Sitrep proudly presents contributions from the new generation of Canadian scholars: selected papers from the 16th CDAI Graduate Student Symposium at Royal Military College, October 24–25, 2014

Inside this Issue

The Unjustifiable Aspiration of the Canadian Parliament to Vote on Military Missions by Krystel Chapman ................................................................. 3

‘Armed Attack’ and Cyber Network Attacks in International Law: The Case of Stuxnet by Jeff Collins ................................................................. 6

The “Blue Beret” Myth: Politics and Identity in Canadian Foreign Policy by Colin Chia ................................................................. 10

Pursuing Pirates in the Gulf of Guinea by Paul Pryce ................................................................. 14

www.rcmi.org
For the past three years Issue #1 has featured contributions from some of the brightest young academic minds in Canada. Every October the Conference of Defence Associations Institute (CDAI) holds its annual Graduate Student Symposium in Kingston where students from across Canada present papers on issues related to national security and defence. Your Editor is pleased to announce that this year we have contributions sufficient to fill a number of issues. Such is the growing appeal of Sitrep as a means for aspiring academics to be published for the first time. As you will have read in the latest Members’ News, our first ever Peter Hunter Award was chosen from this same group. Winner OCdt William Buss has had his paper posted on our website as an Otter Paper.

Krystel Chapman focuses on the ongoing debate amongst Parliamentarians in the UK, Canada and Australia on what she calls the unjustifiable proposition that Parliament must approve military deployments. She argues that the greatest risk to the stability of Canadian civil-military relations, and one that has been absent from this debate to date, is the usurpation by Parliament of the power to declare war.

Jeff Collins, a previous contributor, addresses cyber network attacks and international law and whether such an attack meets the threshold of an armed attack as defined in Article 51 of the United Nations (UN) Charter thereby allowing the use of force in self-defence. Will cyberattack lead to unrestrained digital warfare between states that could potentially escalate into even bloodier, more traditional, conventional combat?

Colin Chia debunks the Blue Beret myth held so dearly by so many Canadians—the myth that the Canadian military should not be engaging in aggressive combat missions, and should focus on peacekeeping roles. He posits that traditional peacekeeping is ineffective more often than not today, simply because civil and inter-ethnic “wars of the third kind” have become the most common conflicts since the end of the Cold War. If the CF limited itself to observation and monitoring, it would contribute little to the goal of global peace and security.

Piracy off the Horn of Africa is very well known. Paul Pryce writes of the threat of piracy on the other side, the western side of the continent in the Gulf of Oman. He suggests that a solution to the piracy problem could be found by outsourcing counter-piracy operations to private maritime security services, such as those conducted successfully in the Gulf of Aden and the Gulf of Oman.

By the time you have received this Issue we will have held (on January 29th) our first Security Studies Speaker’s event of 2014 featuring Reza Akhlagi from the Foreign Policy Association, Manhattan NY. Please join us for our second Security Studies Luncheon on February 26th featuring Professor Stuart Hendin Q.C., a member of RCMI, currently deployed to Kabul, Afghanistan, under the aegis of the International Development Law Organization, as an International Training Advisor in the Ministry of Justice.

I look forward to seeing you at the Institute.

Sincerely,
Colonel Chris Corrigan (retired) CD, MA
Executive Director, Editor and Chair of the Security Studies Committee

Copyright © 2014 RCMI ISSN 0316-5620. Sitrep may be fully reproduced in whole or in part for academic research or institutional purposes, provided that the author’s and the institute’s copyright is acknowledged. The views expressed are those of the author(s) and do not necessarily represent the views of the Institute or its members.
Parliamentarians in the UK, Canada, and Australia have been demanding a greater role for the legislature in determining the roles and missions of the military. The British Parliament authorized military action in Iraq one day before the start of hostilities in 2003, and again in Libya in 2011. This past summer, the British Prime Minister reluctantly accepted that the UK would not be involved in an eventual mission in Syria, after losing a vote on this issue. Yet despite an apparent trend towards Parliamentary votes on troop deployments, MPs continue to protest what they perceive is a limited and inconsistent role. For example, Australian troops were committed to Iraq, and Canadian troops were originally sent to Afghanistan, without Parliamentary approval. The Conservative Opposition in the UK also criticized the Government in 2006 after finding out through the media about an additional deployment of 4,000 troops to Afghanistan. In response, the House of Lords undertook a study of potential changes to Royal Prerogative Powers that would give the British Parliament a greater role in declarations of war and troop deployments. Canadian MPs were similarly outraged when they found out through media reports about the nature of Canada’s post-2011 role in Afghanistan. They learned that troops would not be confined to the relative security of Kabul, but would also be training Afghan security forces in Mazar-i-Sharif and Herat.

It has been argued that the Canadian Parliament should “have the right to vote on the most serious decision a government can make: sending military personnel into combat where they might die in pursuit of its foreign policy objectives.” Such votes are seen as an expression of the public will that meet a need for “democratic legitimacy.” It has also been suggested that parliamentarian deliberations would result in “more considered decision-making” and would “serve an important symbolic purpose.” Those who oppose a parliamentary vote on troop commitments, on the other hand, have argued that such a practice would lead to excessive and dangerous operational delays in times where expeditious military action may be necessary, and may endanger national security if secret details disclosed to parliamentarians in order to inform their decision are then leaked. In this paper, I argue that the greatest risk to the stability of Canadian civil-military relations, and one that has to date been absent from this debate to date, is the usurpation by Parliament of the power to declare war.

Powers of the Executive and the Legislature in Defence Policy

The Constitution Act, 1867, grants separate powers to the Executive and legislative branches with regards to matters of national security. Sections 15 and 19 of the Constitution assigns the Executive with the prerogative to create an army, appoint the Chief of Defence Staff, enter into international treaties, and most importantly, declare war. The Constitution unambiguously allows Cabinet to declare war or commit troops to a military operation without even consulting with Parliament, let alone obtaining its approval. Cabinet also sets the defence budget, makes senior military appointments, determines the government’s agenda, and in times when the reigning party holds a majority of seats in the House of Commons and the Senate, largely controls parliamentary committees.

Section 91(7) of the Constitution Act, 1867, in turn assigns legislative authority over “the Militia, Military and Naval Service, and Defence” to Parliament. Members of Parliament and Senators do not have access to the same level of details surrounding threat assessments and operations than do members of the Privy Council. As such, they have traditionally been involved in budget approval, execution and audit, rather than in the development of defence policy. Parliamentarians nonetheless play a vital role in all stages of policy-making.

While the Prime Minister and the Minister of National Defence have legislative authority to manage and direct the defence establishment, an array of mechanisms is available to parliamentarians to assess the Executive’s stewardship. This separation of power ensures that decisions regarding matters of national security can be taken quickly and efficiently, while at the same time making the Executive accountable for those matters.
decisions to Parliament. The powers accorded to Parliament allow interested Parliamentarians to partake in civil oversight of the military and to hold the Executive to account on its defence policy. They have the opportunity to question the Government on national defence policy while reviewing bills and motions, as well as during take-note debates and in the highly mediatised Question Period. In fact, the involvement of Parliament in matters of war and peace is not new. The long-standing tradition of parliamentary involvement includes matters which have traditionally belonged in the legislative realm, such as budget oversight. For example, Westminster rejected a request by King Charles for an increase in taxation to cover the costs of naval war against Spain. As this historical case demonstrates, while the Executive has legislative authority to manage and direct the defence establishment, an array of mechanisms is available to parliamentarians to assess the Executive’s stewardship without expanding Parliament’s current areas of responsibility.

