JURISDICTIONAL CHALLENGES IN THE 21ST CENTURY SECURITY ENVIRONMENT: SUBNATIONAL DESIGN-BASIS THREATS

William McAuley, Centre for Military, Security and Strategic Studies, University of Calgary[1]

Abstract

What security and intelligence strategies do subnational governments require to protect themselves and the social, cultural, economic, and safety interests of their citizens? Although subnational governments wield important levers in areas now inhabited by an expanding array of domestic and foreign threat actors, few have any coherent security and intelligence culture, architecture, or strategy. This paper seeks to address the conspicuous absence of discourse on contemporary subnational security challenges, suggesting that subnational security strategies are an inescapable requirement of the 21st century security environment. Given that the inception of any form of polycentric security strategy with an enabling architecture and culture is a complex undertaking, the utility of the design-basis threat concept is explored to provide a tangible starting point for evaluation of key drivers for analysis in the contemporary subnational security environment. A simplified framework for a provincial-level design-basis threat analysis is proposed as a gateway to deeper analysis.

Introduction

What security and intelligence strategies do subnational governments require to protect themselves and the social, cultural, economic, and safety interests of their citizens? Although subnational governments wield important levers in areas now inhabited by an expanding array of domestic and foreign threat actors, few have any coherent security and intelligence culture, architecture, or strategy. A healthy discourse on contemporary subnational security challenges is also conspicuously absent in Canada, which should be concerning given the well-recognized effects of globalization at local and regional levels. Traditional jurisdictional assumptions in the national security domain have been blurred by the "spatio-temporal dimensions of globalization" (Held, McGrew, Goldblatt, & Perraton, 2003, p. 68)[2], namely extensity (stretching), intensity, velocity and impact.

---

[1] McAuley is a Canadian Armed Forces veteran and graduate of the University of Calgary's Centre for Military, Security and Strategic Studies (CMSS). McAuley is currently employed in a public security role with a provincial government. The author can be contacted at wjmcaule@ucalgary.ca.

[2] Held et al. characterize globalization as encompassing four elements: a *stretching* of political, economic, and social activities across political frontiers; an *intensification* of

Global drivers such as the international order's return to near-peer competition and exponential growth in attack surfaces brought on by the Fourth Industrial Revolution call for cohesive institutional and public resiliency across all levels of government. Yet, a mismatch between the evolving subnational threatscape and "inconsistent and uninformative" (National Security and Intelligence Committee of Parliamentarians, 2020, pp. 65, 105) federal engagement with provincial, municipal, and Indigenous governments is readily apparent.

Within a traditional monocentric view, whereby federal government policies, strategies, and agencies provide the required safeguards and 'steer' subnational systems to meet national security objectives, provincial/territorial, and municipal governments merely respond to local manifestations of criminal, public order, and public health threats. Subnational governments do not hold primary jurisdictional responsibilities for national security matters[3] from a constitutional or legislative perspective, as the distribution of legislative powers in sections 91/92 of the *Constitution Acts,* the *National Defence Act,* and *Security Offences Act* sensibly enshrine national security strategy as a federal responsibility. However, the structural, spatial, and operational complexities of the 21st century security environment are arguably more consistent with an increasingly polycentric national security system (Canadian Security Intelligence Service, 2020).

While a reasonable response to complexity, the incorporation of polycentric interests within Canada's national security system is not without potential repercussions. Observers might challenge the "heterogeneous field of menace" (Boyle & Dafnos, 2019, p. 81) justification for expansion of subnational governments into the national security space as a dangerous infringement of liberty. Growing intelligence infrastructure, the "civilianization of military concerns," and "creeping militarization of civilian governance" (Boyle & Dafnos, 2019, p. 81) are legitimate civil liberty concerns. Unanticipated iatrogenic effects of interventions within the national security space can indeed be more acute and require careful consideration. Without a doubt, balancing these concerns with the fundamental responsibility to protect and advance the

interconnectedness within flows of finance, trade, culture, migration, and culture; increased *velocity* in the diffusion of goods, information, ideas, people, and capital; and the *blurring* of boundaries between domestic matters and global affairs. The evolution of these elements continues to shape the national security threat environment. (Held, McGrew, Goldblatt, & Perraton, 2003, pp. 67-68)

[3] "Militia, Military and Naval Service, and Defence" under s.91 of the *Constitution Acts,* 1867 to 1982.

physiological and safety needs[4] of all citizens is paramount for all levels of liberal democratic governance (Hancock, 2015). Failure to use reasonable care to prevent foreseeable physical, social, and economic harms from a growing mismatch between national security systems and the threat environment would represent negligence. Hence, subnational security strategy is arguably an inescapable, yet overlooked component of the contemporary security environment.

