July 2025

Deterrence Through Whole-of-Society Resilience

Meeting the Challenge of Hybrid Threats in the Grey Zone

Michael A. Rostek,
Defence Research and Development Canada

Peter Gizewski,
Royal Military College of Canada

**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

The world remains a dangerous place. Security analysis affirms that not only does the world remain uncertain and unpredictable but also highly challenging in terms of security concerns that are both traditional and unconventional. Terrorist attacks in France, Belgium, and Canada; military action in Ukraine, Syria, Iran, and Israel and political turbulence in Turkey, United Kingdom (UK) and the United States (US) among others, exemplify that complexity and uncertainty remain dominant characteristics of the global and domestic security environment. A renewed ideological competition has emerged between a 21st century form of authoritarianism in Russia, China and other countries and largely democratic nations. Meanwhile regional security challenges (Iran, North Korea. South China Sea), as well as threats emanating from transnational terrorist organizations (e.g., Islamic State, Boko Haram) and weak and/or fragile states (also known as ungoverned spaces) continue to pose a significant challenge to the international community. Non-traditional security challenges, such as the instability brought about by accelerating climate change, mass migration and pandemics, demand equal attention from our security infrastructure.

In addition to the complex security challenges noted above, the world is now witness to the emergence of hybrid warfare being waged in the intermediate spaces, or the seams of traditional ways of thinking referred to as the grey zone.[1] Conducted just below the threshold of armed conflict, hybrid activity involves coordinated application of diplomatic, informational, cyber, military and economic instruments to achieve strategic or operational objectives.[2] Advances in technology have made "hybrid" or "grey zone" attacks in the cyber and information domains especially prominent and have included such actions as intellectual property theft, privacy breaches, and the use of civilian companies or research institutions to advance military goals. Adversaries exploit these vulnerabilities to weaken our defence industrial base, compromise our industrial supply chains and interfere with our sovereign decision-making processes."[3]

Recent years reveal that Canada is hardly immune from such threats. For instance, not only has concern over the potential impact of influence and disinformation campaigns been evident in past electoral politics, but it was also on display during the nation's battle against COVID-19. Evident more recently still are concerns that have arisen over foreign influence in areas of university research,[4] and over disinformation presented on social media regarding Russia's ongoing armed invasion of Ukraine. Not surprisingly, Canada's defence policy has recognized the increasing use of "…hybrid methods in the "grey zone" – as a clear and growing security concern noting that, "…hybrid warfare in the grey zone will continue to evolve and present complex security challenges that undermine the credibility and legitimacy of national government(s) (and) international alliance(s)."[5]

Societal institutions must develop the resilience necessary to cope with the broad and unconventional threats and challenges which hybrid activities pose. In the context of national security, this refers to the ability to draw upon all elements of society to manage threats and risks, to adapt to them, and to recover from them should an attack or event occur, without losing the ability to provide basic functions and services to the members of that society.[6] Indeed resilience involves the ability of social institutions to absorb and adapt to the shocks and setbacks they are likely to face.

Notably, such capability not only promises to reduce the impact of aggressive actions but to raise the prospect of preventing them. In fact, societal resilience may be especially effective in deterring hybrid challenges not easily addressed by a reliance on military power, posing the prospect of inoculating a nation from the adverse impacts of actions which adversaries often conduct. Not only can such resilience help to deter attacks against a nation's material assets, but prevent challenges in the information domain as well. Once achieved, societal resilience can work to effectively delegitimize the attempts at malign influence which such hybrid activities often involve. Indeed, a key benefit stemming from the possession of societal resilience is its capacity to enable "deterrence by de-legitimization," Simply put, societal resilience can serve to reduce the ability, and ultimately the willingness, of aggressors to employ messages in the information domain aimed at gaining publicity, sympathy and /or reducing the cohesion of a targeted population.[7]

How does a society increase resilience and enhance deterrence against hybrid threats? Central is the development of a Whole-of-Society (WoS) approach, one that extends beyond core federal stakeholders or Whole-of-Government (WoG) to society as a whole. Such an approach would feature close cooperation and coordination between society and the various government institutions, organizations and agencies responsible for defence and security. When pursued effectively, the result promises not only the development of a true partnership between state and society in the pursuit of national security, but an expansion of the capabilities needed for better deterring many of the challenges that hybrid actions pose.

