IV

October 2025

Building Citizen Resilience

Preparing Canadians for an Age of Grey-Zone Conflict

Juliana Haras
Department of National Defence

The Centre for International and Defence Policy
138 Union Street, Suite 403. Queen's University,
Kingston, Ontario Canada K7L 3N6
cidp@queensu.ca

Research Report

Introduction

As Canada navigates an ever more hostile and combustible world, beneath the fog of uncertainty lies a complex web of threats to national security. Seismic shifts in the global strategic environment are presenting risks both familiar and new for liberal democracies, whose societies and economies have become mission-critical targets for revisionist powers. In the pursuit of regional and global dominance, an era of renewed major-power competition is playing out above and below the threshold of armed conflict. Lethality is once again asserting itself as the adjudicating force in international relations – hard power politics and conquest are back – as hostile states display the capability and intent to use physical force to advance their strategic objectives. In pursuit of those same goals, neo-imperialist, rogue, and other disruptive states are waging war below the threshold of armed conflict (in what is known as the grey zone) in mutually reinforcing ways. Their aggressive statecraft is leveraging multiple vectors of attack across domains of conflict, dynamically employing all instruments of national power – to gain and deny military and economic advantage, exploit weakness, and sap the will of free societies to defend themselves.[1]

With the human mind having become a battlefield[2], the degree to which citizens are targeted invites critical reflection on whether enough is being done to prepare Canadians for the daily reality of grey-zone warfare (as well as for the unlikely, but no longer implausible, contingency of armed attack). The latter falls outside the scope of this paper. Building societal resilience against both forms of national security threat, however, warrants serious deliberation; not only does the threat environment demand it, but every NATO member has committed to it. Rooted in Article 3 of the Alliance's founding treaty, the national responsibility to "prepare for, resist, respond to, and quickly recover from shocks and disruptions" at the individual and collective levels is meant to reduce vulnerability to the full spectrum of threats above and below the threshold of armed conflict. Integral to national resilience is civil preparedness, which in turn requires the resilience of all members of society and shared responsibility for the nation's security. All Allies are subject to NATO's Resilience Baseline Requirements, which set minimum standards for civil preparedness, and over the course of the last decade, summit commitments have placed ever greater emphasis on grey-zone threats and societal resilience.[3] Canada's Allies are operationalising these commitments at speed.[4]

This paper will argue for federal leadership in raising the level of ambition of efforts to inoculate young Canadians against threats in the grey zone. It will start by establishing the case for change – laying out change drivers; adversaries' ends, ways, and means; gaps between threat and threat perception; and the deterrence imperative. It will then situate education policy within the cognitive-defence toolkit, exploring the merits of curricular measures and their practice in Canada and abroad. It will close by recommending a way forward and highlighting key considerations for policy development.

The Threat

Grey-zone aggression is by no means a new phenomenon; disinformation, for one, is as old as warfare itself. What is new is the level of sophistication and resourcing, and the proliferation of threats and vulnerabilities. The scale, volume, and ubiquity of grey-zone activity are unprecedented, as are its speed and precision. Technological change and the digital living

that accompanies it, from the internet of things to social media, have generated an array of new threat vectors and vulnerabilities, enabling hostile states to reach across borders for everything from malicious cyber activity to influence operations directly targeting foreign citizens. The widespread adoption of technologies like artificial intelligence holds even greater disruptive potential. The social distance entrenched by the COVID-19 pandemic – favouring work from home and digitally-mediated interaction – is likely to have accelerated the erosion of social capital and increased citizens' susceptibility to malign influence; over time, accumulating "bonding capital" (by connecting with like-mindeds, mostly in the digital space) over "bridging capital" (by interacting with those with fundamentally different perspectives, mostly in the physical space) tends to weaken the fabric of social trust, along with trust in institutions.[5, 6] The interconnectedness that has come with globalisation, meanwhile, has multiplied interdependencies between nations; while they were long believed to incentivise responsible state behaviour, the twenty-first century has seen states cultivate and instrumentalise strategic economic dependencies as critical points of leverage. With "the weaponisation of everything", as Mark Galeotti aptly frames the emergent character of war, everyone and everything has become a target, and threats to security are everywhere – yielding a potent mix of intent, capability, and opportunity for hostile states to bend people and institutions to their will.

Indeed, increasingly capable adversaries are conducting persistent, systematic, integrated grey-zone campaigns that blur the boundaries between foreign and domestic, between public and private, between civilian and military, between war and peace. Foreign interference is perhaps the most familiar part of the playbook. Its key tactics include information manipulation, centred on propagating and amplifying false, misleading, and inflammatory content and narratives; cultivating relationships and dependencies with public officials, the press, and influential political, business, and social figures; and interfering in electoral and other political processes. Threat actors also conduct a range of disruptive and destructive cyber activities that enable espionage and provide the capacity to impair or hold critical infrastructure at risk (alongside other means of sabotage, e.g. severing subsea communication cables). Economic espionage, subversion, and coercion see hostile states exploit access to sensitive data, technologies, and know-how (for instance, via research partnerships and infiltration of research institutions/companies) while exercising leverage gained by embedding themselves in strategic sectors as key suppliers, buyers, lenders, and investors. On the diplomatic front, their tactics include dividing and conquering in multilateral fora to erode consensus, weaponising the law, and augmenting and abusing privileged positions in international institutions to legitimise their practices at home and abroad. Examples of activities that instrumentalise and target individuals include hostage diplomacy, weaponisation of migrant flows, mass conferral of citizenship to strategic groups abroad, and transnational repression. Closer to the threshold of armed conflict, hostile states' tactics range from militarisation of disputed territory and harassment through projection of military force, to provocations, deployment of disguised warfighters, and false-flag operations.

To appreciate the gravity of the threat, it is helpful to consider a few defining characteristics of grey-zone aggression:

- It is distinct from legitimate, routine statecraft. Malign in intent, activities in the grey zone tend to be clandestine, deceptive, manipulative, subversive, threatening, and/or coercive, though not necessarily illegal. They can be overt and outwardly benign, but in all cases, they are detrimental to the national interest.

- Cumulative impacts can approximate the effects of an armed attack[7], without triggering meaningful responses. Grey-zone threats embody a contactless, perpetual state of war.[8] They are designed to be diffuse and achieve incremental gains, their gradualism and ambiguity circumventing thresholds of detection, attribution, and response. Threat activities are often conducted by way of proxies in sectors like traditional and social media, cultural industries, academia, elected office, corporate leadership, civic associations, and religious and diaspora organisations. Obscuring hostile states' intent and involvement enables plausible deniability and lowers the risk of retribution.

- Grey-zone operations are calibrated to exploit the vulnerabilities inherent in open societies and economies, while disrupting and overloading the capacity for situational awareness, decision-making, and timely response. Enjoying low barriers to entry and high returns on investment, they offer a cost-effective means of weakening an opponent while compensating for inferior conventional warfighting capabilities.

- Grey-zone and traditional military threats are intimately related. Adversaries' freedom of action in the grey zone is backstopped by the deterrent effect of their growing conventional and strategic capabilities, which have benefited from decades of military modernisation while their opponents reaped the peace dividend of the unipolar moment and concentrated public spending on other priorities. Their corrosive activities in the grey zone, meanwhile, prime the target for eventual armed conflict[9]. Grey-zone aggression is, thus, best understood in the context of adversaries' multi-domain strategies of contestation, which integrate kinetic and non-kinetic capabilities along the continuum of conflict.

All of this – to what end? Synchronising effects in the grey zone allows the adversary to shape the battlefield: influence public policy in target countries in its favour, and deprive their citizens of the capacity to make free and informed decisions; erode trust in, and de-legitimise, liberal-democratic institutions, processes, and values; de-stabilise core power structures, and demoralise foreign publics and their armed forces; create paralysis, confusion, distraction, and apathy; polarise debates, sow discord, and undermine social cohesion; silence criticism, dissent, and opposition; fracture alliances; and weaken the system of international norms, rules, and institutions that regulate state behaviour.[10] Common to Russia and China, the most prolific of grey-zone aggressors, is an intent to thereby reshape the world order to be more hospitable to authoritarianism and expansionism, with a view to preserving regime stability at home and expanding national power abroad.