It would be entirely naïve to believe that the inception of any form of subnational security strategy with an enabling architecture and culture is a simple undertaking. Strategy formulation is complex, and rather than being known for timely adaption and innovation, Colin Gray's observation of "strategic theoretical parasitism"[5] persists within Canada's record of strategic thought.[6] A more tangible starting point is required. This paper will, therefore, explore a deceptively simple question: What are the design-basis threats upon which subnational governments should design their security strategies and safeguards?[7]

Design-Basis Threat

Design-basis threat—a profile of the type, composition, and capabilities of an adversary—may appear to be an overly tactical and technical perspective for discourse on issues of national security concern, but there are two key reasons why this concept has disguised utility. First, it is a means to avoid the traditional jurisdictional merry-go-round that, although it may pass through the subnational space, is driven by, attended from, and always starts and stops within the federal domain. This is not to say that there is no jurisdictional element to the design-basis threat, as there is most certainly a 'government backstop' component. Its utility is in getting one's hands dirty drilling down into the muck of what it means to protect something in the real world, notwithstanding existing jurisdictional boundaries. Second, a solution to this rather concise question is intrinsically complex, in that it involves pulling at multiple threads in order to unweave the situational fabric. There are at least five interdependent elements of analysis underlying a solution set to the design-basis threat question: *Criticality* – what

[4] The 'basic needs' within Maslow's hierarchy of needs (Maslow, 1943).
[5] Gray argued that the long-term effectiveness of Canada's national defence and foreign policies were being mortgaged as a result of "dependence for intellectual nourishment upon the debates of others" (Gray, 1971, p. 7).
[6] For a detailed discussion of Canadian strategic thought, see (McAuley, 2017).
[7] Design-basis threat (DBT) is a common methodology used for high-risk applications, such as the protection of nuclear materials and facilities (International Atomic Energy Agency, 2009) and designing buildings to resist blast loading (Canadian Standards Association, 2017).

assets or systems need protecting? *Adversarial* – from whom are we protecting targets? *System Performance* – how well do we need to protect targets? *Ascendency* – who is responsible for determining criticality and protective system performance? And, *Jurisdictional* – who is responsible for protecting targets?[8]

Figure 1

The Design Basis Threat Method[9]

Figure 1 provides a simplified representation of the design-basis threat threshold in relation to a general threat spectrum and the responsibility for protection. Nassim Taleb's concept of a 'black swan' event—an unpredictable event that is beyond what is normally expected of a situation and has potentially severe consequences—has been incorporated to loosely portray an upper limit of threat mitigation (Taleb, 2007). It is reasonable to allow that an asset or system defender's cost/benefit analysis must have an upper limit of protection against highly improbable - extreme consequence threats.

Aside from possible negligence and incompetence factors, it is also reasonable to deduce that at a facility, local or regional level, the rational risk appetite will loosely align with some expectation (real or perceived) of a government 'backstop' at the upper end of the threat spectrum. Asset owners and operators commonly prefer to cede responsibility for protecting against extraordinary threats, such as those associated with national emergency (Emergency Preparedness Canada, 1991, p. 17) or sophisticated nation state actors (Hoaglund, 2015, p.13), to law enforcement and government.

[8] These elements have been informed and adapted from a system performance approach for security effectiveness analysis (Hoaglund, 2015, p. 7).
[9] Adapted from (Hoaglund, 2015).

Vital Points & Critical Infrastructure

An upper limit of risk responsibility is evident in initiatives such as the U.S. Terrorism Risk Insurance Act (TRIA). Enacted following the 11 September 2001 attacks, the U.S. federal government acts as an insurer of last resort to ensure access to terrorism risk insurance for commercial property and casualty losses resulting from certified acts of terrorism (US Department of the Treasury, 2020). While Canada has not implemented a similar government-backed terrorism insurance scheme (McMillan LLP, 2015), the various forms of the Vital Points Programme (VPP) that ran from 1914 until the 1990s,[10] and subsequent critical infrastructure programming, provide a tangible example of government backstopping. Alongside private sector owners and operators, federal, provincial, and territorial governments, and local authorities share risk management responsibilities for "processes, systems, facilities, technologies, networks, assets, and services essential to the health, safety, security or economic well-being of Canadians and the effective functioning of government" (Public Safety Canada, 2009, p. 2).

Beyond those national assets and systems considered critical for military operations and defence production, the protection of 'civil vital points' has historically been considered "a civil law and order function in which the owners or occupants [are] responsible for providing the normal, first line protection. The various levels of government having jurisdiction [are] responsible for the provision of appropriate emergency response and backup protective services" (Geddes, 1988, p. 5). Physical threat was generally gauged based on an evaluation of the intent of an actor, coupled with their capability to carry out an attack (Office of Critical Infrastructure Protection and Emergency Preparedness, 2003). During war or serious civil crisis, RCMP or military resources would have been tasked to provide protective services from the design-basis threat of "sabotage by means of an attack by a single well armed adversary or a small similar group of 2 to 6 persons approaching from outside the facility" (Emergency Preparedness Canada, 1991, p. 8).

