THE CIP REPORT

CENTER FOR INFRASTRUCTURE PROTECTION VOLUME 8 NUMBER 1

JULY 2009
INTERNATIONAL CIP

Contact: CIPP02@gmu.edu
703.993.4840

This issue of *The CIP Report* highlights the diverse international facets of critical infrastructure protection. This year, we are pleased to feature the contributions of Australia, Israel, Italy, and the United Kingdom. In addition, various international issues such as piracy, military medical services, pandemics, and NATO military operations are discussed.

GEORGE MASON UNIVERSITY
School of Law
CENTER for INFRASTRUCTURE PROTECTION

Infrastructure Australia, established by the *Infrastructure Australia Act of 2008*, illustrates their development of a national approach towards providing infrastructure protection services to the government as well as providers and users of infrastructure in Australia. We provide a summary of a report published by the Homeland Security Institute which discusses the participation of the Israeli public in counterterrorism and emergency preparedness practices.

A representative from Italy discusses and promotes the necessity of developing a megacommunity approach towards infrastructure protection, particularly with cyber security and information and communication technology. The Royal United Services Institute (RUSI), which recently hosted its annual Critical National Infrastructure conference in the United Kingdom, discusses the challenges involved with protecting critical infrastructure in a changing world.

An economics professor from George Mason University, who recently authored the book, *The Invisible Hook: the Hidden Economics of Pirates*, analyzes the legal and economic issues of the current piracy threat that is plaguing international seas. The role of international military medical services in destabilized countries is explored by two military physicians who served in Afghanistan. The efforts of North Atlantic Treaty Organization (NATO) Allied Command Operations (ACO) medical authorities with regards to planning and preparing for potential cases of Pandemic Influenza A "H1N1" within NATO operational forces are also featured.

This month *Legal Insights* analyzes two cyber security bills that were recently introduced into the Senate and the implications these bills may have for the Internet Consortium for Assigned Names and Numbers (ICANN). *Cyber Conflict Perspectives* discusses the cyber security agenda of the NATO Cyber Defence Programme. Finally, this issue includes information about the 3rd National Conference on Security Analysis and Risk Management that the Center for Infrastructure Protection recently co-hosted.

We hope you enjoy this issue of *The CIP Report* as well as find it useful and informative. Thank you for your support and feedback.

Mick Kicklighter
Director, CIP
George Mason University, School of Law

Australian Infrastructure Protection

by Infrastructure Australia

Infrastructure Australia was borne out of the recognition that nation-building required a coordinated national approach, as opposed to a centralised or even decentralised model as had existed at various times in Australia's past. As an organisation, Infrastructure Australia comprises three distinct groupings: the Infrastructure Australia Council, a group of twelve experienced practitioners in infrastructure matters from the public and private sectors under the leadership of Sir Rod Eddington; the Office of Infrastructure Coordinator, which supports Infrastructure Australia's day-to-day operations, under the leadership of Infrastructure Coordinator Michael Deegan, who brings a wealth of both public and private sector experience in the infrastructure sector to the role; and the Major Cities Unit, which is co-located with Infrastructure Australia.

Infrastructure Australia's express purpose, from its inception, has been to provide advice to government, providers, and users of infrastructure as to the nature of infrastructure that Australia as a nation so desperately needs, primarily in the transport, communications, energy, and water sectors.[1] To facilitate this process, Infrastructure Australia began to take submissions from the public and private sectors, as well as the general public, in order to gauge views and gain some insight into what was considered to be most needed. This process began in June 2008 with initial submissions being received from the Federal, State and Territory Governments. The public submissions process began on 31 August 2008, and by the conclusion of that process, over 1000 projects had been received.

The first taste that the nation received of Infrastructure Australia's submissions and subsequent analysis process was the release of *A Report to the Council of Australian Governments* on 19 December 2008. The release of this report marked the completion of the preliminary analysis period which saw 94 projects short-listed by Infrastructure Australia as worthy of further consideration for receipt of Commonwealth funding from the Nation Building Funds. To coincide with the release of the 2009 Federal Budget, Infrastructure Australia released its *National Infrastructure Priorities – Infrastructure for an economically, socially, and environmentally sustainable future*. This document proposed funding for 10 projects ranging across International Gateways (Ports, Airports, Intermodal), National Freight Initiatives (Rail & Road), and Public Transport and Urban Road Initiatives (Busways, Motorways, Urban Rail and Rapid Transport).[2] In addition to receiving submissions on National Infrastructure Priorities, Infrastructure Australia has also been involved in pivotal policy and regulatory reform, an example of this being the National Public Private Partnerships Guidelines, which were adopted by the Council of Australian Governments (COAG) on 29 November 2008. Infrastructure Australia also undertakes regulatory reform alongside other statutory bodies, such as the National Transport Commission. This work is essential to ensuring the

(Continued on Page 16)

[1] See Richard Webb's *The Commonwealth Government's Role in Infrastructure Provision* Research Paper No. 8 2003-04, Department of Parliamentary Services, Canberra.

[2] The Government made a range of funding decisions, including some projects from a pipeline proposed by Infrastructure Australia.

Israel's Counterterrorism Efforts

by Alexandra Tyson, CIP Intern

To Americans, 9/11 had shock value, and it certainly left more than just structural damage in its wake. Though it has been close to 8 years since a terrorist attack on American soil, it is an unfortunate truth that substantial threats still exist. Individuals and groups have expressed their intent to attack the United States. Messages from these terrorist organizations are often broadcast on major news networks; the American public may have become disaffected by their content. Complacency has dominated, while comments addressing the ominous possibility of an attack are shot down with claims of "fear-mongering".

Although progress in deterring terrorism has been made since 9/11, as evidenced by the subsequent lack of an incident, the ultimate objective of creating an active and confident citizenry outlined by the most recent version of the National Strategy for Homeland Security has yet to be achieved. This may be attributed to a variety of reasons. Perhaps the threat of terrorism may not be as insidious as in other countries, such as Israel, which has been struggling to cope with terrorism and emergency management since its founding. Nevertheless, the United States would benefit from adopting certain counterterrorist policies and activities created by the Israeli government. While not all of Israel's policies are flawless, Israeli citizens' feedback indicates approval. However, in the United States, both private and public sector critics deem the public and governmental response inadequate. To address this issue, the Homeland Security Institute (HSI), a federally funded research and development center established under the Homeland Security Act of 2002, recently reviewed counterterrorism efforts in Israel in order to evaluate the benefits and efficiency of Israel's policy. Despite the large cultural, social, economic, legal, and governmental differences between the U.S. and Israel, HSI recommends pursuing a more systematic and comprehensive terrorism awareness program in the U.S., much like the one in Israel.

In the 146-page report, HSI primarily recounts Israel's approach to encouraging public engagement in counterterrorism efforts and points to some of the practices that Israel successfully uses to foster a resilient and qualified public that deters terrorist attacks. The report compares the U.S. and Israeli methods of dealing with terrorism across all levels of society and government. The major differences boil down to how the U.S. and the Israeli public react in conjunction with their governments in dealing with terrorism. While the Israeli people view themselves as partners in combating terrorist activity, Americans generally defer their individual responsibility of preventing terrorism to the U.S. government.