The oversight functions and abilities of Parliament have grown incrementally over the last decades, namely through the creation of the Senate Standing Committee on National Security and Defence, the advent of Access to Information Requests, and the introduction of parliamentary reforms such as take-note debates. Take-note debates are a relatively new parliamentary procedure that was introduced by Jean Chrétien in 1994 to canvass the opinion of Parliamentarians on the future of peacekeeping in the former-Yugoslavia. Take-note debates allow “members to participate in the development of government policy, making their views known before the government makes a decision,” and are frequently used by the Executive to address defence matters within the confines of Parliament.

From September 2001 to March 2011, 12 debates (notwithstanding exchanges occurring during Question Period) took place in the House of Commons on the military aspects of the mission in Afghanistan: two debates to adopt motions condemning the terrorist attacks on the United States of America, three take-note debates on Canada’s commitments in Afghanistan, three debates to extend Canada’s military presence in Kandahar, one motion to create a special parliamentary committee on the Afghan mission, two motions to end the mission by diplomatic means, and one motion for the Government to produce documents on the detainees issue. Although this number may seem low given the length and human and financial costs associated with the mission, it in fact reflects a trend that began in the 1990s towards increased parliamentary debates on international military deployments. Prior to the Afghan war, the involvement of Canada in the former Yugoslavia had “been by far the most debated inter-

The five debates on the former-Yugoslavia and the nine debates on Afghanistan represent an improvement in civil oversight of the armed forces from past practices; in the 21 peacekeeping missions in which Canada participated from 1947 – 1989, only six Parliamentary debates were held, regarding six of those missions. Parliamentarians have clearly expressed their interest in the Afghan deployment by debating the issue several times over the course of the mission.

While parliamentary debates on defence matters in majority situations have typically provided little more than a forum in which defence policy can be validated for the Canadian public or where opposition parties attempt to embarrass the Executive, a notable change occurred in the winter of 2008. The Government’s policy shift on an exit-date for the Afghan mission represents the first time in Canadian history that Parliamentarians forced the Executive to reverse a previously-announced decision on an international deployment. Prime Minister Stephen Harper committed to submit the extension of the Afghanistan mission beyond 2009 to a parliamentary vote; within a matter of weeks, the Conservative and Liberal parties brokered an arrangement whereas the mission was extended beyond February 2009 – a position opposed to by the Bloc Quebecois and the New Democratic Party – but also imposed a cessation date for the combat mission, a timeline that the Prime Minister had previously refused to commit to. This new development reignited calls for the Canadian Government to adopt legislation that would make it mandatory for any decision to commit troops to war to be approved by Parliament. It did not, however, create a precedent negating the Executive’s exclusive hold on the commitment of troops and declarations of war as set-out in s.15 and 19 of the Constitution Act. Canada has a codified Constitution with a clear amendment formula. The Constitution is the supreme law of the country, and cannot simply be amended through an emerging ‘convention’ or by legislation adopted by Parliament. In contrast, constitutional conventions in the United Kingdom, where there is no written constitution, can be more easily modified by the adoption of a law in the House of Commons. Parliamentary vote on UK troop deployments has been acknowledged by former Prime Minister Tony Blair as a new political convention, given that he “cannot conceive of a circumstance in which the government goes to war without consulting parliament.”

A Danger to Healthy Civil-Military Relations

Civilian and military actors have a range of tools at their disposal to work collaboratively to establish and maintain subjective, objective and effective civil control of the military. Canadian political leaders exercise subjective control through constitutional arrangements, laws, statutes and decrees, like the National Defence Act, while the military sphere, by means of objective civil control, must impose upon itself “professional standards and meaningful integration with civilian values.” Officers “internalize the belief that their subordination is ap-
propriate and should not be lightly set aside.” They do so by abiding to a set of fundamental values and beliefs that make-up the Canadian military ethos, which all members of the military agree to embrace: to defend the Canadian Government and its citizen honourably by abiding to the highest standards of excellence. For the relationship to achieve a degree of stability, however, the political sphere must go beyond institutional and ceremonial control. To exercise “effective civil control,” political leaders and their staff must possess a sophisticated knowledge of military affairs in order to claim any control – let alone credibility – over the military institution. Politicians cannot claim to control the military if they solely rely on the advice of Generals to make, implement, and evaluate policy decisions. In order to competently implement legal instruments and to exercise effective civil control, civilian leaders must have a sufficient level of understanding of the requirements, capabilities and operational workings of the military. Civilian leaders have to foster a climate in which the military can voluntarily submit itself to civil control. Policymakers must therefore ensure that policy objectives are put into operation by military officers, and that the influence of the armed forces in defining those political goals be limited.

Debating and voting on military deployments in the House of Commons could erode the tradition of healthy civil-military relations by creating a vacuum space to be filled by the military. Scenarios where the Executive favours war, but Parliament opposes it, create uncertainty and ambiguity for senior military leaders. Several historical cases demonstrate that Parliamentary votes on matters of war and peace create political instability. The American War of Independence ignited a debate about the role of the British Parliament in raising militias. The House of Commons voted against the Government’s attempt to create a new militia that would be deployed to bring reinforcements to the war in the United States. The vote followed a defeat at Yorktown the year before and was defeated by 19 votes. Lord North immediately resigned as Prime Minister, and is reported to have said: “Oh God, its all over,” as his government became the first government in history to lose a vote of no-confidence in the House of Commons. There’s also been an increased tendency in the past decade towards minority governments; in such contexts, securing a majority vote in favour of a deployment has proved to be a risky enterprise. Italian Prime Minister Prodi resigned in February 2007 after losing a senate vote on his foreign policy programme, which included a troop commitment in Afghanistan. The Dutch government also fell, after the coalition Cabinet collapsed over disagreement on whether to extend its military presence in Afghanistan. An election over Afghanistan was narrowly avoided in Canada in 2008 after the Liberals and Conservatives brokered a deal on the extension of the mission.

Other ambiguous circumstances could also arise, whereby Parliament could approve a motion submitted by the Opposition during one of the Opposition Days committing troops abroad, without the approval of the Government. While the latter scenario has not occurred in any parliamentary democracy to date, in both cases elections would be triggered since votes on troop deployments are considered matters of confidence in Canada. Elections triggered by disagreement in the House of Commons over military policy, particularly whether to wage war, create uncertainty and ambiguity for leaders of the armed forces, who are left without clear political direction for the duration of the electoral campaign and until the swearing-in of the new Government. In many cases, these weeks could render armed action – or inaction – irrelevant. Conflicts in the post-Cold War era have been intense and speedy; for example, it is estimated that the majority of the killings during the Rwandan genocide occurred over the span of a mere two weeks; the campaign in Kosovo, while lasting longer than anticipated by NATO planners, was over within

Continued on page 16
‘Armed Attack’ and Cyber Network Attacks in International Law: The Case of Stuxnet

by Jeff Collins

Estonia in 2007, Georgia in 2008, and Iran in 2010 represent well-known examples of states that have been hit with cyberattacks. Now considered by many of the world’s major powers as the fourth domain of warfare—after air, land, and sea—cyberattacks against state systems and infrastructure have increased in such frequency in the last decade and a half that they have now become a key component in many states’ defence capabilities. As one report notes, there are now over 120 states currently investing in cyber capabilities and defences. The resultant changing security environment brought about by this new technology is raising legal questions as well. Specifically, for analysts of international law, one of the key issues regarding cyberattacks is whether they can meet the threshold of an armed attack as defined in Article 51 of the United Nations (UN) Charter and thereby precipitates a use of force in self-defence. The very nature of cyberattacks, particularly in that they are digital and not physical in character and are difficult to attribute is driving this debate. As such, much concern exists that cyberattacks will foster an environment of unrestrained digital warfare between states that could potentially escalate into even bloodier, more traditional, conventional combat.