The Inoculation Imperative

Threat Perception

The hostile intent of threat actors like Russia and China, along with their ways and means of pursuing it, are well established. Canada's experience of their grey-zone capabilities is also far-reaching and increasingly well documented in the public domain. It is not clear, though, that members of the Canadian public are generally conscious of the range of tactics employed against them or how to respond. Over two in five Canadians report that they do not believe themselves to be knowledgeable about national security threats and issues facing Canada and Canadians[11], and even elected officials struggle to distinguish between routine diplomatic activity and foreign interference (or to recognise what to do when targeted)[12]. What is more, public opinion research suggests that younger generations of Canadian adults – whose views appear to be persisting as they age – are more susceptible to hostile states' influence than older generations. Polling suggests that they are considerably more sympathetic to states hostile to Canada, its allies, and like-minded partners; less prepared to alter their positive views as awareness of those states' aggression grows; and less likely to believe facts that counter their perception.[13]

The data point to a generational divide with potentially serious implications for national security and defence. They arguably highlight the effectiveness of adversaries' systematic grey-zone campaigns. The causal factors behind the gap require study. Among them is likely to be a dulling of threat sensitivity following the Cold War among generations who grew up when the Russian threat, for a time, had faded from view and China's emergence as a strategic competitor was not yet fully in view. It is, however, also probable that the same states' grey-zone operations during the formative years of these generations (which are much more likely, for instance, to consider social media more trustworthy than traditional media14) have played a non-negligible role. The covert/clandestine nature of many threats in the grey zone tends to render them invisible to the naked eye, and where historical or national security literacy is uneven, seemingly benign overt activities can also escape notice. Furthermore, hostile states have exploited inherent cognitive vulnerabilities and increasingly potent technological tools to shape cognition, situational awareness, sense-making, attitudes, and behaviours[15, 16] – how populations, including Canada's, think and act. For, at the core of the psychological defeat mechanism is cognitive warfare ("war in the human consciousness"[17]), which seeks to "manipulate public opinion, disrupt decision-making processes, and ultimately, weaken military capabilities"[18]. Creating effects in the cognitive dimension of the operating environment transforms the battlespace and enables adversaries to degrade and dislocate a key strategic centre of gravity – the power derived from a country's civilian population. In a contest for cognitive superiority, hostile states are pursuing relative advantage by degrading rationality and distorting perceptions of reality. Younger Canadians' more favourable view of foreign states that seek to disempower them is likely illustrative of the fruits of that labour.

Deterrence by Denial

With hostile states persistently targeting Canada and Canadians in the grey zone, building cognitive defences takes on particular importance and urgency. While this paper focuses

on the grey-zone strategies of adversaries, among states that Canada otherwise considers partners are those that have also come to pose a threat, albeit narrower, to the security of the state and of the individual. Beyond the neo-imperialist, rogue, and other disruptive states of today's world order, moreover, it is not difficult to conceive of states that have not yet developed or deployed grey-zone capabilities deciding to leverage the growing number of threat vectors to pursue asymmetric advantage in the grey zone. Pervasive grey-zone aggression is likely to persist, even if reincarnated, and the more permissive the target, the more it invites aggression – the more readily adversaries are able to "win without fighting". Conversely, a discerning and resilient target has the power to deny them the benefits of their malign practices by minimising impact – altering their decision-making calculus and ultimately reducing the incidence and severity of hostile action.[19] Given that the scope to deter hostile states in the grey zone by imposing costs (deterrence by punishment) is limited, deterrence by denial becomes essential.[20] At the heart of it is societal resilience.

Mounting a robust deterrence posture requires expanding the traditional conception of defence well beyond the military, to a comprehensive, whole-of-society approach in which all citizens see themselves as defence actors who share responsibility for keeping the country secure. That means information consumers and voters contextualising developments at home and abroad, and thinking critically about the messaging that they accept as true, share, and act upon; journalists, content creators, and influencers discerning and, in turn, avoiding amplifying narratives promoted by hostile states; political party and public officials distinguishing recruitment and cultivation from appropriate engagement by foreign actors; operators of critical infrastructure proactively reducing cyber vulnerabilities that expose their industrial control systems to attack; entrepreneurs and researchers conducting due diligence on prospective partners; exporters limiting their exposure in/to commercially appealing but hostile foreign markets; and so forth. With all of society a target, all of society becomes the first line of defence. To fulfil their civic role in the new security environment, citizens need the understanding and dispositions to recognise risk, vulnerability, and attempts at malign influence, subversion, and coercion. Where they are a target, they need the situational awareness and capacity to resist.

Cognitive Defence

The concept of cognitive defence remains under construction. A common interpretation is that of Sweden's Psychological Defence Agency, which characterises psychological defence as "society's common capabilities for detecting and resisting malign information influence…by antagonistic foreign powers" that seek to influence perceptions, decisions, or behaviour. For the purposes of this paper, cognitive defence (used interchangeably with "citizen resilience") is defined more broadly, as the ability to recognise and resist threats posed by hostile states in the grey zone between traditional conceptions of war and peace. The operational definition extends beyond defence against weaponised information, to capture the array of grey-zone activities that have the effect of shaping perceptions, ways of thinking, attitudes, beliefs, behaviours, and decision-making (kinetic action can, of course, also deliver cognitive effects[21]).

The information domain tends to be the focus of interventions aimed at building citizen resilience. The overriding goal in war, however, is to convince the opponent to bend to one's will, and this is done by various means across domains; "the ultimate target of all conflict is the human mind"[22] and, as cognitive-security expert Andrew Whiskeyman duly points out, "all warfare is cognitive". Threat activities like political interference, economic coercion, and weaponised migration may not have as direct an impact on cognitive processes as information manipulation, but the (cumulative) cognitive effects that they, too, generate are important to grasp. What is more, hostile states read and target adversaries as systems of interconnected components, and they seldom employ just one instrument of their toolkit (or instruments in isolation). Grey-zone aggression, thus, needs to be understood as an integrated whole. Its power and peril lie in the sum of its parts.

The Role of Education Policy

No instrument in the cognitive-defence toolkit is more uniquely suited to the requisite paradigm shift than education policy, though others are valuable and necessary. These include candid, timely, and accessible strategic communications; pre- and de-bunking of disinformation; rapid selective declassification and disclosure of intelligence to expose threat actors' false narratives, actions, and hostile intent; and threat briefings to communities commonly targeted by hostile states.[23] Public awareness campaigns, training, workshops, and resources also have a role to play. Indeed, Canada's federal government is deploying an ever-broader set of instruments to raise public awareness of threats in the grey zone.[24] The measures designed for youth are narrow in focus, however, and interventions in adulthood are inherently limited in reach. Although they are generally available to all, those who avail themselves of opportunities to grow their awareness tend to be predisposed to taking interest in civic issues – dispositions often formed early in life.

Upstream interventions aimed at children and youth, particularly measures in the education system, come with a distinct set of complementary advantages. One relates to time – both the timeliness of engaging citizens in a period critical to the formation of habits of mind, and the scope to unpack complexity and connect dots over time. Another is depth. While outreach in adulthood can cultivate awareness, curricular interventions (if designed and implemented thoughtfully) have much greater potential to translate civic knowledge into understanding, understanding into attitudes, beliefs, and values, and those dispositions into behaviour.[25] Ever more so when paired with extracurricular offerings and a school environment that reinforce what is learned in the classroom.[26] Yet another advantage is reach. The universal nature of interventions in K-12 allows building the capacity of young people from all segments of society, ensuring that the most vulnerable benefit. Such equalisation of opportunity has been shown to compensate for disparities in parental background and families' socioeconomic status[27], which tends to shape early socialisation and be a predictor of civic and other literacies[28]. These advantages add up to more broad-based, potent, and enduring inoculation for young minds, along with ripple effects on the adults in their lives.