Strangely enough, despite counting on a government-citizenry partnership to secure the homeland, the federal government's funding for public education and training programs on terrorism-related issues is small. HSI calls this a sign of lax management at the national level, and it contrasts unfavorably with Israel's.

A fundamental difference between the U.S. and Israel is in their respective definitions of the word "public". According to the report, in the United States' official emergency management and security/counterterrorism programs, the term "the public" is generally understood to refer only to uniformed or official first responders. Therefore, substantial parts of the public at large are excluded from these programs. This exclusion causes public participation to plummet in counterterrorism efforts and readiness programs for catastrophic incidents — both natural and manmade — including terrorism-related emergencies. In contrast, the Israeli government's definition of "the public" includes the general populace in addition to official responders.

(Continued on Page 4)

Israel *(Cont. from 3)*

Israel's policy for public engagement is as follows:

The Israeli government appears to pursue a fourfold strategy to inspire effective public participation in counterterrorism efforts. First, a comprehensive and extensive public education and awareness program on terrorism ensures public understanding of the threat, its serious consequences, and the need for readiness and response skills. Second, the public is educated on how to handle and report suspicious activity, persons, and vehicles. Third, the public is treated as the true first responders and its ability to effectively handle emergencies is regularly tested through periodic training and drills. Fourth, the Israeli government's risk communications with the public on terrorism-related issues are balanced, precise and honest. They also reflect adequate differentiation in the messaging in accordance with the audience and intent.[1]

HSI writes that Israel's program to prevent terrorism is hardly infallible and certainly would not fit all areas of U.S. policy. HSI does not suggest a complete adoption of Israel's strategies, but suggests that adopting selected practices could be advantageous.

Although the United States' policy of preventing terrorism has managed to deter an attack since 9/11, public confidence in homeland security efforts is low. Perhaps due to the prevalence of attacks in Israel, terrorist activity is simply seen as a part of daily life. Rather than trying to deny its existence or avoid difficult discussions, both the government and populace have made the decision to provide as much information as possible on successful counterterrorism strategies. Under the direction of their government agencies, Israelis have produced pamphlets and have designated websites that discuss a wide variety of topics such as disaster recovery, how to cope with an emotional crisis in the wake of a disaster, and methods that should be used to evade injury. Due to its sustained attempt to focus public attention on these topics, the Israeli public is seemingly able to better cope with the psychological risks of terrorism.

In addition to these awareness campaigns, Israeli authorities pursue a generational approach to promoting a national culture of preparedness to keep the highest possible level of responsiveness; hence many educational programs target children and start very early. These informative programs convey that terrorism is a form of psychological warfare, and can be combated with education and preparedness. Conversely, U.S. public education programs on terrorism are typified by limited and cursory information on the issue. For example, they often exclude information on the psychological ramifications or psychological warfare aspect of terrorism. Most programs hesitate to speak openly with the public and children about terrorism.

In Israel, it has been confirmed that public awareness and vigilance have been substantial factors in preventing terrorist attacks. The public accepts that reporting suspicious activities and individuals is a part of their civic duty. To facilitate this reporting, the Israeli government has created detailed websites and pamphlets and has posted signs to help people identify a suicide-terrorist or a suspicious vehicle, to indicate what to do if you suspect something, and to indicate how to behave if you are in the proximity of a suicide bombing or shooting. When an activity is reported, all information goes to the National Police, who then report the information to the proper agencies and persons. This guidance not only provides tangible information, but makes the public feel more at ease. According to this report, unlike the Israeli government, the U.S. government has neglected to create nation-wide programs to encourage public vigilance and participation in preventing terrorism by reporting suspicious activities and objects. Likewise, the American public has neglected to perceive the urgency that its counterpart in Israel does.

HSI acknowledges that the study does not systematically and carefully consider all the differences between Israel and the United States. They account for contextual differences in culture, population, and structure, but not in as precise and detailed a manner as may be desired. Despite

(Continued on Page 21)

[1] *Public Role and Engagement in Counterterrorism Efforts: Implications of Israeli Practices for the U.S.*, Final Report (2009): http://www.hstoday.us/images/public_role_in_ct_israeli_practices_task_08-22.pdf.

Critical Information Infrastructure Protection: the Megacommunity Approach

by Andrea Rigoni, Senior Advisor
Booz & Company

New forms of cooperation between governments, private companies, and the civil sector are required to tackle new threats of the Internet and the interconnection of systems. The megacommunity for Cyber Security is the answer.

The Internet, and more generally, information and communication technology, have become a key element in modern society: almost every critical service, such as electricity, water, telecommunications, transportation, and financial services, depends on them.

We have witnessed a disturbing increase of cyber attacks. In some cases, they have been a harbinger of a cyber war, such as the attacks against Georgia in the summer of 2008 and the massive attack against Estonia and Lithuania in the spring of 2007.

Cyber Security has become a significantly serious issue and is considered a national security problem by many governments of industrialized countries.

On May 29 2009, President Barak Obama stated that, "it is now clear this cyber threat is one of the most serious economic and national security challenges we face as a nation. We are not as prepared as we should be, as a government or as a country". He has also announced the creation of a Cyber Security Office at the White House that will report to the president, to the National Security Council, and to the National Economic Council. He also underlined that economic prosperity today depends on Cyber Security. In June, the Department of Defense announced the creation of a cyber command.

In Europe, the attention on Cyber Security is also very high. Many European Union Member States have already released their Cyber Security National Strategies. Even the European Commission announced its intention to establish a policy initiative to protect the European Critical Information Infrastructures. In this communication, released on March 30 by the Information Society and Media Directorate-General, the Commission identifies public-private partnerships, international cooperation, and information sharing as key elements of the European strategy for Cyber Security.[1]

One of the difficulties we encounter in protecting the Internet and its services is its fragmentation and the fragmented control of the networks. The Internet is by definition a network of networks, owned and managed almost entirely by private companies. There is no one in a position who has a complete view and control of the Internet. This fragmentation is leveraged by criminals, terrorists, hackers, activists, and spies: attacks and intrusions are perpetrated hopping through different networks, compromising as many unprotected computers as possible to avoid being tracked.

"Bad guys" are leveraging the enormous potential of new collaboration tools, information sharing, and coordination offered by new Internet services as blogs, social networks, forums, and peer-to-peer services; furthermore, they do not have to comply with various regulations and laws that could limit the exchange of information at the international level.

For all of these reasons, it is necessary to adopt a new approach to mitigate the looming cyber threat: governments, private organizations, experts, researchers, customers, and citizens all share the same need for safer digital service and electronic communications. They need to come together in a "Megacommunity", where leaders from the governments and private and civil communities confront

(Continued on Page 17)

[1] http://ec.europa.eu/information_society/policy/nis/strategy/activities/ciip/index_en.htm.

The Paradox of UK Critical Infrastructure Protection

by Anthony McGee, Head of Resilience, RUSI, London

In April, the Royal United Services Institute (RUSI) held the latest of its annual Critical National Infrastructure conferences, CNI 2009. The theme for this year's event was 'Protecting Infrastructure in a Changing World'. The Institute was delighted to play host to a range of the world's leading CIP experts for discussion on the unprecedented rate of change the world is currently experiencing and the implications for critical infrastructure. With much of the emphasis on the UK's Critical National Infrastructure, what became clear from the cross-disciplinary discussions was that, at the heart of our efforts around critical infrastructure, there lies a worrying paradox.

