been agreed upon by the international community, then that's the standard."

China agreed to delay releasing detailed regulations pending negotiations, but has not postponed the May enforcement deadline. No date has been set for more talks.

"We don't really view them announcing a delay in publication as a resolution to the issue," the American official said.

The agency that will enforce the rules, the China Certification and Accreditation Administration, said in a written statement they are meant to protect national security and "advance industry development." But it did not respond to questions about what information companies must disclose and how foreign technology will be judged.

An official of one foreign business group said companies were reluctant to talk publicly for fear of angering Chinese authorities while negotiations were under way.

Microsoft, Cisco, Sun Microsystems Inc. and security-software makers McAfee Inc. and Symantec Corp. did not respond to requests for comment. A spokesman for chip maker Intel Corp. said it would obey Chinese law, but did not respond to questions about how it might be affected.

A spokesman for personal computer maker Dell Inc. said it could not comment until detailed regulations are released. A spokesman for IBM Corp. said its products are not covered by the rules.

China has one of the largest technology markets, with more than 253 million Internet users and 590 million mobile phone accounts. It has tried to sway that to promote its high-tech industries, which lag foreign competitors.

China prompted an outcry in 2006 when it tried to require computer and phone companies to use its wireless encryption standard, called WAPI, or WLAN (Wireless Local Area Network) Authentication and Privacy Infrastructure. That would have given Chinese companies that developed the standard a head start in creating products and let them collect royalties from foreign competitors. Beijing dropped its demand after Washington complained it was a trade barrier.

In 2001, Beijing tried to require computer and software suppliers to disclose how their encryption systems worked. That was scrapped after companies said the demand was too broad and trade secrets might fall into the hands of Chinese competitors.

China also developed its own standard for third-generation mobile phones to compete with two global standards. But it agreed to let Chinese carriers use all three standards after U.S. and European officials expressed concern that it might try to keep out foreign technology.

Information for this article was contributed by Bonnie Cao of The Associated Press.

http://www.nwanews.com/adg/Business/246748/

(Return to Articles and Documents List)

The Wall Street Journal

Opinion: Information Age

Internet Attacks are a Real and Growing Problem

A *new report says cyberwar isn't science fiction.*
By L. GORDON
15 December 2008

In the 1960s, the Pentagon looked for a secure way to keep its lines of communication going in the event of all-out war. The interlinked packet networks of computers became the Internet. Fast-forward to today, and that system of open protocols brings the enormous benefits of the Web to civilian life. But the Web has also become an open field for cyber warriors seeking to harm the U.S.

We're only now realizing that many of these attacks have happened, as evidence mounts that outsiders accessed sensitive government networks and other databases. A report based on closed-door information about cyber attacks reached a sobering conclusion: Foreign governments and terrorist groups are focused on cyber offensives in a "battle we are losing."

Last week's Center for Strategic and International Studies report disclosed that the departments of Defense, State, Homeland Security and Commerce all have had intrusions by unknown foreign entities. The Pentagon's computers are probed "hundreds of thousands of times each day." An official at the State Department says terabytes of its information have been compromised. The Commerce Department's Bureau of Industry and Security had to go offline for several months. NASA has stopped using email before shuttle launches. Jihadist hackers are trying to confuse military computers into mistaking the identities of friendly and unfriendly forces in Afghanistan and Iraq.

The quasigovernmental commission revealing these cyber attacks is made up of private-sector information executives, military and intelligence officials, and two members of Congress. The study found that no department knew the extent of damage done to other departments. The extent of the harm is not known.

"The organization of the federal government, which dates to the 1930s or earlier, is part of the reason we are vulnerable," says the report. "Our industrial-age organization makes a cyber-dependent government vulnerable and inefficient. A collection of hierarchical 'stovepipes' is easier to attack and harder to defend because security programs are not of equal strength (the weakest link compromises all) and stovepiped defenders cannot appreciate the scope of, and respond well to, a multiagency attack."

As the first to build out an Internet grid, the U.S. is more vulnerable than countries that have built their infrastructure later. China, for example, constructed its Internet much later, on a more secure set of protocols. "Many Americans believe that our nation still leads in cyberspace, just as many Americans in 1957 believed that the U.S. led in space until a Soviet satellite appeared over their heads," the study says.

It's telling that the U.S. doesn't have a publicly stated doctrine on cyber defense that warns enemies and commits to taking action in response. Likening today's issues to the Cold War, the report says there should be clear rules about who will be punished how for what. It's in the nature of cyber attacks that it's hard to know exactly who's responsible, but some response must be made. "These uncertainties limit the value of deterrence for cybersecurity," the report says. "The deterrent effect of an unknown doctrine is quite limited."

One problem is that Russia and China are the main suspects, but the U.S. defense establishment hesitates to say so too loudly. It's true that few cyber attackers are ever clearly identified. No one knows for sure who brought down the Internet in Estonia in 2007, when Moscow was outraged when a Soviet-era war memorial was relocated in Tallinn. Or who was behind the cyber attacks that virtually shut down government communications and financial transactions in the former Soviet republic of Georgia earlier this year. Likewise, many foreign visitors had their PCs and BlackBerrys compromised during the Olympics in Beijing, where cybersnooping equipment is widely available.

Data are lost, communications are compromised, and "denial of service" attacks bring down selected Web sites and national networks. Supposedly confidential corporate information, the report warns, is almost certainly being hacked. As more individuals and companies rely on "cloud computing" -- storing information and services such as email remotely on supposedly secure servers -- foreign intelligence agencies and commercial snoops may have access.

A former official at Darpa, the Pentagon research agency that launched the Web, testified to Congress last year that a major cyber attack on the U.S. could knock out electricity, banking and digital-based communications. Americans

would be left rooting around for food and water, trading with one another for firewood (presumably not on eBay). Even if end-of-the-world visions are overdone, it's past time to assess risks and justify countermeasures.

The report has recommendations for the Obama administration, including a new government structure for cyber protection and working more closely with the private sector on security research. The broader point is that it's about time that we knew the extent of the cyberwarring against us. The first step to fighting back is to admit that there's a fight on.

http://online.wsj.com/article/SB122930102219005425.html?mod=googlenews_wsj

(Return to Articles and Documents List)

The Heritage Foundation
December 16, 2008

Building Cyber Security Leadership for the 21st Century

by James Jay Carafano, Ph.D. and Eric Sayers
Backgrounder #2218

The issue of cyber security, cyber competitiveness, and cyberwarfare has weighed heavily on the minds of policymakers as the severity and complexity of malicious cyber attacks have intensified over the past decade. These attacks, directed against both the public and private sectors, are the product of a heterogeneous network of state and non-state actors whose actions are motivated by a host of factors. Helping to ensure that the federal government achieves a high level of competency on cyber security issues is an imperative for the next Congress.

Indicative of how important cyber security has become, Director of National Intelligence Mike McConnell raised this issue for the first time this past February as part of his testimony on the 2008 Annual Threat Assessment. When asked if he believed the United States was prepared to deal with cyber-security threats to the civilian and military infrastructure, McConnell noted that the country is "not prepared to deal with it. The military is probably the best protected, the federal government is not well protected, and the private sector is not well protected. So the question is: How do we take some of the things that we've developed for the military side, scale them across the federal government? And then the key question will be: How do we interact with the private sector?" Properly answering these questions begins with developing cyber-strategic leadership skills in the U.S. government and private sector.

Even as Washington wrestles with issues concerning organization, authorities, responsibilities, and programs to deal with cyber competition, it must place more emphasis on developing leaders who are competent to engage in these issues. This will require a professional development system that can provide a program of education, assignment, and accreditation to develop a corps of experienced, dedicated service professionals who have an expertise in the breadth of issues related to the cyber environment. This program must be backed by effective public-private partnerships that produce cutting-edge research, development, and capabilities to operate with freedom, safety, and security in the cyber world.

What's at Stake: The Heartbeat of America

Over the past quarter century, the cyberspace domain has rapidly expanded to dominate almost every aspect of

human interaction. Americans now depend on cyberspace more then ever to manage their banking transactions, investments, work and personal communication, shopping, travel, utilities, news, and even social networking. Indeed, the global online networks that carry people, goods, information, and services make the world what it is today. With this growing dependence inevitably comes an increased vulnerability. A massive interference with global trade, travel, communications, and access to databases caused by a worldwide Internet crash would create an unprecedented challenge, particularly if it occurred concurrently with any requirement to deploy U.S. forces.[1] Additionally, an attack aimed solely at the U.S., similar in scope to the cyber attacks suffered by Estonia in April and May 2007, could severely disrupt the U.S. economy and increase Americans' concerns regarding their vulnerability.

How to Think About the Problem: It's a Competition

Addressing cyber issues begins with the premise that all national security challenges are a series of actions and counteractions between competitors, and inquiring how these competitions might progress in the future. Looking for single "silver-bullet" solutions will not work. There is no technology, government policy, law, treaty, or program that can stop the acceleration of competition in the cyber universe.