According to Geddes (1988), reconsideration of this conventional design-basis threat started to occur in the late 1980s, acknowledging that:

[10] In 1970, the Wartime Vital Points List was augmented by the creation of a Peacetime Vital Points List. The RCMP, who were responsible for security surveys of the wartime vital points, was made responsible for coordinating security surveys for the peacetime list. Collaboration with provincial authorities was coordinated through Canada Emergency Measures Organization machinery (Privy Council Office, 1970).

> The fence, padlock and security guard will no longer provide adequate protection during times of war and serious civil crisis. Consequently, a shift is required in thought processes from World War II era protection to protection from sabotage in a high-tech era characterized by computer crime, mass destruction terror and mind manipulating communications. (p. 5)

Although situationally dependent in terms of criticality and consequence factors, this limit of reasonable protection is rapidly shifting upwards and outwards in concert with a contemporary threat spectrum of increasing breadth and depth. 'Top-up' emergency response and the deterrence effect of a Mountie or militia member with a rifle guarding the perimeter of an industrial facility are clearly no longer logical defences in an age of cyber threats to software supply chains (Cybersecurity and Infrastructure Security Agency, 2020) and industrial control systems (Ginter, 2018).

Although partnership across all levels of society have taken various forms over time, the exponential growth in the criticality and adversarial elements cause a rapid greying-out of the historical boundary assumptions within the ascendency and jurisdictional elements. Given the multitude of interdependencies of current infrastructure systems within both physical and informational domains, trying to assemble a coherent list of critical assets and associated jurisdictional interests quickly overwhelms analytical resources. Protection of privately-owned assets and systems in a complex world is increasingly a self-help problem, whereby the upper limit of reasonable protection is a business decision unbounded by any government defined performance metric or tangible backstop. There is merit in expecting critical infrastructure governance to self-adapt to the security environment by ingraining characteristics such as heterogeneity, modularity, redundancy, responsiveness, feedback loops, adaptive mechanisms, trust, and reciprocity within managerial and operational systems (Reeves, Levin, & Ueda, 2016).[11] However, governments cannot fully offload responsibilities for due

[11] As conceived by Reeves *et al*. in relation to corporate survival: *Heterogeneity* involves ensuring a sufficient "reservoir" of diversity amongst individuals, philosophies, innovations, and endeavors for new variations and combinations of adaptive units to emerge. *Modularity* refers to the presence of firewalled or loosely linked modular components that minimize the "contagion risk" of environmental shocks in one part of a system perpetuating throughout the entire ecosystem. *Redundancy* involves the overlapping of roles between components, such as the multiple lines of defence inherent to an immune system. *Responsiveness* acknowledges the fact that the emergent behaviour or properties of a complex adaptive system cannot be accurately forecasted. *Feedback loops* are critical as a means of detecting environmental changes and identifying advantageous adaption corridors by facilitating *adaptive mechanisms*

diligence where there are foreseeable forms of physical, social, or economic harm involved.

The questions of who decides and who acts within the *Criticality-Adversarial-System Performance-Ascendency-Jurisdictional* matrix is perhaps most visible in the modern critical infrastructure protection domain, but any expectation of a clear delineation of subnational security roles and responsibilities in other societal domains is also fleeting given the increasing impact of global drivers.

Global Drivers of 'Hometown Security'

Effective national security has shifted to incorporate simultaneous macro (national), meso (regional), and micro (local) arenas, as former U.S. Secretary of Homeland Security, Janet Napolitano, observed in 2010 during her remarks to New York city first responders; a switch from homeland security to "hometown security" (Department of Homeland Security, 2010, para. 10). Consider Infrastructure Canada's efforts to empower municipalities, local or regional governments, and Indigenous communities to adopt 'smart cities' (Government of Canada, 2020). While this certainly seeks to improve the lives of urban residents through innovation, data and connected technology, these advanced communications networks will also present dual-use opportunities to influence and manipulate the socio-cultural aspects of societies (Goldberg & Lee, 2020). Safeguarding open and democratic societies means securing this infrastructure from adversaries seeking to influence and subvert liberal democracies (Lee, Rasser, Fitt, & Goldberg, 2020). Unfortunately, these subnational governments generally lack an in-house capability to assess and defend against risks integral to the 'digital authoritarian toolkits' (Goldberg, 2020) being exported via initiatives such as China's Digital Silk Road. Determining the balance between improving the lives of urban residents, while avoiding the introducing of cost-effective technologies that have potential to subvert liberal democratic norms and values is a multifaceted task. Subnational governments must now contend with the local manifestations of "the weaponization of information technologies [that threaten] to jeopardize democracies' ability to govern and protect their national

---

that encourage "variation, selection, and propagation of innovations" through "iterative experimentation." *Trust* characterizes the need to foster cooperation between agents and aggregates within a complex adaptive system that has no central command and control mechanism. *Trust* interacts with critical mass, leadership, and knowledge to encourage sustainable self-organization. Acting in a manner that provides value to other agents or aggregates within the ecosystem encourages the development of *reciprocity* norms and enforcement mechanisms. (Reeves, Levin, & Ueda, 2016, pp. 50-55)

security, and to undermine people's trust in democracy as a system of government" (Rosenbach & Mansted, 2018, para. 2).