Terrorism is a phenomenon with which the UK has long struggled. Prior to the modern Al Qaeda-inspired threat, the UK mainland has endured sporadic IRA campaigns over some 20 years. Both republican and jihadist terrorists have been acutely aware of the value of the UK's critical networks and systems as targets for attack and the potential for disruption and loss of life which can ensue. The result of this long experience is a regime of protective security around our critical infrastructure which is among the best in the world. After the flooding chaos and infrastructure failures which besieged parts of the UK in the summer of 2007, this regime of protection from malicious threats is slowly being extended to improve the resilience of infrastructure to natural hazards and the more frequent bouts of extreme weather for which we seem destined.

Throughout this same period, the UK has embarked on a programme of extensive privatisation of assets and delivery of essential services which mean that today up to eighty-five percent of its critical national infrastructure is in private hands. Twenty-five years ago, the sale of British Telecom by the Thatcher government marked the beginning of an exodus from the public to the private sector. Typically, these privatisations were accompanied by the creation of a regulator to act as a guardian for the interests of the public and to guard against the huge private monopolies which were being created. With acronyms such as OFCOM, OFWAT, and OFGEM, these regulators have subsequently been driven by an unerring focus on forcing down prices through the reduction of costs and achieving of efficiencies, so-called 'asset sweating'.

After two decades of this approach, the limits of such a single-minded focus on price are clear and the economies of reducing spare capacity are being exposed as short term in their nature. Capital investment throughout the period has been inadequate and, as growth drives the demand for essential services, the day when supply no longer equals demand looms. While the failure of supply is the nightmare scenario for security professionals, in fact, long before the taps run dry, high prices resulting from an inability to increase supply have a devastating impact on the economy and the most vulnerable sections of society.

The questionable priorities of our regulatory regime have been compounded by its siloed nature. Individual regulators do not, and are not expected to, view their sector in the context of the UK's CNI as a whole. They take no account of how their particular service impacts upon other critical infrastructure and do little, if any, co-ordinating work as a group of infrastructure regulators. This stove-piped approach was likely unwise two decades ago when first introduced. In the modern economy, when the interdependence of so many services and sectors is so intrinsic, it is potentially disastrous.

(Continued on Page 21)

Piracy, Economics, and the Law

by Peter T. Leeson*

Although recent news gives the opposite impression, the problem of modern piracy remains small. Last year, there were fewer than 300 attempted pirate attacks globally. While that represents an 11 percent increase over the number of attempted pirate attacks in 2007, it represents a 34 percent decrease over the number of such attacks in 2003. Viewed over the course of the last four or five years, rather than the last one or two, piracy is on the decline, not rise.

Furthermore, only about two-thirds of attempted pirate attacks in 2008 were successful. As a proportion of the number of commercial vessels traveling the world's waters globally each year, the number of such attacks is small. Even in the most pirate-infested waters in the world — those near stateless Somalia — there were a mere 44 successful pirate attacks last year. That represents less than just one tenth of one percent of the thirty-some thousand commercial ships operating in this pirate-infested part of the globe.

Yet when pirates do successfully attack, the problem is significant indeed. Last year Somali pirates took 815 sailors hostage. Pirates may hold hostages for weeks and even months. During their captivity, merchant sailors are deprived of their freedom and must endure the stress of an uncertain fate and separation from their families. Few hostages die in pirate hands or are seriously hurt. Only four of the 815 hostages seized by Somali pirates in 2008 — or about one half of one percent — died in pirate captivity, and just two others were injured. But this is little consolation for a hostage while he remains in pirate captivity.

Besides the human cost of piracy, there is also an economic cost. Hijacked commercial ships cannot resume their course until their pirate captors release them. Further, the specter of hijacking in especially pirate-prone waters has led to rising insurance costs for vessels traveling through them. For example, some London-based insurers have begun charging ships traveling through sea dog hot spots, such as those near Somalia, a "pirate surcharge" upwards of $20,000 a trip.[1]

The most significant cost borne by commercial ship owners unlucky enough to have their vessels taken by pirates, however, is the price they must pay to have their sailors, ship, and cargo released. Modern pirates raise their revenue by ransom. After capturing their prize, a pirate negotiator contacts the commercial ship owner whose insurance company (often through a negotiator of its own) negotiates the ransom price for the captured vessel and crew's release. Commercial ship owners are understandably reluctant to reveal what they have paid pirates in ransom; though we know that at least one recent payout exceeded $1 million.

Despite this, since the probability of pirate capture is extremely low, a commercial ship owner's expected cost of sending even a defenseless ship through pirate-infested waters remains small — less than it would cost most ships to hire armed guards, as some U.S. government officials have begun to encourage American-flagged vessels to do following the Maersk Alabama's capture earlier this year. For example, the Congressional Research Service estimates that hiring armed guards would cost the hiring commercial vessel between $40,000 and $60,000 per trip.[2] This dwarfs the expected cost of even a million-dollar ransom. Thus most commercial ships, rationally and predictably, choose to take their chances. It is not that they cannot muster the effort required to prevent or "defeat" pirates. Given the current scale of the problem, it simply is not worthwhile to do so.

(Continued on Page 8)

[1] David Herbert, "Who's Afraid of Somali Pirates?," *National Journal*, 5.16.2009, p. 52.
[2] Herbert, p. 52.

Piracy *(Cont. from 7)*

The smallness of the modern pirate problem is also largely responsible for why the world's governments have not taken seemingly obvious steps to further stem the Somali pirates, such as sending still more of their naval vessels to protect their merchant shipping in the area. The cost of doing so exceeds the benefit given current levels of piracy. For instance, while it is very expensive to deploy more of the United States' scarce naval resources to suppress piracy, the prospective gains of such expenditures are paltry. Only one American-flagged ship has been taken by pirates in nearly two centuries.

International naval forces currently patrolling for Somali pirates, such as NATO's, face a similar situation. A combination of large costs — for instance, the additional resources required to effectively monitor the Gulf of Aden — and small benefits — recall that only 44 ships, counting those of all nations, were seized by Somali pirates last year — make the desirability of ridding the waters of pirates questionable at best. Simple cost-benefit considerations such as these help explain what so many observers have been perplexed by, namely, why it is that naval forces many times stronger than the rag-tag Somali pirate crews they might be sent to confront do not overwhelm the watery rascals.

This cost-benefit approach to piracy is not new. It is the same approach Britain took in the early 18th century when the Caribbean pirates of contemporary pop-culture infamy plied the seas. It was not until the early 1720s that the British government, owing to the relaxation of competing demands on its naval resources on the one hand, and the growth of the pirate problem on the other, decided to "get serious" about the piracy problem and devoted the effort required to suppress sea dogs.