Accepting this premise (that an evolving cyber competition is a permanent character of the global environment) requires responses that offer a comprehensive, multi-disciplinary approach to analysis: looking at the full range of factors that shape and alter the security environment of the future including social, political, technological, and economic trends, as well as dynamic responses that eschew one-time or simple technical fixes to security challenges.

Required--Strategies of Resiliency

Strategies must be national in character and international in scope. Nearly every domestic cyber program--from managing movement of goods, people, services, and ideas to controlling a border to investigating terrorist groups--requires international cooperation. This dimension of safeguarding the home front is nowhere more important than in addressing national infrastructure, supply-chain issues, and public-private partnerships. America is part of a global marketplace with a global industrial base. Virtually no nation is self-sufficient.[2]

Efforts to safeguard the homeland tend to focus solely on the unrealistic task of protecting infrastructure. However, the politically charged "failure is not an option" approach to classify all infrastructure as "critical" is detrimental to prioritizing national security missions.

Instead, the U.S. needs leaders who understand the need for creating and implementing strategies of resiliency, or methods for ensuring that basic structures and systems of global, national, and local economies remain strong even after a cyber attack or other malicious acts or acts of war.[3]

A strategy of resiliency does not mean abandonment of preventive measures. At its core, resiliency is far more complex--and effective--than simply protecting critical infrastructure against natural and man-made threats.

Protection alone cedes the initiative to the enemy.

Required: Cyber-Strategic Leaders

Due to the vulnerability of cyberspace, one initiative that should be prominent in constructing a resiliency strategy for the 21st century is a cyber-strategic leadership program. Cyber-strategic leadership is not a specific technical skill or person, but a set of knowledge, skills, and attributes essential to all leaders at all levels of government and in the private sector.

The recipe of education, assignment, and accreditation that worked so successfully following the Goldwater-Nichols Act of 1986 can also be used to foster critical interagency skills among national security professionals. No institutions are currently designed in Washington, academia, or elsewhere to carry out such a task. A national effort with national standards should be initiated along with a new government institution to help foster interagency learning should be built in Washington, D.C. This professional development program could integrate a shared body of common knowledge, practices, and experiences, as well as trust and confidence among practitioners. Amongst the skills and attributes this institution could provide would be an expertise in the cyber environment, risk management, best practices, effective interagency cooperation, and public-private partnerships. Just as senior leaders in government and the private sectorare expected to have an understanding of accounting and informational technology (IT), a working knowledge of cyber security must also become commonplace.

Knowledge, Skills, and Attributes for Cyber-Strategic Leaders

Understand the Cyber Environment. Beginning in 1988 with the infamous "Morris Worm" attack, cyber security has grown in importance along with the degree of reliability the United States and other nations have placed on the cyber domain.

The effectiveness of cyberwarfare stems from its dynamic characteristics. In addition to low costs to entry, making it more attractive to terrorists and other non-state actors inclined to pursue low-end asymmetric strategies, the historical boundaries of warfare do not apply to the cyber realm.

Although decentralized, cyberspace remains dependent on the physical network of computer servers, fiber-optic cables, and the immense system of cables that have been laid across the world's oceans. A familiarity with the physical aspects of cyberspace forms the foundation of a larger education on the topic.

The complexities of cyberspace begin with the distinction between its two existing theaters. First, the commercial Internet. Reserved for the day-to-day activities of the public, and traditionally the target of non-state actors, the vulnerability of this theater has been magnified in the wake of the Estonia and Georgia cyber attacks that occurred in April and May 2007 and August 2008, respectively. Second, the military network. Over the past two decades, as the military has attempted to enhance its warfighting capabilities through network-centric warfare, an increased reliability on information technology has had the cumulative effect of ensuring a growing liability should the

network fall under attack.[4]

There are various types of actors that may pose a threat to the commercial and military cyber networks. First, individuals acting on their own to exploit security gaps or commit cyber crimes, such as identify theft. These hackers are commonly referred to as "Black Hats." Second, cyber terrorists attempting to manipulate the cyber environment to advance political or social objectives.[5] Islamist hackers took their fight to the target-rich environment of the Internet years ago. Thanks to its low barriers to entry, the cyber environment has proven itself to be one of the most efficient asymmetric tools for Islamist terrorists to incite hatred, violence, and plan and carry out attacks.

Finally, nation-states are increasingly employing cyberwarfare to attack other states or entities, either solely in the cyber domain or as part of a full-spectrum military maneuver.[6] Specifically, states like China and Russia, which remain inferior to the United States militarily, have identified America's cyberspace vulnerability and worked diligently to exploit it.[7] As we have learned from Chinese military journals, the People's Liberation Army (PLA) has focused intensely on attacking the U.S. military's C4ISR network with a variety of weapons, including anti-satellite (ASAT) weapons and cyberwarfare.[8]

The predominant tool used for cyber attacks are botnets. A botnet is a network of computers that have been compromised by malicious code and may be remotely controlled by a single computer, called a "bot herder" or "bot master." When the power of thousands of computers is combined, it can be used to launch denial-of-service attacks to shut down desired Web sites. Due to the rapidly changing nature of software, including improved commercially available security programs, the dissemination of botnet code has evolved from using e-mail attachments to pop-up spam messages and even silent uploads that take advantage of vulnerabilities in Internet browsers.[9]

Cyber espionage constitutes another threat. Not only are such tactics being used to advance the interest of private corporations as they work to compete in the global market, but states have also employed this tool to both monitor the capabilities of adversaries and steal valuable, top secret, and proprietary information. Everything from the Pentagon's most sensitive plans to invaluable intellectual property is at risk. Many officials have identified China as the main culprit in this effort, citing numerous major attacks against the Department of Defense and defense contractors that originated from the Chinese mainland.[10]

Finally, international legal mechanisms that govern cyber activity remain wanting. This is due in part to the decentralized nature of cyber attacks. During the Estonia attacks, for instance, although the perpetrator was believed to be the Russian government, and many computers that assisted in the attack were located in Russia, computers all over the world were used to launch the attack. Any direct evidence linking the attacks to Russia was thus highly circumstantial. During the crisis, questions lingered regarding what magnitude of cyber attack or evidence of perpetrators was necessary to invoke an Article V response under the auspices of NATO. Additionally, questions were asked regarding what constituted an appropriate response from Estonia and other NATO members. NATO Secretary General Jaap de Hoop Scheffer largely summarized the prevailing answers to these questions when he

stated that "no member state is protected from cyber attacks."[11] Efforts to construct a framework to help guide the activities of varying actors in cyberspace remain essential.

Think Strategically. There are many "first order" questions that deserve serious thought as the nation considers the next steps in keeping the "cyber commons" open to the free flow of services and ideas while thwarting the activities of malicious actors. These include everything from defining how "deterrence" works in cyberspace to understanding the realistic application of the "rule of law" in a place that in many ways is still lawless. Strategic thinkers must understand the costs and benefits of operating in cyberspace, the nature of the actors, the character of the environment, and how traditional concepts of security and war and peace translate to the cyber world.

Understand Risk and Risk Management. Quantifying and determining optimal responses to risk is a process called risk management. Properly assessing and reducing risk is central to a resiliency strategy. There are three types of risk assessment methodologies, all consisting of similar components.[12]

Threat assessment: Examines what an adversary can accomplish and with what degree of lethality or effect.

Criticality assessment: Evaluates the effect that will be achieved if the adversary accomplishes his goals. This examines both physical consequences, social and economic disruption, and psychological effects. Not all consequences can be prevented. In order to assist in prioritization, there is a process designed to identify the criticality of various assets: What is the asset's function or mission and how significant is it?

Vulnerability assessment: Studies a country's vulnerabilities and how they can be mitigated, including weaknesses in structures (both physical and cyber) and other systems and processes that could be exploited by terrorists. It then asks what options are available to reduce the vulnerabilities identified or, if feasible, to eliminate them.

Adapt Best Practices. Best practices and lessons learned can be effective tools. Ensuring that these are updated and applied should be government's first priority. Only programs that establish clear tasks, conditions, and standards and ensure that they are rigorously applied will keep pace with determined and willful efforts to overcome security efforts. This is especially true in the cyber domain, where the center of gravity is persistently shifting as the rapid evolution of technology and skills pull it in new directions.

Understand Effective Interagency and Public-Private Cooperation. Properly understanding the performance of the interagency process requires dividing it into three components.

Policy: The highest level of the interagency process. At this level, policymakers make broad agreements about how they will support overall U.S. policy. Improvements in this area require a renewed focus on the qualities and competencies of executive leadership, and an intelligence capability and information-sharing culture that allows leaders to obtain the highest-quality information available so that they are positioned to make the best-informed decisions.

Operations: It is at this level where the record of government is mixed. While the Department of Defense's

Combatant Command structure has proven itself capable ofmanaging military operations at the regional level, there are very few other established bodies that are able to monitor and manage operations over a geographical area.

