

ANALYSE DE
L'INSTITUT DE LA CAD



CDA INSTITUTE
ANALYSIS

THE CONFERENCE OF DEFENCE ASSOCIATIONS INSTITUTE

L'INSTITUT DE LA CONFÉRENCE DES ASSOCIATIONS DE LA DÉFENSE



Canada's Defence Policy and the New Security Challenges of Terrorism and Cyber Warfare

by
Dur-e-Aden

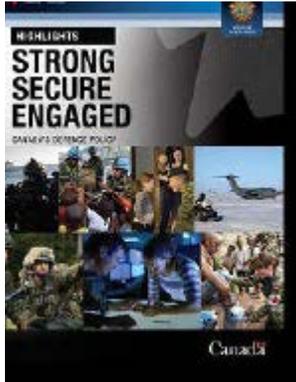
August | août 2017

This article is one of a series of short, focused analyses of the new Canadian Defence Policy "Strong, Secure, Engaged" which was launched in June 2017. In this article, CDA Institute Student Research Assistant Dur-e-Aden discusses the policy from the perspective of terrorism and cyber warfare.

BGen (Ret'd) Matthew Overton MA

Research Director and Senior Editor /

Directeur de la recherche et Editeur en chef



Introduction

Terrorism and cyber warfare in today’s world are often termed as new security challenges. While the issue of terrorism is not new, its evolving speed has made it difficult for states to proactively deal with this threat. Moreover, as the recent US elections illustrated, state actors can significantly influence outcomes in another state in the cyber arena. Considering these changing security dynamics, no defence policy can be complete until it addresses both these issues comprehensively. Hence, the purpose of this analysis is twofold: First, to provide a brief overview of how the threats of terrorism and cyberwarfare are addressed in the new Canadian Defence Policy “Strong, Secure, Engaged.” Second, to identify issues which are not explicitly addressed, yet should be considered as this policy is put into practice.

While focusing on the borderless nature of these problems, “Strong, Secure, Engaged” clearly recognizes that the distinction between domestic and international threats is becoming less relevant.¹ Locally, “individuals have engaged in promoting violence online, radicalizing peers, recruiting and fund-raising.”² Globally, violent extremism is a scourge that is an attack on Canadian values,³ and the evolving cyber arena is making the threat environment more lethal and complex.⁴ Thus, the policy predicts three future conflict trends while accounting for the importance of non-state actors: 1) the changing nature of the conflict, where non-state actors have shown greater willingness to use violence to achieve political ends; 2) the evolving balance of power, where power is now diffusing from states to non-state actors; 3) and the rapid evolution of technology, which makes it easier for non-state actors to influence outcomes to their liking.

What Does the Policy get Right?

Because of the evolving and unpredictable nature of these new security challenges, the policy clearly articulates that Canada needs to be strong at home. To ensure that strength, “Strong, Secure, Engaged” outlines **four** relevant steps for this discussion.

¹ Canada’s Defence Policy. “Strong, Secure, Engaged” (2017). Available at <http://dgpapp.forces.gc.ca/en/canada-defence-policy/docs/canada-defence-policy-report.pdf>. p. 14

² Ibid., p. 53

³ Ibid., p. 49

⁴ Ibid., p. 38

First, in the domestic arena, Canadian armed forces will be assisting local law enforcement while dealing with the threat of terrorism.⁵ While there are protocols in place that govern CAF's role in assisting local law enforcement, the policy does not clearly identify the *threshold* where a domestic terrorism incident would warrant military involvement, leaving the issue of possible over-reaction unaddressed once this policy is being translated into action. The case of France illustrates this problem. The state of emergency enforced since the Paris attacks of 2015 has come under intense criticism from the UN and Human Rights Organizations for employing arbitrary procedures, restricting freedom of speech and association, and breaching several fundamental freedoms of citizens.⁶ Within Canada, the RCMP commissioner, Bob Paulson, has presented parallel fears related to the militarization of police which can increase the reliance on force, "rather than the problem-solving, community-oriented, prevention approach that is better suited to the Canadian context."⁷ Although "Strong, Secure, Engaged" recognizes that "counter-radicalization and community outreach efforts are necessary to deal with this problem at home,"⁸ it is vague on what could be the responsibilities of the Canadian Armed Forces when it comes to community engagement. Therefore, Government of Canada has more work to do in terms of providing a specific framework for DND regarding its collaboration with other government departments while working on domestic security issues such as community engagement.⁹