Crucially, however, when it did become efficacious for the British government to focus its energies on exterminating pirates in the early 18th century, the legal regime required to do so was in place. Until 1700, Britain's colonies did not, in general, have authority to try and convict pirates on location. In 1700, parliament introduced An Act for the More Effectual Suppression of Piracy, which empowered colonial governments to do this. As a result, when, in the early 1720s, the government's earnest crackdown on sea robbers entered full swing, the legal regime needed to execute this crackdown was available.[3]

Although the data suggest that we are not yet at the point at which it makes sense to "get serious" about capturing modern pirates, if this point were to come today, legally, we may not be as well prepared as Britain was to handle its pirate problem in the early 18th century. The potential legal obstacles to addressing modern piracy are primarily international in nature. Although the United Nations Convention on the Law of the Sea empowers any nation that seizes pirates to try and convict them in its domestic courts, such nations appear reluctant to exercise this authority because of perceived obstacles relating to international law. As Eugene Kontorovich points out, "Quite simply, making a criminal case against armed foreigners seized in remote parts of the world is very difficult."[4]

"In brief, pirates today are entitled to all of the protections of criminal defendants and also a portion of those afforded to enemy prisoners, but potentially without some of the disabilities of both classes."[5] For example, unlike with the pirates of old, international law prohibits modern governments and others from killing sea rovers encountered on the high seas except in self-defense. Today's pirates must be apprehended and dealt with via the criminal justice system. As Kontorovich also discusses, the Geneva Convention, designed to protect prisoners of war, may unintentionally provide protection for pirates if they can make an argument that they should be entitled to POW status.[6] Indeed,

(Continued on Page 19)

[3] For a discussion of the legal regime relating to piracy, and pirates responses to changes in this regime, in the early 18th century, see Peter T. Leeson, *The Invisible Hook: The Hidden Economics of Pirates* (Princeton University Press, 2009).

[4] Eugene Kontorovich, "A Guantanomo on the Sea: The Difficulty of Prosecuting Pirates and Terrorists," *California Law Review*, forthcoming, p. 28.

[5] Kontorovich, p. 19.

[6] For an excellent discussion of the impediments to prosecuting pirates created by international law, see Kontorovich.

Roles for International Military Medical Services in Stability Operations and Security Sector Reform

by Martin C.M. Bricknell* and Donald F. Thompson**

International military services play a key contributing role in providing stability and security in countries where functioning governments do not exist, thereby reducing the likelihood that these ungoverned territories will provide a breeding ground for terrorists. Recent military operations in Iraq and Afghanistan have broadened the formal role of military forces to include these 'stability operations'. The U.S. Department of Defense defines 'stability operations' as '*military and civilian activities conducted across the spectrum from peace to conflict to establish or maintain order in States and regions*'.[1] This operational task may include helping to develop or rebuild indigenous institutions including various types of security forces, correctional facilities, and judicial systems necessary to secure and stabilize the environment — so called 'security sector reform'. The international community provides this help through a combination of governmental or international organizations and military forces.

Furthermore, security of the population is a key counterinsurgency (COIN) principle.[2] The need to restore and develop a robust security sector to support emerging governments in a post-conflict environment is not new, and is consistent with COIN doctrine. The Organization for Economic Cooperation and Development further defines the overall objective of security system reform (SSR) as '*to create a secure environment that is conducive to development, poverty reduction and democracy*'.[3] A functional security system enables the government to execute its responsibility for the security of its people and allows the eventual withdrawal of international military forces. The United Kingdom emphasizes the need for 'joined-up' partnering between the departments of foreign affairs, interior, and defense when providing external support to SSR[4], while the United States stresses that a comprehensive approach between all departments and agencies of the United States Government, intergovernmental and non-governmental organizations (NGO), multinational partners, and private sector entities is necessary to achieve unity of effort toward the shared goal of stability operations.[5] These functions in Stability Operations are not new and formed a significant element of military plans in other COIN campaigns in places such as Malaya, Oman, and Northern Ireland. The contemporary SSR model is based on 'embedded training teams' (ETTs) from international military forces who provide training and mentoring to local security forces. This is complemented by the attachment of mentors and liaison officers to support the chain of command in the local security forces and by the provision of training support in central military and police training centers. Finally the international community may offer out-of-country training to individuals or groups from the supported country.

International Military Medical Tasks in Security Sector Reform

Governance

International military medical services play a vital role in contributing to stability by facilitating the development of combat casualty care and rehabilitation capacity in host

(Continued on Page 10)

[1] Department of Defense Directive Number 3000.05, November 28, 2005, Military Support for Stability, Security, Transition, and Reconstruction (SSTR) Operations.

[2] United States Army Counterinsurgency Field Manual, FM 3-24, 2006.

[3] Security System Reform and Governance – ISBN 92-64-00786-5– Paris OECD 2005.

[4] Understanding and Supporting Security Sector. Department for International Development. London. 2005. www.difd.gov.uk accessed 19 Jul 2006.

[5] United States Army Stability Operations Field Manual, FM 3-07, 2009.

Military *(Cont. from 9)*

nation security forces. This is particularly important in the context of an underdeveloped civilian healthcare delivery system. Military medical leaders must carefully consider what interventions may lead to sustainable medical and public health sector capacity development in host nation security forces. While it is important for the medical services of the local security forces to meet the specific needs of each agency, it is clearly inefficient for each to establish its own healthcare infrastructure in competition with civilian public health services, as each will be competing in the same personnel pool for healthcare professionals produced by the national education system. Such an overlap exists in many international health economies, and is often sustained by the variation in investment based on substantial differences in political power between the defense and other security sector ministries compared to the ministry of health. This imbalance is perpetuated by extending access to the military healthcare system to political dignitaries and dependents of military personnel. There is international evidence to suggest that these arrangements become unsustainable when the cost of meeting the demand from the dependent population (particularly when this includes retirees and elderly relatives) starts to distort the allocation of funds for operational health services. Eventually the ministry of defense is forced to transfer the responsibility for non-uniformed beneficiaries to the civilian sector such as the ministry of public health or private providers.

The most important element of the international military medical task in supporting security sector reform is to establish good governance: the 'right' central structure and relationships within and between ministries. Investment and development needs to achieve the right balance between infrastructure, the operational health system, and individual clinical services while ensuring that medical procurement, training and education, preventive medicine (including selection and screening of recruits) and research are also enabled. Senior international and host nation military commanders involved in the transformation process must understand and support the role of health services in order to ensure that it is sufficiently resourced to provide the patient treatment, evacuation, preventive medicine, and medical logistic services required to care for security force casualties from the point of injury to definitive care.

Combat Casualty Care Capacity Development

The first, and most immediate, task for international military forces is to facilitate 'in extremis' medical support for security sector forces. It is highly unlikely that either the civilian healthcare system or the medical system for indigenous security forces will be functioning effectively in the immediate aftermath of conflict or instability and thus the international military medical system may be the only source of casualty care. The provision of visible and effective combat casualty care is as much an important moral and morale component of motivation for local security forces as it is for the international military forces. Troop contributing nations may be concerned that providing access for local security forces to international military medical facilities has the potential to conflict with the capabilities and capacity available for international forces. However, as local security forces become more involved in security operations, international military casualties should be reduced. It is vital that the clinical care provided to casualties is appropriate to the technology and clinical care available locally and is not just a replication of 'western' trauma surgery. The local civilian health system may not be able to provide the necessary clinical care, or the security situation may make these patients vulnerable to attack if treated outside the security cordon. This can be ameliorated if international military medical forces assist the security forces hospital system to initially develop capacity for nursing and rehabilitation services, with a long-term goal of developing capacity for these services across the entire host nation health sector.