Concerns over computer network attacks can be traced to the 1980s. But it was the popularization of the internet, as noted by the Clinton Administration’s 1996 Commission on Critical Infrastructure, which raised the level of concern towards computer-driven attacks. Since the 9/11 terror attacks this discussion no longer remains relegated to the abstract: states have invested and continue to invest in both offensive and defensive cyber-technologies. By its most basic definition, cyberwar refers to those hostile actions that occur in cyberspace. These actions can, broadly, come in three forms:

First, are cyber network attacks (CNA), which aim to “disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves”. CNAs are a “hostile use of cyber force” and can take the form of an isolated action, “the first strike of an armed conflict, an attack in the context of an already initiated armed conflict, or a reaction against a previous conventional or cyberattack”.

Further, a CNA can be either state-to-state or non-state-to-state and can produce damage “extrinsic to the computer or network”, such as shutting air-traffic control radars.

Second, there are cyber network exploitation (CNE) actions, which are those cyber activities that involve espionage and intelligence-gathering. While CNE is in violation of most states’ domestic laws espionage in and of itself does not violate international law. Finally, there are computer network defence (CND) actions, which are those “actions taken to protect, monitor, detect, and respond to unauthorized activity within...information systems and computer networks”—in other words, preventing CNA and CNE through the use of counterintelligence, intelligence, and law enforcement. CNAs, in contrast, are those forms of cyberwar which are used against another state’s military and civilian infrastructure - like the Stuxnet attack on Iran’s nuclear centrifuges in 2010 - and are consequently the subject of jus ad bellum.

The fear surrounding CNAs has to do with the transnational nature and anonymity characteristic of the technology. Advanced states with high-tech economies remain vulnerable to cyberattacks due to their dependence on sensitive computer systems. At the most extreme, it is been suggested that an effective CNA could disable “critical networks providing power, transportation, national defence and medical services.” Such
actions could lead to large loss of life or economic turmoil. In the late 1990s, a major cyberattack dubbed ‘Solar Sunrise’, launched through computers in the United Arab Emirates by teenagers in California and Israel, hit the Pentagon’s supposedly secure networks, stealing large amounts of secret information. This attack was one of the first to demonstrate, at least to American policy-makers, the potential harm that can be inflicted by CNAs.

Furthermore, until the Stuxnet attack CNAs were thought to be mostly non-kinetic in nature, that is, they lacked a direct physical impact, their effects resemble those brought about by sabotage operations “carried out by guerrillas or special forces, than like warfare in the sea, land, or air domains...” As such, many states, including the US and China, have come to regard CNAs less as a standalone weapon and more of a support platform for conventional weaponry. This was perhaps most evident in the 1999 NATO air campaign against Serbia, Operation Allied Force. In that conflict US President Bill Clinton had approved a “top secret plan to destabilize Yugoslavian leader Slobodan Milosevic by using computer hackers to infiltrate and attack foreign bank accounts held by Yugoslavia in order to siphon off funds that might be used for military purposes”. Notably, while the airstrikes were continuing, NATO also proceeded with a coordinated cyber-attack on Serbia’s command and control systems, creating confusion in that country’s communication and air defense networks. Likewise, in 2008 Russian conventional attacks on Georgia operated in parallel with cyberattacks on Georgian command and control systems. Nevertheless, the advances in the sophistication of CNA, as represented by the attacks in Iran in 2010, for example, mean that the possibility of direct kinetic effects is possible.

As a general rule, since the ratification of the UN Charter in 1945 there exists a prohibition on the use of force in international relations. This prohibition, found in Article 2(4) of the Charter, prohibits the “threat or use of force against the territorial integrity or political independence of any state.” As one legal commentator has noted, Article 2(4) remains “the core international legal rule on the right to resort to armed force”. The prohibition on the use of force is also found in international customary law (ICL)—that is, legal principles formulated on the basis of what states say (opinio juris) and do (state practice). The prohibition on the use of force in ICL is most evident in the pronouncements of three key General Assembly resolutions: the 1970 Friendly Relations Declaration, 1974 Definition of Aggression, and the 1987 Declaration on the Non-Use of Force. Notably, as a result of crystallization as customary international law, the prohibition on the use of force is widely regarded as having achieved jus cogens status, meaning that it is now binding on all states regardless of whether they are party to the Charter or not.

Nevertheless, there remain two key exceptions to Article 2(4): first, Article 42 permits the UN Security Council to authorize member states to use force in the event of the Council determining the existence of a threat to international peace and security. Secondly, and most relevant to the discussion at hand, Article 51 allows for the right to self-defence. A holdover from the pre-Charter era, Article 51 declares that, “Nothing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security” (author’s italics). This right is said to be inherent—i.e. derived from ICL—and therefore permits a state to use force in self-defence as long as it is in compliance with the ICL rules of necessity and proportionality.

The most important component of Article 51 for this paper is the term ‘armed attack’. As legal scholar Yoram Dinstein writes, the importance of knowing when an armed attack has occurred is critical in determining who the aggressor is and who the victim state is, thereby legitimizing the use of force by the aggrieved state. The importance of this point has been emphasized in ICL as well with Article 2 of the 1974 General Assembly resolution, The Definition of Aggression, which refers to the first use of force as prima facie evidence of aggression.

The problem is that armed attack remains undefined in treaty law. Some treaty provisions do provide insight into what can constitute an armed attack however there remains no consensus. But, the overall effect on international law, because of the absence of a definition, remains the same: it is difficult to determine whether or not there has been an armed attack—minus, of course, the blatant use of mass conventional military force. Armed force, in the traditional sense of the term, often meant kinetic, or physical, force such as artillery barrages and airstrikes. However, as Michael Schmitt notes, “cyber operations do not fit neatly into this paradigm [of armed attack] because although they are ’non-forceful’, their consequences can range from mere annoyance to death.” In effect, how can a cyberattack amount to an armed attack?