Second, the policy provides armed forces a clear mandate to use hard power in the international realm for Canadian defence, and recognizes the importance of actions such as gathering good intelligence and engaging in defence diplomacy.¹⁰ As a result, the policy includes multiple global initiatives such as: i) participating in multilateral initiatives and capacity building of other nations to defeat terrorism; ii) investing in joint intelligence, surveillance and reconnaissance both nationally and internationally; iii) working with transnational partners, particularly in the Middle East, to address the threat from violent extremist organizations; iv) increasing the number of Special Operations Forces; v) and developing a combat ready military force, along with intelligence experts who collect, analyze and disseminate information.

⁵ Ibid., p. 86

⁶ Pierre-Louis Caron. "UN Rights Experts Say France's State of Emergency Imposes 'Excessive Restrictions'." *Vice News*. January 20, 2016. Available at <https://news.vice.com/article/un-rights-experts-say-frances-state-of-emergency-imposes-excessive-restrictions>

⁷ Lee Berthiaume. RCMP commissioner expresses fears over militarization of police forces." *Global News*. February 6, 2017. Available at <http://globalnews.ca/news/3231792/rcmp-commissioner-expresses-fears-over-militarization-of-police-forces/>

⁸ "Strong, Secure, Engaged." p. 53

⁹ It is important to note that at some instances, this issue will require DND to collaborate with relevant provincial and municipal departments as well, and not just other federal departments.

¹⁰ "Strong, Secure, Engaged." p. 49; p. 93

Nevertheless, while good and actionable intelligence is identified as an important component of both local and global aspects of counter-terrorism, the policy does not clearly spell out the relevant requirements for experts who will be required to engage in this endeavor. Due to the ever-changing and non-military nature of terrorism and cyber threats, there will be an increasing need to employ *civilian* analysts with area and linguistic expertise within DND and government at large who will be responsible for collecting and analyzing the required intelligence. Therefore, going forward, Government of Canada would need to do two things to attract the best talent in this arena: 1) reexamine their hiring policies to clearly layout the requirements for public servants interested in working within the intelligence analysis field of DND, and 2) provide opportunities that signal the diverse needs of the DND which extend beyond individuals in uniform.

Third, “Strong, Secure, Engaged” addresses the topical issue of investing “in a range of remotely piloted systems, including an armed aerial system capable of conducting surveillance and precision strikes.”¹¹ While the policy makes clear that the use of this system (commonly referred to as drones) will follow both domestic and international law,¹² and the CAF have a clear framework in place to support kinetic targeting decisions,¹³ the defense policy itself it does not present a framework of directly *communicating* these issues to the public to prevent misinformation from informing the debate regarding their use. If the US drone policy is any indication, misinformation has the potential to quickly spread in relation to two questions:

- a) Who is the target of the “precision strikes?” (sometimes referred to as targeted killings in the public discourse).

In the public’s imagination, the use of the term “targeted killing” invokes the notion of people being targeted because of the availability of this tool while government bypasses the option of capture.¹⁴ As a result, the term itself, and the platform associated with it, become synonymous with indiscriminate targeting of militants and civilians alike. Therefore, it is the responsibility of the Government of Canada to clarify to the public that any form of targeted killing is not a drone issue, but a combat issue. Drones are just another platform in the military arsenal, similar to a piloted aircraft in the sky or a sniper rifle.

¹¹ “Strong, Secure, Engaged.” p. 73

¹² Ibid.