Training

The development of the operational medical system should be designed around a time-phased strategy of training, equipment, and

(Continued on Page 18)

Pandemic Influenza "H1N1" and NATO Operations

by Captain Chuck Rhodes, United States Navy
Force Health Protection Officer, J-4 Medical Branch
NATO Supreme Headquarters Allied Powers Europe

Over the last few months, North Atlantic Treaty Organization (NATO) Allied Command Operations (ACO) medical authorities have been hard at work, revising existing contingency plans and producing updated guidance in order to ensure that NATO operational forces are prepared in the event that cases of Pandemic Influenza A "H1N1" begin occurring among their deployed military and civilian personnel. Due to the nature of military deployments, characterized by living in close quarters and austere working environments on military operations, deployed forces are often at greater risk of exposure to various disease threats. Indeed, throughout history, it is disease rather than battle injury that has caused the most casualties in almost all conflicts. This is true for Pandemic Influenza H1N1 as well. However, given the relatively mild nature of this disease thus far, it is the impact on the business of military operations that is more significant.

Fully recognizing the potential H1N1 threat and aware of the impact of past influenza outbreaks and pandemics on military operations and forces, NATO medical advisors and staff at all levels began numerous preventive and preparatory actions early on.

The intent was to reduce the overall "H1N1" threat to worldwide NATO operations. Included in this effort was a reassessment of the status of previously prepared Pandemic Influenza response plans. Most of those were initially developed due to previous concern over the "H5N1" Avian Influenza threat. These efforts led to identification of which plans needed to be beefed up or redrafted to better reflect the requirements that the current H1N1 Pandemic has now thrust upon us.

Simultaneously, ACO Command medical advisors and staff began briefing their respective Commanders and other senior and key staff members on the nature and risks of the H1N1 virus. They also provided advice and recommendations for enhanced protection and prevention of cases among NATO deployed forces. More recently, the NATO Supreme Headquarters Allied Powers Europe (SHAPE) /ACO Chief of Staff signed an "ACO Medical Operational Guidance Regarding Pandemic Influenza H1N1" paper at the request of the ACO Medical Advisor. This offered H1N1 related guidance to all ACO Commands and Operational Commanders, as well as recommendations to nations participating in NATO operations. Information was provided on how to prepare for and prevent occurrence of H1N1 cases among NATO personnel deployed, with particular emphasis on precautions for personnel preparing for deployment to NATO Operational Theatres such as Afghanistan. Here the role of the individual nations deploying personnel into the NATO Operational Theatres is critical. This role includes basic health screening of personnel for potential signs and symptoms of influenza and delaying deployment of any individuals with potential influenza signs and symptoms until they are healthy again and medically cleared for deployment.

To further augment these efforts, the ACO Medical Advisor, as well as the medical advisors at the NATO Joint Force Commands and the Operational Commands, are maintaining close liaison to ensure the exchange of information regarding H1N1. They are also ensuring that their respective Commanders are kept up to date with the changing situation, as well as watching for any potential

(Continued on Page 20)

Legal Insights

U.S. Senate Cybersecurity Bills Would Give the President Wide Powers to Secure Cyber Infrastructure, Restrict ICANN Agreement

Timothy P. Clancy, JD, Senior Program Manager, Cybersecurity/IT

Earlier this year two bills were introduced in the Senate by Senators Jay Rockefeller (D-WV) and Olympia Snowe (R-ME) Chairman and Ranking Member of the Senate Commerce, Science and Transportation Committees, to counter cybersecurity threats. The bills' introduction coincides with the Cyberspace Policy Review ordered by President Obama that was released at the end of May.

The first bill, S. 778, would create within the Executive Office of the President, the Office of the National Cybersecurity Advisor. According to the bill, the Advisor shall be appointed by the President subject to Senate confirmation and be designated as an Assistant to the President. The second bill, S. 773, is the Cybersecurity Act of 2009.

While these bills have broad implications for cyber security across the government and the private sector, these bills do not pertain to homeland security, law enforcement, military, intelligence, or diplomatic aspects of cybersecurity. This is primarily due to jurisdictional concerns — the Senate Commerce Committee has jurisdiction over the Department of Commerce, the National Institute of Standards and Technology (NIST), the Executive Office of the President and the National Science Foundation.

If enacted, S. 773 would have important implications internationally — specifically in regards to the Internet domain name system which is managed by the Internet Consortium for Assigned Names and Numbers (ICANN), an international non-government organization based in Geneva, Switzerland.

ICANN performs this function under a Joint Project Agreement (JPA) with the U.S. Department of Commerce, an arrangement dating back to the early days of the commercial Internet. The agreement is slated to expire this year on September 30.

S. 773 would restrict the ability of the Department of Commerce to modify the JPA without consent of Congress and other U.S. entities. In addition, the bill mandates the Department of Commerce to develop a strategy to implement a secure domain name system, known as DNSSEC, instead of ICANN.

The JPA between the U.S. government and ICANN has been criticized by other nations and international stakeholders in the domain name system. These stakeholders have advocated for the expiration of the JPA, arguing that ICANN should be independent and free from any U.S. government control or influence.

However, many in the United States Congress take the opposite view, questioning whether the agreement should be allowed to expire. Lawmakers have cited concerns over Internet security, stability, and reliability as reasons for extending U.S. involvement in the management of the domain name system through the JPA with ICANN. At a recent House subcommittee hearing on ICANN and the domain name system, several members of Congress called for the U.S. to continue its role in Internet governance and criticized ICANN for lack of transparency and accountability.

Beyond the ICANN provisions, the bill attempts to influence cybersecurity practices more broadly through a variety of carrots and sticks. The biggest stick is the delegation of authority (Sec. 18) to the President to:

> *declare a cybersecurity emergency and order the limitation or shutdown of Internet traffic to and*

(Continued on Page 13)

Legal Insights *(Cont. from 12)*

> *from any compromised Federal government or United States critical infrastructure information system or network. . . and to order the disconnection of any Federal government or United States critical infrastructure information systems or networks in the interest of national security. declare a cybersecurity emergency and order the limitation or shut down of Internet traffic to and from any compromised Federal government or United States critical infrastructure information system or network. . . and to order the disconnection of any Federal government or United States critical infrastructure information systems or networks in the interest of national security.*[1]

Section 18 represents a broad grant of authority to the President but Section 18's potential impact is unclear since its language is vague on several key points. First, the term "cybersecurity emergency" is undefined; under what specific circumstances would the President make a declaration? Further, the terms "disconnect," "limit," or "shut down" are also not defined, and it is unclear what would constitute a compromised critical infrastructure information system or network under the legislation.

This section also orders the President to designate an agency responsible for coordinating restoration for any system/network that was disconnected/limited/shut down by the President and also orders periodic mapping of "U.S. critical infrastructure information systems or networks" (public and private) and requires metrics to be developed to measure the effectiveness of the mapping process.

This is an ambitious effort, and from a legal perspective, problematic. The legislation would give the federal government sweeping authority over large portions of private industry in the United States. It is likely that the proposed authority will encounter widespread opposition from private sector infrastructure owners and operators.