In answering this question lawyers have turned to ICL for guidance. Notably, the International Court of Justice (ICJ) has recognized over the years that the lack of defining what is an armed attack has created a ‘gap’ between Articles 2(4) and 51. To elaborate, the former prohibits the use or threat to use force while the latter states that the use of force can only be used in self-defence in light of an armed attack. This creates the implication that there are some uses of force which, while illegal, do not meet the threshold of an armed attack. In such situations a state’s remedies would be limited to “non-forceful actions, countermeasures or recourse to the Security Council”. As an aside, Heather Dinniss argues that a state suffering from a cyber-attack not meeting the threshold of an armed attack can respond in kind with a similar cyberattack of its own. The ICJ in the Nicaragua case affirmed this gap, writing that “measures which do not constitute an armed attack... may nevertheless involve a use of force”; hence, the Court argues, it is “necessary to distinguish the most grave forms of the use of force from other less grave forms” (the latter of
which the Court referred to as “mere frontier incident[s]”). Importantly, the Court recognized that an armed attack is no longer said to require a large conventional military force of one state attacking another given that the sending of “armed bands” (guerrillas) into another state is sufficient enough to amount to an armed attack; a scenario that was also included in *The Definition of Aggression*. Indeed, in the *Tehran* case the Court, rather controversially, clarified that the supplying of weapons and logistical support to an armed band could amount to a use of force but still not meet the threshold of an armed attack—particularly if the subsequent acts of the group are not themselves attributable to the state. The Court went to say that the key factor in distinguishing the degree of severity in a use of force situation was the “scale and effects” of the force involved. The logic stemming from this judgment is that an armed attack requires “serious consequences, epitomized by territorial intrusions, human casualties or considerable destruction of property”. Therefore, it is argued that if a cyberattack creates a similar level of effects like those generated by a kinetic use of force then it could be said to have amounted to an armed attack. In Matthew Hoisington’s words, “cyberattacks intended to directly cause physical damage to tangible property or injury or death to human beings are reasonably characterized as a use of armed force and, therefore, encompassed in the prohibition of 2(4)

For Harold Koh, the current Legal Adviser to US State Department, this is exactly the view the US has taken. As he posits, a cyberattack “that [may] proximately result in death, injury, or significant destruction would likely be viewed as a use of force.” This is particularly telling as the US does not make a distinction between a use of force and an armed attack. Therefore, the Americans would see such a use of force as equivalent to an armed attack under Article 51 of the UN Charter invoking “a state’s national right to self-defense”. In light of Koh’s comments Graham proposes a three-model analysis to determine whether the effects of a CNA equate to a use of force amounting to an armed attack. The first model invoked is the instruments-based approach. This model focuses on determining whether the “damage caused by a cyberattack could have previously been achieved only by a kinetic attack”. The second approach is the effects-based which is focused on the overall effect of the CNA on a state. Finally, there is the strict liability approach which “automatically deems any cyberattack against critical national infrastructure to be an armed attack, based on the severe consequences that could result from any attack on such infrastructure systems”.

The first model is seen as best representing the “scale and effects” view articulated by the ICJ in *Nicaragua*. Moreover, it is the model that the drafters of the UN Charter opted for when they framed Article 51. As such, this model is widely used by states and international organizations in policy discussions on CNAs. Michael Schmitt, however, argues that states should be adopting the strict-liability model as the instruments-based approach remains too constrained and cannot account for “the possibility of devastating consequences caused by non-kinetic cyberattack”. For Schmitt, the strict-liability, or consequence model best captures “the essence of an ‘armed’ operation”, which he explains “is the causation, or risk thereof, of death or injury to persons or damage to or destruction of property and other tangible objects”. If a particular use of force operation can do this it can be considered as an armed attack under Article 51. In contrast, Marco Roscini argues that Schmitt’s approach is unconstrained. Roscini claims that Schmitt’s model “blurs the distinction” between economic coercion and “the traditional use of force classification characterized by armed attacks”. Likewise, ICL and Article 51 make no distinction between the type of weapon(s) used in an armed attack; in a word, the technicalities of a weapon is irrelevant in determining whether an armed attack has occurred—a point affirmed by the ICJ in the *Nuclear Weapons* advisory. This issue was also affirmed by two Security Council resolutions following the 9/11 terror attacks - each of which implicitly recognized that those attacks, perpetuated using hijacked commercial airliners, amounted to an armed attack. Lastly, Schmitt’s modelpresumes that a cyberattack is on par with other, more traditional, forms of attack by an intentional harmful act committed by a state’s adversary. The problem is that the very nature of CNAs makes it extremely difficult to determine the origin of an attack, and to assess “readily at the time of the attack [the] magnitude and the permitted response”. In other words, attribution is very difficult in the case of a CNA and remains a practical restraint on any justified use of force brought about by an armed attack.

The problem of determining attribution in a CNA is rooted in the “technical complexity” of cyberwarfare generally as CNAs are often shrouded in anonymity. An attack that may appear to originate from the computer network of one country does not entirely mean that the country of origin is responsible for the attack. One form of CNA, distribute denial of service (DDoS), was used against Estonian government and private websites in 2007, crashing the state’s servers. The attack, however, originated from more than a million computers based in more than 100 countries. Kyrgyzstan suffered a similar attack in 2009. In both cases Russia was thought to be the culprit but it could never be entirely proven. While non-state actors are capable of committing an armed attack against a state (Article 51 does not limit the source of an armed attack to states while ICL in both *Nicaragua* and the 9/11 Security Council resolutions recognize non-state actors as capable of armed attacks) a state’s control over ‘hackers’ is difficult to ascertain. As Roscini notes, “hackers may not be *de jure* organs of a state but rather individuals or corporations hired by states in order to conduct cyberattacks”. According to the non-profit US Cyber Consequences Unit the 2008 CNAs against Georgia, for example, were tied to a cybercrime syndicate known as the Russian Business Network. But the link...
between the Russian government and the criminal enterprise could not be concretely made. In *Nicaragua* the ICJ wrote that in order for the actions of a non-state actor to be attributed to a state there must be evidence “that [the] State had effective control of the military or paramilitary operation in the course of which the alleged violations were committed.” As demonstrated above, and will be illustrated with the Stuxnet case below, even if a CNA met the threshold for an armed attack the aggrieved state would still have difficulty in locating the appropriate source of the attack. Some scholars are therefore calling for multilateral treaties to better create the legal mechanisms necessary to determine attribution.

In June 2010 reports emerged that a cyber ‘worm’, known as ‘Stuxnet’, had infected Iran’s Natanz nuclear enrichment facility. This particular CNA had targeted 60,000 computers - 30,000 of which were in Iran - in more than a dozen countries, including the US, the UK and China. Drawing on a “Frankenstein patchwork of existing tradecraft, code and best practices from the global cyber-crime community” Stuxnet’s sophistication and genius allowed it to take over the remote control systems of the Natanz plant’s centrifuge equipment. The worm began alternating “the frequency of the electrical current that powers the centrifuges, causing them to switch back and forth between high and low speeds at intervals for which the machines were not designed.” Eventually the centrifuges spun out of control and broke but only after the worm had remained active in the equipment for nearly a year, fooling the plant’s operators into thinking that the machinery had been working fine. The International Atomic Energy Agency, upon investigating the facility, noticed that the centrifuge equipment had a suffered a major breakdown resulting in a 23 percent decline in the number of operational centrifuges. Of critical importance to international law and the use of force, however, is that the “Stuxnet virus marked a watershed in cyber warfare because it demonstrated that cyber activity can have kinetic, physical effects.”

The issue of course is whether the Stuxnet CNA amounted to an armed attack. The initial response is that Stuxnet, while constituting a use of force, does not appear to meet the threshold of an armed attack. An armed attack - in following the first of three model approaches identified above in a CNA - remains concentrated on equivocating the scale and effects of a CNA to those of a kinetic attack. This effectively means that any action must lead to a loss of life and/or substantial destruction of property. An appropriate comparative example would be the Israeli air strikes against the Iraqi Osirak reactor and the Syrian Al Kibar reactor in 1981 and 2007 respectively. Those scenarios could qualify as an armed attack given the level of destruction and loss of life inflicted. While some of the centrifuges in Natanz were clearly destroyed it is difficult to conclude that this qualifies as being severe under the “scale and effects” test. Although Natanz is a state owned, military-aligned facility and therefore, any singular attack on it would meet the threshold, set down by the ICJ in *Oil Platforms*, to suffice as an armed attack. More importantly, without the loss of human life it remains challenging to state that an armed attack occurred. The fact that the Iran has downplayed the action, arguing that Stuxnet caused a minimal amount of destruction strengthens the argument that an appropriate level of “scale and effect” required for a use of force to qualify as an armed attack.