Impactful as education policy can be, there are a few things that it cannot accomplish. As one of many agents of socialisation, and one of many instruments that need to be employed in support of societal resilience, it cannot deliver results on its own; efforts to reduce citizens' susceptibility to grey-zone aggression can also only go so far without concerted and sustained effort to earn their trust in institutions (strengthen democratic ideational resilience), renew the social contract, and build social capital.[29] It cannot deliver quick wins; the gestation period of educational interventions is long (transformational change takes time). Finally, it cannot harden all targets or render targets impenetrable; there will always be "'semi-witting or witting' participants in the efforts of foreign states"[30], and it is unreasonable to expect that even well-intentioned, threat-conscious citizens will manage to resist all attacks all the time. Take information-based influence, for instance, which is exercised using compelling emotive appeal and cognitive overload tactics.[31] Absent a rewiring of human nature, the organic reach of disinformation will never be reduced to zero.[32]

Current State

The potential of education policy to support citizen resilience-building in Canada is largely untapped. Curricular measures across the provinces and territories – limited to digital media literacy – provide a narrow treatment of the grey-zone threats facing Canadians of all ages. Existing interventions are mostly tactical/skill-based (exploring what disinformation looks like and what to do about it), optional, introduced late in the K-12 cycle, and reliant on forward-leaning teachers as champions. They tend to be delivered piecemeal (often in the language arts curriculum), and the national landscape consists of a patchwork of siloed provincial/territorial approaches. Civil society organisations and educators have been advocating for integration of digital media literacy into the K-12 curriculum, both mainstreamed and as a standalone subject. They have been urging the federal government to take a leadership role in establishing a national commitment to digital media literacy, advancing national standards, and mobilising a funded national strategy.[33, 34]

Equally of interest to the cognitive defence discussion is the civic education landscape. Civics is the discipline with which digital media literacy education is most tightly linked (internationally, the latter is often characterised as digital citizenship education), and it may similarly be the conceptual home for broader grey-zone/citizen resilience education. Even in its traditional construct, civics has the capacity to enhance resilience by way of the foundational knowledge, critical thinking, and agency that it is meant to foster. Civic education in Canada is more institutionalised than the digital media literacy (sub-)field, with civics-related courses compulsory in every province and territory. In few cases is civics offered as a standalone course, nor is it mainstreamed across curricula; rather, it is embedded primarily in high school social studies courses.[35] Results have been mixed. Educational interventions in recent decades do not appear to have prevented Canada's civic literacy deficit from persisting and even deepening. It is, likewise, unclear that they have generated the desired behavioural outcomes.[36] The community of practice points to several causal factors, chief among them – an "unfunded mandate", a say-do gap that has "severely de-prioritized" civic education in practice, and an acute lack of the training, time, resources, and institutional support required for teachers to deliver "consistent, equitable access to high-quality civic education".[37] As with digital media literacy, it sees a central role for the federal government in convening

stakeholders, promoting coherence and information-sharing, and providing stable funding for the development, implementation, and evaluation of programming.[38]

The successes and deficiencies of education policy in Canada offer lessons for the citizen resilience agenda, and so does the experience of international peers. An international scan does not yet yield examples of comprehensive grey-zone resilience education. Calls for curricular interventions are growing, however. In 2020, a prominent US think tank launched a national strategic dialogue on civics as a national security imperative, emphasising the need to prioritise civic education as a means of cultivating among citizens an appreciation of how foreign threats to democracy manifest and how to counter them.[39] Most recently, in putting forth a competence development model for hybrid threats (a term often used interchangeably with "grey-zone threats"), a group of Norwegian academics made the case for introducing the topic into school curricula – cautioning that failing to do so risks leaving society unprepared to accept or see the need for future countermeasures.[40]

It is no coincidence that voices promoting educational interventions in support of grey-zone literacy are emanating from the Nordic region. Finland, Sweden, and Norway have deep experience, and have long been regarded as leaders, in building societal resilience against threats both kinetic and non-kinetic. Integral to their total defence / comprehensive security models are curricular measures that hone critical thinking from early childhood, including by mainstreaming civic and digital media literacy across the curriculum (as in Finland and, beyond the region, France), from math to visual arts.[41, 42] The Baltic states are also on the vanguard; in Estonia, for instance, digital media literacy is a cross-curricular lens starting in kindergarten, and a compulsory "Media and Manipulation" course is now offered in high school.[43, 44] France, Finland, and Estonia are the EU countries with the highest number of teaching hours dedicated to civic education and include it as a compulsory subject from primary through high school.[45] The Nordic and Baltic states' long history of contending with a full-spectrum aggressor next door has, of course, fostered the conditions for heightened threat awareness and purposeful, systemic efforts to build citizen resilience. Across much of the European Union, where approaches vary considerably, it is noteworthy that teacher education has struggled to keep pace with the demands of an expanding civic-education agenda, and teachers have lacked confidence in their preparedness to meet them. Despite educators' knowledge, skills, and attitudes being critical to the development of digital media literacy in learners, relevant training has been slow to make it into teacher education programs. Researchers have stressed the importance of aligning teacher preparation (pre- and in-service) with curriculum demands, with a view to reducing reliance on individual teachers' level of interest and motivation for developing the requisite expertise.[46]

Future State: Recommendations for a way forward

Applying lessons from research and practice, the recommendations below seek to inform the federal government's approach to helping build young Canadians' cognitive defences – their capacity to recognise and resist threats in the grey zone:

1. At a minimum, support the digital media literacy agenda and reinvigorate the broader civic literacy agenda in education systems across Canada by taking on the strategic role advocated by civil society (as highlighted in the "Current State" section of this paper).

2. Expand the mandate of, and resource, Canadian Heritage's Digital Citizen Initiative to encompass the full range of grey-zone threats. Leverage the Digital Citizen Contribution Program to fund the development of a research and program delivery ecosystem generating learning opportunities in the classroom and beyond (within the school and broader community).

3. Leverage Canada's membership in the European Centre of Excellence for Countering Hybrid Threats – which maintains an extensive research program and reaches into a network of states at the forefront of societal resilience-building – to advocate for a workstream dedicated to citizen resilience education.

4. Establish citizen resilience education as a national priority by committing to supporting its development. The forthcoming national security strategy and strategies that will be nested within it offer opportunities to elevate and formalise the priority.

    a. Designate a lead department for mobilising the policy initiative. Assigning the role to Canadian Heritage would have the advantage of building on existing stakeholder networks, program structures, and funding vehicles.

    b. Resource the effort accordingly, by way of long-term funding for implementing partners and the federal machinery necessary for coordination. In a period of fiscal restraint, new federal funding will be in short supply. In an era of relentless grey-zone aggression, however, a sober assessment of threats, national security imperatives, and returns on investment yields a robust case.

5. Map the community of practice and co-create a framework for collaboration.

6. Kick-start a national dialogue on the introduction of citizen resilience education in Canadian schools. Bring partners and stakeholders – many of them already actively engaged in the civic and digital media literacy efforts – to the table to establish shared understanding of the problem, a shared vision, and the realm of the possible. Foremost among these organisations: federal (e.g. Canadian Heritage, Privy Council Office, Public Safety, Canadian Security Intelligence Service, National Defence, Communications Security Establishment, Elections Canada, Global Affairs Canada), provincial/territorial (e.g. Council of Ministers of Education, Canada, ministries of education), professional (e.g. Social Studies Educators Network of Canada, Canadian Teachers' Federation), teacher education (i.e. university faculties of education), and civil society (e.g. Digital Public Square, The Dais, Samara Centre for Democracy, CIVIX, MediaSmarts).