Another important stick strengthens federal procurement rules related to cybersecurity threats, providing more stringent requirements for compliance with NIST computer security standards for federal information systems. Central to this approach is Section 6 of S. 773 which reads in part:

> *Within one year after the date of enactment of the legislation, NIST shall establish* ***measurable and auditable cybersecurity standards*** *[emphasis added] for all Federal Government, government contractor, or grantee critical infrastructure information systems and networks.*[2]

This section concerns implementation of auditable information cybersecurity standards for federal IT systems. These IT security standards would be similar to the Consensus Audit Guidelines proposed recently by the SANS Institute and various CIO's. If implemented, this section would mandate stricter cybersecurity management standards for federal computer systems that could be auditable, greatly strengthening federal information security management practices currently conducted under the Federal Information Security Management Act (FISMA). Implications for private-sector owners and operators are significant as such standards could become de facto cybersecurity liability standards if widely adopted beyond the federal sector or mandated to cover certain CI/KR sectors such as the Defense Industrial Base.

This standard would also be well beyond federal agencies since it would apply to private-sector and non-profit contractors and federal grantees including public and private universities.

Carrots in the bill include NIST programs to bolster U.S. cybersecurity technical standards through improved research, technical assistance, and international outreach on standards. Also, the bill boosts cybersecurity research and education at the National Science Foundation, and it creates a network of State and Regional Cybersecurity Enhancement Centers focused on cybersecurity assistance to small- and medium-sized businesses to

(Continued on Page 17)

[1] S.773, Cybersecurity Act of 2009, Section 18: http://thomas.loc.gov/cgi-bin/query/F?c111:1:./temp/~c111x7ho2z:e54375.
[2] S. 773 Cybersecurity Act of 2009 Section 6: http://thomas.loc.gov/cgi-bin/query/F?c111:1:./temp/~c111x7ho2z:e21187.

Cyber Conflict Perspectives

NATO Cyber Security Perspectives

by Eneken Tikk, M.Jur.

The North Atlantic Treaty Organisation (NATO), an alliance of 28 member states, was established in 1949 to protect international peace and security. As cyber security has expanded into national and international security domains, it has developed into a focus area for the Alliance.

The NATO cyber defence initiative, which dates back to 2002, is to an extent related to a distributed denial of service (DDoS) experience. Namely, the NATO public affairs website portraying the Alliance's perspective on the Kosovo conflict fell under DDoS attacks and became inoperable for several days.

The same year, at the Prague Summit, the formal NATO Cyber Defence Programme was introduced and resulted in establishing the NATO Computer Incident Response Capability (NCIRC), the entity that basically operates as computer emergency response team (CERT) for NATO. For several years, NATO's first attention in cyber security was directed towards protection of its internal systems and resources. This situation changed after the 2007 cyber attacks against Estonia. As Estonia requested NATO's attention towards the politically motivated government and critical information infrastructure-targeted cyber attacks, the Alliance sent an expert to a small Internet-addicted country. In less than a year after the Estonian event, NATO's view on international cyber security had expanded significantly.

Two documents adopted by early 2008 — NATO Cyber Defence Policy and NATO Cyber Defence Concept — took a more comprehensive approach to cyber security by NATO. The Policy establishes the basic principles and provides direction to NATO's civil and military bodies in order to ensure a common and coordinated approach to cyber defence and any response to cyber attacks. It also contains recommendations for individual NATO countries on the protection of their national systems. In line with this, NATO's Military Committee agreed upon a Cyber Defence Concept which adds practical action programmes to fit within the overarching policy. The Cyber Defence Management Authority (CDMA), created as part of NATO's cyber defence policy, serves as a central command for the technical, political, and information-sharing efforts of Alliance members, and is responsible for directing and managing existing NATO cyber defence entities. Upon request, the CDMA is able to coordinate or provide assistance in a concerted effort if an Ally or Allies fall victim to a cyber attack of national or Allied significance.

NATO cyber security agenda is different from many other international organisations' plans in the field. In a way, NATO's concern is the most severe domain of hostile cyber activities — the threats that are regarded as threats to national security and therefore have the potential of endangering international cyber security. This niche is unique in that there is no other international cyber security agenda with the same focus. This has resulted in new debates about the applicability of the Law of Armed Conflicts and potentially Article 5 of the North Atlantic

(Continued on Page 21)

[1] http://www.nato-otan.org/issues/cyber_defence/index.html.

[2] http://www.nato.int/cps/en/SID-D30474D0-A97D6B01/natolive/topics_49193.htm.

[3] Sverre Myrli, Draft Report "NATO and Cyber Defence", available at http://natopa.ibicenter.net/Default.asp?CAT2=1765&CAT1=16&CAT0=2&COM=1782&MOD=0&SMD=0&SSMD=0&STA=&ID=0&PAR=0&PRINT=1.

3rd National Conference on Security Analysis and Risk Management

The CIP co-hosted the Security Analysis and Risk Management Association's (SARMA) 3rd National Conference on Security Analysis and Risk Management: New Perspectives on Security Risk Management. The event was held on George Mason University's Arlington campus from June 16-19, 2009. The conference featured nine keynote and plenary session speakers, 39 technical sessions with over 40 speakers, and 7 exhibitors.

The topics of the conference presentations ranged from national policy to international standards and best practices, including recent advances in homeland security analysis and risk management techniques; physical-security risk analysis; terrorism risk analysis; common-crime risk analysis; information-security risk analysis; espionage risk analysis; and numerous other efforts to advance the professional discipline of security analysis and risk management.

The CIP was pleased to once-again co-host this valuable conference and further develop its partnership with SARMA.

For more information on the conference, please visit http://cip.gmu.edu/research3rdSARMA conference.php or http://sarma.org/events/pastevents/3rdannualconferenc/. Information on SARMA and its many initiatives can be found at http://sarma.org/.

Australia *(Cont. from 2)*

achievement of fundamental change in the manner in which infrastructure projects are undertaken in Australia.

Although not provided the same coverage as that undertaken by Infrastructure Australia, the work undertaken by the Major Cities Unit is equally as important to the nation-building task. The Major Cities Unit is presently looking at policies which aim to secure the long-term viability and environmental sustainability of Australia's major cities. Central to this is the development of a national urban policy. The fundamentals of a national urban policy are predicated on the advice provided by Infrastructure Australia to the Australian Government. Projects endorsed by Infrastructure Australia that could form the cornerstone of a National Urban policy include the Seaford Rail Extension in Adelaide, which was proposed in order to accommodate for expected population growth.

The building of critical infrastructure, primarily in the communications, energy, and water sectors, is essential in order to sustain and promote growth, not simply to accommodate it. To this end, Infrastructure Australia has indicated support for a number of essential critical infrastructure projects with a view to the nation's future requirements including the development of a national broadband network; the development of an energy strategy; the development of a water strategy to ensure water security; and a regional towns water quality review. These projects are essential in laying the foundations for Australia in the 21st Century, as they will underpin long-term economic viability and growth. Whilst taking steps to ensure the viability of our economic infrastructure, Infrastructure Australia has also studied infrastructure provision for Australia's indigenous communities. Infrastructure Australia has proposed the Infrastructure for Indigenous Communities Framework. The purpose of this framework is to enable the provision of the types of critical infrastructure to indigenous communities that many other communities have long taken for granted, as an attempt to redress social and economic inequalities.