Furthermore, the problem of attribution remains. While the Stuxnet case garnered a lot of press the widespread origin of the CNA—thousands of computers across many countries—complicates who is responsible. Various accounts place the US and Israel as the source of the CNA. Without definitive evidence that Stuxnet qualified as an armed attack, an Iranian use of force in self-defence would be constrained in its actions.

This paper has demonstrated that contemporary *jus ad bellum* rules are capable of covering cyber-network attacks. International customary law has evolved over the past half-century to the point that it is sufficient in providing explanatory power on when a CNA can amount to an armed attack. ICJ case law over the past three decades has provided more nuance to what is meant by an armed attack. As detailed above, non-kinetic uses of force, regardless of the type weapon used, can initiate an armed attack. Moreover, non-state actors can also launch a CNA against a state which can also amount to an armed attack. The issue, again, is one of scale and effect: how much damage and loss of life, if any, have been inflicted, and on what target, in order for a particular use of force to qualify as an armed attack under Article 51 of the UN Charter.

But, as the Stuxnet case illustrates cyberattack technology has some way to go in order to meet a threshold high enough to suffice as an armed attack. The 2010 CNA on the Natanz nuclear facility was the first, and so far only example of a CNA causing physical damage. When compared to an airstrike, like those carried out by Israel against Iraq and Syria, than it is clear that CNAs are nowhere near the destructive capability necessary to justify a use of force in self-defence. In the meantime, though, CNAs are being used more frequently by states and their non-state allies against governments around the world. Further discussion is therefore required on the relationship between cyberattacks and the prohibition on the use of force given that some states, like the U.S., see no distinction between uses of force and armed attacks. Moreover, CNAs are likely to remain with us for some time. They are too cheap and effective for states to simply dispose of.

*The views expressed are those of the author and do not necessarily reflect the views of the Institute or its members.*
The “Blue Beret” Myth: Politics and Identity in Canadian Foreign Policy

by Colin Chia

In 2000, Molson Breweries decided to give its marketing a nationalist flavour. In the iconic “I am Canadian” television commercial a young man wearing a plaid shirt declared, among other things, that because he is Canadian, he believes in “peacekeeping, not policing”. While its use in mass advertising suggests the strength of peacekeeping in the popular image of Canada’s military, more concrete evidence can be found in a 2009 Ipsos Reid poll which found 50 per cent of Canadians “observation and monitoring” should form the primary overseas missions for the Canadian Forces (CF)—in other words, traditional blue-beret peacekeeping. The Environics Focus Canada 2012 study also found that “peacekeeping” is most commonly named as Canada’s most positive contribution to the world, with a wide margin over “foreign aid” in second place. A prevalent view has therefore developed among the general public that the Canadian military should not be engaging in aggressive combat missions, and should focus on peacekeeping roles.

The truth is that the traditional peacekeeping reputedly pioneered by Lester B. Pearson is today ineffective more often than not, simply because civil and inter-ethnic “wars of the third kind” have become the most common conflicts since the end of the Cold War.1 If the CF limited itself to observation and monitoring, it would contribute little to the goal of global peace and security. Furthermore, as I will argue here, overseas deployments of the CF since 1999 have had much more to do with upholding Canada’s credibility among a select group of culturally and politically similar allies. However, partly because political leaders are unwilling to puncture the middle power myth and continue to frame foreign policy and CF deployments in terms which recall the liberal internationalism of Canada’s supposed “foreign policy golden age”, public opinion has tended to lag behind. As a result, a problematic gap has developed between national identity and foreign policy in Canada, which will likely pose continuing difficulties in formulating a Canadian foreign policy that is both coherent and politically legitimate.

If peacekeeping is ingrained in the public imagination, the middle power myth has had a similar pull in policymaking. There is little agreement on just how to define a “middle power”, although there is near-universal consensus that Canada is one. The middle power concept is useful up to a point because it clarifies the key issue of Canada’s place in the world: a “leading non-great power”, a state with significant capabilities and global interests but unable to unilaterally challenge the status quo of the international system. Because middle powers like Canada are relatively weak in hard power terms, it is usually in their interest to promote an international order which can constrain more powerful states through norms and rules. Influence in alliances, organizations, and other multilateral arrangements tend to be the most effective way for them to achieve foreign policy objectives. Facing inherent limits on their military and economic power, middle powers can nevertheless achieve relatively more through soft power influence, and therefore tend to be concerned with ensuring that other states perceive them favourably as a “model citizen” of the global order.

One major problem is that a behavioural attachment to the middle power concept has at times taken hold in foreign policy thinking.2 This mindset defines middle powers in terms of a state’s conformity to the observed behaviour of states already defined as being middle powers. It has created a misleadingly circular notion that in order to maintain its stature in the world as a “middle power” and avoid relegation to “small power” status, Canada must necessarily behave as a multilateralist, good global citizen. This confuses the means with the ends of foreign policy, and it backgrounds a good deal of the prevalent misconceptions of Canada’s foreign policy interests. Taken to an extreme, it suggests that Canada should not have national interests at all. In fact, utilizing multilateral approaches and avoiding actions which might be perceived as aggressive and belligerent is often very much in Canada’s self-interest.

Indeed, the Pearsonian “golden age” of Canadian foreign policy, looked back on with nostalgia in some quarters, was a successful period because the pursuit of idealistic goals corresponded with Canada’s basic national interest. A fundamental national security concern during the Cold War was to reduce the possibility of nuclear war between the rival superpowers. Given the tendency for local conflicts to turn into US-Soviet proxy wars, like the Korean War or Vietnam War, peacekeeping operations and acting as the honest peace-broker was consistent with the need to avert potential escalations of conflicts. However, foreign policy must be responsive to external conditions, and simply adopting the same approach today as during the 1960s would not necessarily bring the same positive results. The global security environment has changed fundamentally, and with it the nature of “operations other than war” that the CF undertakes. And the fact that perceptions have not caught up with the post-Cold War world creates a gulf between the myths and realities of Canada’s foreign and security policy.

Colin Chia is an MA (Political Science) student at McGill University and graduated from the University of British Columbia. His research interests focus on nationalism in international relations, political and voting behaviour, and Asia-Pacific security studies.
Politics, portrayals, and perceptions of CF missions

Canada’s military role abroad has always had much more to do with alliance defence than the popular perception of Canadian soldiers as peacekeepers. Even during the heyday of traditional UN peacekeeping during the Cold War, far more Canadian troops were stationed with NATO forces in Europe to deter Soviet invasion than were wearing blue berets on UN missions. Peacekeeping has always been the attractive side-show which politicians have preferred to promote over the main event. Today, the side-show has left the stage but political leaders have continued to keep up the portrayal of overseas CF deployments as altruistic “peace building” missions.