Field activities: Interagency cooperation on the ground has generally been effective. The country teams led by U.S. ambassadors around the world offer a strong example. However, when challenges grow beyond the control of the local government apparatus, robust support mechanisms are normally lacking. Attention to improved doctrine (how to best conduct joint planning and response during a cyber crisis), sufficient investment in human capital, and appropriate decision making are required in such situations. Effective interagency cooperation does not begin at the policy level, but requires a more responsive operational environment that can meet the challenges of local leadership.[13]

While it is the responsibility of government to prevent terrorist attacks, determining the criticality of assets should be a shared public-private activity. This starts by establishing a common appreciation of roles and responsibilities for the public-private partnership.

Because vulnerability should be the primary responsibility of the partner that owns, manages, and uses the infrastructure, it is largely the private sector's duty to address vulnerability by taking reasonable precautions in much the same way that society expects the private sector to take reasonable measures for safety and environmental protection.[14]

An Agenda for the New Administration

Step 1: Facilitate Cross-Talk. There is a plethora of ongoing cyber security and cyberwarfare initiatives. The tendency of any new Administration is to conduct grand reviews of existing efforts, issue sweeping strategies, centralize management, and reorganize operations and responsibilities. That is a mistake. Such moves are as likely to stunt momentum and slow innovation as they are to achieve any efficiencies of operation. Instead, the Obama Administration's first priority must be to facilitate cross-talk between the members of the national "cyber team."

Today, those responsible for "offensive" cyber-security measures (for example, identifying and countering malicious actors) have little contact, familiarity, or collaboration with those working on "defensive" measures, and vice versa. Likewise, agencies and organizations conducting "covert" activities have scant interaction with those engaged in "public" programs. This must change. To close gaps, minimize duplication and overlap, facilitate joint action, and build trust and confidence between members of the public-private team, establishing routine and consistent dialogue must be an immediate priority. This is a vital first step in building a community of professional cyber-strategic leaders.

Step 2: Research, Research, Research. Building cyber-strategic leaders will be like building castles on sand unless the knowledge and skills imparted to them is based on comprehensive, practical, and unbiased research. As a 2007 Computer Science and Telecommunications Board research report concluded, however, the national research and

development program is wholly inadequate:

[B]oth traditional and unorthodox approaches will be necessary. Traditional research is problem-specific, and there are many cybersecurity problems for which good solutions are not known.... Research is and will be needed to address these problems. But problem-by-problem solutions, or even problem-class by problem-class solutions, are highly unlikely to be sufficient to close the gap by themselves. Unorthodox, clean-slate approaches will also be needed to deal with what might be called a structural problem in cybersecurity research now, and these approaches will entail the development of new ideas and new points of view that revisit the basic foundations and implicit assumptions of security research. Addressing both of these reasons for the lack of security in cyberspace is important, but it is the second--closing the knowledge gap-- that is the primary goal of cybersecurity research..."[15]

The report goes on to lay out an appropriate research agenda including such issues as deterring would-be attackers and managing the degradation and reconstitution of systems in the face of concerted attacks.

Step 3: Get Safe. Encouraging innovation is perhaps the quickest and most effective way to promote public-private engagement and build a national ability to mitigate and respond to cyber threats. Providing liability protection is one proven means of promoting private-sector innovation.

Since 9/11, Congress has acted decisively and to good effect in one area of liability protection: The Support Anti-Terrorism by Fostering Effective Technologies (SAFETY) Act lowered the liability risks of manufacturers that provide products and services used in combating terrorism. The act, passed in 2002, protects the incentive to produce products that the Secretary of Homeland Security designates as "Qualified Anti-Terrorism Technologies." The Department of Homeland Security has made a concerted effort to implement the program, and about 200 companies have obtained SAFETY Act certification.[16] This program should be used to accelerate the fielding of commercial products and services for cyber security.

Step 4: Implement the National Security Professional Development Program. The Obama Administration should build on the National Security Professional Development, a process to educate,certify, and track national security professionals.[17] This program should be modified based on the experience of the last two years in attempting to implement the program and be used to develop leaders skilled in cyber-strategic leadership and other critical national security missions.[18]

The First Step on a Long Road

Efforts to use the cyber domain for malicious purposes have matured in scope and sophistication over the past two decades. This threat will only intensify as terrorists continue to embrace its low costs to entry and states operationalize its power as a new domain of 21st-century warfare. Meeting this challenge in both the public and private sectors will require careful planning and consideration in the coming years. Initiating a professional-development, cyber-strategic leadership program to begin training future leaders in the complexities of the cyberspace arena is imperative to the future security of America's cyber infrastructure.

James Jay Carafano, Ph.D., is Assistant Director of the Kathryn and Shelby Cullom Davis Institute for International Studies and Senior Research Fellow for National Security and Homeland Security in the Douglas and Sarah Allison Center for Foreign Policy Studies, a division of the Davis Institute, at The Heritage Foundation. Eric Sayers is a Research Assistant in the Allison Center.

---

[1]See, for example, Madeline Drexler, *Secret Agents: The Menace of Emerging Infections* (Washington, D.C.: John Henry Press, 2001), pp. 158-200.

[2]See, for example, James Jay Carafano and Richard Weitz, "Enhancing International Collaboration for Homeland Security and Counterterrorism," Heritage Foundation *Backgrounder* No. 2078, October 18, 2007, at *http://www.heritage.org/Research/HomelandDefense/bg2078.cfm*.

[3]James Jay Carafano, "Resiliency and Public-Private Partnerships to Enhance Homeland Security," Heritage Foundation *Backgrounder* No. 2150, June 24, 2008, at *http://www.heritage.org/Research/HomelandDefense/bg2150.cfm*.

[4]Rebecca Grant, "Victory in Cyberspace," The Air Force Association, October 2007, at *http://www.afa.org/media/reports/victorycyberspace.pdf* (December 2, 2008).

[5]James Jay Carafano and Richard Weitz, "Combating Enemies Online: State-Sponsored and Terrorist Use of the Internet," Heritage Foundation *Backgrounder* No. 2105, February 8, 2008, pp. 3-4, at *http://www.heritage.org/Research/nationalSecurity/bg2105.cfm*.

[6]*Ibid.*, pp. 1-3.

[7]See John J. Tkacik, Jr., "Trojan Dragons: China's International Cyber Warriors," Heritage Foundation *WebMemo* No. 1735, December 12, 2007, at *http://www.heritage.org/research/asiaandthepacific/wm1735.cfm*, and James Jay Carafano, "When Electrons Attack: Cyber-Strikes on Georgia a Wake-Up Call for Congress," Heritage Foundation *WebMemo* No. 2022, August 13, 2008, at *http://www.heritage.org/research/nationalsecurity/wm2022.cfm*.

[8]Roger Cliff, Mark Burles, Michael S. Chase, Derek Eaton, and Kevin L. Pollpeter,"Entering the Dragon's Lair: Chinese Antiaccess Strategies and Their Implications for the UnitedStates," RAND Corporation, 2007, p. 18, at *http://www.rand.org/pubs/monographs/2007/RAND_MG524.pdf*(December 2, 2008).

[9]Clay Wilson, "Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress," Congressional Research Service, January 29, 2008, at *http://www.fas.org/sgp/crs/terror/RL32114.pdf*(December 2, 2008).

[10]Josh Rogin, "Cyber Officials: Chinese Hackers Attack 'Anything and Everything,'" FCW.com, February 13,

2007, at *http://www.fcw.com/online/news/97658-1.html*(December 4, 2008).

[11]Tony Halpin, "Putin Accused of Launching Cyber War," May 18, 2007, *Times Online*, at *http://www.timesonline.co.uk /tol/news/world/europe/article1805636.ece* (December 2, 2008).

[12]James Jay Carafano, "Risk and Resiliency: Developing the Right Homeland Security Public Policies for the Post-Bush Era," testimony before the Subcommittee on Transportation Security and Infrastructure Protection, Committee on Homeland Security, United States House of Representatives, June 24, 2008, at *http://www.heritage.org/Research/HomelandSecurity/tst062408a.cfm*.

[13]James Jay Carafano, "Managing Mayhem: The Future of Interagency," March 1, 2008, at *http://www.heritage.org/press/commentary/ed030308b.cfm*.

[14]Carafano, "Resiliency and Public-Private Partnerships to Enhance Homeland Security."

[15]Computer Science and Telecommunications Board, *Toward A Safer and More Secure Cyberspace* (Washington, DC: National Academies Press, 2007), p. 61.

[16]James Jay Carafano, "Fighting Terrorism, Addressing Liability: A Global Proposal," Heritage Foundation *Backgrounder* No. 2138, May 21, 2008, at *http://www.heritage.org/Research/NationalSecurity/bg2138.cfm*.

[17]The White House, "Executive Order: National Security Professional Development," May 2007, at *http://www.whitehouse.gov/news /releases/2007/05/20070517-6.html*(December 2, 2008).