7. Depending on the outcomes of the national dialogue, consider:

    a. Appointing a committee of experts (education, defence, and security practitioners, academics, and officials; civil society organisations) to lead the phased development of reference curricula and associated learning resources for K-12 and teacher education (pre- and in-service). The intent – to design developmentally-appropriate content that:

i. Explores the ends, ways, and means of hostile states in the grey zone; concepts in behavioural psychology (e.g. cognitive bias, psychology of subconscious influence) that demonstrate how the human mind is wired and its vulnerabilities are exploited to manipulate[47]; and good practices in defending against grey-zone aggression. Building capacity to think critically about grey-zone threats and connect the dots in everyday situations requires understanding what hostile states do, in what contexts, how, and why. Preserving freedom of thought, meanwhile, requires understanding own cognitive vulnerabilities at least somewhat as well as those who seek to exploit them;

ii. Can form the basis of standalone courses, be integrated into existing subjects, and be mainstreamed as a cross-curricular theme;

iii. Is delivered using pedagogically and andragogically sound methods that are as inquiry-based, organic, and experiential as possible – incorporating concrete real-world examples and case studies drawn heavily from the Canadian context, along with plausible, age-appropriate scenarios, exercises, simulations, and gaming to train learners' pattern-recognition and response muscles.

iv. Is delivered in partnership with civil society organisations. The latter bring expertise and capacity complementary to that already in the classroom, tend to have national reach, and stand to reinforce the legitimacy of curricular interventions, as trusted non-governmental sources on a subject that some communities approach with apprehension if not distrust.[48]

The Hybrid Threats and Hybrid Warfare Reference Curriculum recently developed under the auspices of the Partnership for Peace Consortium of Defence Academies and Security Studies Institutes can serve as a launching point for curriculum development, and the learning resources in MediaSmarts' Digital Media Literacy Framework for Canadian Schools provide examples of turnkey solutions for educators.[49, 50]

b. Using conditional grants to incentivise provinces and territories to experiment with the reference curricula. Given that baselines of civic and digital media literacy interventions differ considerably, as will appetite for revisiting curriculum, start with a coalition of the willing. To pilot new approaches, partner, for instance, with those that have the most mature curricular interventions.

c. Supporting stakeholders and partners in building their capacity for program delivery. Examine the merits of standing up an entity akin to the former Canada Studies Foundation[51] (which developed new approaches to – and materials for – teaching about Canada, established a pan-Canadian network of educators, and provided teacher training) or France's Centre pour l'éducation aux médias et à l'information (which provides teacher training and learning materials at scale in support of school-based media and information literacy interventions).

Key Considerations

Any multi-stakeholder policy initiative, especially across orders of government, will involve challenges and trade-offs. At the operational level, some fundamental questions will need to be considered. For example, introducing new curriculum content will require sacrificing existing content; within which subject areas can it be displaced at acceptable risk? Should citizen resilience education be folded into an expanded, reframed civic education agenda, or stood up as a discipline functionally distinct from an already saturated civics / social studies curriculum? At the strategic level, two foundational questions stand out: what is an appropriate role for the federal government, and is it prudent to grow young people's defence-mindedness at the risk of alarming them?

Canada's constitutional division of powers places education under the jurisdiction of provincial and territorial governments. The federal government, however, is responsible for assuring national security for all Canadians (one of its core functions). Leaving it to the provinces and territories alone to build young people's resilience against foreign aggression that cuts across sub-national borders would be a high-stakes abdication of responsibility – a responsibility that no province, beyond uneven investments in digital media literacy, has thus far sought to claim. What is more, the federal government has a long history of influencing (and building capacity for) citizenship education in Canadian schools, through instruments ranging from program-specific financial incentives and bilateral agreements with the provinces and territories, to institutional infrastructure, learning materials, joint curriculum development, teacher training programs, funding for research, and support for civil society organisations as delivery partners.[52] Rather than periodically express concern about the level of threat awareness among the Canadian public but continue to be dissuaded by the complexities of federalism, it is time to seek ways to support the provinces and territories in exercising their authority in this critical space. The federal government is uniquely positioned to play a strategic, catalytic role that leverages its convening and spending power – generating momentum, connecting stakeholders and partners, creating the conditions and mechanisms for coordinated action, fostering coherence, supplying expertise, and funding policy innovation and delivery.

When it comes to the risk of resilience-building raising alarm among the public (a question often posed), as deterrence expert Elisabeth Braw once noted, "don't worry about worrying people", as the consequences of an unprepared citizenry are much greater. How governments go about sensitising the public to threats is important (alarmist approaches do much more harm than good), but failing to develop its situational awareness is disempowering. Equipping young Canadians with the capacity to contend with threats in the grey zone stands to reinforce a vital sense of agency. The implicit transparency on the part of government also has the potential to strengthen the very trust in institutions that adversaries seek to undermine – organically reinforcing the pillars of citizen resilience.[53] Without a broad-based understanding of the grey zone and its impacts, few other societal resilience-building efforts are likely to sustainably bear fruit; citizens are left ill-equipped to participate in democratic discourse on national security, fulfil their civic role, and hold government accountable for keeping them secure; strategic culture in the state's institutions remains complacent; and both society and those it entrusts with governing risk continuing to be seized with the

symptoms of public problems, often yielding misdiagnosis and minimally effective (if not counterproductive) countermeasures. Problems like polarisation and declining trust, for instance, have legitimate drivers, but they are also actively fuelled by grey-zone strategies that over-polarise beliefs and without which they would be less likely to reach boiling point. They can no longer be unpacked or tackled without understanding the external influences manipulating thought processes, attitudes, and behaviours. This is as important for the individual citizen as it is of the policymaker, both left preventably susceptible to hostile foreign influence.

Fortunately, embedded in the proliferation of threats to national security is a kernel of opportunity. A confluence of events in recent years and months has not only heightened the urgency of raising the level of ambition of resilience-building, but created the conditions for it. Forming in real time is a kind of openness to new understandings and ways of doing things that tends to come when vulnerability becomes tangible in the eyes of a population – when the realisation sinks in that the house is no longer fireproof. The emergence of a threat to Canada's sovereignty from its closest ally has dealt a strategic shock. Widely-publicised independent reviews of foreign interference and of the government response, coupled with high-profile cases of attribution of grey-zone activities, have stirred a public awakening. Concepts like information operations and transnational repression are no longer confined to the community of practitioners and academics who navigate and study grey-zone waters for a living. Experts and practitioners from civil society, academia, industry, and government are urging the federal government to review the threshold for intelligence disclosure.[54] Business leaders are seeking support for Canada's companies in recognising and defending against economic-based threats to national security, including through disclosure of intelligence, training, and advice.[55] The recent Public Inquiry into Foreign Interference in Federal Electoral Processes and Democratic Institutions recommended (with a focus on social media) that the federal government step up collaboration with other orders of government on strategies supporting educational interventions that build young Canadians' capacity to critically assess the polluted information environment.[56]

Within these developments lies a mandate to act, along with fertile ground for a transformation long overdue – an opportunity to leverage the focus increasingly on defence and security to build a more resilient Canada. This, however, is not to say that leveraging the country's education systems to advance national security priorities will not encounter resistance. Change management will require particular consideration. Mindsets already shaped by grey-zone campaigns and distrust of public institutions suggest that some will meet the effort with hostility. Foreign threat actors, in turn, are likely to amplify that hostility. Introducing even tactically-focused digital media literacy education in Canadian schools has generated its share of controversy. Foresight and precision in framing what a given measure is and is not, paired with meaningful civil society partnerships, will be needed to help overcome resistance. So will structurally addressing legitimate concerns through a considered approach to the design of educational interventions, one that centres on the development of critical thinking in learners.

Conclusion

This paper has sought to plant the seeds of a conversation. It opened by examining the instruments and intent of hostile states in the grey zone between traditional conceptions of war and peace. It then considered gaps between threat and threat perception among young Canadians, the cognitive-defence imperative, and the role of education policy in meeting that imperative. It drew lessons from curricular interventions in Canada and abroad and recommended a way forward. In doing so, it argued that the case is strong, and the time ripe, for a more proactive, systematic approach to building Canadians' capacity to recognise and resist the interconnected threats that adversaries pose in the grey zone. Defending Canadian interests and values in the new normal requires a paradigm shift that cannot be accomplished without early, sustained, and universal educational interventions.

In the effort to reduce citizens' vulnerability to grey-zone aggression, education policy will not be a panacea, and its effectiveness will be critically dependent on the quality of front-line implementation. But an essential instrument it is. Defending the mind is about defending freedom of thought – the capacity of citizens to think for themselves, to ask the right questions, and to contextualise the influences around them. It is vital for a functional liberal democratic society. Challenging as federal-provincial/territorial dynamics can be, generations that do not know a world without digital and globally-interconnected living deserve governments that make common cause to protect them from the foreign threats that it transmits. Getting there will require internalising that:

- Grey-zone aggression is, indeed, an existential threat to Canada and Canadians' way of life, and failing to strengthen cognitive defences cedes advantage to hostile states to shape the world in their favour;
- Governments and militaries alone no longer suffice as a defence against foreign adversaries, nor do existing countermeasures;
- Citizen resilience is a national security imperative within a necessarily expanded conception of national defence;
- Education systems are a key part of the security policy toolkit – agents of change with potential to deliver enduring strategic effects; and
- Preparing young Canadians for an era of grey-zone conflict is a shared federal-provincial/territorial responsibility.