The following discussion elaborates on the observations offered above. It examines the meaning of resilience, its potential role as a means of deterring hybrid actions, and the importance of adopting a WoS approach for achieving it and exploiting its deterrent potential. It then examines the experiences of Finland and Australia, two nations both noted for their active pursuit of WoS resilience and its use in deterring hybrid activities. The study concludes by advancing a number of potentially useful insights and recommendations for the pursuit of WoS resilience as a means of bolstering the deterrence of hybrid threats and challenges within the Canadian context.

Whole-of-Society Resilience

Growing concern over the use of hybrid activities underlines the fact that many of the virtues inherent in open societies can be readily exploited by those seeking to undermine them in pursuit of their own interests and objectives. Indeed, the state restraint, pluralism, free media and economic openness often lauded as the key advantages of open societies can just as easily provide openings for malign actors to undermine their internal cohesion and accelerate polarization and dissent through use of tactics such as disinformation and influence campaigns, targeted assassinations, kidnappings, cyber-attacks, hostile business practices and even occupation by unofficial militias aligned with foreign powers.[8]

The fact that such tactics are often non-kinetic and subtle can make attribution of their source difficult and effective counters hard to devise. Not surprisingly, resourceful adversaries are increasingly using such actions to force wedges into the fault lines of open societies at times with significant effect.[9]

Building societal resilience offers a means of addressing such challenges, reducing both the likelihood and/or the impacts of adversarial actions while at the same time enabling open societies to remain loyal to the norms of behaviour upon which they are based. Resilience increases the capacity of societies to absorb, adapt and recover from disruption, duress, stress and shock.[10]

Achieving resilience requires decision processes that embrace anticipation, adaptation, and flexibility. Moreover, it is a society-wide undertaking, involving the pursuit of activities and actions that are comprehensive in scope and application with efforts aimed not only at resilience building in national institutions but at community, individual and even international levels.[11] While often associated with technical solutions and measures surrounding protection of infrastructure, resilience is also a deeply social or societal phenomenon. In fact, societal resilience is premised on the belief that citizens, communities, organizations and institutions all share responsibility for national security.[12] Inclusion of a diverse range of societal actors and decision makers is therefore essential.

A WoS approach offers a means of harnessing the capacities required to ensure that WoS resilience is realized. The approach represents an inclusive model of cooperation and joint preparedness that aims to bring all relevant actors together into a comprehensive system and involves efforts to diversify and devolve responsibilities for security production to market and societal based actors while maintaining a strong coordinating role for the state.[13] Resilience is pursued as a partnership between the state and civil society with a wide range of social actors playing key roles in building resilience capabilities, supporting the state in maintaining preparedness and in ensuring the continuity of societal functions and supply lines in the face of threat.[14]

Ideally, decision-making is relatively non-hierarchical, networked and highly distributed. This is essential in an environment characterized by complex threats that are themselves often distributed, networked and continually evolving.[15] Non-hierarchical decision-making processes not only tend to match the nature of hybrid challenges, but better enable decision makers to embrace emergent opportunities and adapt quickly to address the threats faced.[16] In fact, the self-organization of actors is seen as a key foundation for more sustainable and diffuse responses to identifying and addressing diverse threats.

Inclusiveness, open communication, information-sharing and transparency regarding the nature of threats, their identification and how they can be countered are key to the success of such an approach. In fact, an educated, engaged and empowered citizenry is essential. So too is a government that is proactive in facilitating inclusive societal participation in building resilience and maintaining it once it is achieved. Not only does this involve developing genuine partnerships between government and local institutions and groups in designing activities to increase resilience, but sharing responsibility and also authority and control over such initiatives so as to empower local officials and organizations to take the lead in resilience building efforts.