[18]James Jay Carafano, "Missing Pieces in Homeland Security: Interagency Education, Assignments, and Professional Accreditation," *Executive Memorandum* No. 1013, October 16, 2006, at *http://www.heritage.org/Research/HomelandSecurity/em1013.cfm*.

http://www.heritage.org/Research/NationalSecurity/bg2218.cfm

(Return to Articles and Documents List)

Monday, Dec 15, 2008, Page 9
Taipei Times

Modern Society Faces Growing Cyber-terror Threat

By Joseph Nye

In August, Russian troops moved into Georgia. Observers dispute who fired first, but there was a little noticed dimension of the conflict that will have major repercussions for the future.

Computer hackers attacked Georgian government Web sites in the weeks preceding the outbreak of armed conflict. The Russia-Georgia conflict represents the first significant cyber attacks accompanying armed conflict. Welcome to

the 21st century.

Cyber threats and potential cyber warfare illustrate the increased vulnerabilities and loss of control in modern societies. Governments have mainly been concerned about hacker attacks on their own bureaucracy's information technology infrastructure, but there are social vulnerabilities well beyond government computers.

In an open letter to the US president in September last year, US professionals in cyber defense warned that "the critical infrastructure of the United States, including electrical power, finance, telecommunications, health care, transportation, water, defense, and the Internet, is highly vulnerable to cyber attack. Fast and resolute mitigating action is needed to avoid national disaster."

In the murky world of the Internet, attackers are difficult to identify.

In today's interconnected world, an unidentified cyber attack on non-governmental infrastructure might be severely damaging. For example, some experts believe that a nation's electric power grid may be particularly susceptible. The control systems that electric power companies use are thought vulnerable to attack, which could shut down cities and regions for days or weeks. Cyber attacks may also interfere with financial markets and cause immense economic loss by closing down commercial Web sites.

Some scenarios, including an "electronic Pearl Harbor," sound alarmist, but they illustrate the diffusion of power from central governments to individuals. In 1941, the powerful Japanese navy used many resources to create damage thousands of miles away. Today, an individual hacker using malicious software can cause chaos in far-away places at little cost to himself.

Moreover, the information revolution enables individuals to perpetrate sabotage with unprecedented speed and scope. The so-called "love bug virus," launched in the Phillipines in 2000, is estimated to have cost billions of dollars in damage. Terrorists, too, can exploit new vulnerabilities in cyberspace to engage in asymmetrical warfare.

In 1998, when the US complained about seven Moscow Internet addresses involved in the theft of Pentagon and NASA secrets, the Russian government replied that phone numbers from which the attacks originated were inoperative. The US had no way of knowing whether the Russian government had been involved.

More recently, last year, China's government was accused of sponsoring thousands of hacking incidents against German federal government computers and defense and private-sector computer systems in the US. But it was difficult to prove the source of the attack, and the Pentagon had to shut down some of its computer systems.

When Estonia's government moved a World War II statue commemorating Soviet war dead last year, hackers retaliated with a costly denial-of-service attack that closed down Estonia's access to the Internet. There was no way to prove whether the Russian government, a spontaneous nationalist response, or both aided this transnational attack.

In January, US President George W. Bush signed two presidential directives that called for establishing a comprehensive cyber-security plan, and his budget for next year requested US$6 billion to develop a system to protect national cyber security.

President-elect Barack Obama is likely to follow suit. In his campaign, Obama called for tough new standards for cyber security and physical resilience of critical infrastructure, and promised to appoint a national cyber adviser who will report directly to him and be responsible for developing policy and coordinating federal agency efforts.

That job will not be easy, because much of the relevant infrastructure is not under direct government control. Just recently, US Deputy Director of National Intelligence Donald Kerr warned that “major losses of information and value for our government programs typically aren’t from spies ... In fact, one of the great concerns I have is that so much of the new capabilities that we’re all going to depend on aren’t any longer developed in government labs under government contract.”

Kerr described what he called “supply chain attacks” in which hackers not only steal proprietary information, but go further and insert erroneous data and programs in communications hardware and software — Trojan horses that can be used to bring down systems. All governments will find themselves exposed to a new type of threat that will be difficult to counter.

Governments can hope to deter cyber attacks just as they deter nuclear or other armed attacks. But deterrence requires a credible threat of response against an attacker. And that becomes much more difficult in a world where governments find it hard to tell where cyber attacks come from, whether from a hostile state or a group of criminals masking as a foreign government.

While an international legal code that defines cyber attacks more clearly, together with cooperation on preventive measures, can help, such arms-control solutions are not likely to be sufficient. Nor will defensive measures like constructing electronic firewalls and creating redundancies in sensitive systems.

Given the enormous uncertainties involved, the new cyber dimensions of security must be high on every government’s agenda.

Joseph Nye is a professor at Harvard University and an author.

http://www.taipeitimes.com/News/editorials/archives/2008/12/15/2003431163

(Return to Articles and Documents List)

U.S. News & World Report

When Do Online Attacks Cross the Line Into Cyberwar?

The rising number of cyberattacks prompts calls from a commission to define the threat more clearly

By Alex Kingsbury

Posted December 9, 2008

The international community urgently needs to establish legal norms when it comes to computer and online crimes to help define and deter a problem that is escalating in severity, cyber security experts say.

A bipartisan commission examining the nation's cybersecurity infrastructure concluded this week that the next president needs to clearly articulate the value of the nation's cyber domain. Of course, many groups are already looking at the issue, from NATO, which is focused on military applications, and the Department of Homeland Security to the European Union.

But the commission urged action from the White House directly. " The president should state as a fundamental principle that cyberspace is a vital asset for the nation and that the United States will protect it using all instruments of national power, in order to ensure national security, public safety, economic prosperity, and the delivery of critical services to the American public. "

Of course, just the act of codifying cyberattacks, cybercrimes, or cyberwar would do little to physically prevent them from happening, says Jonathan Zittrain, a law professor at Harvard University and author of *The Future of the Internet and How to Stop It*. But it could have a deterrent effect, establishing a legal basis for punishing states that sponsor such incidents.

Two years ago, military officials reported that China had downloaded between 10 and 20 terabytes of information from Pentagon computers — a volume of data equivalent to twice the number of printed pages in the Library of Congress. The Chinese government has routinely denied all allegations of espionage, and Pentagon officials aren't saying if they believed the Chinese government or simply hackers based in or routed through China were responsible.

In many countries, breaking into a computer network and copying files is no different from physically stealing paper documents from an office desk. But could such cyberattacks be consider ed an act of war, equivalent to attacking a pair of destroyers off the coast of Asia or striking a group of battle s hips at anchor in Hawaii?

The U.S. military , meanwhile , lacks a formal doctrine on offensive military operations in cyberspace, although the Bush administration is " racing " to finalize such a policy before it leaves office, says one person familiar with the White House ' s work on the issue.

In the past few years, there has been a flood of attacks against U.S. computer assets, including classified and unclassified military networks and business and commerce sites, not to mention personal computers. Coordinated cyberattacks against Georgia, which coincided with Russian military action, and Estonia have raised even more concerns about what role cyberattacks could play in future conflicts.

Online assaults have also been mounted against America's enemies, including al Qaeda. For days before the anniversary of the 9 / 11 attacks this year, coordinated attacks were carried out against several websites known for posting messages from al Qaeda ' s leadership. Al Qaeda's anniversary message did eventually make its way onto the N et, but only days later.

No one claimed responsibility for the al Qaeda site attacks, and they could have simply been the work of vigilante computer experts, hackers, or other players entirely.

That's another vexing aspect of cyberattacks—they are often conducted across multiple national borders, making it very difficult to affix blame. For instance, some of the computers used (unwittingly) in the cyberattacks against Georgia were based in the United States, among other places, computer security experts say.

There are three central issues with which the international legal community must grapple as the debate continues, says James Lewis, the project director of the Commission on Cybersecurity of the 44th Presidency, which issued its report this week. Each country might have different answers, but the questions will be universal.

- At what point does a cyberattack constitute an act of war or a violation severe enough to justify a response?
- How do we protect the civil liberties of the Internet-using public while improving security?
- Which legal authorities will assume responsibility for investigating a cyberattack—the intelligence community, the military, or law enforcement?

The debate over codifying cyberattacks, Lewis points out, echoes some debates over terrorism, including whether it should primarily be a law enforcement or military concern and how to respond to attacks by state-sponsored actors.

http://www.usnews.com/articles/news/world/2008/12/09/when-do-online-attacks-cross-the-line-into-cyberwar.html

(Return to Articles and Documents List)

Defense News

EU Report: Ban Nuke Materials Production

By JULIAN HALE, BRUSSELS
Published: 16 December 2008

The world's nations need an agreement to ban the production of weapons-grade uranium, according to a European Union report on the implementation of the group's five-year-old European Security Strategy.

"Negotiations should begin on a multilateral treaty banning production of fissile material for nuclear weapons," it said.

The report, adopted by EU heads of state and government at their Dec. 11-12 summit, noted that several threats have grown since the strategy was adopted in 2003, including the proliferation of weapons of mass destruction, maritime piracy, and cyber attacks.