¹³ Canadian Forces Joint Publication, CFJP 3-9, Targeting 1st Edition, Promulgated: 12 December 2014.

¹⁴ The focus here is on the ordinary public not aware of all the nuances of military operations, not the experts in the field. The public debate regarding drones in the US evolved in this manner even while the administration argued that it followed all the necessary legal and ethical procedures. See for example, <https://www.aclu.org/issues/national-security/targeted-killing>

While using *any* of these platforms, an individual is only targeted after a *lawful* decision regarding their elimination has been made. Certainly, in those instances, a targeted strike is better than an *untargeted* one.¹⁵

Of course, this gives rise to a much complicated second question:

- b) how a target is chosen in the first place, particularly in modern conflicts where the distinction between combatants and civilians is significantly blurred?

The current conflicts involving insurgency and terrorism are changing rapidly, but the law of armed conflict is lagging far behind. For example, in 2015, when a 21-year-old British Citizen, Reyaad Khan, was killed by an RAF drone strike in Syria, the debate that followed in UK illustrated the complexity of this issue. The UK's PM at the time, David Cameron, told the house that "the lethal drone strike in Syria was 'a new departure': the first time, in modern times...that a British military asset had been used in a country in which the UK was *not involved* in a war" (emphasis added).¹⁶ The strike therefore, was part of the government's *counter-terrorism* strategy whose goal is to disrupt and prevent plots against the UK. On the other hand, his statement was contradicted on the same day by the UK's Permanent Representative to the UN who argued that the action had been taken in the "collective self-defense of Iraq... and was merely a conventional use of force abroad by the UK in an armed conflict in which the UK was already involved."¹⁷ The disagreement on which laws and policies govern the use of this platform within one country illustrate the urgent necessity of aligning our laws with technological innovations. Moreover, clarification of law is important not just for the public, but for officials involved in these decision-making processes. UK's Parliament's joint committee on Human Rights argued that "ongoing uncertainty about the Government's policy might leave front-line intelligence and service personnel in considerable doubt about whether what they are being asked to do is lawful, and may therefore expose them, and Ministers, to the risk of criminal prosecution for murder or complicity in murder."¹⁸ These concerns were also articulated at the international level by the UN's Special Rapporteur on extrajudicial, summary or arbitrary executions who noted that while drones are not illegal weapons, countries need to guard against the wide and permissive interpretations of international legal regimes, and underline their transparency and accountability obligations.¹⁹

¹⁵ Brooks, Rosa. "What's not wrong with drones." *Foreign Policy*. September 5, 2012. Available at <http://foreignpolicy.com/2012/09/05/whats-not-wrong-with-drones/>

¹⁶House of Lords, House of Commons, Joint Committee on Human Rights. "The Government's policy on the use of drones for targeted killing." Second Report of Session 2015-2016. Available at <https://www.publications.parliament.uk/pa/jt201516/jtselect/itrights/574/574.pdf> p. 5

¹⁷ Ibid.

¹⁸ Ibid. p. 6

¹⁹ United Nations General Assembly. "Report of the Special Rapporteur on extrajudicial, summary or arbitrary executions." September 13, 2013.

Hence, while there are legitimate questions to be asked regarding the use of drones, it needs to be communicated to the public that the focus should be on the *interpretation of laws* governing their use, as opposed to *solely on the platform*. Additionally, debating these questions will ultimately benefit Canada in the long run. As Minister Freeland's recent foreign policy address made clear, Canada's interest as a middle power is in an international order based on rules where powerful countries are constrained.²⁰ As Canada criticizes actors such as Russia and ISIS for their violation of territorial integrity and borders, it would not want to lose moral high ground for being accused of the same thing. Kremlin backed media often uses the issue of US drones and its lack of respect for international law and borders to criticize western nations.²¹ In the age of fake news and alternative facts, *perception* is becoming more important than reality. Therefore, it is very important to not lose public trust while using a platform which is designed to defend them from terrorist threats in the first place.