Developing a culture of grey-zone literacy and resilience will require leadership at the senior-most levels to expand the conversation with Canadians about the new threat environment and the imperative for change – empowering them to hold all orders of government to account for doing their part in protecting them and their children from foreign threats. It will require vision, a sense of urgency, and an eye to the long term, accepting that results will be difficult to measure or attribute and will take longer to achieve than the average government's lifespan. In profound ways, the defence of what Canadians hold most dear depends on it.

Annex:
Threat Perception

Polling conducted in 2024 suggests that younger generations of Canadian adults are considerably more sympathetic to states hostile to Canada, its allies, and like-minded partners; less prepared to alter their positive views as awareness of those states' aggression grows; and less likely to believe facts that counter their perception.

- In polling conducted by Research Co.[57, 58], respondents aged 18 to 34 were twice as likely (30%) as 35-54 year-olds (13%) to hold a positive view of Russia, and 4 times as likely as those over age 55 (7%). Whereas those 35 and over were much less likely to view the country positively compared to 2020 (presumably in light of its full-scale invasion of Ukraine), 18-34 year-olds remained just as likely to do so. (According to the Pew Research Centre[59], in many countries, younger adults tend to hold a more favourable view of Russia than do older generations, with a gap of 10 percentage points or more.) Similarly, respondents aged 18-34 were twice as likely (41%) as 35-54 year-olds (18%) to hold a positive view of China, and five times as likely as those over age 55 (8%). Whereas those 35 and over were much less likely to hold a positive view of the country compared to 2020, the proportion of 18-34 year-olds viewing it positively increased by 8 percentage points. The generational divide was not reflected in respondents' views of most other countries listed.

  A survey conducted by Angus Reid Institute surfaced a significant but narrower gap between younger and older adults' views of Russia and China.[60]

- In a survey fielded by Digital Public Square, the China Governance Lab at the Munk School of Global Affairs and Public Policy, and Abacus Data[61], respondents from Generation Z (18-29 year-olds) rated the favourability of the Chinese government at 4.0 on a 10-point scale, and Millennials (30-44 year-olds) rated it at 3.4, compared to 3.0 among Generation X (45-59 year-olds) and 2.3 among Baby Boomers (aged 60 and over). The generational divide was not reflected in their views of other governments (namely, those of the EU, US, or Canada).

- According to the same survey[62], 39% of respondents from Generation Z and 45% of Millennials, compared to 52% of Generation X and 60% of Baby Boomers, believed that the Chinese government interfered in Canada's 2021 general election; 44% of Generation Z and 35% of Millennials, compared to 31% of Generation X and 23% of Baby Boomers, thought that reports about Chinese government interference were exaggerated because of anti-China bias; and 37% of Generation Z and 30% of Millennials, compared to 25% of Generation X and 20% of Baby Boomers, thought that the Canadian government was trying to marginalise Chinese Canadians.

Artificial intelligence was not used at any stage of the conceptualisation, research, or writing of this paper.

The author's qualifications include professional experience in geo-strategic assessment and deterrence policy, along with university degrees in defence studies, public policy, education, and economics.

This paper contains facts and views that the author alone considered appropriate for the subject. It does not necessarily reflect the position of the Department of National Defence or the Government of Canada.

Bibliography

Angus Reid. *Favourability of Nations (Canada) Tables*. Angus Reid, 2024. https://angusreid.org/wp-content/uploads/2024/06/2024.06.13_Favourability_of_Nations_CAN_tables.pdf.

Blasko, Zsuzsa, Patricia Dinis da Costa, and Esperanza Vera-Toscano. *Civic attitudes and behavioural intentions among 14-year-olds. How can education make a difference towards a more democratic and cohesive Europe?*. Publications Office of the European Union, 2018. https://publications.jrc.ec.europa.eu/repository/bitstream/JRC109180/jrc109180_iccs_science_for_policy_report_final_pubsy.pdf.

Braw, Elisabeth. "How to Involve Civil Society in Grey Zone Defence." In *Hybrid Threats and Grey Zone Conflict: The Challenge to Liberal Democracies*. Edited by Mitt Regan and Aurel Sari. Oxford University Press, 2024. https://academic.oup.com/book/56327.

Braw, Elisabeth, and Peter Roberts. *Societal Resilience as a Deterrent.* NATO Science and Technology Organization, 2019. https://www.sto.nato.int/publications/STO%20Meeting%20Proceedings/STO-MP-SAS-141/MP-SAS-141-11.pdf.

Buchanan, Tom. "Why Do People Share Disinformation on Social Media?" Centre for Research and Evidence on Security Threats, September 4, 2020. https://crestresearch.ac.uk/resources/disinformation-on-social-media.

Business Council of Canada. *Economic Security is National Security: The Case for an Integrated Strategy*. Business Council of Canada, 2023. https://www.thebusinesscouncil.ca/wp-content/uploads/2022/07/Economic-Security-is-National-Security-Report_digital.pdf.

Center for Strategic and International Studies. "Civics." Accessed March 3, 2025. https://www.csis.org/programs/defending-democratic-institutions/civics.

CIVIX. *Civics on the Sidelines: A National Survey of Canadian Educators on Citizenship Education*. CIVIX, 2023. https://civix.ca/wp-content/uploads/2024/04/CIVIX-Civics-on-the-Sidelines-Report-EN-1.pdf.

Costigan, Sean S., and Michael Hennessy. *Hybrid Threats and Hybrid Warfare Reference Curriculum*. NATO Headquarters Brussels, 2024. https://www.nato.int/nato_static_fl2014/assets/pdf/2024/7/pdf/241007-hybrid-threats-and-hybrid-warfare.pdf.

European Centre of Excellence for Countering Hybrid Threats. *Deterrence: Proposing a more strategic approach to countering hybrid threats*. European Centre of Excellence for Countering Hybrid Threats, 2020. https://www.hybridcoe.fi/wp-content/uploads/2020/07/Deterrence_public.pdf.

European Centre of Excellence for Countering Hybrid Threats. *Deterring Hybrid Threats: A Playbook for Practitioners*. European Centre of Excellence for Countering Hybrid Threats, 2020.

European Commission: European Education and Culture Executive Agency. *Citizenship education at school in Europe*, *2017*. Publications Office of the European Union, 2017. https://data.europa.eu/doi/10.2797/536166.

Fagan, Moira, Sneha Gubbala, and Jacob Poushter. "Views of Russia and Putin." Pew Research Center, July 2, 2024. https://www.pewresearch.org/global/2024/07/02/views-of-russia-and-putin-july-24.

Falk, Barbara J. *Strategic citizens: Civil society as a battlespace in the era of hybrid threats*. European Centre of Excellence for Countering Hybrid Threats, 2020. https://www.hybridcoe.fi/wp-content/uploads/2020/11/SA25_Strategic-Citizen.pdf.

Government of Canada. *Pan-Domain Force Employment Concept: Prevailing in a Dangerous World*. Government of Canada, 2023.

Government of the Netherlands. "Government works to increase resilience against military and hybrid threats." Accessed March 4, 2025.

Hartley III, Dean S., and Kenneth O. Jobson. *Cognitive Superiority*. Springer, 2020. https://doi.org/10.1007/978-3-030-60184-3_1.

Hiebert, Kyle. "In 2024, National Security Requires a Whole-of-Society Approach." Centre for International Governance Innovation, June 20, 2024. https://www.cigionline.org/articles/in-2024-national-security-requires-a-whole-of-society-approach.

Horn, Bernd. "War, Not War – War in the Shadows: Below Threshold Threats." In *Threat & SOF / Special Operations Response*, edited by Bernd Horn and Patricia J. Blocksome. CANSOFCOM Education & Research Centre, 2024. https://publications.gc.ca/collections/collection_2024/mdn-dnd/D2-474-2024-eng.pdf.

