

Conference of Defence Associations Institute
12TH ANNUAL GRADUATE STUDENT SYMPOSIUM

Date: 30-31 October 2009

Towards total defence: An examination of international responses to non-traditional threats and its implications for Canada

Submitted by:

George Heng

Master of Strategic Studies candidate,

Centre for Military and Strategic Studies,

University of Calgary

Introduction

The dynamics of conflict have evolved drastically in recent times. Apart from the traditional threat of conventional war, nations have to contend with non-traditional threats that may not necessarily require the use of arms, and that can target the populace in subtle but far-reaching ways. These threats may be ends in themselves, or precursors to subsequent armed conflicts. The primary objective of this paper is to examine the issue of non-traditional warfare within the context of total defence as a response strategy.

The paper shall be divided into three parts: The first attempts to provide a working definition of “non-traditional threats” and a typology for characterizing such events. The second portion examines a cross section of international responses to these potential threats; for example, the formation of the Department of Homeland Security in the US or the implementation of the “Total Defence” concept in countries like Singapore. The third and final section provides a contextual analysis of the responses and suggests a best practices approach for countries yet to develop or fully implement a “total defence” policy.

What are non-traditional threats?

From the perspective of national security, a non-traditional (or unconventional) threat is distinct from a conventional one in two major aspects. First, it features unusual forms of conflict, including terrorism and guerrilla actions; in terms of weaponry, this could include the use of CBRN¹ weapons or weapons of mass destruction (WMDs). Second, non-traditional threats are further characterized by the use of new or novel forms of technology in both attack and defence. Technology in this respect refers not only to tools, weapons and hardware, but also to the methods and institutions required to apply

¹ Chemical, Biological, Radiological and Nuclear

them effectively.² As such, non-traditional warfare (NTW) embraces a wide range of contingencies, possibilities, techniques and weapons. For the purposes of this discussion however, we refer to non-traditional warfare as the “unconventional forms of conflict that are characterized by the use or application of new or novel forms of technology.” Within this context, NTW can be broadly classified into two categories: biological and electronic. Each of these parent categories shall be examined in due course.

Biological NTW

Some of the more exotic accounts of biological NTW include the use of insects as weapons, whether as agricultural pests, direct agents or as transmitters of disease (disease vectors).³ One historical account has the Mongol Kahn Janibeg ordering flea-infested, disease-ridden corpses catapulted into the city of Kaffa in 1343. The inhabitants of the city withdrew by sea, along with their disease-riddled rats and accompanying fleas, and, by docking at various ports in the Mediterranean, inadvertently brought the plague to Europe. By 1350, a pandemic was raging in the continent; twenty-five million people were indirect casualties of Janibeg’s entomological war.⁴ Nightmare scenarios about genetically altered mosquitoes that can transmit the AIDS virus have also been postulated, and – given technological advances and the globalization of terrorism – are not as far-fetched as one might think.⁵

While the use of insects and biological warfare is related, the latter can be more appropriately defined as “the use of a biological organism or biologically derived toxin or

² Schilling, *Nontraditional Warfare*, xv

³ Lockwood, *Six-Legged Soldiers*, 5

⁴ Lockwood, *Six-Legged Soldiers*, 52-54

⁵ Lockwood, *Six-Legged Soldiers*, 5

other substance to cause lethal or incapacitating effects.⁶ This definition can be further expanded to include the killing or damaging of animals or plants for military⁷ or political objectives. The use of biological agents and pathogens is also not without precedent. During the First World War, Germans developed anthrax, glanders⁸, cholera and wheat fungus for use as biological weapons. In the Second World War, the Japanese conducted bio weapons experiments on Chinese prisoners and exposed more than 3000 victims to plague, anthrax, syphilis and other agents.⁹ Perhaps the most infamous of these were the experiments of General Ishii Shiro and his Unit 731. As a result of experiments, field tests, and attacks with biological weapons, the Japanese killed a total of 580,000 Chinese.¹⁰

The United States (US), Britain, former Soviet regime and Canada have all conducted research and field-testing in bio weapons at one point or another.¹¹ More recently, in 1971, Cuba accused the US of unleashing an African swine fever epidemic (which resulted in the culling of 500,000 pigs), and in 1997, of spraying crops with biological agents.¹² During the Cold War, the US made detailed plans to destroy staple crops of its adversaries, like wheat in Russia and rice in China.¹³ It is estimated that the US spent approximately \$14.5b on biowarfare related research, during fiscal years 2001-2004.¹⁴ Ironically, the anthrax that caused the US panic in 2001-2002, resulting in 32 exposures and four deaths¹⁵ was a weapons-grade strain generated by the US military, the most