Fourth, while recognizing the importance of the cyber arena, "Strong, Secure, Engaged" articulated the need for Canada to adapt "a more assertive posture in the cyber domain by hardening our defenses, and by conducting active cyber operations against potential adversaries in the context of government-authorized military missions."²² While Canada's previous cyber policy has been criticized for not assigning clear responsibilities to different departments depending on their mandate, the new defence policy, along with Bill C-59, addresses this issue. The defence policy clearly identifies that the military will be working within the bounds of set military missions and will not be targeting foreign governments, whereas Bill C-59 has given CSE a proactive mandate to target threats that fall outside the realms of preapproved military missions.²³ The division of responsibilities between the two entities according to their mandates ensures that while dealing with cyber threats, Canada's cyber policy has both defensive and offensive postures. Moving forward, there will be a need to coordinate both policies to create mechanisms for deconfliction and to avoid redundancy.

Available at <https://www.justsecurity.org/wp-content/uploads/2013/10/UN-Special-Rapporteur-Extrajudicial-Christof-Heyns-Report-Drones.pdf>

²⁰ "Address by Minister Freeland on Canada's foreign policy priorities." June 6, 2017. Available at https://www.canada.ca/en/global-affairs/news/2017/06/address_by_ministerfreelandoncanadasforeignpolicypriorities.html

²¹ John Horgan. "U.S. Lacks Moral Authority to Criticize Russia for Intervening in Ukraine." *Scientific American*. March 2, 2014. Available at <https://blogs.scientificamerican.com/cross-check/us-lacks-moral-authority-to-criticize-russia-for-intervening-in-ukraine/>

²² "Strong, Secure, Engaged." p.15

²³ Amanda Conolly. "CSE getting 'proactive' mandate overhaul in major national security reform bill." *ipolitics*. June 20, 2017. Available at <https://ipolitics.ca/2017/06/20/goodale-pitches-panel-of-experts-in-major-national-security-reform-bill/>

What is missing?

In addition to above mentioned policy elements which directly deal with the new security threats, there are **five** issues which need to be addressed while preparing for a “Strong, Secure and Engaged” defence of Canada, even if they don’t directly fall under the mandate of DND.

First, while the defence policy discusses counter-radicalization efforts, there is no discussion regarding the *process* of radicalization, and at what points the counter-radicalization efforts are most useful to prevent it. Since the policy emphasizes a “whole-of-government” approach throughout the document, where the Department of National Defense is mandated to work alongside Public Safety, Global Affairs, and organizations under their umbrella,²⁴ one can expect the defence policy to be clearer regarding which department *it will be working with* on the critical issue of counter-radicalization. Generally, Public Safety Canada has taken the lead in dealing with preventing violence extremism within Canada, as was evident in the recent opening of the Canada Centre for Community Engagement and Prevention of Violence.²⁵ Going forward, this research based center can provide important insights for the DND regarding junctures where its involvement is most needed.

Second, while the policy mentions terrorist groups “sponsoring or inspiring” attacks as a threat,²⁶ it doesn’t consider the increasing sophisticated nature of ISIS “remote controlling” attacks. In these instances, ISIS central is often *directing* individuals till the last minute, even as they appear lone wolves in the first instance.²⁷ While such an attack has not happened in Canada yet, recent events in Europe show ISIS’ reach. As part of the defence policy is to anticipate threats, it is important that while implementing this policy, the government adapts a wider initiative (of which DND is an important part) to prepare for thwarting such attacks before they become normalized and disturb social peace between communities.