At the heart of the Infrastructure Australia process can be found one word; rigour. This is a quality which was not only demanded of project proponents to ensure that what was put to us was the best possible project, but it was also a quality demanded of ourselves at Infrastructure Australia to ensure that we committed ourselves to achieving the goals of the nation-building exercise on which we embarked when the organisation came into existence in mid-2008. This point was underscored in a post-budget interview that our chairman, Sir Rod Eddington, gave on the *Inside Business* program, broadcast on 17 May 2009, when he stated that "the quality of the submissions varied across the piece, and we put forward the submissions we felt met all the criteria and where the work had been done with the rigour that we demanded".[3] This demonstrates Infrastructure Australia's commitment to evidence-based policy, which has existed from our very inception. In an industry address in Adelaide South Australia on 9 October 2008, Infrastructure Coordinator Michael Deegan pointed out that "[t]he linkage to goals and problems is weak. Evidence-based analysis is weak. Quantified costs and benefits is weak. There is a tendency for solutions to jump to concrete — let's just build more road or rail or something, without consideration of the regulatory, pricing, policy and governance solutions."[4] The quick-fix solution without rigorous, deep analysis is one of the many practices that Infrastructure Australia was created to put an end to. Infrastructure Australia has already gone a long way toward ensuring that there is lasting change in the way that decisions are made in infrastructure policy and regulation in Australia, however, there is always more that can be done to ensure that Australia begins to realise its potential, and the key to this is ensuring that the right foundations for critical infrastructure continue to be laid. ❖

[3] http://www.abc.net.au/insidebusiness/content/2009/s2572777.htm.
[4] http://www.abc.net.au/pm/content/2008/s2386937.htm.

Legal Insights *(Cont. from 13)*

improve cybersecurity. However, as an authorization bill, the bill only provides authority for the creation these programs — no appropriations are provided and no funding for such activities have been requested by the President.

Neither bill has been acted on by the Commerce Committee or the Senate. Also, several other committees will likely have say over any future cyber bill, so jurisdictional conflicts and potential strong opposition from the private sector could sink any attempt at comprehensive cyber security legislation. However, the two bills represent one of the first major legislative attempts by this Congress to address the threat posed by cybersecurity vulnerabilities in critical infrastructures in the U.S. Several of the bills' provisions are consistent with the new cyberspace policy review announced by President Obama, so there is a chance that a consensus cybersecurity bill could be achieved during the next year. ❖

Italy *(Cont. from 5)*

together the problems that none can solve alone. These leaders have the capability to share resources, knowledge, skills, and experiences to identify common solutions.

The megacommunity approach is described in the book *Megacommunities*.[2] A megacommunity is a public sphere in which organizations and people deliberately join together around a compelling issue of mutual importance, in this case Cyber Security. A megacommunity contains organizations that sometimes compete and sometimes collaborate, but a megacommunity is not strictly a business niche. Nor is it a public–private partnership, which is typically an alliance focused on a relatively narrow purpose. A megacommunity is a larger ongoing sphere of interest where governments, corporations, NGOs, and others intersect over time. The participants remain interdependent because their common interest compels them to work together, even though they might not see or describe their mutual problem or situation in the same way.

Cyber Security is one of the best examples where the megacommunity approach could help each participant to increase its protection. Sharing information about new vulnerabilities, threats, and incidents as sharing available resources is the best way to move from a trench to a satellite view.

For the very nature of Internet and information and communication technologies, most of the critical information infrastructures share the same technological components: servers, applications, desktops, routers, switches, etc. These infrastructures therefore constitute a "hidden interdependency". A vulnerability in one component can become the vulnerability of hundreds or thousands of organizations and companies around the world. ❖

For more information, please contact Andrea Rigoni at ANDREA.RIGONI@NE.BOOZ.COM. Mr. Rigoni also runs a blog on CIP, containing daily news and articles on CIP with a particular focus on Europe and select key topics that are discussed in the United States. The blog can be accessed at: http://thecipblog.com.

---

[2] "Megacommunities" manifesto can be found at: http://www.strategy-business.com/resiliencereport/resilience/rr00035.

Military *(Cont. from 10)*

manpower, rather than focusing on infrastructure development. A 'field medic' training program might be considered to be the 'pump-primer'. The paucity of professional medical staff means that this program is the best mechanism to provide good quality casualty care, and it allows the identification and mentoring of soldiers who display promising characteristics of becoming non-commissioned officers and future leaders. The 'field medic' can also provide limited primary care, and maintain health and hygiene standards in the field. The literacy, culture, and religious experience of young people will require the syllabus and methods of delivery for all medical subjects to be adjusted from that taught to standard 'western' military forces. A 'field medic' syllabus and teaching materials should be standardized and shared between international military medical ETTs so as to minimize the likelihood of discrepancy due to variation between national 'field medic' training. This requires synchronized pre-deployment training of international military medical forces, using the field medical equipment, supplies, and processes that will be used within the host nation.

Health System Infrastructure Development

The development of health care infrastructure for the security sector should be aligned to the development of civilian health services. While there may be very good reasons for a separation between these health sectors, if this occurs, it must be a positive choice and not the result of lack of awareness of the issues. The international community may be supporting the country for a prolonged period of time in order to establish a stable, governable society, so it must assure that it does not contribute to a disparity in medical capacity development between the security sector and the general population that leads to discontent.

Health sector infrastructure for the security forces will be based on fixed medical facilities in garrisons, at regional commands, and at the national level. The capability of these facilities should reflect the need for medical and surgical services in the country, the need to provide trauma care to injured security forces personnel, and the availability of effective civilian healthcare facilities. It is likely that the distribution of these facilities will reflect the distribution of international military medical units; therefore, there is potential for partnership between the two medical communities. In addition to general medical topics, education programs for security force medical staff should cover subjects such as advanced trauma care, incident management, military medical ethics, and war surgery.

Mentoring

Finally, mentoring and support required at ministry of defense and ministry of health levels must be considered. It is likely that politically senior members of the local community will be holding appointments at this level, so advisory and mentoring services must take into consideration particular needs in the technical, management, strategic planning, and executive leadership areas. Organizations providing external financial assistance for security sector development may wish to have their own representatives inside the relevant ministries in order to ensure probity in the expenditure of their money. Thus there will almost certainly be a requirement for senior representatives of the international military medical community to act as mentors and conduits for external investment. While it is naturally assumed that Western military medical personnel have the competence to provide this advice, it may be more appropriate to invite nations from the international coalition with practical experience of developing military medical services during a period of economic and political transition to provide this mentorship function. A similar strategy must be developed to support mentoring at the regional, provincial, and district levels.

An important, intangible aspect of the engagement of the international military medical community is the sharing and monitoring of ethical standards. Medical personnel play an important role in observing and reporting the behavior of security forces towards the population they serve. While local policing and judicial frameworks will reflect the local cultural and security situation, it is important that the security forces' medical services align to

(Continued on Page 19)

Military *(Cont. from 18)*

internationally agreed standards of behavior and do not become accessories in the maltreatment of detainees or members of the security forces.

It is unlikely that any single nation will be able to provide the quantity or variety of resources to meet the full range of tasks that have been outlined above. Thus the international military medical community must work within an international framework that includes military, civilian, academic, private sector, and NGO sources. The lack of such a framework has challenged the effectiveness of security sector reform by military medical forces to date. Success requires shared and mutual understanding of the intent and mechanisms for delivery of the task. While some assets such as mentors or ETTs will be dedicated to the tasks described, others assets such as pre-existing international military medical treatment facilities will have to balance their role in security sector reform with their main function of providing medical support to international military forces. There may be scope for other innovative methods of delivery such as the use of external civilian agencies or contractors in addition to using conventional military forces. This pluralistic model requires a significant investment in coordination and sharing of resources in order to achieve unity of effort even if the arrangements preclude unity of command. This includes pre-deployment orientation and training for ETTs, sharing of training resources and best practices, transparent funding arrangements for all parties, and communication of plans and policies so as all parties understand the intent.