Most fundamentally, achieving WoS resilience involves a capacity and commitment to sound and ethical management of security issues on the part of authorities, active and sustained engagement with those potentially impacted, and a strict adherence to the rule of law and existing societal norms and values throughout the process. Indeed, the practice of such principals is essential for generating the societal trust and social capital needed to actively pursue societal resilience and maintain it in a sustained and effective manner.

Resilience, Deterrence and De-legitimization

WOS resilience offers significant deterrent potential. While not strictly conceived of as a deterrence strategy, WoS resilience can nonetheless bolster it. Yet unlike traditional state-based notions of deterrence which focus largely on the use the military power of armed forces to prevent attack, WoS resilience offers greater potential to deter the various activities that hybrid threats often involve.

This is especially evident in cases involving non-kinetic tactics such as disinformation campaigns, hostile business practices, economic subversion and the provision of financial support to radical political movements within target societies. Identifying the origins of such actions can be difficult, and even when successful, military responses generally lack the proportionality required for such deterrent threats to be credible. In fact, engaging in such action may well prompt widespread criticism, both internationally and domestically, and even unwarranted escalation.

In contrast, WoS resilience offers a range of means more directly relevant to deterring such threats. Some, such as the physical hardening of critical infrastructure, networks and services, as well as resource planning are relatively technical in character and enhance deterrence by virtue of their capacity to reduce the vulnerability of such assets to attack. Yet many others emphasize the capacity to employ soft power resources to protect society from the hybrid threats and tactics that aggressors employ.[17]

Here, measures that reflect democratic values and norms as well as the promotion of transparency, rule of law and citizen activism are particularly prominent and offer key means to support deterrence of hybrid actions. In this regard, cultivating an informed and engaged citizenry capable of critically assessing information and identifying suspicious activity, enhancing transparency in areas such as business, politics, media and the non-profit world, developing strong anticorruption laws and regulations and initiatives aimed at better integrating diaspora communities and minorities into society are exemplary. Not only can such measures provide considerable capacity to identify and accurately assess instances of hybrid interference, but also the ability to expose them publicly and counter their impacts. In short, pursuit and realization of resilience increases the prospects of society-wide involvement in deterrence.[18]

In fact, a number of scholars now contend that WoS resilience stands as a key component in what has become a fifth wave of thinking on deterrence. Such thinking distinguishes itself from previous waves by focusing on the deterrence of state and sub-state use of hybrid threats through strict reliance on non-military, vice military, means, developed and implemented by government in partnership with society at large.[19]

Achieving WoS resilience increases the capacity to fashion effective deterrent strategies in a number of ways. Certainly, it can provide the physical and military-technical means helpful for deterring military aggression. Yet by harnessing the power of shared societal norms and values through the development and use of narratives based on them, resilience can also serve to counter many of the informational threats that hybrid activities involve as well.

Such norms and values provide guidance to both authorities and society at large regarding the truth and legitimacy of action and the proper methods and processes required for effectively determining it. Once they are widely internalized and practiced, this alone can work to diminish a society's susceptibility to information warfare by bolstering its ideational and collective resilience.[20] In essence, development of state-society partnerships and collective allegiance to the national norms, values and laws can serve as a normative shield against informational attack.

Yet soft power resources also hold the potential to alter an adversary's capacity and willingness to engage in such interference by providing the ability to fashion narratives that systematically challenge or "delegitimize" the veracity of the information advanced and the motivations and goals that inform it. Societal resilience deters by de-legitimization, by denying would-be aggressors the fertile ground upon which their malicious narratives can thrive.[21]

Possible deterrent actions in this vein can include efforts to discredit the rhetoric of terrorist organizations in support of their agendas (e.g., al Qaeda) as well as future disinformation campaigns launched by various state adversaries (e.g., China, Russia) and their operatives. Still others can involve initiatives at the multi-lateral or international levels to establish norms aimed at proscribing behaviour or establishing red lines regarding various types of information operations,[22] as well as more general efforts to discredit, denounce and shame groups or individual leaders engaged in weaponizing the information environment.[23] In the former case, defenders would aim to ensure that violation of the norms developed would generate a level of international opprobrium sufficient to deter challengers from engaging in the proscribed action. As for the latter, deterrence would stem from the threatened release of embarrassing intelligence or other information about an adversary that undermines its reputation and credibility.