The report said Iran and North Korea have yet to gain the trust of the international community regarding weapons of mass destruction, and so it calledfor a successful outcome to the Non-Proliferation Treaty Review Conference in 2010 and says work is needed on bio-safety, bio-security, proliferation of delivery systems, and other issues.

The report suggests EU members explore a joint approach to cyber security, raising awareness and improving international cooperation.

"Attacks against private or government IT systems in EU Member States have given this a new dimension, as a potential new economic, political and military weapon," it said.

The report took note of the EU's first maritime European Security and Defence Policy mission - to deter pirates operating off the Somali coast - and said that "piracy in the Indian Ocean and the Gulf of Aden has made this issue more pressing in recent months."

Regarding civilian missions, the report noted a need to bring together trained staff with a range of skills and expertise and to have full interoperability between national contingents. EU member states have agreed to draw up national strategies to make experts available, complemented by more deployable staff for mission support, including budgeting and procurement.

"The ways in which equipment is made available and procured should be made more effective to enable timely deployment of missions," it said.

For military missions, the report stressed "mutual collaboration and burden-sharing arrangements" and says that more needs to be done, particularly on key capabilities such as strategic airlift, helicopters, space assets and maritime surveillance.

The report can be seen online at

http://www.consilium.europa.eu/ueDocs/cms_Data/docs/pressData/en/esdp/104631.pdf

http://www.defensenews.com/story.php?i=3865586&c=HOM&s=TOP

(Return to Articles and Documents List)

Strait Times, Singapore

Russia: New Missiles by 2020

17 December 2008

MOSCOW - RUSSIA'S armed forces will be equipped with new nuclear-capable missiles by 2020 that can overcome defensive measures like the controversial US missile shield, the military said on Wednesday.

'By 2015-2020 the Russian strategic rocket forces will have new complete missile systems with improved combat characteristics,' said General Nikolai Solovtsov, the commander of Russia's missile forces.

'They will be capable of carrying out any tasks, including in conditions where an enemy uses anti-missile defence measures,' Gen Solovtsov said, quoted by Russian news agencies.

Moscow has sharply criticised Washington's plans to put an anti-missile radar facility in the Czech Republic and interceptor missiles in Poland, despite US assurances that the system is not directed against Russia.

President Dmitry Medvedev and Prime Minister Vladimir Putin have urged US president-elect Barack Obama to drop the system, which was planned by the outgoing administration of George W. Bush.

Gen Solovtsov said the Russian rocket forces are 'developing and putting new missile systems on combat duty and perfecting their capabilities in line with the threats that are currently apparent.'

Russia is working to upgrade its Soviet-era missile forces and has repeatedly tested new missiles in recent months.

The military has said Russia will from December 2009 deploy its new RS-24 intercontinental ballistic missile, designed to counter defence systems like the controversial US missile shield. -- AFP

http://www.straitstimes.com/Breaking%2BNews/World/Story/STIStory_315564.html

(Return to Articles and Documents List)

New York Times
December 18, 2008

Russia Plans to Test Obama, U.S. Diplomat Says

By REUTERS

WASHINGTON (Reuters) — Russia has become more rigid in dealing with the United States on issues like the Bush administration's plans for a missile shield in Europe, and it looks ready to test the administration of President-elect Barack Obama, a senior American diplomat said Wednesday.

The diplomat, John Rood, under secretary of state for arms control and international security, said that talks in Moscow this week had failed to narrow differences between Russia and the United States on the missile shield plan and suggested that Russia was pausing to take stock of the Obama team.

"They have paused with the election of a new administration in the United States, and they are looking carefully at the position of the new team," Mr. Rood told reporters.

"My assessment is that the Russians intend to test the mettle of the new administration and the new president," he said.

Russia's stance on the missile shield and other issues was less flexible, Mr. Rood said, than it had been in previous talks.

Russia rejects the American position that it needs to place interceptor missiles in Poland and a radar system in the Czech Republic to shield Europe and the United States from potential missile strikes from Iran.

Russia says the project is intended to undermine Russia as well, and it has threatened to place missiles in its western enclave of Kaliningrad, near Poland.

Mr. Obama, who is to be sworn in as president on Jan. 20, has said he will make sure any missile defense system has been demonstrated to work before permitting its deployment.

Russia, whose brief war with Georgia in August sent relations with the United States to the lowest level since the end of the cold war, has tried to strike a generally positive tone on Mr. Obama since his election last month.

Prime Minister Vladimir V. Putin of Russia said this month that the United States would quickly feel a change in attitude from Moscow if the new president altered American policies toward Russia.

http://www.nytimes.com/2008/12/18/world/europe/18russia.html

(Return to Articles and Documents List)

Friday, 19 Dec, 2008 | 12:28 PM PST

Russia to Abandon Missile Plans if US Drops Shield

MOSCOW: Moscow is ready to abandon plans for a wholesale renewal of its nuclear missile arsenal if Washington stops deployment of a controversial missile shield, a top Russian general said on Friday.

'If the Americans give up their plans to deploy the third position area and other elements of strategic missile defence, then undoubtedly we will respond in kind,' said Nikolai Solovtsov, commander of Russia's strategic missile forces, quoted by Interfax news agency.

'And an array of programmes, expensive programmes, will simply not be necessary for us,' he added.

The term 'third position area' refers to planned US missile defence facilities in Poland and the Czech Republic that have aroused a furious reaction from Russia.

'Today we do not have ideological reasons for confrontation. And as we realise plans for the development of the strategic missile forces, we are not planning to frighten anyone,' Solovtsov said.

'We are simply doing that which is called for by today's realities.'

On Wednesday, Solovtsov told reporters that by 2020 Russia would replace its Soviet-era nuclear missile arsenal with new systems featuring 'improved combat characteristics' and capable of overcoming defences like the US missile shield.

Russia has been working hard to upgrade its ageing missile forces and has tested new missiles in recent months.

The tests came as Moscow repeatedly lashed out at US plans — spearheaded by outgoing US President George W. Bush — to deploy an anti-missile radar facility in the Czech Republic and interceptor missiles in Poland.

Russia views the planned facilities in the two former Soviet-bloc countries as a threat to its national security.

However the United States insists that its missile shield is not directed against Russia and is instead meant to protect against 'rogue states.'

Bush's successor, US president-elect Barack Obama, has yet to give a clear signal about whether he will continue the project.

In addition to the facilities in Eastern Europe, Russia has also objected to what it views as US intentions — denied by Washington — to put elements of missile defence in space.

http://www.dawn.net/wps/wcm/connect/Dawn%20Content%20Library/dawn/news/world/russia-to-abandon-missile-plans-if-us-drops-shield--qs

(Return to Articles and Documents List)

Friday, 19 Dec, 2008 | 12:35 PM PST

Top Lashkar-i-Taiba Militant Killed in Kashmir

The senior militant, identified only as Mudassir, was killed along with two other gunmen from the Lashkar-i-Taiba rebel group fighting Indian rule in divided Kashmir, the spokesman said.

India says it has firm evidence - backed by US intelligence - that the militants who attacked Mumbai last month were trained by the Kashmir-based Lashkar outfit.

Friday’s shootout occurred in the southern Kashmiri district of Doda.

‘The security forces had cordoned off an area on a tip off. The militants were asked to surrender, but refused and a fierce gunfight erupted,’ the spokesman said.

Another alleged top Lashkar operative was killed in Doda on Thursday.

Indian-administered Kashmir is been host to a violent long-term insurgency against Indian rule.

http://www.dawn.net/wps/wcm/connect/Dawn%20Content%20Library/dawn/news/world/top-lashkar-e-taiba-militant-killed-in-kashmir-yn

(Return to Articles and Documents List)

December 09, 2008

Bush Doctrine's Defeat in Somalia

By PATRICK SEALE

The announcement from Addis Ababa that Ethiopian troops are withdrawing from Somalia by the end of this month means that the United States has suffered a defeat in the Horn of Africa - to add to the long list of U.S. foreign policy failures in the Arab and Muslim world.

With American backing, small numbers of Ethiopian troops entered Somalia in July 2006, growing into a force of some 30,000 men over the following moths. Their aim was to drive from power the Union of Islamic Courts (UIC) - a coalition of Islamist insurgents - which had taken control of the Somali capital, Mogadishu, the previous month.

The Islamists had managed to put to flight corrupt and extortionate warlords and, after years of anarchy in Somalia, had set about restoring some form of law and order.

But for U.S. President George W. Bush, Islamic rule in Somalia could not be allowed to stand. However beneficial it might be for the local population, it did not square with Bush's global war on terror, launched after the Sept. 11, 2001 terror attacks on the United States. The CIA then sought to overthrow the Islamists by means of Ethiopian forces, and of Abdullahi Yusuf's Transitional Government of Somalia (TGS), a pro-Western and pro-Ethiopian phantom administration, based in Baidao.