Third, while meaningful community outreach is presented as one of the solutions to deal with the problem of radicalization, there is no specification as to which “community” needs to be engaged; this is particularly important as while groups like AQ and Daesh are mentioned specifically, there is no mention

²⁴ “Strong, Secure, Engaged.” p. 89

²⁵ Public Safety Canada. Canada Centre for Community Engagement and Prevention of Violence. More info available at <https://www.publicsafety.gc.ca/cnt/bt/cccepv-en.aspx>

²⁶ “Strong, Secure, Engaged.” p. 53

²⁷ Rukmini Callimachi. “Not ‘Lone Wolves’ After All: How ISIS Guides World’s Terror Plots from Afar.” *The New York Times*. February 4, 2017. Available at https://www.nytimes.com/2017/02/04/world/asia/isis-messaging-app-terror-plot.html?_r=0

of the far-right terrorism. The Quebec City mosque attack in Canada, the Finsbury park attack on a mosque in UK, and the rise of far right within Western contexts illustrate that this issue cannot be ignored. A recent intelligence report by CBSA cautioned that right wing groups, such as the Soldiers of Odin in Canada, are “not afraid to use violence.”²⁸ Therefore, it is important that not any particular community, but the population as a whole is engaged and better educated about the threat of terrorism, regardless of its source and its impact on social harmony.

Fourth, while discussing the framework of “grey zone,” and the “hybrid conflict,” the policy explicitly mentions the use of cyber tools by adversaries to achieve strategic and operational objectives. However, there is no explicit discussion of how terrorism fits within this framework, and its impact on bilateral and multilateral relations between states. Considering the emphasis on Article 5 in Minister Freeland’s speech, and the threat of terrorism to both Canada and its allies, it is surprising that “Strong, Secure, Engaged,” doesn’t discuss the potential of this threat in dragging Canada into conflicts where it might not be directly threatened.

Additionally, the issue of “grey zone” becomes important in relation to countries who Canada wants to engage (e.g., Saudi Arabia), but who are also accused of sponsoring non-state terrorist groups which harm Canada and its allies. Since Canada’s current foreign policy framework is based on the principles of rule of law, human rights, territorial integrity, multilateralism and feminism, DND would need to work closely with Global Affairs while engaging with states who don’t always follow the principles that Canada wants to promote, and at the same time can be a source of global instability and threat to Canada.²⁹

Fifth, while discussing the cyber threat, “Strong, Secure, Engaged” does not define what would constitute a “cyber war,” and how will DND, along with its Government of Canada’s partners, attempt to resolve the issues of accountability due to the decentralized nature of this threat.³⁰ Moreover, the policy does not discuss the role of non-state actors and the private sector, who possess the expertise, and control most of the infrastructure in the cyber realm. These actors often compete with government to

²⁸ Stewart Bell. “Far-right Soldiers of Odin members ‘not afraid to use violence,’ intelligence report warns.” *Global News*. June 28, 2017.

Available at <http://globalnews.ca/news/3562798/far-right-soldiers-of-odin-members-not-afraid-to-use-violence-intelligence-report-warns/>

²⁹ For example, non-state actors who pose a threat in the realm of cyber and terrorism while being state-sponsored by countries such as Russia and Saudi Arabia. For more, see here: “Fighting, While Funding, Extremists.” *The New York Times Editorial Board*. June 19, 2017.

<https://www.nytimes.com/2017/06/19/opinion/saudi-arabia-qatar-isis-terrorism.html>

³⁰ For example, see here: Andrew Higgins. “Maybe Private Russian Hackers Meddled in Election, Putin Says.” *The New York Times*. June 1, 2017.

<https://www.nytimes.com/2017/06/01/world/europe/vladimir-putin-donald-trump-hacking.html>

protect their trade secrets, as well as to maintain their competitive advantage. Therefore, these are not limited to the defence policy, rather, the Government of Canada must grapple with them in relation to their mandates for other departments as well. Government of Canada, including the DND, would require to engage and often partner with both these actors while dealing with cyber threats that can arise suddenly. While the priority is to attract young talent to work for the government, if the departments within the Government encounter difficulty while competing with the private sector, they can create creative programs in partnerships with the private sector, along with the legal framework, which will allow individuals with the requisite knowledge to lend their expertise to the government on contractual basis while at the same time protecting their identity as a “commercial actor” when they return to their old job.