⁶ Kalia, *Bio-Terrorism: Threat Perception*, 85

⁷ Guillemin, *Biological Weapons*, 2

⁸ A disease that primarily affect horses, but can be transmitted to humans and other animals

⁹ Kanwal, *Biological Warfare Agents: Defining the Threat*, 54

¹⁰ Lockwood, *Six-Legged Soldiers*, 104

¹¹ Ketkar, *Biological Weapons: A Chronology*, 198

¹² Ketkar, *Biological Weapons: A Chronology*, 200

¹³ Gautam, *Biological Weapons and Bio-Terrorism*, 126

¹⁴ Boyle, *Biowarfare and Terrorism*, 53

¹⁵ Ketkar, *Biological Weapons: A Chronology*, 201

likely source of which was one of its own labs at Fort Detrick, Maryland.¹⁶ Indeed, it has been argued that the US biotech industry's lobby efforts, and the government's active involvement in biological "defense" programs may very well be the breeding ground and source of future incidents.¹⁷

As a non-traditional threat, in terms of efficacy, biological weapons are the weapons of choice since they are characterized by low visibility, high potency, substantial accessibility and relatively easy delivery.¹⁸ In 1997, US Secretary of Defense William Cohen emphasized that an equivalent five-pound bag of anthrax, if sprayed over Washington DC would kill half its population.¹⁹ Proliferation also appears to be on the rise, according to Rutgers University molecular biologist Richard H. Ebright, who in a 2005 publication estimated that over 300 scientific institutes and 12,000 individuals have access to pathogens suitable for biowarfare and terrorism.²⁰

Agricultural and environmental weapons, while a subset of biological warfare, can be no less destructive or malicious, albeit in different ways. In one example, the introduction of the seemingly harmless water hyacinth to Africa's Lake Victoria led to the creation of "a breeding ground for the water snail that transmits schistosomiasis²¹ and diarrhoeal disease organisms.²²" In addition, a single plant can multiply into millions in a year and upset the ecosystem, decimating the fish stock, leading to famine and other consequences.²³ The intrusion of alien species into local habitats can also have long-

¹⁶ Boyle, *Biowarfare and Terrorism*, 13

¹⁷ Boyle, Boyle, *Biowarfare and Terrorism*, 31, 39-43

¹⁸ Kalia, *Bio-Terrorism: Threat Perception*, 85

¹⁹ Guillemin, *Biological Weapons*, 161

²⁰ Boyle, *Biowarfare and Terrorism*, 30

²¹ A disease caused by parasitic worms that breed in certain species of water snails

²² Gautam, *Biological Weapons and Bio-Terrorism*, 131

²³ Gautam, *Biological Weapons and Bio-Terrorism*, 132

standing, devastating effects on the environment, for example, the arrival of rats via ships in Seychelles and New Zealand, hedgehogs in Scotland, rabbits in Australia and the Asian longhorn beetle in North America.²⁴

The exchange of ships' ballast is another means through which biological war can be waged, with undesirable consequences for the environment. This is an effective mode of transmission as it is difficult to trace the originator and source of contamination – approximately 10 billion tonnes of ballast water are transferred each year across the world.²⁵

Electronic NTW

Where biological non-traditional weapons target organic matter, electronic non-traditional weapons target computer hardware, software or infrastructure. Computing is such an integral part of society, that the survivability of information infrastructure is vital to our everyday life. In this respect, there are three basic types of threats to information systems: theft, corruption and destruction.²⁶

Information theft occurs when computer “hackers” gain unauthorized access to data through cyber attacks. In typical cases, the hackers may use the data for personal financial gain, or not at all. Breaking into a database to steal credit card information or industrial secrets are examples of information theft and may be undertaken by individuals or groups (e.g. in organized crime). In more serious cases where the attacks are planned and financed by an adversarial state, hackers can breach networked

²⁴ Gautam, *Biological Weapons and Bio-Terrorism*, 132

²⁵ Gautam, *Biological Weapons and Bio-Terrorism*, 138

²⁶ McDonnell, *Information Systems Survivability in Nontraditional Warfare Operations*, 30

communications and sensor systems, steal confidential designs or even secrets pertaining to national security.