Ipsos. "Young Canadians More Trusting of Information on Social Media Than Other Generations." Ipsos, December 23, 2022. https://www.ipsos.com/en-ca/news-polls/Young-Canadians-More-Trusting-of-Information-on-Social-Media-Than-Other-Generations.

Jackson, Nicole J. "Deterrence and Strategic Disinformation: An Overview of Canada's Responses." In *Deterrence in the 21st Century: Statecraft in the Information Age*, edited by Eric Ouellet, Madeleine D'Agata and Keith Stewart. University of Calgary Press, 2024. https://www.jstor.org/stable/jj.11141796.

Magnussen, Leif Inge, Glenn-Egil Torgersen, Ole Boe, and Herner Saeverot. "Competence for Hybrid Threats: A strategic competitive development model." In *Preparing for Hybrid Threats to Security: Collaborative Preparedness and Response*, edited by Odd Jarl Borch and Tormod Heier. Routledge, 2025. https://library.oapen.org/handle/20.500.12657/93079.

Masakowski, Yvonne R., and Janet M. Blatny. *Mitigating and Responding to Cognitive Warfare.* NATO Science and Technology Organization, March 2023. https://www.researchgate.net/publication/369305190_Mitigating_and_Responding_to_Cognitive_Warfare.

McAleese, Samantha, and Kara Brisson-Boivin. *From Access to Engagement: Building a Digital Media Literacy Strategy for Canada*. MediaSmarts, 2022. https://mediasmarts.ca/sites/default/files/2023-01/From%20Access%20to%20Engagement%20-%20Building%20a%20Digital%20Media%20Literacy%20Strategy%20for%20Canada%202022.pdf.

McDougall, Julian, Marketa Zezulkova, Barry van Driel, and Dalibor Sternadel. *Teaching media literacy in Europe: evidence of effective school practices in primary and secondary education*. Publications Office of the European Union, 2018. https://nesetweb.eu/wp-content/uploads/2019/06/AR2_Full_Report_With_identifiers_Teaching-Media-Literacy.pdf.

MediaSmarts. *Use, Understand & Engage: A Digital Media Literacy Framework for Canadian Schools*. MediaSmarts, 2024. https://mediasmarts.ca/sites/default/files/2023-06/digital-media-literacy-framework.pdf.

Morden, Michael, Stewart Prest, Jane Hilderman, and Kendall Anderson. *Investing in Canadians' civic literacy: An answer to fake news and disinformation*. Samara Centre for Democracy, 2019. https://www.samaracentre.ca/articles/investing-in-canadians-civic-literacy.

Muñoz Mosquera, Andrés B., and Nikoleta Chalanouli. "Decoding Grey Zone Environments." In *Hybrid Threats and Grey Zone Conflict: The Challenge to Liberal Democracies*, edited by Mitt Regan and Aurel Sari. Oxford University Press, 2024. https://academic.oup.com/book/56327.

National Security and Intelligence Committee of Parliamentarians. *Special Report on Foreign Interference in Canada's Democratic Processes and Institutions.* National Security and Intelligence Committee of Parliamentarians, 2024. https://www.nsicop-cpsnr.ca/reports/rp-2024-06-03/special-report-foreign-interference.pdf.

NATO. "Resilience, civil preparedness and Article 3." Accessed March 1, 2025. https://www.nato.int/cps/en/natohq/topics_132722.htm.

NATO. "Strengthened Resilience Commitment." Accessed March 1, 2025. https://www.nato.int/cps/en/natohq/official_texts_185340.htm.

NATO. "Vilnius Summit Communiqué." Accessed March 1, 2025. https://www.nato.int/cps/en/natohq/official_texts_217320.htm.

NATO. "Warsaw Summit Communiqué." Accessed March 1, 2025. https://www.nato.int/cps/cn/natohq/official_texts_133169.htm.

NATO. "Washington Summit Declaration." Accessed March 1, 2025. https://www.nato.int/cps/en/natohq/official_texts_227678.htm.

NATO Allied Command Transformation. "Allied Command Transformation develops the Cognitive Warfare Concept to Combat Disinformation and Defend Against "Cognitive Warfare"." Accessed January 26, 2025. https://www.act.nato.int/article/cogwar-concept.

NATO Allied Command Transformation. "Cognitive Warfare." Accessed January 26, 2025. https://www.act.nato.int/activities/cognitive-warfare.

Neundorf, Anja, Richard G. Niemi, and Kaat Smets. "The Compensation Effect of Civic Education on Political Engagement: How Civics Classes Make Up for Missing Parental Socialization." *Political Behavior* 38, no. 4 (2016): 921-949. https://link.springer.com/article/10.1007/s11109-016-9341-0.

OECD. *Facts not Fakes: Tackling Disinformation, Strengthening Information Integrity*. OECD Publishing, 2024. https://www.oecd.org/content/dam/oecd/en/publications/reports/2024/03/facts-not-fakes-tackling-disinformation-strengthening-information-integrity_ff96d19f/d909ff7a-en.pdf.

Ong, Lynette. *Foreign Interference and the Health of Canadian Democracy: Report from a Nationwide Public Opinion Survey*. Digital Public Square, 2024. https://orgsite.cdn.prismic.io/orgsite/ZzZS168jQArT04yL_V10-ReportPublicOpinionSurveyofForeignInterferenceinCanada.pdf.

Open Society Institute – Sofia. *The Media Literacy Index 2023: Measuring Vulnerability of Societies to Disinformation*. Open Society Institute – Sofia, 2023. https://osis.bg/wp-content/uploads/2023/06/MLI-report-in-English-22.06.pdf.

Public Inquiry into Foreign Interference in Federal Electoral Processes and Democratic Institutions. *Final Report, Volume 1*, Public Inquiry into Foreign Interference in Federal Electoral Processes and Democratic Institutions, 2025. https://foreigninterferencecommission.ca/fileadmin/report_volume_1.pdf.

Public Inquiry into Foreign Interference in Federal Electoral Processes and Democratic Institutions. *Final Report, Volume 4*. Public Inquiry into Foreign Interference in Federal Electoral Processes and Democratic Institutions, 2025. https://foreigninterferencecommission.ca/fileadmin/PIFI_-_Final_Report_Vol._4__2025_.pdf.

Public Inquiry into Foreign Interference in Federal Electoral Processes and Democratic Institutions. *Final Report, Volume 5*. Public Inquiry into Foreign Interference in Federal Electoral Processes and Democratic Institutions, 2025. https://foreigninterferencecommission.ca/fileadmin/report_volume_5.pdf.

Public Safety Canada. "National Security Public Opinion Research Snapshot." Public Safety Canada, 2022. https://www.publicsafety.gc.ca/cnt/ntnl-scrt/cntr-trrrsm/pblc-pnn-rsrch-snpsht-2021-en.aspx.

Research Co. *Poll conducted by Research Co. on Views of Other Countries in Canada*. Research Co., 2020. https://researchco.ca/wp-content/uploads/2020/01/Tables_Countries_CAN_10Jan2020.pdf.

Research Co. *Poll conducted by Research Co. on Views of Other Countries in Canada*. Research Co., 2024. https://researchco.ca/wp-content/uploads/2024/07/Tables_Countries_CAN_24Jul2024.pdf

Roi, Michael. "Cognitive Warfare." Paper presented at Inaugural Homeland Defense Symposium, Carlisle Barracks, PA, February 2024.

Salomaa, Saara, and Lauri Palsa. *Media Literacy in Finland: National Media Education Policy.* Ministry of Education and Culture, 2019. https://medialukutaitosuomessa.fi/mediaeducationpolicy.pdf.

Sears, Alan. "Instruments of policy: How the National State Influences Citizenship Education in Canada." *Canadian Ethnic Studies* 29, no. 2 (1997): 1-21. https://www.proquest.com/scholarly-journals/instruments-policy-how-national-state-influences/docview/1293198091/se-2.

The Dais. *Building Democratic Resilience to Foreign Disinformation in Canada*. The Dais, 2024. https://dais.ca/wp-content/uploads/2024/06/PCO-Workshop-Final-Paper_V7.pdf.