Fierce fighting between Ethiopian troops and the Union of Islamic Courts escalated throughout December 2006, causing some 4,000 dead and wounded. By the end of the month, Ethiopian troops, backed by U.S. airstrikes, captured Mogadishu, hours after Islamist fighters fled the city. By Jan. 1 2007, the southern port of Kismayo - the last UIC stronghold - fell to the Ethiopians, while the U.S. navy patrolled the Somali coastline to prevent Islamists escaping by sea.

The Islamists were routed, but they were not beaten. Almost at once, they started guerrilla operations against Ethiopian troops, trapping them in ambushes and inflicting casualties on them by means of improvised explosive devices, the lethal weapon which the United States had come to dread in Iraq.

As was predictable, the conflict attracted to Somalia a motley group of Islamist fighters from the Muslim world, intent on waging jihad against Ethiopia's occupying army and its American backers.

To the alarm of Ethiopia's Prime Minister Meles Zenawi, his country's intervention in Somalia also served to breathe fresh life into two insurgent groups in Ethiopia itself - namely the Oromo Liberation Front, which has been fighting for autonomy in southern Ethiopia, and the Ogaden National Liberation Front, largely made up of ethnic Somalis, which demands self-determination in eastern Ethiopia.

American help for Ethiopian forces - in the form of training, weapons supply, clandestine missions, air strikes, and the capture and interrogation of "terrorist" suspects – seems to have been of little avail. On the contrary, it has united rival Somali groups against their common enemies - Ethiopia and the United States.

After gaining ground in recent months, the Islamist insurgents now control much of the south of Somalia - including the ports of Kismayo, Merka and Brava. Casting a noose around Mogadishu itself, they are evidently preparing for a final push, once the Ethiopians go home.

As the tide of war turned against him, Zenawi clearly had enough. On Nov. 28, he sent a message to the United Nations and to the African Union to say that Ethiopian troops would leave Somalia before the end of the year.

This brings to a close a disastrous war that has ravaged the country, killed thousands, displaced over 700,000 from Mogadishu alone, and created a pitiful humanitarian crisis. It is one more nail in the coffin of the Bush Doctrine.

What next? A "moderate" Islamist leader, Sheikh Sharif Ahmed, who broke away from the UIC, has announced that he would welcome an international force to replace the Ethiopians. His appeal looks like an attempt to promote his own prospects. As he already has some support in Eritrea, Djibouti and Yemen, an international force - he no doubt believes - could put him in power.

But Ahmed faces stiff competition from another Islamist leader, Sheikh Dahir Aweys, and indeed from the Shebab, a still more militant Islamist group. The war caused splits within the Islamic movement, which seem likely to result in a new struggle for power.

Preoccupied by the rise of maritime piracy off the Somali coast, Western states are putting together a naval force to combat the pirates. But, after the Ethiopian experience, no country seems prepared to send ground troops into the Somali snake pit.

--

Patrick Seale is a leading British writer on the Middle East, and the author of "The Struggle for Syria"; also, "Asad of Syria: The Struggle for the Middle East"; and "Abu Nidal: A Gun for Hire".

http://www.metimes.com/Opinion/2008/12/09/bush_doctrines_defeat_in_somalia/3706/

(Return to Articles and Documents List)

December 16, 2008

Huge Saudi Security Operation Foils Al-Qaida Plot Against Hajj

By RICHARD SALE (Middle East Times Intelligence Correspondent)

Alerted by Saudi and other intelligence agencies that al-Qaida planned to launch a bloody assault on Muslim pilgrims taking part in the annual pilgrimage - the Hajj - the Saudi government last week launched a huge counterterrorism operation, one of the largest in recent memory, according to U.S. intelligence officials.

Over 3 million Muslims flocked to Mecca for the Hajj pilgrimage which retraces a route taken by the Prophet Mohammed 14 centuries ago. This year's event began Dec 6 under the nervous eye of Saudi security forces that included 20,000 ground forces, flights of combat helicopters and a large number of armored vehicles deployed at key locations, U.S. officials said.

In and around Mecca, one of the two most holy sites in Islam, technical and other surveillance was increased and the site was monitored by 10,000 security cameras and Saudi agents mixed in with the pilgrims. Communications between Saudi fast reaction and special security units was improved and capability augmented, U.S. sources said.

No four-wheel vehicles were allowed because of fears of car bombings, these sources said.

There was also a much more strict enforcement of permits required of pilgrims. Those who didn't have current permits were deported, U.S. officials said.

The Saudi operation began three months ago with preemptive raids by Saudi security forces on suspected al-Qaida cells, according to a former senior CIA official. Several hundred suspects were taken into custody, he said.

U.S. officials would not comment on the nature of the intelligence of a probable terrorist incident, but in November 2007, Saudi security forces arrested 208 al-Qaida suspects accused of planning an attack during the Hajj. Another 28 suspects were arrested the following month.

"The number of al-Qaida in Saudi Arabia isn't very large, but they are just as lethal as ever," said a former senior U.S. intelligence official.

Washington-based Middle East expert Tony Cordesman agreed: "It only takes one truck with a fertilizer bomb to cause a major calamity."

Several U.S. officials said that al-Qaida is withering within the kingdom thanks to repeated defeats and continual assaults by Saudi security sources. Abdel Aziz bin Saqr al-Ghamdi, president of the Gulf Center for Strategic Studies and Research told the Saudi Gazette that a recent letter distributed by the Al-Qaida Organization of the Southern Arabian Peninsula to its Saudi followers declared that the terrorist organization in planning to shift some of its operations to Yemen in order to target tourists there. He attributed the shift to the incessant pressure on the terrorists.

The Saudi government's war with al-Qaida got off to a shaky start. After the Sept. 11, 2001 attacks, the kingdom's rulers were evasive and shifty about the existence of the terrorist group and its presence in the country since 15 of the 9/11 attackers were Saudis.

Yet Riyadh's mood turned to vengeful implacability after suicide attacks occurred on May 12 and Nov. 8, 2003, killing 93 people, demonstrating that ordinary Saudis along with members of the House of Saud were the terrorists' primary targets, even more than Americans.

The government's next actions were forceful and incisive. They began arresting radical clerics, closed militant religious schools and started rounding up suspects. Later that year Saudi security forces put up wanted posters in restaurants, shop windows, and the front pages of daily newspapers of 26 top al-Qaida suspects. A bounty of $287,000 was posed for each. The reward for supplying leads on an al-Qaida cell was $1,867,000.

The countrywide crackdown had begun.

The government also closed down al-Qaida's shadowy financiers and also moved toward educational and gender reforms, U.S. officials said.

The al-Qaida attack on the kingdom was not a smart move," said Cordesman. "It backfired and mobilized the ordinary Saudi."

One example of this took place early 2004 when a resident of Riyadh phoned a Saudi anti-terrorist hotline to report that Othman al-Amiri, one of the 26 had stopped at his home while driving through the neighborhood. Othman was tracked and later killed by Saudi security forces.

U.S.-Saudi intelligence cooperation has grown by leaps and bounds from the Saudi stonewalling days of the 1996 terror attacks on Saudi Arabia's Khobar Towers, U.S. officials said. Currently teams of U.S. Treasury Dept. agents along with FBI and CIA operatives and analysts are based in Riyadh and working together.

"Coordination couldn't be better," said a former senior CIA official.

Thanks to U.S. prodding, the Saudis installed heat sensitive cameras on barbed wire fences along weapons smuggling routes into the country from Yemen, Syria and Iraq, sources said.

For the last few years, Saudi efforts to disperse and disrupt al-Qaida have known no rest. In March 2006, 40 suspects were arrested and weapons seized in several parts of the country including the cities of Mecca and Medina. In 2007, another operation captured 172 would-be terrorists in April, and another 139 suspects were arrested that year including a would-be suicide bomber. In March 2008, the leader of al-Qaida in Saudi Arabia, Fahd Feraj al-Juwair, was among five terrorists killed by eastern Riyadh security forces, and by June of 2008, the government had arrested 701 al-Qaida suspects accused of plotting attacks against the kingdom's economic and oil installations and preparing to free jailed members, in one of the largest dragnets executed by the Saudi government at that time.

According to Ghamdi, 9,000 al-Qaida suspects have been arrested and another 3,106 remain in detention.

Said Cordesman: "The fact is that al-Qaida has not enjoyed a major success [in the kingdom] since 2003," when it launched a series of suicide bombings.

Thanks to the intensity of current Saudi efforts directed against the group, "the place today is a lot more relaxed, " he said.

http://www.metimes.com/International/2008/12/16/huge_saudi_security_operation_foils_al-qaida_plot_against_hajj/6212/

(Return to Articles and Documents List)

December 18, 2008

Iraqi Officer Arrests Related to 'Terror': General

by Sammy Ketz

BAGHDAD (AFP) A top Iraqi general said on Thursday that security forces reportedly arrested in connection with an attempted coup were actually detained on suspicion of aiding "terrorism."