It is important to take a long-term view and to create international civil-military partnerships that can develop managerial structures and processes for sustainable, capable and effective local medical systems. ❖

Portions of this article were previously published in the Journal of the Royal Army Medical Corps, and are reprinted with permission.

*Colonel Martin Bricknell, British Royal Army Medical Corps, was Chief Medical Advisor, Headquarters International Security Assistance Force, Afghanistan.

**Colonel Donald Thompson, United States Air Force Medical Corps, was Command Surgeon, Combined Forces Command – Afghanistan and Combined Security Assistance Command – Afghanistan.

Piracy *(Cont. from 8)*

matters as simple as procuring and presenting evidence capable of proving cases against pirates in a manner consistent with the demands of international law also pose potential impediments to prosecuting sea dogs. Such difficulties are further exacerbated since the military is involved in pirates' capture.

On the other hand, there may be reason for optimism when it comes to straightening out legal issues relating to piracy. If the pirate problem grows large enough to earn the attention of governments that consequently capture growing numbers of sea scoundrels, the benefit of finding solutions to these legal issues will grow too, helping incentivize the relevant parties to find solutions to existing problems that hinder pirates' prosecution. ❖

*Peter T. Leeson is an economics professor at George Mason University and author of, *The Invisible Hook: The Hidden Economics of Pirates* (Princeton University Press, 2009).

H1N1 *(Cont. from 11)*

weakness or other threats to overall NATO Operational Pandemic Influenza H1N1 prevention and preparedness.

NATO medical advisors and staff have also established contact, and are maintaining liaison with, other non-NATO agencies and organizations such as local national public health authorities, the World Health Organization, as well as other NATO national military medical services. This effort has allowed wide dissemination of H1N1 related information and common issues among all in the interest of better overall readiness.

In full recognition that the present H1N1 Pandemic situation is dynamic and could become a more serious health threat, NATO medical authorities will continue to maintain vigilance and readiness to adapt future guidance. Once a vaccine is available, a H1N1 immunization program will be managed among nations for their deployed personnel on NATO missions. The impact of threats to health among the host nation population on operations and how NATO forces might respond to requests from the host nation authorities or international agencies for *in extremis* support from military forces in a humanitarian emergency are also being considered. Policy guidance is currently in preparation and will be issued in the near future, although appropriate responses have already been discussed with in-theatre commanders by the ACO Medical Advisor on his recent visit to Afghanistan. The over-riding responsibility of military medical staff is to support maximum operational and combat readiness of deployed NATO personnel through robust attention to the H1N1 situation in the months ahead. ❖

Senior Program Director Comments:

This article reflects some of the unique challenges faced by military authorities when the threat of a communicable disease is present. Military forces must maintain freedom of movement, but this movement may put the military forces at increased risk of infection if they must enter an area where disease transmission is occurring. On the other hand, they may become the vehicle of transmitting infection from one location to another, while deploying or redeploying, or while on operations in a particular area. Military medical leaders take many precautions against such infectious diseases, both to protect the military forces and to protect the civilian populations with whom they interact. Preventive countermeasures include multiple immunizations and chemoprophylaxis — taking medications to prevent an infection should disease exposure occur. Furthermore, surveillance for diseases in military populations has greatly improved in recent decades, so early detection of outbreaks and rapid response can take place.

Influenza offers unique challenges to military forces, particularly when an effective preventive vaccine is not available. Crowded living conditions and international troop movement is thought to have contributed to the 1918 influenza pandemic and the high levels of morbidity and mortality in both military and civilian populations. The interested reader can find more detail in "Fever of War: the Influenza Epidemic in the United States Army during World War I" by Carol Byerly for more observations and implications of military requirements in the face of an influenza pandemic.

Close communication and coordination between military and civilian medical and public health authorities is essential in planning for and responding to any public health emergency, both in the United States and internationally. Shared situational awareness of disease data in near real-time, coordinated civil-military and interagency course-of-action analysis and decision support, and a strong understanding of the very complex interdependencies of the medical, public health, transportation, and other sectors are all essential to effectively respond to a global pandemic. Such coordination is even more crucial when pharmaceutical interventions such as immunizations and antiviral medications may be in short supply, and social distancing and movement restrictions become necessary to contain and manage the pandemic.

— Donald F. Thompson, MD, MPH&TM
Senior Medical and Public Health Program Director
Center for Infrastructure Protection

Israel *(Cont. from 4)*

this, HSI argues that the implementation of some Israeli practices may be vital in strengthening the American public's efforts in participating in preparedness drills and exercises. By instilling confidence in Americans, the U.S. government and public have the ability to undermine and deal a blow to terrorist organizations throughout the globe and at home. Perhaps it is time that the U.S. arms itself with Israel's greatest weapon — awareness. ❖

RUSI *(Cont. from 6)*

Herein lies the paradox. While the UK has invested huge resources and energy into protecting its critical infrastructure from external shocks such as terrorism, privatisation and failures of regulation have been quietly making the UK increasingly vulnerable. It is the prospect of systemic failure which now poses by far the most pressing threat to the UK. Arguably, our critical infrastructure is now at more risk than at any point in our history, all as a result of things which we have done to ourselves.

Left unabated, this is a trend which will continue. As the demand for services delivered through our critical infrastructure continues to grow, and the interdependencies between them become more complete, a fundamental rethink around the oversight of much of the UK's critical infrastructure may now be necessary. ❖

Cyber *(Cont. from 14)*

Treaty to cyber attacks. At the same time, the international cyber security is merely the sum of relevant national concerns, often related to critical information and infrastructure that on their entity level are mainly concerned with practical information assurance, not so much with cyber defence.

That puts NATO in the position where their area of interest may overlap with the one of the European Union, ITU as part of the UN or even Council of Europe in regard of cyber crime cooperation. While this indicates the need to clearly define the focus of each organisation, the overlap is good in that it raises again the issue of definitions and concepts that need to be cleared on both national and international level. The terms "cyber security", "cyber attacks", "cyber warfare" etc. need revision in order to cover not only the business interests related to security of information systems, but also to the potential impact of security breaches for national security.

NATO initiatives in the cyber security area have brought new light to existing national cyber security strategies. In order to be compatible with the Alliance's goals, national security procedures need to consider practical national threat assessments, lessons learned from international cyber incidents as well as links between national and international cyber security. While there is a number of issues that can be resolved on a national or entity level, some efforts (like building zero-tolerance or coordinating responses to sophisticated cross-border cyber attacks) to secure cyberspace need to be made in cooperation. ❖

The Center for Infrastructure Protection works in conjunction with James Madison Univerity and seeks to fully integrate the disciplines of law, policy, and technology for enhancing the security of cyber-networks, physical systems, and economic processes supporting the Nation's critical infrastructure. The Center is funded by a grant from the National Institute of Standards and Technology (NIST).

If you would like to be added to the distribution list for *The CIP Report*, please click on this link:
http://listserv.gmu.edu/cgi-bin/wa?SUBED1=cipp-report-l&A=1