As opposed to “brute force” attacks, where a hacker would try multiple combinations of passwords to gain access to a system, a more sophisticated approach would be to deploy a “Trojan horse” following a breach. The latter is a program that is inserted into the host system and remains hidden until the information collected is retrieved by the attacker.²⁷

The second type of threat involves attacks that are aimed at the deliberate corruption of information. For example, the attacker would insert false data (or algorithms) in order to deceive, paralyse or manipulate the system.²⁸ If the number “4” were replaced with “5”, all subsequent calculations would be rendered unreliable and inaccurate. In extreme cases, the corrupted data could lead to malfunctions, or even deactivation (or activation) of weapons systems or defences, which potentially lethal consequences.

In the third type of threat, hackers can destroy information or even the system itself, depending on the level of access they have. The most common method is to plant a computer “virus” into the system. The virus is a program with malicious code that self-replicates and often can “infect” other systems and storage devices through data sharing or transfer. Viruses may also be used as carriers of “logic bombs”, which are executable programs designed to activate based on specific external triggers.²⁹

²⁷ McDonnell, Information Systems Survivability in Nontraditional Warfare Operations, 30

²⁸ McDonnell, Information Systems Survivability in Nontraditional Warfare Operations, 32

²⁹ McDonnell, Information Systems Survivability in Nontraditional Warfare Operations, 31

Other examples of malicious programs include “mutating” viruses, programs that can “defend” themselves by altering their nature during replication, and “worms”, which travel from host to host until they reach their intended targets. The latter is an executable program disguised as a legitimate file or attachment that typically “disappears” when run. Upon reaching its intended destination, the worm completes its mission.³⁰ Worms may carry a Trojan horse, virus, logic bomb or some combination thereof.

To summarize, non-traditional threats are characterized by unconventional conflicts that feature new or novel use of various technologies. These threats can be broadly categorized into biological and electronic non-traditional warfare. The former can include the use of bio weapons like anthrax, insects as disease vectors, agricultural and environmental contamination, and the incursion of alien species, while the latter encompasses the attacking of informational infrastructure through various electronic means, in the hope of stealing, corrupting or destroying information. The weapons used in non-traditional warfare can be directed at both military and civilian personnel or infrastructure, although one could argue that the individuals or organizations employing NTW would target civilian populations and centres for maximum publicity and effect.

Apart from the above applications, other potential NTW scenarios can include:

- a. Attacking water/power supply infrastructure of major cities
- b. Contaminating food or medical supplies
- c. Dispersing poisonous chemicals in public areas or heating³¹
- d. Propaganda, sedition or other forms of psychological operations

³⁰ McDonnell, Information Systems Survivability in Nontraditional Warfare Operations, 32

³¹ McDonnell, Information Technology Applications to Counter Nontraditional Warfare Threats, 123-124

In the next section, we shall examine the concept of total defence as a response to NTW and various countries' strategies to counter the array of non-traditional threats that exist today.

Total Defence Strategies

Total Defence is a mobilization strategy that involves both civilian and military sectors in joint efforts to maintain national security through public safety. It was conceptualized as a means to manage civil emergencies as a result of natural disasters, hazards,³² and by extension, non-traditional warfare. Total Defence is characterized by centralized command and control, shared national objectives and multilateral cooperation across government, military and civilian agencies (at least in theory). As Total Defence is designed to manage civil emergencies, it is a cornerstone in the development of a strategy to counter non-traditional warfare.

A number of countries³³ practice some variation of Total Defence as an extension of their national defence policy, and typical components include the armed forces, civil defence (including police), economic defence, psychological defence, health care, and emergency planning.³⁴

In the United States, following the events of September 11, Congress approved the creation of the Department of Homeland Security (DHS) by uniting twenty-two agencies in 2002.³⁵ While the DHS was formed in response to 9/11 to protect the American way of

³² Yost, *Peace Through Security*, 4

³³ Countries like Sweden, Denmark, and Norway are good examples. Yost, *Peace Through Security*, 25