After the catastrophic failures of traditional UN peacekeeping in places like Srebenica, Rwanda and Somalia, NATO’s intervention in Kosovo marked a key turning point in CF overseas missions. This was the first time NATO had fought as a military coalition and it went ahead despite the lack of approval by the UN Security Council. It showed the recognition that traditional peacekeeping was inadequate to deal with the sorts of ethnic and intra-state conflicts that were emerging in the post-Cold War era. Although the Kosovo mission had a clear humanitarian purpose, it could equally be argued that stabilizing a crisis in NATO’s European backyard was the real priority. Canada’s interests here were not in Kosovo itself, but in very visibly contributing to NATO and thus gaining credibility within the alliance. Indeed, CF deployments are generally remarkable for the lack of constraints which other NATO states routinely place upon their troops, meaning that Canada usually punches above its weight and takes on heavy lifting roles. The need for close defence cooperation with the US is obvious regardless of any other factors, but NATO is also not just another military alliance. Especially post-Cold War, NATO has also become a political coalition of ideologically and culturally similar countries. Subsequently, the centrality of NATO and Washington in Canadian security and foreign policy, as well as the treatment of the UN as mostly irrelevant, became even more apparent.

October 2001 and Operation Enduring Freedom are a special case because of the extraordinary circumstances. There were no illusions that Canada’s participation in the initial invasion of Afghanistan was fighting a war on the American side against a common enemy, and this was publicly acceptable to clear majorities of Canadians. But such was the speed at which the Bush administration squandered the international sympathy generated by the 9/11 attacks that just two years later, opposing the Iraq War was the politically expedient option for the Chrétien government. The strong unpopularity of the war, especially in Quebec, created the potential for a national unity crisis with a federal election due the following year, on top of a threat of a party leadership challenge against Chrétien. However, despite Canada’s clearly-stated opposition to the war, Canada actually had more soldiers in Iraq than most members of the “coalition of the willing” due to our military exchange programs with the US and UK. Future Chief of the Defence Staff Walter Natynczyk even earned a medal for commanding combat troops in Iraq. Three ships were also quietly deployed to the Persian Gulf in an attempt
to stay on the good side both of Washington and of Canadian public opinion.

But Canada still got something of a cold shoulder, with intelligence cooperation being cut off in retaliation at one point. The reason this would happen in spite of efforts in Washington back rooms to ensure awareness of Canada’s contribution was that the US did not necessarily want or need Canada’s clandestine military contributions. Australian academic Mark Beeson described his country’s role in Iraq as part of a “militarily marginal but ideologically indispensable supporting cast.” Canada’s overt support was desired for similar reasons: the legitimacy that Canada would have brought to the highly controversial operation was what the Americans really cared about.

This was the background for Canada’s involvement in Kandahar, which should be understood as a distinct case from the initial involvement in 2001. This was a choice to take on a more dangerous, combat-oriented mission, but also one that would put Canada’s military in the spotlight and provide a vehicle for the CF’s rejuvenation. An in-depth examination of this decision can be found in chapter 10 of The Unexpected War. With the Martin government’s rejection of American proposals for an anti-ballistic missile shield, there was a strong concern within the defence establishment that Canada needed to do something to restore the military relationship with the United States. Gen. Rick Hillier has written that Prime Minister Martin’s original preference was for a deployment to Darfur—closer to the “blue berets” image—rather than to Afghanistan. At another decision-making juncture, a mission in Kandahar was chosen over NATO’s desire for Canada to deploy in Herat, in part because Herat offered less visibility for the CF.

Once the decision had been made, however, the government communicated it in a way that drew on the peacekeeping myth. Liberal defence minister Bill Graham told the public that the mission was “quintessentially Canadian,” and when the Harper government took power its 2007 Throne Speech stated that progress in Afghanistan could be measured in how many children were going to school, and talked about “security” and “men and women in uniform” rather than combat and soldiers. Of course, Canada has a direct interest that weak states do not harbour terrorist groups. Afghanistan was hardly the only such problem area in the world, but it was the one which was construed as a threat to our allies. This was apparently reason enough to engage the CF in a combat deployment which consumed nearly its entire fighting strength and made any other significant deployment impossible. The path to Kandahar was therefore paved by what were considered to be the imperatives of Canada’s role as an alliance partner to the US and within NATO, especially within in the defence establishment.

Most recently, the Canadian military was involved in the 2011 Libyan civil war with the deployment of CF fighters and Canadian general taking command. Canada was fighting alongside NATO allies, wanting to be seen as doing our bit. Even if not to the alliance itself, Canada was coming to the support of Britain and France, who had been key in pushing for the alliance to take a hand and who saw their own interests implicated in Libya. Whatever security interest Canada had in the downfall of the Gaddafi regime was indirect. The same pattern thus emerged of an alliance-driven Canadian commitment justified on humanitarian grounds; the intervention was necessary, it was argued, to stop the Gaddafi regime from further violence against its own people. The CF obviously cannot be deployed to intervene in every humanitarian crisis or to stop all atrocities, not least because Canada lacks the military capacity to act alone in a meaningful way. But the CF’s participation in Libya allowed Canada to demonstrate its capabilities and desires to take on big responsibilities. It was a reinforcement of the theme set by Kosovo and Kandahar, signalling a strong commitment and contribution to Canada’s partnership with the US and NATO, which had little to do with peacekeeping or humanitarian motivations.

**National pride and foreign policy**

The popularity of the peacekeeping ideal has much to do with the desire to believe that Canada is a force for “good” in the world. Seen in another way, the ability to intervene abroad also demonstrates Canada’s strength. These sentiments are ultimately connected to national pride and identity which in turn are attached to individual feelings of belonging and loyalty to the nation as a social group. National identity and foreign policy are interlinked and mutually constitutive—each deeply influences and imposes constraints on the other. Foreign policy has difficulty achieving credibility abroad as well as legitimacy at home if it is too far out of line with conceptions of that country’s national identity. The image citizens want their country to project abroad is an issue leaders are obliged to be sensitive to. This is especially true in democracies, and not just because it might affect the government’s re-election chances, but also because the ultimate aim of Canada’s foreign policy is to protect those democratic values.

Having taken on and settled into a conception of the “middle power” role in the international system, Canada has decided to pursue global interests with inherently limited material capabilities. The evidence suggests that in pursuit of this, recent military deployments have been driven by the desire to please and impress Canada’s allies. The approach has thus been to use the CF to earn influence with the US and within NATO, even while successive governments have sold military deployments to the public by appealing to the national stable of idealistic myths. This is not necessarily a problem for Canadian foreign policy. Canada certainly needs to work with other states to get things done. While not free of problems, NATO has proven to be a more effective and efficient conduit to serve Canada’s security interests compared to the United Nations. Canada’s commitment to the alliance of Western democracies is probably the best option since it
is rare that Canada’s interests and those of the US or NATO strongly diverge. Yet this carries the risk of getting sucked into fights our allies want but which have little to do with Canada’s security interests, and if such a situation were to occur in the immediate future the CF would be even more hard-pressed as it copes with steep budget cuts. Being the alliance’s eager beavers has gained Canada a great deal of influence and credibility within NATO, and leveraging this into tangible outcomes will mean not being shy about taking credit.