Weaponization of technology is not a novel concept characteristic to the 21st century. As Martin Van Creveld (1991) observed:

> …war is completely permeated by technology and governed by it. The causes that lead to wars, and the goals for which they are fought; the blows which campaigns open, and the victories with which they (sometimes) end; the relationship between armed forces and the societies that they serve; planning, preparation, execution, and evaluation; operations and intelligence and organization and supply; objectives and methods and capabilities and missions; command and leadership and strategy and tactics; even the very conceptual frameworks employed by our brains in order to think about war and its conduct – not one of these is immune to the impact that technology has had and does have and always will have. (p. 1)

What is unique about the 21st century, is that the information domain has become central to geopolitical competition. It is here that a crucial divide is forming between how democracies and autocracies perceive opportunities within the information space.

As autocracies see opportunities to gain advantage through shaping the information space, strategic influence operations are now an integral part of their geopolitical toolboxes. As Rosenberger and Gorman (2020a) note:

> Democracy is built on the crucial compact that citizens will have access to reliable information and can use that information to participate in government, civic, and corporate decision-making. The technologies of the Information Age were largely built on the assumption that they would strengthen this compact. However, as typified by Russia's ongoing use of information operations against the United States and Europe, key information technologies have evolved quickly over the past five years and been weaponized against democracies. The trajectory of data-driven technologies, including machine learning and other aspects of artificial intelligence, will increase the scale, complexity and effectiveness of adversary information operations. As technology advances, and as geopolitical and ideological tensions between democratic and

> authoritarian states rise, information operations are likely to become more numerous, insidious, and difficult to detect. (p. 75)

A non-kinetic battle for the survival of democratic discourse is playing out within the social fabric of local communities. While democracies often claim a level of resilience against this 'strategic contest of values' (Rosenberger & Gorman, 2020b), it represents a concerning new national security paradigm towards vulnerable subnational arenas.

The onset of the Fourth Industrial Revolution (4IR) is accelerating this paradigm shift through the convergence and integration of digital, biological, and physical systems. The resulting societal transformations affect the incentives, rules, and norms of economic life, impact on human identities, communities, and political structures, and provide incentives and opportunities for weaponizing market access and global supply chains (Schwab, 2018). The conditions being set by the 4IR are also driving a displacement of the military domain by the economic and technological as the primary realms of geostrategic competition (Cheney, 2019). This has been a significant factor in the international order's return to near-peer competition between the United States and China, which has shifted the field of geostrategic play into domains of civil society (United States House Permanent Select Committee on Intelligence, 2020). Where diplomacy was once the exclusive domain of diplomats and carried out 'over there', hostile foreign interests are now being injected directly into the subnational domain.

This shifting of strategic technological competition towards civil society has also coincided with a particularly dangerous vulnerability, a digital fragmentation of the social topographies of liberal democracies. Dubbed 'virtual societal warfare', the evolution of advanced information environments is degrading classic forms of information security and subjecting populations to new forms of social manipulation. New forms of cyber aggression have been facilitated by a public bias in digital culture towards cheaper negative stimuli and a move from an online advertisement model to behavioural modification (Mazarr, Bauer, Casey, Heintz, & Matthews, 2019). A rise of machine learning algorithms biased towards data patterns versus normative values and socio-cultural rules facilitates propagation and reinforces in-group dynamics, cognitive bias, and extreme overvalued beliefs via online echo chambers and filter bubbles. This fragmentation of social topography expands the limits of exploitation, thereby allowing persistent targeting in the micro arena to have strategic effects.

The *Resocline*

The foremost danger of the apparent national security paradigm shift is that the threat spectrum has broadened in the places where the least number of defensive resources exist.[12] There is something akin to a *thermocline*—the zone where the temperature of the ocean begins to decrease rapidly with depth—that occurs at subnational levels of governance. National security resources tend to be concentrated in a thin *surface layer*, where the water temperature (i.e., resources) remains rather uniform and subject to continual mixing from waves and tides (i.e., organizational critical mass) and solar heating (i.e., policy attention). As one moves into the provincial and municipal domains, a '*resocline*'—a rapid decline in security resources and situational understanding—occurs. Framing in an oceanic sense facilitates a complementary analogy to the *shadow zone* in anti-submarine warfare–a zone in which little sound from a particular source can penetrate, usually because of refraction of the sound rays. Without delving into the science of sonar propagation, sound velocity profile, surface ducts, and sonic layer depth, the point is that the dynamics of sound and environmental conditions create a shadow zone that is a favoured depth for submarines to operate. An optimum depth to operate at can be calculated to remain invisible to active sonar of a surface ship (i.e., national security resources). Much of the activity of the 21st century security environment is arguably occurring within a subnational shadow zone.