"The office of the commanding general of the armed forces announces the arrest of 24 officers from the ministries of interior and defence who have nothing to do with an attempted coup," said a statement from General Qasem Atta, spokesman for Iraq's military command.

Earlier an unidentified senior interior ministry official said almost 40 policemen were in custody accused of plotting a coup against the Shiite-led government and trying to bring the Baath Party of ousted dictator Saddam Hussein back to power.

Atta said the arrests were carried out "following information that certain officers have aided terrorist activity, outlaws and henchmen from the former regime."

The interior ministry official had said earlier that 37 traffic policemen "and seven police charged with security at the interior ministry have been detained for an attempted coup."

The interior ministry said in a statement that members of other security-linked ministries were among those arrested.

Earlier, a security official announced the arrest of 50 interior ministry staff including senior officials over a plot against the government headed by Shiite Prime Minister Nuri al-Maliki.

"They were linked to the Al-Awda (The Return), a clandestine group that was working to bring the Baath Party back into power," the official said.

Al-Awda first surfaced in June 2003 just three months after the launch of the US-led invasion that ousted Iraqi dictator Saddam Hussein and his feared ruling Baath Party regime.

It groups former members of the Baath party, Saddam's former elite Republican Guard and his security services, which were dismantled in the aftermath of the war.

The interior ministry's intelligence chief General Ahmad Abul Raghif accused regional countries of involvement.

"We have taken very serious measures to counter the influence of regional countries which are hostile to Iraq and seek to damage our security, especially the interior ministry," he said.

News of the arrests comes just days after a farewell visit to Iraq by US President George W. Bush, who met Maliki during his trip.

The New York Times reported on Thursday that a top interior ministry official said those linked to Al-Awda paid bribes to officers to recruit them, and that substantial amounts of money were found in raids.

Reacting to the alleged coup reports, Selim Abullah, spokesman for Sunni party the Iraqi Concord Front, said his group had not been given any "clear explanation on the arrests or on the people arrested."

Liwaa Smaissim, head of the political office of radical Shiite cleric Moqtada al-Sadr, was sceptical that a coup was being planned.

"We are under occupation and it's impossible to believe in this type of story unless the coup was supported by the occupiers who want to change the regime," he said.

But an MP with the dominant Shiite coalition, Abbas al-Bayati, said the arrests were a success for the intelligence services against continued efforts by "the enemies of Iraq to damage the democratic process."

Maliki's critics have accused the prime minister of arresting political enemies to consolidate his power ahead of provincial elections due at the end of January, the New York Times said.

Maliki himself was persecuted by Saddam's Sunni-led regime, but five years after the invasion hundreds of members of the Baath party have returned to public life.

It followed the approval in January of a controversial law to allow the return of certain former Baathists to government posts.

The initiative was seen as a way to unite Iraq's rival factions, and a means to reverse what is widely seen as one of the huge blunders committed by the US occupiers in post-Saddam Iraq.

The decision by then head of the US adminstration Paul Bremer to disband the Iraqi army and sack all Baathists from the government led to the rise of a deadly insurgency that has since claimed tens of thousands of lives.

http://www.metimes.com/Politics/2008/12/18/iraqi_officer_arrests_related_to_terror_general/afp/

(Return to Articles and Documents List)

December 18, 2008

Britain Confirms Iraq Troop Pullout, Rebuffs Afghan Link

Michael Thurston

LONDON (AFP) Britain will withdraw all but 400 of its troops from Iraq by the end of next July, Prime Minister Gordon Brown said Thursday, but rejected any link with pressure to send more forces to Afghanistan.

The British premier also rebuffed growing calls for a formal inquiry into Britain's decision to join US President George W. Bush in the controversial US-led invasion of Iraq in 2003.

Speaking in the House of Commons a day after making a surprise visit to the violence-scarred country, Brown confirmed that British forces would almost all leave just over six years after they arrived.

"The fundamental change of mission... will take place at the latest by May 31," he said, referring to a term he coined earlier this year to reflect restoring ties with Baghdad similar to its relations with any other country.

"At that point we will begin a rapid withdrawal of our troops, taking the total from just under 4,100 to under 400 by July 31. The majority of those remaining troops will be dedicated to naval training," he added.

The timetable is in line with a bill approved by the Iraqi cabinet calling for all foreign troops except for US forces to end their missions by the end of May and pull out definitively by the end of July.

The deployment of US troops is governed by a landmark security pact.

Most of Britain's remaining troops in Iraq are based near the southern Iraqi city of Basra, which Brown visited on Wednesday after an unannounced trip to Baghdad.

Brown's predecessor Tony Blair was widely criticised for his decision to join the US administration in the 2003 invasion of the country to oust Saddam Hussein.

The Labour government has long resisted calls for a formal inquiry into that decision, but Brown's confirmation of an end to Britain's military presence has fuelled renewed calls for such a probe once troops are out.

David Cameron, the leader of the main opposition Conservatives, welcomed the withdrawal announcement but questioned why Brown had not announced a "robust, independent inquiry" into the war.

But Brown insisted that the question of an inquiry would only be considered "once our troops have come home".

A total of 178 British soldiers have died in Iraq since the invasion, including 136 from hostile action.

Meanwhile the British leader is under growing pressure to send more troops to Afghanistan.

Britain has around 8,000 troops there as part of the NATO-led International Security Assistance Force (ISAF). They are largely based in Helmand, where they are battling Taliban insurgents.

On Monday Brown confirmed that Britain had sent an extra 300 troops until next August, while US president-elect Barack Obama is expected to push for more troops there after taking power in January.

On Thursday Brown made no comment on shifting forces from Iraq to Afghanistan, adding that it was wrong to compare the two missions.

"We will look at the situation in Afghanistan, as we do, on its own merits, on what needs to be done because of what is happening in Afghanistan itself and to that extent it is unrelated to any decisions that we make in Iraq," he said.

British troop numbers in the Iraq campaign peaked at 46,000 in March and April 2003 for the invasion.

After British troops leave next year, relations between London and Baghdad will in theory revert to those in any other country.

This was "in other words the realisation of the normal defence relationships, similar to that we have with our other key partners in the region, (which) was our joint objective for 2009," said Brown.

http://www.metimes.com/Politics/2008/12/18/britain_confirms_iraq_troop_pullout_rebuffs_afghan_link/afp

(Return to Articles and Documents List)

Washington Post

U.N. Authorizes Land, Air Attacks on Somali Pirates

International Effort to Secure Sea Route May Stumble Amid Political Disarray in East African Nation

By Colum Lynch
Washington Post Staff Writer

Wednesday, December 17, 2008; A14

UNITED NATIONS, Dec. 16 -- The U.N. Security Council voted unanimously Tuesday to authorize nations to conduct military raids, on land and by air, against pirates plying the waters off the Somalia coast even as two more ships were reportedly hijacked at sea.

The vote represented a major escalation by the world's big powers in the fight against the pirates, who have disrupted commerce along one of the world's most active sea routes and acquired tens of millions of dollars in ransom. It came as China -- which has had several ships commandeered in recent months -- said it is seriously considering joining U.S., European and Russian warships policing the region.

The U.S.-drafted resolution authorizes nations to "use all necessary measures that are appropriate in Somalia" in pursuit of pirates, as long as they are approved by the country's transitional federal government. The resolution also urges states to deploy naval vessels and military aircraft to carry out the operations, and it calls for the creation of a regional office to coordinate the international effort.

U.S. Secretary of State Condoleezza Rice, who personally pushed for the resolution's passage, said the vote sends "a strong signal of commitment to combat the scourge of piracy. Piracy currently pays. But worse, pirates pay few costs for their criminality; their dens in Somalia provide refuge from the naval ships in the Gulf of Aden."

Rice said the United States would help establish a contact group of governments to share intelligence and to coordinate naval and military operations in the region.

She also called on the shipping industry to strengthen the defenses of commercial vessels and urged countries victimized by piracy to detain captured pirates and prosecute them in their own courts. An unwillingness to apprehend and prosecute pirates captured on the high seas has hindered the global response to the threat, Rice said.

More than 60 ships have been seized by pirates this year, including two on Tuesday -- a Turkish cargo ship and an Indonesian tugboat under contract with the French oil firm Total.

Rice's diplomatic achievement in the council was tempered by the unraveling political and security situation in Somalia, which could jeopardize the international effort. Somalia's government has been hobbled by a power struggle between its president and prime minister.

U.N. Secretary General Ban Ki-moon warned that Somalia may descend into "chaos" by the end of the month, when an Ethiopian occupation force leaves the country. He said his efforts to muster an international force strong enough to stabilize the situation have been unsuccessful.

Ban rejected Rice's proposal for a U.N. peacekeeping mission in Somalia, suggesting that conditions there were not secure enough. Instead, he asked the Security Council to increase funding for a financially strapped African Union force that has struggled to secure strategic sea and air ports.