Wilner, Alex. "Deterrence by De-legitimization in the Information Environment: Concept, Theory, and Practice." In *Deterrence in the 21st Century: Statecraft in the Information Age*, edited by Eric Ouellet, Madeleine D'Agata and Keith Stewart. University of Calgary Press, 2024. https://www.jstor.org/stable/jj.11141796.

Yee, Amy. "The country inoculating against disinformation." BBC, January 30, 2022. https://www.bbc.com/future/article/20220128-the-country-inoculating-against-disinformation.

Endnotes

1 Government of Canada, *Pan-Domain Force Employment Concept: Prevailing in a Dangerous World* (Government of Canada, 2023), 13-14.

2 Barbara J. Falk, *Strategic citizens: Civil society as a battlespace in the era of hybrid threats* (European Centre of Excellence for Countering Hybrid Threats, 2020), 4-6, https://www.hybridcoe.fi/wp-content/uploads/2020/11/SA25_Strategic-Citizen.pdf.

3 See https://www.nato.int/cps/en/natohq/topics_132722.htm, https://www.nato.int/cps/cn/natohq/official_texts_133169.htm, https://www.nato.int/cps/en/natohq/official_texts_185340.htm, https://www.nato.int/cps/en/natohq/official_texts_217320.htm, https://www.nato.int/cps/en/natohq/official_texts_227678.htm.

4 The Netherlands' whole-of-government, whole-of-society undertaking to boost resilience – an effort being led by the ministers responsible for justice, security, and defence – is a good example. See https://www.government.nl/latest/news/2024/12/06/government-works-to-increase-resilience-against-military-and-hybrid-threats.

5 Elisabeth Braw, "How to Involve Civil Society in Grey Zone Defence," in *Hybrid Threats and Grey Zone Conflict: The Challenge to Liberal Democracies*, ed. Mitt Regan and Aurel Sari (Oxford University Press, 2024), 563-564, https://academic.oup.com/book/56327.

6 Falk, *Strategic citizens*, 5-6.

7 Cyber attacks on critical infrastructure, on their own, have the potential to cause physical damage and harm, as well as disrupt civil order. See Elisabeth Braw and Peter Roberts, *Societal Resilience as a Deterrent, NATO Science and Technology Organization* (March 2019), 11-4, https://www.sto.nato.int/publications/STO%20Meeting%20Proceedings/STO-MP-SAS-141/MP-SAS-141-11.pdf.

8 Bernd Horn, "War, Not War – War in the Shadows: Below Threshold Threats," in *Threat & SOF / Special Operations Response*, ed. Bernd Horn and Patricia J. Blocksome (CANSOFCOM Education & Research Centre, 2024), 82, https://publications.gc.ca/collections/collection_2024/mdn-dnd/D2-474-2024-eng.pdf.

9 Andrés B. Muñoz Mosquera and Nikoleta Chalanouli, "Decoding Grey Zone Environments," in *Hybrid Threats and Grey Zone Conflict: The Challenge to Liberal Democracies*, ed. Mitt Regan and Aurel Sari (Oxford University Press, 2024), 336-337, https://academic.oup.com/book/56327.

10 Horn, "War, Not War – War in the Shadows," 86-89.

11 Public Safety Canada, "National Security Public Opinion Research Snapshot (Public Safety Canada, 2022), https://www.publicsafety.gc.ca/cnt/ntnl-scrt/cntr-trrrsm/pblc-pnn-rsrch-snpsht-2021-en.aspx.

12 Public Inquiry into Foreign Interference in Federal Electoral Processes and Democratic Institutions, *Final Report, Volume 4* (Public Inquiry into Foreign Interference in Federal Electoral Processes and Democratic Institutions, 2025), 126, https://foreigninterferencecommission.ca/fileadmin/PIFI_-_Final_Report_Vol._4__2025_.pdf.

13 The polls are telling. See the annex to this paper for analysis and data sources.

14 According to an Ipsos poll conducted on behalf of Global News in December 2022, 14% of Baby Boomers, 25% of Generation X, 37% of Millennials, and 46% of Generation Z are more likely to trust information on social media platforms than traditional media. See https://www.ipsos.com/en-ca/news-polls/Young-Canadians-More-Trusting-of-Information-on-Social-Media-Than-Other-Generations.

15 Yvonne R. Masakowski and Janet M. Blatny, *Mitigating and Responding to Cognitive Warfare. NATO Science and Technology Organization* (March 2023), ES-1, https://www.researchgate.net/publication/369305190_Mitigating_and_Responding_to_Cognitive_Warfare.

16 NATO Allied Command Transformation, "Cognitive Warfare," accessed January 26, 2025, https://www.act.nato.int/activities/cognitive-warfare.

17 Horn, "War, Not War – War in the Shadows," 82.

18 NATO Allied Command Transformation, "Allied Command Transformation develops the Cognitive Warfare Concept to Combat Disinformation and Defend Against "Cognitive Warfare"," accessed January 26, 2025, https://www.act.nato.int/article/cogwar-concept.

19 For additional insight, see European Centre of Excellence for Countering Hybrid Threats, *Deterrence: Proposing a more strategic approach to countering hybrid threats* (European Centre of Excellence for Countering Hybrid Threats, 2020), 9-17, https://www.hybridcoe.fi/wp-content/uploads/2020/07/Deterrence_public.pdf.

20 Braw and Roberts, *Societal Resilience as a Deterrent*, 11-2 – 11-6.

21 Michael Roi, "Cognitive Warfare," paper presented at Inaugural Homeland Defense Symposium, Carlisle Barracks, PA (February 2024), 20.

22 Dean S. Hartley III and Kenneth O. Jobson, *Cognitive Superiority* (Springer, 2020), 15, https://doi.org/10.1007/978-3-030-60184-3_1.

23 European Centre of Excellence for Countering Hybrid Threats, *Deterring Hybrid Threats: A Playbook for Practitioners* (European Centre of Excellence for Countering Hybrid Threats, 2020), 20-27.

24 Under the Critical Election Incident Protocol, the federal government brings threats to electoral integrity to the public's attention. Through Rapid Response Mechanism Canada, it highlights emerging disinformation trends and tactics attributed to specific hostile states that target Canada and Canadians. The security and intelligence community sheds light on foreign interference and transnational repression through threat-focused publications; guides and toolkits for elected officials, community leaders, and public servants; threat briefings to Parliamentarians and party leadership; and stakeholder outreach. Departments and agencies offer a host of resources on risks to research security and best practices in mitigating them. Last but not least, through Canadian Heritage's Digital Citizen Contribution Program, the federal government funds citizen-facing projects by non-governmental organisations that develop and deliver public awareness programming, training, and learning materials in support of civic and digital media literacy. Of the measures designed for Canadian youth, the focus is on disinformation and cyber threats.

25 Zsuzsa Blasko et al., *Civic attitudes and behavioural intentions among 14-year-olds. How can education make a difference towards a more democratic and cohesive Europe?* (Publications Office of the European Union, 2018), 9, 11, https://publications.jrc.ec.europa.eu/repository/bitstream/JRC109180/jrc109180_iccs_science_for_policy_report_final_pubsy.pdf.

26 Blasko et al., *Civic attitudes and behavioural intentions among 14-year-olds*, 11-12.

27 Anja Neundorf, Richard G. Niemi and Kaat Smets, "The Compensation Effect of Civic Education on Political Engagement: How Civics Classes Make Up for Missing Parental Socialization," *Political Behavior* 38, no. 4 (2016): 946, https://link.springer.com/article/10.1007/s11109-016-9341-0.

28 Michael Morden et al., *Investing in Canadians' civic literacy: An answer to fake news and disinformation*, (Samara Centre for Democracy, 2019), 7, https://www.samaracentre.ca/articles/investing-in-canadians-civic-literacy.

29 Wilner, Alex. "Deterrence by De-legitimization in the Information Environment: Concept, Theory, and Practice," 72-73 and Nicole J. Jackson, "Deterrence and Strategic Disinformation: An Overview of Canada's Responses," 204, both in *Deterrence in the 21st Century: Statecraft in the Information Age*, ed. Eric Ouellet, Madeleine D'Agata and Keith Stewart (University of Calgary Press, 2024), https://www.jstor.org/stable/jj.11141796.