The Informational Element

The existence of a subnational shadow zone was identified in relation to the antiquated Vital Points Program. Geddes (1988) observed that:

> the main limitation in the Canadian Vital Points Program is the practice of self-help, amateur security intelligence estimates. It provides a dangerous base for the contingency planning of the protection of the nation's vital points, and must be replaced by the professional security intelligence processes. (p. 5)

This highlights a sixth element of the design-basis threat problem – the *Informational* component that underlies the entire *Criticality-Adversarial-System*

[12] Resources refers not only to security risk management personnel, but the capability to generate situational understanding across the analytical spectrum – to include descriptive (Who? What? Where? When? How?), explanatory (Why?), evaluative (What does it mean?), and estimative analysis (What happens next?). (Pherson & Pherson, 2013, p. 48)

Performance-Ascendency-Jurisdictional matrix. As a threat and risk assessment based upon available intelligence generally underlies any design-basis threat process (Canadian Standards Association, 2017), access to sufficient quantity and quality of information, intelligence, and technical knowledge is a prerequisite for all lines of convergent analysis.

The importance of the informational component highlights a significant problem. While the threat environment has intensified the need for increasingly complex design-basis threat analysis at local and regional levels, the *resocline* hampers the availability of bespoke security intelligence estimates at these levels,[13] and this allows adversaries to operate within the subnational shadow zone without much defensive friction. This situation is the justification for the need for subnational governments to develop security and intelligence strategies to protect themselves and the social, cultural, economic, and safety interests of their citizens.

Factors for an Estimate

There is no default design-basis threat upon which subnational governments can design their security strategies and safeguards. An ever-evolving solution set is what must ultimately result from this line of inquiry, and this is well beyond the scope of a single paper. This is a complicated process for even a small-municipality, and an extremely complex endeavour at a regional or provincial level. However, what can be offered here is a simplified framework for identifying the key factors to be incorporated into such estimates. Figure 2 provides a sense of what considerations should be a part of a provincial-level design-basis threat analysis.

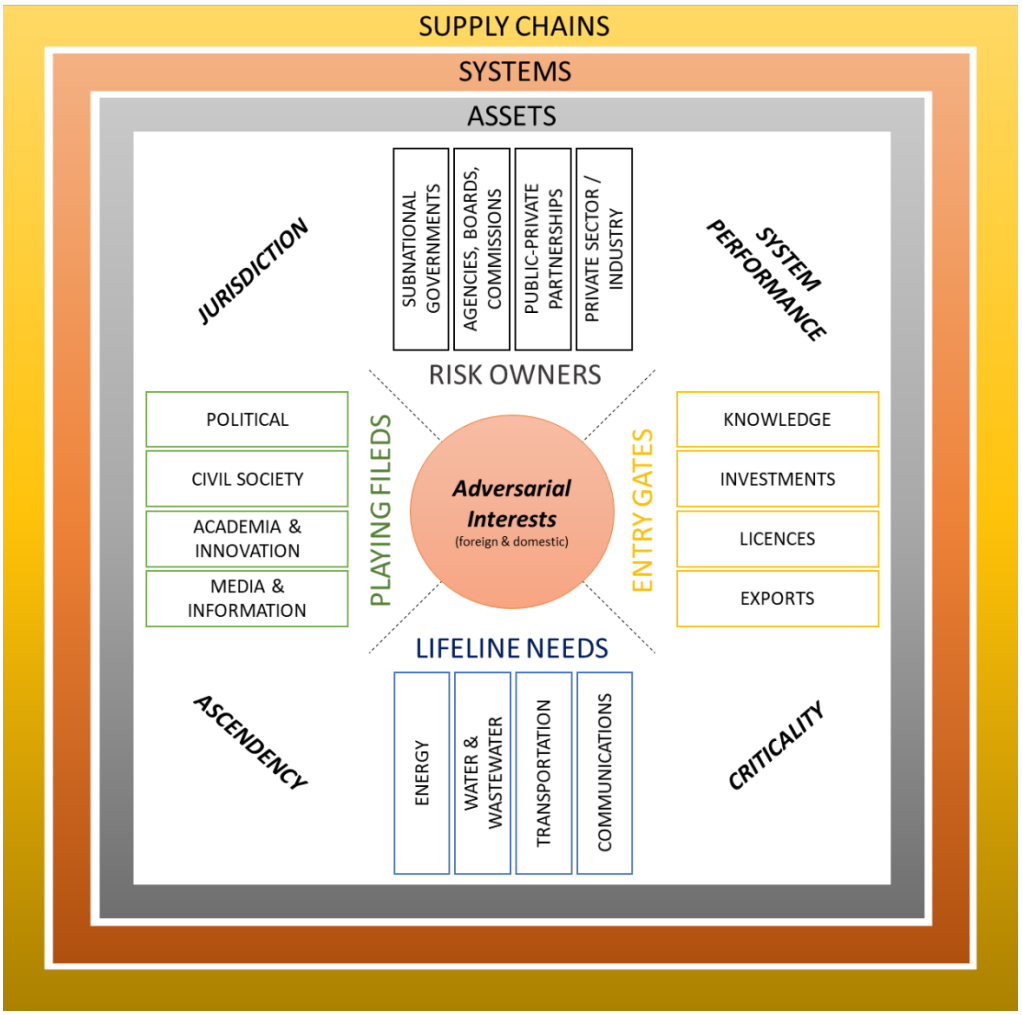
At its core, the framework is based on a quartet of factors, each with a quartet of sub-factors. Consideration must be given to the interrelations between the four principal risk owners: subnational governments who hold policy levers and public safety responsibilities; public agencies, boards, and commissions who act as regulators, financial gatekeepers, or knowledge brokers; public-private partnerships that governor interfaces and operate between boundaries; and the private sector / industry that own and operate infrastructure, drive innovation,