³⁴ Yost, *Peace Through Security*, 27, 38, 52

³⁵ White, *Terrorism and Homeland Security*, 396

life and instil a culture of awareness,³⁶ the agency is well positioned (at least theoretically) to counter the kinds of non-traditional threats discussed in this paper. Towards this end, the DHS contains elements that coordinate or oversee the following: science and technology, intelligence and analysis, legal issues, civil liberties, public affairs, immigration and border security, law enforcement, nuclear detection, transportation security, cyber security, FEMA,³⁷ the US Secret Service and the US Coast Guard.³⁸

In the case of Sweden, a large land mass and a sparsely populated country necessitated the adoption of a Total Defence policy that involved all sectors of society.³⁹ Despite the fact that the country is non-aligned in peacetime and neutral in wartime, Sweden recognized that its continued independence hinged upon its ability to defend itself from both foreign and domestic threats. Its Total Defence components include the armed forces, civil defence, economic defence, psychological defence, and emergency planning.

The DHS equivalent in Sweden is the MSB⁴⁰, which is part of a larger national defense network that includes collaboration with, and support from, the defense force's Military Intelligence and Security Unit (MISU), the National Security Service, the military's National Defense Radio Establishment (Försvarets Radioanstalt/FRA), and the National Defense Research Agency and the National Intelligence Commission.⁴¹ Sweden has a

³⁶ Department of Homeland Security, One Team, One Mission, Securing our Homeland, 4

³⁷ Federal Emergency Management Agency

³⁸ Department of Homeland Security, One Team, One Mission, Securing our Homeland, 38-39

³⁹ Yost, Peace Through Security, 27

⁴⁰ MSB or Myndigheten för Sam-hällsskydd och Beredskap. O'Dwyer, Defense News, 12 October 2009

⁴¹ O'Dwyer, Defense News, 12 October 2009

part volunteer, part professional army, and all citizens between the ages of 16 and 65 may be called upon to serve in civil defence roles.⁴²

In contrast, Singapore is a densely populated country with a small land mass⁴³. Its concept of Total Defence was based and adapted from Swedish and Swiss models and comprises five aspects: Military Defence, Civil Defence, Economic Defence, Social Defence and Psychological Defence.⁴⁴ Introduced in 1984, the objective of Total Defence was to augment the country's conscripted regular army and provide a framework to respond to non-traditional threats:

...destroying social cohesion by exploiting differences in race, language, religion, culture, social or economic class; weakening national resilience by using psychological warfare to play on the people's fears and apprehensions; or waging economic warfare through economic boycotts, trade sanctions or acts of sabotage to bring down the economy.⁴⁵

Implications

Although developing a unified strategy for combating those who employ non-traditional weapons presents enormous complexities on civil, legal, military, bureaucratic, political, ethical and operational levels, a Total Defence approach is nonetheless a sound framework for security and emergency planning. The US Department of Homeland Security aptly summarizes the challenges that it – and other adopters of Total Defence – continues to face:

⁴² Yost, *Peace Through Security*, 27

⁴³ 710 sq km. Statistics Singapore, <http://www.singstat.gov.sg/stats/keyind.html#popnarea>

⁴⁴ http://www.totaldefence.sg/imindef/mindef_websites/topics/totaldefence/about_td.html

⁴⁵ http://www.totaldefence.sg/imindef/mindef_websites/topics/totaldefence/about_td.html

1. Clarifying, defining, and communicating leadership roles, responsibilities, and lines of authority at all government levels;
2. Strengthening accountability systems that balance the need for fast, flexible response with the need to prevent waste, fraud, and abuse;
3. Consolidating efforts to integrate the Department's critical mission of preparedness; and
4. Enhancing our capabilities to respond to major disasters and emergencies, including catastrophic events, particularly in terms of situational assessment and awareness, emergency communications, evacuations, search and rescue, logistics, and mass care and sheltering.⁴⁶

In developing a Total Defence policy, other questions have to be addressed as well:

- What is the organizational framework of the lead agency, and is it robust enough, given its mandate?
- What are the critical nodes⁴⁷ (military and civilian) and are they represented in the lead agency?
- What kinds of early warning indicators are required, and how can they be operationalized?
- What are the required partnerships with civilian agencies and support networks and what types of resource models can be developed (e.g. acquiring laboratories for chemical analysis)?
- What is the communications policy when dealing with the media and the public?
How can the media be employed as a strategic resource in times of emergency?
How is information to be disseminated internally and externally?