Rice countered that it would be better to place the Africans under a U.N. flag, which would require the world body's 192 members to fund the operation. She urged the council to authorize a peacekeeping mission by the end of the year but said the United States was not yet prepared to present such a resolution to the council. "While the conditions may not be auspicious for peacekeeping, they will be less auspicious if chaos reigns in Somalia," she said. She voiced concern that Islamist extremists could take advantage of a breakdown in security to stage a return to power for the second time in three years.

Aid groups, meanwhile, said the approval of military raids could worsen the situation on the ground. "Expanding anti-piracy operations inside Somalia risks further complicating the conflict and could exacerbate an already dire humanitarian crisis," said Nicole Widdersheim, who heads Oxfam International's New York office. She urged nations to focus on reducing violence within the country, rather than "the threat to commercial interests from piracy off the Somali coast."

The commander of the U.S. Navy's 5th Fleet warned last week that ground attacks on suspected Somali pirates would put the lives of innocent civilians at risk. Rice told reporters Tuesday, "What we do or do not do in cases of hot pursuit we'll have to see, and you'll have to take it case by case."

The Security Council meeting, which was attended by Russian Foreign Minister Sergei Lavrov and British Foreign Secretary David Miliband, marked the end of a two-day effort by Rice to showcase progress on a series of international crises, including the Middle East conflict and Iran's nuclear ambitions. Early Tuesday, the council adopted a rare Middle East security resolution, which highlighted international efforts to end the conflict.

http://www.washingtonpost.com/wp-dyn/content/article/2008/12/16/AR2008121602848.html?hpid=sec-world

(Return to Articles and Documents List)

International Herald Tribune

China Confirms its Navy will Fight Somali Pirates

By Mark McDonald
Thursday, December 18, 2008

HONG KONG: The Chinese government confirmed Thursday that it would send naval ships to the Gulf of Aden to help in the fight against piracy there. The mission, which is expected to begin in about two weeks, would be first modern deployment of Chinese warships outside the Pacific.

The announcement came as the captain of a Chinese cargo ship that was attacked Wednesday in the gulf said his crew had used beer bottles, fire hoses and homemade incendiary bombs to battle a gang of pirates that had boarded his vessel.

A Chinese Foreign Ministry spokesman, Liu Jianchao, said Thursday that 1,265 Chinese merchant ships had passed through the gulf this year. Seven have been attacked.

"Piracy has become a serious threat to shipping, trade and safety on the seas," Liu said at a news briefing in Beijing. "That's why we decided to send naval ships to crack down on piracy."

He gave no details about the size of the naval mission, but a Beijing newspaper, The Global Times, reported that the navy was likely to deploy two destroyers and a supply ship.

"We absolutely welcome all nations, because as we've said all along, piracy is an international problem that requires an international solution," Lieutenant Nathan Christensen, a spokesman for the U.S. Fifth Fleet, said Thursday from Bahrain.

Cyrus Mody, a spokesman for the International Maritime Bureau in London, a clearinghouse for piracy information and maritime-safety issues, also welcomed the news of the Chinese mission when told about it.

"It's definitely a positive development, and it will be welcomed," he said. "The sea area being threatened there is vast, and the number of assets from the international navies is not sufficient."

The maritime bureau said 109 ships had been attacked in the gulf this year and 42 had been hijacked. Fourteen ships are currently being held for ransom, including the Sirius Star, a Saudi supertanker, and the Faina, a Ukrainian cargo ship carrying 32 armored tanks and other heavy weapons.

Mody said Thursday that negotiations with the hijackers were continuing for the release of the ships. "But the owners don't like to talk about that, for the safety of the crew members," he said.

The Chinese Navy, officially known as the People's Liberation Army Navy, has long concentrated on coastal defense and regional maneuvers. But in recent years it has embarked on an ambitious modernization plan.

The principal mission for Chinese naval vessels in the Gulf of Aden would presumably be the escorting of Chinese cargo ships and oil tankers from the Middle East bound for Chinese ports. Policing patrols, some maritime experts suggested, would be secondary.

But Mody said Thursday it would be important for the Chinese effort to be melded "on an operational level" with other navies already patrolling in the gulf. The European Union recently began an anti-piracy operation in the gulf, and several other nations have a naval presence there, including India, the United States and Russia. "We would like to see cooperation so everyone is in the loop," Mody said. When a hijacking attempt occurs, "whoever's closest can respond as fast as possible."

Peng Weiyuan, the captain of the Chinese cargo ship that was attacked Wednesday in the gulf, gave a harrowing account of his crew's battle on deck with the Somali pirates. His remarks came in an interview with China Central Television.

After seven pirates managed to board his vessel, the Zhenhua 4, Peng said his crew fought the gang to a standstill using whatever was at hand until the pirates "gestured to us for a cease-fire." The crew then retreated to a locked area on the boat and sent a distress signal.

According to a duty officer at the Piracy Reporting Center in Kuala Lumpur, Malaysia, a nearby Malaysian warship was alerted and sent a helicopter to the scene. When the helicopter fired around the Chinese boat, the pirates panicked and fled in a speedboat.

The Malaysian warship did not apprehend the pirates, Mody said, because international rules are still unclear about where the pirates could be detained and how they could be tried.

Mody said the Zhenhua 4 operates under the flag of St. Vincent and the Grenadines. At 26,000 tons, it is an average-size cargo vessel that might have been carrying machinery.

http://www.iht.com/articles/2008/12/18/africa/pirates.php

(Return to Articles and Documents List)

Washington Post

China to Aid in Fighting Somali Pirates

By Maureen Fan
Washington Post Foreign Service
Thursday, December 18, 2008; A20

BEIJING, Dec. 18 -- As international forces rescued a hijacked Chinese ship from Somali pirates Wednesday, state news media reports said China planned to send a naval fleet to fight pirates in the Gulf of Aden and Somali waters.

An unnamed military source told the state-run English-language China Daily that the operation would be "a significant peacekeeping mission," but a National Defense University professor of military strategy told The Washington Post it would be the first time China has taken part in a "battle task."

"It is also a very good opportunity to rehearse sea rescue tasks and telecommunication with other military forces," said the professor, who is also a senior figure in the navy and asked to be identified only by his surname, Zhang. "Although we've attended U.N. peacekeeping tasks before, we were not involved in military actions. This is the first time China is taking part in a battle task."

Piracy off Somalia has increased shipping insurance costs, forced ships onto roundabout routes and sparked international alarm. Nearly 400 people and 19 ships are being held for ransom along the Somali coast, according to the Kenya-based East African Seafarers Assistance Program, prompting international anti-piracy operations and a U.N. Security Council resolution authorizing states to "undertake all necessary measures" to stop the pirates.

On Tuesday, Chinese Vice Foreign Minister He Yafei said China was "seriously considering" sending naval ships to the Gulf of Aden, which is a link between the Mediterranean Sea and the Indian Ocean.

The next day, the Chinese cargo ship Zhenhua 4 was seized by pirates. The 30 Chinese sailors on board managed to lock themselves in their cabins and radio for help. A multilateral force with helicopters hovered over the ship, firing at the pirates, and succeeded in rescuing the ship several hours later, state news media said.

Six Chinese ships have been attacked by pirates, prompting China to step in and defend its interests, Zhang said, adding that two destroyers would be sent.

A Chinese journalist told the state-run Global Times newspaper Tuesday that the operation is expected to last three months. The two destroyers and a depot ship will leave Sanya port after Christmas, the Global Times reported Thursday. The first phase of the operation is expected to last three months.

"Our future military cooperation with other countries will still be limited to attacking pirates and terrorists or non-battle tasks such as medical service and rescue work," Zhang said. "Before, China didn't have an externally oriented economy, so the Chinese navy just needed to stay in Chinese waters. Now, the externally oriented economy has developed so well, the sea interests of China have expanded to other places, so the power of the Chinese navy should reach those places, too."

Researcher Zhang Jie contributed to this report.

http://www.washingtonpost.com/wp-dyn/content/article/2008/12/17/AR2008121703345.html

(Return to Articles and Documents List)

December 18, 2008

Address Piracy's Root Causes, U.N. is Told

CAIRO, Dec. 18 (UPI) -- Egypt's ambassador to the United Nations called on the international community to address the root causes of the piracy threat in Somalia's coastal waters.

Maged Abdel Fattah, Egypt's permanent representative to the United Nations, said in a recent speech in front of the U.N. Security Council in New York that in order to effectively combat the growing threat of piracy in the Gulf of Aden, more needs to be done to address the root causes of widespread problems in the Horn of Africa region, the Egyptian government reported.

Somalia has been without a functioning national government since 1991, and ongoing violence in the country has displaced hundreds of thousands of civilians. Fattah called on the international community to deal with the overall situation in Somalia in order to better address the reason people are increasingly resorting to organized crime and piracy in the Horn of Africa.

Fattah said there needs to be "coordinated efforts of these countries (in the Horn of Africa) in order to secure the international navigation and prevent acts of piracy," the release said.

http://www.metimes.com/Security/2008/12/18/address_piracys_root_causes_un_is_told/7cc8/

(Return to Articles and Documents List)