Conclusion

Canada’s new defence policy clearly identifies new security challenges facing the country, and the steps that are required to deal with them. It also categorizes the local and international dimensions of the borderless threats of terrorism and cyber, and recognizes that different contexts require different responses. However, given that the policy document is flexible enough to accommodate changing trends as it is put in practice, “Strong, Secure, Engaged” should be viewed as a strong starting point, as opposed to the final word.

Dur-e-Aden is a PhD student and a SSHRC CGS Doctoral Scholar in the Department of Political Science at University of Toronto, Research Assistant at the CDA institute, and a Junior Researcher affiliated with Canadian Network for Research on Terrorism, Security and Society (TSAS). She holds a MA in Political Science from the University of British Columbia. Her research focuses on the recruitment patterns of both men and women in terrorist/insurgent groups. She can be contacted at aden.dur.e.aden@mail.utoronto.ca.

**CHAIR OF THE BOARD |
PRÉSIDENT DU CONSEIL**

Major-General Daniel Gosselin,
CMM, CD (Ret'd)

**CHIEF EXECUTIVE OFFICER
| PRÉSIDENT-DIRECTEUR
GÉNÉRAL**

Tony Battista

**SERIES EDITOR | RÉDACTEUR
DE LA SÉRIE**

BGen Matthew K Overton (Ret'd), MA

ABOUT THE SERIES |

À PROPOS DE LA SÉRIE:

CDA Institute Analyses are a series of short policy briefs that explore topical security and defence issues of interest to Canadians. Views expressed here are those of the authors and do not necessarily reflect those of the CDA Institute.

Les Analyses de l'Institut de la CAD sont une série de courts exposés de politique qui explorent des questions de sécurité et de défense pertinentes aux Canadiens. Les opinions exprimées sont celles des auteurs, et ne reflètent pas nécessairement les opinions de l'Institut de la CAD.

Copyright © 2017

Conference of Defence Associations Institute

The Conference of Defence Associations Institute is a charitable and non-partisan organisation whose mandate is to provide research support to the CDA and promote informed public debate on security and defence issues and the vital role played by the Canadian Armed Forces.

Conference of Defence Associations Institute

151 Slater Street, suite 412A
Ottawa, Ontario K1P 5H3
613 236 9903
www.cdainstitute.ca

All logos and trademarks used are the property of their respective holders.

Use in this publication is under non-commercial and normative fair use provisions of applicable Canadian law.

Institut de la Conférence des associations de la défense

L'Institut de la Conférence des associations de la défense est un organisme caritatif et non partisan dont le mandat est de fournir l'appui de recherches à la CAD, et de promouvoir le débat public sur les questions de sécurité et de défense, et le rôle essentiel des forces armées canadiennes.

Institut de la Conférence des associations de la défense

151 rue Slater, bureau 412A
Ottawa (Ontario) K1P 5H3
613 236 9903
www.cdainstitute.ca

Tous les logos et les marques de commerce utilisés sont la propriété de leurs détenteurs respectifs.

L'utilisation qui en est faite dans cette publication l'est en vertu des dispositions de la loi canadienne applicable sur l'utilisation équitable non commerciale et nominative.

ANALYSE DE
L'INSTITUT DE LA CAD



CDA INSTITUTE
ANALYSIS

The CDA Institute was created in 1987, with charitable status, to provide research support to the CDA and to promote informed public debate on security and defence issues and the vital role played by the Canadian Armed Forces.

CONFERENCE OF DEFENCE ASSOCIATIONS INSTITUTE /
L'INSTITUT DE LA CONFÉRENCE DES ASSOCIATIONS DE LA DÉFENSE

151 Slater Street, suite 412A , Ottawa, Ontario K1P 5H3
Phone / Téléphone: +1 (613) 236 9903

 @CDAINstitute |  www.cdainstitute.ca