⁴⁶ Department of Homeland Security, One Team, One Mission, Securing our Homeland, Letter from the Secretary, 2008

⁴⁷ E.g. Healthcare, postal services, the media, transportation, agriculture and food security, etc.

- What are the ways of engaging the public and enhancing preparedness in peacetime?
- How can the international community be engaged to mitigate the threat from non-traditional weapons?

Conclusion

“In general, in battle one engages with the orthodox and gains victory through the unorthodox.” *The Art of War*⁴⁸

Although Total Defence has been adopted as a means to prevent, manage and counter the effects of terrorism, it can also be deployed as a strategy to mitigate the influence and impact of non-traditional weapons and threats. As the nature of modern-day conflict continues to evolve, and new scenarios of non-traditional warfare continue to emerge, the question is not if Total Defence would be adopted as part of national security policy, but when, and how.

⁴⁸ Sun Tzu, *The Art of War*, 187

References

- Boyle, Francis A. *Biowarfare and terrorism*. Atlanta: Clarity Press, 2005
- Chandran, Suba. Non-State Actors in South Asia: Who will use Bio-Weapons and Against Whom? *Bio-Terrorism and Bio-Defence* P.R. Chari, Suba Chandran, eds. New Delhi: Manohar Publishers & Distributors, 2005
- Gautam, P.K., Biological Weapons and Bio-Terrorism. *Bio-Terrorism and Bio-Defence* P.R. Chari, Suba Chandran, eds. New Delhi: Manohar Publishers & Distributors, 2005
- Guillemin, Jeanne. *Biological Weapons*. New York: Columbia University Press, 2005
- Kalia, V.M., Bio-Terrorism: Threat Perception. *Bio-Terrorism and Bio-Defence* P.R. Chari, Suba Chandran, eds. New Delhi: Manohar Publishers & Distributors, 2005
- Kanwal, Gurmeet, Biological warfare Agents: Defining the Threat. *Bio-Terrorism and Bio-Defence* P.R. Chari, Suba Chandran, eds. New Delhi: Manohar Publishers & Distributors, 2005
- Ketkar, Prafulla, Biological Weapons: A Chronology. *Bio-Terrorism and Bio-Defence* P.R. Chari, Suba Chandran, eds. New Delhi: Manohar Publishers & Distributors, 2005
- Lele, Ajey. Biological Weapons and Bio-Terrorism: Meeting the Threat. *Bio-Terrorism and Bio-Defence* P.R. Chari, Suba Chandran, eds. New Delhi: Manohar Publishers & Distributors, 2005
- Lockwood, Jeffrey A. *Six-Legged Soldiers: Using Insects as Weapons of War*. New York: Oxford University Press, 2009.
- McDonnell, Michael D. Information Technology Applications to Counter Nontraditional Warfare Threats. *Nontraditional Warfare: Twenty-First Century Threats and Responses*. William R. Schilling, ed. Dulles: Brassey's Inc., 2002
- McDonnell, Michael D. and Terry L. Sayers. Information Systems Survivability in Nontraditional Warfare Operations. *Nontraditional Warfare: Twenty-First Century Threats and Responses*. William R. Schilling, ed. Dulles: Brassey's Inc., 2002
- Swiss Neutrality and Security*. Marko Milivojevic and Pierre Maurer, eds. Providence: Berg Publishers, 1990
- Tzu, Sun. *The Art of War*, Ralph D. Sawyer, trans. Boulder: Westview Press, 1994.
- White, Jonathan R. *Terrorism and Homeland Security*. Belmont: Wadsworth Cengage Learning, 2009
- Yost, William J. *Peace through Security: A Total Defence Approach*. Ottawa: Conference of Defence Associations, 1987.

Internet references:

Department of Homeland Security. One Team, One Mission, Securing our Homeland: US Department of Homeland Security Strategic Plan, Fiscal Years 2008-2013.

http://www.dhs.gov/xlibrary/assets/DHS_StratPlan_FINAL_spread.pdf

O'Dwyer, Gerard. Defense News, Published 12 October 2009.

<http://www.defensenews.com/story.php?i=4321230>

Singapore, Total Defence, 30 December 2008.

http://www.totaldefence.sg/imindef/mindef_websites/topics/totaldefence/about_td.html