The problem of identity in Canadian foreign policy, however, has led to an incoherence which threatens to undermine the legitimacy and effectiveness of foreign policy decision-making. Some of this could be seen in negative reactions when Gen. Hillier commented that the job of the CF is “to be able to kill people,” but the paradoxical vision of the CF as an armed force for peace should not be overstated. There has been a tendency to interpret poll findings such as those cited earlier to mean that public opinion is hopelessly quixotic on foreign policy issues and, therefore, these decisions are best made within the defence and security establishment echo chamber and then spun in a way that Canadians will mostly swallow it. Due to the fear that there are more votes to be lost than won in confronting deeply-ingrained national myths, political leaders have generally shied away from engaging the public in foreign policy discussions except to justify decisions which have already been made.

Indeed, this is part of a wider pattern of opacity and centralization in Ottawa’s decision-making. A lack of public engagement not only allows misconceptions like the peacekeeping myth to persist, but undermines the democratic legitimacy of foreign policy choices. When these choices involve soldiers being sent into harm’s way, this can increase the danger since it encourages adversaries to believe that resolve is weak and they can force withdrawal by focusing their efforts on causing Canadian casualties. Moreover, the fear of backlash may well be unfounded; Gen. Hillier’s public influence and popularity grew because he was seen as the only leader giving the public the straight goods about why Canadian soldiers were fighting and dying in Kandahar. Nonetheless, this ought to have been a role filled by the elected ministers of the Crown responsible for these matters. These matters of state cannot just blow in the winds of public opinion, but if the government really thinks Canadians will decisively reject a military deployment if it were clearly and honestly explained, it is almost certainly the wrong decision.

Conclusion

Respect and credibility is necessary for Canada to have the influence and moral authority which allows it to exceed the possibilities of its limited hard power capacities. But simply following along with the Americans and NATO is no substitute for a coherent foreign and defence policy, or a clear idea of what Canada’s interests are. The apparent tendency for attempts at conveying multiple messages to different audiences, through the words and actions of Canada’s foreign and defence policy, is problematic. The most important of these problems is that it needlessly politicizes issues and introduces a muddle where clarity is needed. Foreign Affairs has become just another portfolio through which Prime Ministers have shuffled a parade of short-tenured ministers—seven in the last ten years. Canada has been able to get away with these deficiencies because our fortunate strategic position means there is no pressing imperative to correct them, but can this incoherence really be sustained indefinitely?

The way forward is for national interests and ideals to be realigned. Upholding the moral legitimacy of the current world order suits Canada’s security and prosperity, and that means constructively contributing to its capability to solve humanitarian crises. Neither can it be complacently assumed that the era of inter-state war is over; encouraging a universally acceptable international status quo will be key to forestalling the resurgence of great power rivalries. These understandings would form a good starting point on the path towards a foreign policy vision for Canada which achieves a wide consensus on what our interests are and what needs to be done to pursue them.

The views expressed are those of the author and do not necessarily reflect the views of the Institute or its members.

Notes
8 Stein and Lang, The Unexpected War, chp. 10.
9 Rick Hillier, A Soldier First: Bullets, Bureaucrats and the Politics of War (Toronto: HarperCollins, 2009), 9; 263.
10 Ibid., 343.
13 Hillier, A Soldier First, 331.
With the threat of piracy on the rise in the Gulf of Guinea, the Nigerian Navy has undergone a period of rapid development, becoming one of Africa’s leading naval powers. Most of the vessels now employed by the Nigerian military are corvettes and patrol cutters, well-suited to the task of intercepting pirate skiffs in coastal waters. The success in quickly improving Nigerian capabilities to address piracy can in part be attributed to the United States military and its Excess Defence Articles system; for example the NNS Thunder, which now serves as the flagship of the Nigerian Navy, was once a US Coast Guard cutter before decommissioning and transfer to Nigeria in 2011.

But the emergence of Nigerian seapower has carried with it some unforeseen consequences. To some degree, pirates have retreated into the Niger Delta, preying on shipping further inland, such as the abduction in October 2013 of two American sailors from a freighter near the Nigerian port of Brass.1 But the increased patrols by the Nigerian Navy seem to have displaced the majority of pirates to the waters of neighbouring countries that lack the naval power necessary to counter this sudden influx of armed bandits. This has had a particularly negative impact on the economies of Benin and Togo. Indicative of this impact, due to the increase in vessel insurance premiums for shipping companies using the docks at the Beninese port of Cotonou, vessel traffic there has dropped 70% since 2011.2 More than half of Benin’s government revenue is drawn from port fees and custom duties, 80% of which comes from Cotonou. Whereas Benin was once an attractive pit stop for freighters and oil tankers travelling between Europe and Africa, it has simply become too risky to stop in Cotonou.

There has been some attempted push-back from the Beninese and Togolese governments. In September 2012, Togolese patrol boats successfully mobilized in time to repel pirates attempting to hijack a Maltese-flagged tanker entering Togolese waters from neighbouring Ghana.3 Togo has a number of other success stories, frequently involving the protection of tankers travelling eastward from Ghana. Meanwhile, Benin and Nigeria have begun to conduct joint patrols, though these are thus far too limited in scope and number to be a decisive factor in regional counter-piracy efforts.4

It should also be noted that there are glaring limits to what Benin and Togo will be able to accomplish on their own in the fight against piracy. According to the best information available, the Togolese Navy currently consists of only two patrol boats: the Kara and the Mono.5 Though Nigeria has certainly more coastline to patrol and secure than either Benin or Togo, the gap in capabilities drives home how ill-equipped these neighbours are to address the problem of displaced pirates. In comparison to Togo’s two patrol boats, the Nigerian Navy boasts a MEKO 360 frigate produced in Germany, the US Coast Guard cutter re-commissioned as the NNS Thunder, four patrol cutters also obtained from the US Coast Guard, four additional corvettes, 27 in-shore patrol boats, and numerous other specialist vessels, such as minesweepers and troop transports. Even if the Beninese and Togolese governments possessed the financial resources to develop their naval forces in earnest, it would be several years before these countries would be in a position to contribute significantly to the security of international shipping along the West African coast.

However, there may yet be a solution to the piracy predicament. In September 2013, it was announced that the US private maritime security firm AdvanFort would assume partial responsibility for the security of Beninese waters, conducting counter-piracy operations wherever possible.6 AdvanFort, which has recently rebranded itself as AdvanFort International amid the increased global demand for private maritime security services, has successfully conducted counter-piracy operations in the Gulf of Aden and the Gulf of Oman for many years. AdvanFort has attracted some controversy, however, such as the revelation that one of the company’s suppliers provided AdvanFort with firearms without the proper export license in 2011, leading to a fine and two-year probation period from the United States government.

The services of AdvanFort International could be precisely what Benin needs to regain the confidence of international shipping firms and their insurers, bringing that much-needed traffic back to Cotonou. If Togo were also to turn to the services of AdvanFort or another contractor, this would obviously put even further pressure on the region’s pirates. But this is a short-term solution for the Gulf of Guinea, and a more sustainable approach to counter-piracy is urgently needed if a resurgence of pirate activity in future years is to be avoided. Drawing inspiration from NATO’s ‘smart defence’ concept and using Benin’s joint patrols with the Nigerian Navy as a foundation, the regional Economic Community of West African States (ECOWAS) could forge an effective system of defence sharing. Under such a system, the Nigerian Navy might take charge of counter-piracy efforts along the Togolese and Beninese coasts, while Benin and Togo could in turn contribute more troops to the regional brigade of the African Standby Force, a multinational rapid response force. This would in some respects be similar to the cooperation that is seen in NATO’s Baltic Air Policing Mission, where Baltic airspace is secured by air assets from other NATO member states in exchange for the levying of outsized land forces by the Estonian, Latvian, and Lithuanian militaries.