30 National Security and Intelligence Committee of Parliamentarians, *Special Report on Foreign Interference in Canada's Democratic Processes and Institutions* (National Security and Intelligence Committee of Parliamentarians, 2024), 67, https://www.nsicop-cpsnr.ca/reports/rp-2024-06-03/special-report-foreign-interference.pdf.

31 The Dais, *Building Democratic Resilience to Foreign Disinformation in Canada* (The Dais, June 2024), 10, https://dais.ca/wp-content/uploads/2024/06/PCO-Workshop-Final-Paper_V7.pdf.

32 Tom Buchanan, "Why Do People Share Disinformation on Social Media?," Centre for Research and Evidence on Security Threats (September 4, 2020), https://crestresearch.ac.uk/resources/disinformation-on-social-media.

33 Matthew Johnson, "Canada must embrace digital media literacy; To resist disinformation, we need education, writes Matthew Johnson," Leader Post, October 28, 2022, https://www.proquest.com/docview/2729732738?_oafollow=false&accountid=9867&pq-origsite=summon&sourcetype=Newspapers.

34 Samantha McAleese and Kara Brisson-Boivin, *From Access to Engagement: Building a Digital Media Literacy Strategy for Canada* (MediaSmarts, 2022), 7-8, https://mediasmarts.ca/sites/default/files/2023-01/From%20Access%20to%20Engagement%20-%20Building%20a%20Digital%20Media%20Literacy%20Strategy%20for%20Canada%202022.pdf

35 CIVIX, *Civics on the Sidelines: A National Survey of Canadian Educators on Citizenship Education* (CIVIX, 2023), 10, https://civix.ca/wp-content/uploads/2024/04/CIVIX-Civics-on-the-Sidelines-Report-EN-1.pdf.

36 Morden et al., *Investing in Canadians' civic literacy*, 4, 10.

37 CIVIX, *Civics on the Sidelines*, 4, 5, 13.

38 Morden et al., *Investing in Canadians' civic literacy*, 16-18.

39 See Center for Strategic and International Studies, "Civics," accessed March 3, 2025, https://www.csis.org/programs/defending-democratic-institutions/civics.

40 Leif Inge Magnussen et al., "Competence for Hybrid Threats: A strategic competitive development model," in *Preparing for Hybrid Threats to Security: Collaborative Preparedness and Response*, ed. Odd Jarl Borch and Tormod Heier (Routledge, 2025), https://library.oapen.org/handle/20.500.12657/93079.

41 Saara Salomaa and Lauri Palsa, *Media Literacy in Finland: National Media Education Policy* (Ministry of Education and Culture, 2019), 34, https://medialukutaitosuomessa.fi/mediaeducationpolicy.pdf.

42 OECD, *Facts not Fakes: Tackling Disinformation, Strengthening Information Integrity* (OECD Publishing, 2024), 77, https://www.oecd.org/content/dam/oecd/en/publications/reports/2024/03/facts-not-fakes-tackling-disinformation-strengthening-information-integrity_ff96d19f/d909ff7a-en.pdf.

43 Amy Yee, "The country inoculating against disinformation," BBC, January 30, 2022, https://www.bbc.com/future/article/20220128-the-country-inoculating-against-disinformation; and OECD, *Facts not Fakes*, 78.

44 Unsurprisingly, Finland has consistently topped the Media Literacy Index ranking of 35-41 European countries since its inception in 2017, and Estonia has consistently ranked in the top five. The latest edition can be found at https://osis.bg/wp-content/uploads/2023/06/MLI-report-in-English-22.06.pdf.

45 European Commission: European Education and Culture Executive Agency, *Citizenship education at school in Europe, 2017* (Publications Office of the European Union, 2017), 35, 38, https://data.europa.eu/doi/10.2797/536166.

46 Julian McDougall, Marketa Zezulkova, Barry van Driel and Dalibor Sternadel, *Teaching media literacy in Europe: evidence of effective school practices in primary and secondary education* (Publications Office of the European Union, 2018), 61, 62, 75, https://nesetweb.eu/wp-content/uploads/2019/06/AR2_Full_Report_With_identifiers_Teaching-Media-Literacy.pdf.

47 Masakowski and Blatny, *Mitigating and Responding to Cognitive Warfare*, 10-4.

48 The Dais, *Building Democratic Resilience to Foreign Disinformation in Canada*, 8.

49 See Sean S. Costigan and Michael Hennessy, *Hybrid Threats and Hybrid Warfare Reference Curriculum* (NATO Headquarters Brussels, 2024), https://www.nato.int/nato_static_fl2014/assets/pdf/2024/7/pdf/241007-hybrid-threats-and-hybrid-warfare.pdf.

50 See https://mediasmarts.ca/sites/default/files/2023-06/digital-media-literacy-framework.pdf.

51 Originally a private sector initiative, the Canada Studies Foundation (active in the 1970s and 1980s) was jointly funded for a time by the federal government and Council of Ministers of Education, Canada, and eventually, almost exclusively by the federal government.

52 Alan Sears, "Instruments of Policy: How the National State Influences Citizenship Education in Canada," *Canadian Ethnic Studies* 29, no. 2 (1997): 5, 8, 9, 11, https://www.proquest.com/scholarly-journals/instruments-policy-how-national-state-influences/docview/1293198091/se-2.

53 Kyle Hiebert, "In 2024, National Security Requires a Whole-of-Society Approach," Centre for International Governance Innovation (June 20, 2024), https://www.cigionline.org/articles/in-2024-national-security-requires-a-whole-of-society-approach.

54 The Dais, *Building Democratic Resilience to Foreign Disinformation in Canada*, 16.

55 Advocating for new laws, policies, and programs, business leaders are asking the federal government to adopt a comprehensive, proactive, and long-term approach to countering economic-based threats. See Business Council of Canada, *Economic Security is National Security: The Case for an Integrated Strategy* (Business Council of Canada, 2023), 19, 22, https://www.thebusinesscouncil.ca/wp-content/uploads/2022/07/Economic-Security-is-National-Security-Report_digital.pdf.

56 It identified information manipulation as "the single biggest risk to democracy" and "civic resilience as fundamental to combating foreign interference". See Public Inquiry into Foreign Interference in Federal Electoral Processes and Democratic Institutions, *Final Report, Volume 1* (Public Inquiry into Foreign Interference in Federal Electoral Processes and Democratic Institutions, 2025), 6, https://foreigninterferencecommission.ca/fileadmin/report_volume_1.pdf; and Public Inquiry into Foreign Interference in Federal Electoral Processes and Democratic Institutions, *Final Report, Volume 5* (Public Inquiry into Foreign Interference in Federal Electoral Processes and Democratic Institutions, 2025), 41, 46, https://foreigninterferencecommission.ca/fileadmin/report_volume_5.pdf.

57 Research Co., *Poll conducted by Research Co. on Views of Other Countries in Canada* (Research Co., 2024), https://researchco.ca/wp-content/uploads/2024/07/Tables_Countries_CAN_24Jul2024.pdf.

58 Research Co., *Poll conducted by Research Co. on Views of Other Countries in Canada* (Research Co., 2020), https://researchco.ca/wp-content/uploads/2020/01/Tables_Countries_CAN_10Jan2020.pdf.

59 Moira Fagan, Sneha Gubbala and Jacob Poushter, "Views of Russia and Putin," Pew Research Center (July 2, 2024), https://www.pewresearch.org/global/2024/07/02/views-of-russia-and-putin-july-24.

60 See https://angusreid.org/wp-content/uploads/2024/06/2024.06.13_Favourability_of_Nations_CAN_tables.pdf.

61 Lynette Ong, *Foreign Interference and the Health of Canadian Democracy*: *Report from a Nationwide Public Opinion Survey* (Digital Public Square, 2024), 9, https://orgsite.cdn.prismic.io/orgsite/ZzZS168jQArT04yL_V10-ReportPublicOpinionSurveyofForeignInterferenceinCanada.pdf.

62 Ong, *Foreign Interference and the Health of Canadian Democracy*, 13.