[13] There is a general assumption here that although federal agencies are engaged, they often lack the level of fidelity on local conditions, assets, and interests required to provide anything beyond generic estimates.

and provide the economic base. These entities will own a unique set of interlocking risks within aggregated asset, system, and supply chain layers.

Figure 2

Simplified Framework for a Provincial-level Design-basis Threat Analysis



Identification of the set of risks for each 'risk owner' requires consideration of the criticality (what needs to be protected?) and ascendency (who is responsible for determining criticality and performance?) factors against societal lifeline needs and potential adversarial entry gates. For simplicity, the standard ten critical infrastructure sectors are reduced to the four lifeline functions—energy, water/wastewater, communications, and transportation—whose reliable operations are so critical that a disruption or loss of one of these functions will

directly affect the security and resilience of critical infrastructure within and across all other sectors (Cybersecurity and Infrastructure Security Agency, 2019). A similar consideration of the entry gates for targeting economic security enablers and advantages is also required. This involves contrasting the potential nexus of each 'risk owner' with the four gates of economic security (Canadian Chamber of Commerce, 2020; Canadian Security Intelligence Service, 2019) that highlight the ways intangible intellectual property advantages and strategic technological interests may be targeted.

The fourth plane of analysis are the 'playing fields' through, or within, which a threat actor may operate—simplified to the political environment (i.e., elections, public policy, etc.), civil society (i.e., private citizens, diaspora communities, etc.), academia and innovation (i.e., research institutions), and media and the information environment (i.e., social media).

Deductions based on each of these factors (or threads) must be woven together and contrast against known adversarial interests, both foreign and domestic. Threats should be assumed in areas where there is real or potential overlap between adversarial interests and deduced criticality and political, social, or economic advantage. The system performance (how well do we need to protect?) and jurisdictional (who is responsible for protecting?) components then need to be answered to articulate a coherent set of design-basis threats upon which to base reasonable security strategies and safeguards.

Conclusion

Given the complexity of the challenges involved in merely articulating a set of subnational design-basis threats, it is not overly surprising that a robust discourse on contemporary subnational security challenges has not germinated organically in Canada. An absence of local and regional resources limits the ability of subnational governments to accurately reflect on the proactive security and intelligence strategies they may now require. This is not to say that federal resources are not engaged at regional and local levels, but that those resources closest to the ground are more likely to be overwhelmed responding to the tactical details. There appears to be a jurisdiction inversion of resources and awareness, whereby the capabilities needed to identify and mitigate threats are the thinnest in arenas that are now being targeted most heavily. As this inversion provides a frictionless 'shadow zone' ripe for exploitation by a rapidly expanding array of threat actors, subnational security and intelligence strategies are now an inescapable requirement for the 21st century security environment.

Envisioning a broad objective for a subnational security and intelligence strategy is not overly difficult. Improving the ability of subnational leadership to anticipate, adapt to, and effectively address contemporary security risks and vulnerabilities over which they have some jurisdiction agency is the logical goal. It is also relatively easy to infer some broad-brush ways through which these ends could be pursued, such as new mandates and governance structures, investments and ring-fenced resources, evaluations and feedback mechanisms, and enhanced communications and information sharing. Generating the means to execute and sustain security and intelligence activities at a subnational level is where the foundational challenge lies. People, programs, policies, and partnerships must be established to shape and foster a shared vision and clarity of purpose, acquire information and understanding, empower leadership, anticipate and manage change, support continual improvement, and integrate interests, constraints, and levers across multiple levels of government.[14] Isolated examples of these means are starting to materialize in the form of Ontario's Office of the Provincial Security Advisor (OPSA) and Alberta's Provincial Security and Intelligence Office (PSIO), but much remains to be done to illuminate the subnational shadow zone.