Pursuing Pirates in the Gulf of Guinea

by Paul Pryce

Paul Pryce is a Junior Research Fellow at the NATO Council of Canada (formerly the Atlantic Council of Canada) where he is part of the Maritime Nation Program. He is also a member of the Conflict & Terrorism Unit at Consultancy Africa Intelligence.
There have been some hopeful signs that West Africa is moving in this direction. In June 2013, an ambitious summit in Cameroon led to the adoption of by the ECOWAS memberson states of two critical documents: a Code of Conduct on Counter-Piracy Efforts, and a Memorandum of Understanding on Maritime Security. A month later, naval chiefs from thirteen West African countries gathered in the Nigerian port city of Calabar to further articulate a regional counter-piracy strategy and exchange best practices in maritime operations. This dialogue may be precisely what is needed to bring about defence sharing, or at least the intensification of joint patrols.

That ECOWAS and the nearby Economic Community of Central African States (ECCAS) have been able to even carry out these preliminary discussions is a distinct advantage West Africa has over the Horn of Africa, where the lack of functioning state institutions in some crucial countries has necessitated an intervention by the wider international community. This is not to say that the Horn of Africa lacks a regional organization on the level of ECOWAS or ECCAS; the Intergovernmental Authority on Development (IGAD) has fulfilled a similar role of fostering regional integration since its inception in 1986. But its member states lack either the capabilities or the political will to become actively engaged in counter-piracy efforts. For example, Somalia continues to experience instability, while Eritrea renounced its IGAD membership in 2007 during an intense territorial dispute with neighbouring Ethiopia. Aside from Djibouti, the remaining IGAD membership does not have any coastline on the Gulf of Aden (Sudan and Kenya) or simply does not have any coastline at all (Ethiopia, South Sudan, and Uganda).

If West African countries can pull together a concrete framework for defence sharing, the Gulf of Guinea will be well-positioned to avoid the worst of what has unfolded in the Gulf of Aden. International partners are actively investing in the development of Nigeria – and Ghana to a lesser extent – as the maritime bulwarks of West Africa. As previously mentioned, the Nigerian Navy has already received several decommissioned American vessels through the Excess Defence Articles system, but further contributions are expected soon. A former US Navy survey ship and a US Coast Guard cutter of similar specifications to the NNS Thunder are due to be delivered in early 2014. International backing has allowed the Nigerian and Ghanaian navies to contract Nautic Africa, a shipbuilder based in Cape Town, South Africa, to produce a total of seven Fast Multi-Role Patrol Vessels. But the US must also be careful in its engagement with West Africa; investing too heavily in Nigeria’s maritime capabilities could entrench the country’s role as a hegemon, deepening some resentment toward Nigeria among smaller neighbours and undermining the regional interdependence that has traditionally kept Nigerian expansionist impulses in check.

Should the US seek to transfer additional resources to the region, it would be well-served by introducing a policy of conditionality. Namely, the provision of future vessels should only be approved if tangible progress is made in developing the regional counter-piracy framework and if Nigeria commits to expanding its assistance to Benin and possibly Togo. This would be preferable to directly transferring decommissioned vessels to Benin and Togo as neither country has the personnel, know-how or financial resources to maintain maritime forces beyond their current complements of patrol boats. While Ghana’s forces are robust, Nigeria has the institutional foundation which can be built upon with the right application of incentives by international actors. But in the absence of enforced conditionality, Nigerian policymakers will be tempted to regard displaced pirates as simply a problem for Benin and Togo to address independently. The inclusion of joint training opportunities with American personnel could sweeten the deal and improve Nigerian counter-piracy capabilities at the same time; the Africa Partnership Station program and the Africa Maritime Law Enforcement Partnership are both initiatives which have produced positive outcomes in Liberia and other countries further out from the Gulf of Guinea proper.

Piracy is the latest in a slew of challenges to West Africa’s economic and social development. Benin and Togo have bought the region some valuable time by enlisting the services of private maritime security contractors like AdvanFort International. 2014 will be the year to build on the momentum ECOWAS has attained with the adoption of the Memorandum of Understanding on Maritime Security and the Code of Conduct on Counter-Piracy Efforts. Complacency, on the other hand, risks giving pirates and organized crime time to regroup further down the line, drawing out the threat to international shipping and deepening the damage to the region’s economy. In short, the Gulf of Guinea will not be another Gulf of Aden, but with some careful course correction it can be a success story for Africa.

The views expressed are those of the author and do not necessarily reflect the views of the Institute or its members.

Notes

3. Togolese Navy thwart pirate attack, defenceWeb, 13 February 2012.
5. Official site of the Togolese Armed Forces: forcesarmees.tg (available in French only)
78 days; the 2006 Israel-Lebanon War ended after 33 days; and post-electoral violence in Kenya in 2008 abated within two months. By the time Parliament is able to meet again to consider whether to commit troops, the crisis in question is likely to have come to an end, or other states may have filled the gap, as occurred with Germany in Afghanistan after the collapse of the Dutch government in 2008. The Australian intervention in the Solomon Islands is also often “cited as an example where prompt and decisive action was needed, and where a parliamentary approval process would have disadvantaged Australia’s strategic position.”

The two scenarios presented earlier raise questions about the ascendancy of subjective, objective, and effective control of the armed forces. What would happen if the Executive and Parliament were in disagreement over a military deployment, and the military leadership deems that is it within their area of responsibility as concerns their soldiers’ lives to intervene in the debate? While the Constitution Act unambiguously allows Cabinet to declare war or commit troops to a military operation without even consulting with Parliament, could the armed forces acquiesce with Parliament? In Canada, the officer corps is legally responsible for the lives of the troops they command; this overriding liability will always generate a demand for both policy and mandate clarity and timeliness. Generals and Flag Officers will therefore fill any perceived vacuum in producing the strategic guidance they require to accomplish their mission.

The exercise of subjective and objective civil control are indisputably linked. The military cannot impose upon itself professional standards without clear and unambiguous political direction from civilian leaders. This strong political direction “allows a nation to base its values, institutions, and practices on the popular will rather than on the choices of military leaders, whose outlook by definition focuses on the need for internal order and external security.” The prerogative to declare war and to commit troops to foreign deployments should remain within the realm of the Executive to ensure that senior military officers can continue to subject themselves to objective civil control. Interested Parliamentarians have enough outlets available to them as it is to partake in dynamic civil oversight of the military. An examination of the powers and responsibilities accorded to Parliament (such as budget oversight, participation in debates and committee enquiries) demonstrates that there are sufficient outlets to enable interested Parliamentarians to partake in dynamic civil oversight of the military and to hold the Executive to account on its defence policy, including its decision to wage war. While parliamentarians contribute to the implementation of subjective control, their primary function is to hold the Executive to account, rather than to hold the prerogative to declare war. The greatest risk to the stability of Canadian civil-military relations rests in the political ambiguity that such votes may create if the outcome is to set Parliament in opposition of the will of the Executive, thereby creating a policy vacuum space that could be filled by the military. As a result, I conclude that Parliament’s aspiration to vote on all future military missions is unjustifiable.

The views expressed are those of the author and do not necessarily reflect the views of the Institute or its members.

Notes
4. Ibid, p.15.