Addressing this challenge requires a vertical evolution of security and intelligence strategies, frameworks, and policies. This implies challenging traditional assumptions regarding national security responsibilities and requires a deepening of the analytical frameworks down into the relative obscurity of the regional and local resoclines. Highlighting the growing importance of the subnational element provides only a preamble to a more complete exploration of the lurking challenges of 'jurisdictional polycentricism' in the national security domain, particularly in relation to governance. Recognizing that subnational governments wield important levers in areas now inhabited by an expanding array of domestic and foreign threat actors is relatively straightforward, but the thoughtful manipulation of those levels in strategic harmony with federal architectures is perhaps the generational challenge for the current cohort of national security strategists.

Through the vehicle of design-basis threat, a sense of the level of complexity of the contemporary security challenges facing the people, programs, policies, and partnerships at the subnational level is possible. A simplified framework for a provincial-level design-basis threat analysis provides a gateway to deeper

[14] These elements have been inspired and adapted from the organizational resilience attributes and principles articulated in (International Standards Organization, 2017).

analysis, which is critical for stimulating a national discourse on the character of the people and the nature of programs, policies, and partnerships required to shape and underwrite the kinds of polycentric security strategies and safeguards needed to survive and prosper in the 21st century.

References

Boyle, P., & Dafnos, T. (2019). Infrastructures of pacification: Vital points, critical infrastructure, and police power in Canada. *Canadian Journal of Law and Society / La Revue Canadienne Droit et Société, 34*(1), 79-98.

Canadian Chamber of Commerce. [Canadian Chamber of Commerce]. (2020, July 23). *Foreign nterference and economic espionage threats against Canadian business* [Video]. YouTube. https://www.youtube.com/watch?v=QKr1pPD03Q0&t=343s

Canadian Security Intelligence Service. (2020). *CSIS public report 2019.* https://www.canada.ca/content/dam/csis-scrs/documents/publications/PubRep-2019-E.pdf

Canadian Standards Association. (2017). *CSA S850-12: Design and assessment of buildings subjected to blast loads.* CSA America, Inc.

Cheney, C. (2019). *China's digital Silk Road: Strategic technological competiton and exporting political illiberalism* (Issues & Insights Working Paper Vol. 19 WP8*).* Honolulu: Pacific Forum. https://pacforum.org/wp-content/uploads/2019/08/issuesinsights_Vol19-WP8FINAL.pdf

Cybersecurity and Infrastructure Security Agency. (2019). *A guide to critical infrastructure security and resilience.* https://www.cisa.gov/sites/default/files/publications/Guide-Critical-Infrastructure-Security-Resilience-110819-508v2.pdf

Cybersecurity and Infrastructure Security Agency. (2020, December 14). *CISA issues emergency directive to mitigate the compromise of Solarwinds Orion network management products.* United States Government. https://www.cisa.gov/news/2020/12/13/cisa-issues-emergency-directive-mitigate-compromise-solarwinds-orion-network

Department of Homeland Security. (2010, September 10). Remarks as prepared by Secretary Napolitano to New York city first responders. https://www.dhs.gov/news/2010/09/10/remarks-prepared-secretary-napolitano-new-york-city-first-responders

Emergency Preparedness Canada. (1991). *Vital points manual.* https://www.publicsafety.gc.ca/lbrr/archives/jl%2075%20v58%201991-eng.pdf

Geddes, R. R. (1988). *Protecting category II vital points during time of war or serious civil crisis.* Emergency Preparedness Canada. https://www.publicsafety.gc.ca/lbrr/archives/jf%201525.c74%20g43%201988-eng.pdf

Ginter, A. (2018). *The top 20 cyber attacks on industrial control systems.* Waterfall Security Solutions LTD. https://www.fireeye.com/content/dam/fireeye-www/products/pdfs/wp-top-20-cyberattacks.pdf

Goldberg, C. (2020, August 18). *The great 5G technology tussle highlights critical infrastructure shortcomings.* The National Interest. https://nationalinterest.org/feature/great-5g-technology-tussle-highlights-critical-infrastructure-shortcomings-167129

Goldberg, C., & Lee, K. (2020, December 1). *Retooling democratic good governance: The technologies of a more open future in Southeast Asia.* Center for a New American Security. https://www.cnas.org/publications/commentary/retooling-democratic-good-governance

Government of Canada. (2020, August 26). *Smart cities challenge.* Infrastructure Canada. https://www.infrastructure.gc.ca/cities-villes/index-eng.html

Gray, C. (1971). The need for independent Canadian strategic thought. *Canadian Defence Quarterly, 1*(1), 6-12.

Hancock, T. (2015, September 2). Policies should focus on basic needs. *Times Colonist*. https://www.timescolonist.com/opinion/columnists/trevor-hancock-policies-should-focus-on-basic-needs-1.2047484

Held, D., McGrew, A., Goldblatt, D., & Perraton, J. (2003, Fall). Rethinking globalization. In D. Held, & A. McGrew (Eds.), *The global transformation reader: An introduction to the globailization debate* (2 ed.).

Hoaglund, J.R. (2015, April 1). *Security effectiveness analysis (Report No. SAND2015-2580C).* Sandia National Laboratories. https://www.osti.gov/servlets/purl/1248642

International Atomic Energy Agency. (2009). *Implementing guide: Development, sse and maintenance of the design basis threat.* Vienna: International Atomic Energy Agency.

International Standards Organization. (2017). *ISO 22316:2017 Security and resilience – Organizational resilience – Principles and attributes.* https://www.iso.org/standard/50053.html

Lee, K., Rasser, M., Fitt, J., & Goldberg, C. (2020, October 28). *Digital entanglement: Lessonsl learned from China's growing digital footprint in South Korea.* Center for a New American Security. https://www.cnas.org/publications/reports/digital-entanglement

Maslow, A. (1943). A theory of human motivation. *Psychological Review, 50*(4), 370–396.

Mazarr, M. J., Bauer, R., Casey, A., Heintz, S., & Matthews, L. J. (2019). *The emerging risk of virtual societal warfare: Social manipulation in a changing information environment.* RAND Corporation. https://www.rand.org/pubs/research_reports/RR2714.html

McAuley, W. (2017). *Beyond delusions of grand strategy: A cetrifugal national security strategy for Canada.* Unpublished doctoral thesis, University of Calgary, Calgary. doi:10.11575/PRISM/25114

McMillan LLP. (2015, December 5). *Does Canada need a terrorism risk insurance scheme?* https://mcmillan.ca/insights/does-canada-need-a-terrorism-risk-insurance-scheme-2/?print-posts=pdf

National Security and Intelligence Committee of Parliamentarians. (2020). *Annual report 2019*. https://www.nsicop-cpsnr.ca/reports/rp-2020-03-12-ar/annual_report_2019_public_en.pdf

Office of Critical Infrastructure Protection and Emergency Preparedness. (2003). *Threat analysis: Threats to critical infrastructure (Report No.. TA03-001).* Government of Canada. http://publications.gc.ca/collections/collection_2017/sp-ps/PS48-11-2003-eng.pdf

Pherson, K., & Pherson, R. (2013). *Critical thinking for strategic intelligence.* Los Angeles: SAGE/CQPress.

Privy Council Office. (1970). *Protection of vital points.* Cabinet Conclusions 1970-12-23. https://www.bac-lac.gc.ca/eng/CollectionSearch/Pages/record.aspx?app=CabCon&IdNumber=829

Public Safety Canada. (2009). *National strategy for critical infrastructure.* https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/srtg-crtcl-nfrstrctr/srtg-crtcl-nfrstrctr-eng.pdf

Reeves, M., Levin, S., & Ueda, D. (2016, January-February). Biology of corporate survival: Natural ecosystems hold surprising lessons for business. *Harvard Business Review*, 46-55.

Rosenbach, E., & Mansted, K. (2018, October). *Can democracy survive in the information age?* Belfer Center for Science and International Affairs. https://www.belfercenter.org/publication/can-democracy-survive-information-age

Rosenberger, L., & Gorman, L. (2020a). How democracies can win the information contest. *The Washinhton Quarterly*, *43*(2), 75-96. doi: https://doi.org/10.1080/0163660X.2020.1771045

Rosenberger, L., & Gorman, L. (2020b). *Foreign interference is a strategy, not a tactic*. Lawfare. https://www.lawfareblog.com/foreign-interference-strategy-not-tactic

Schwab, K. (2018, May 28). The fourth industrial revolution. In *Encyclopedia Britannica.* https://www.britannica.com/topic/The-Fourth-Industrial-Revolution-2119734

Taleb, N. (2007). *The black swan: The impact of the highly improbable.* Random House.

Terrorism risk insurance program; Updated regulations in light of the terrorism risk insurance program Reauthorization Act of 2019, and for other purposes, 85 F.R. 71588 (final rule November 10, 2020) (to be codified at 31 C.F.R. pt. 50). https://www.govinfo.gov/content/pkg/FR-2020-11-10/pdf/2020-24522.pdf

United States House Permanent Select Committee on Intelligence. (2020). *The China deep dive: A report on the intelligence community's capabilities and competencies with respect to the people's Republic of China.* https://intelligence.house.gov/uploadedfiles/hpsci_china_deep_dive_redacted_summary_9.29.20.pdf

Van Creveld, M. (1991). *Technology and war: From 2000 B.C. to the present.* Toronto: Maxwell Macmillan Canada.

The author can be contacted at wjmcaule@ucalgary.ca

Published by the Journal of Intelligence, Conflict, and Warfare and Simon Fraser University
Available from: https://jicw.org/