Resilience in Practice: Finland and Australia

Examination of the pursuit and practice of WoS resilience in the nations of Finland and Australia provides valuable insights into how resilience is established, practiced, and how it can bolster deterrence. In fact, both offer useful insights for the development and implementation of WoS resilience within a Canadian context.

Much like Canada, both Finland and Australia each boast technologically advanced economies, highly educated populations and long traditions of democratic governance. Both are among the most prominent states that have focused attention on developing societal resilience. And both also have confronted the challenge of ensuring the protection of the rights and privileges of ethnic minorities within their societies. Such similarities suggest that insights derived from each may be more readily applicable to the Canadian context than those provided from an examination of less similar nations.

Finland

Resilience has long been viewed as a robust and essential attribute for achieving Finland's national security. Finland's approach, known as the comprehensive security model (CSM), is detailed in the Government Resolution for the Security Strategy for Society. Formalized in 2003 with the most recent version released in 2017,[24] the strategy lays out the general principles governing preparedness in Finnish society.[25] These principles are based on the concept of comprehensive security whereby all vital functions of society are jointly safeguarded by authorities, business operators, organisations and citizens, and in which there is a readiness to use both military and non-military means to counter both internal and external threats and challenges.[26]

The aim is that during a crisis, the entirety of Finnish society is able to rapidly mobilize resources where needed, recover quickly, and adapt its functions based on lessons learned. As such, the concept is part of a philosophy of good public governance whereby the CSM champions a cooperative approach to security in which all relevant actors share and analyse security information, prepare joint plans as well as train and work together.[27] Indeed, the notion of collaboration lies at its foundation.

The model focuses on the applicability of preparedness principles at all levels of society (i.e., national, regional, local). Seven vital functions of society are identified: Leadership, Psychological Resilience, Functional Capacity of Population and Services, Economy, Infrastructure and Security of Supply Internal Security, Defence Capability and International and European Union Activities. Together they support the broad and cross-sectoral nature of preparedness which the model aims to achieve.[28]

All functions are highly interdependent and interconnected. This not only works to heighten joint awareness of issues and challenges, but the building of trust among all involved in the preparedness process.[29] By bringing actors from across society together to contribute to and share in the preparedness of the nation, the CSM in effect aims to facilitate the development and maintenance of a "culture" of preparedness and resilience.

Institutions, Players and Processes

Senior decision-making is a government responsibility, supported by parliament, but a large number of decisions are delegated to competent authorities. In a crisis situation, the ministry responsible for the function within which the crisis occurs takes a leading role on the response, while other authorities assist as appropriate. A Security Committee, consisting of the permanent secretaries of all government ministries, the directors of the key government agencies, the military, as well as members of the private sector and civil society coordinates and monitors developments to ensure that the strategy remains relevant and revised when necessary. Collaborative forums meet regularly to share information, discuss security issues and plan preparedness exercises.[30]

Actors feeding into the process include: the central government, the authorities, business operators, regions and municipalities, universities, research institutions, organisations, and individuals. The result is a comprehensive security network in which the sharing of information, setting of joint objectives and commitments to co-operation take place. All contributors are considered relevant security actors with those sitting outside of traditional security circles accorded the same importance for the impact they have on the preparedness of wider Finnish society as those belonging to traditional circles.[31] The strategy also highlights the importance of the independent preparedness of business operators, organisations, communities, and households in upholding Finland's resilience. In order to promote the preparedness of citizens, the strategy acknowledges the requirement for systematic dissemination of information and appropriate training opportunities.

A longstanding policy of a military conscription serves to 'produce troops with good combat efficiency and skilled and capable personnel for placement in the wartime units of the Defence Forces.'[32] Indeed, as an essential component of national defence and deterrence, military training helps to 'maintain basic readiness and the capability to raise readiness when necessary.'[33]

Beyond this however, the CSM also ensures the maintenance of a basic level of understanding of defence, preparedness and self-sufficiency skills throughout society, with training opportunities provided to both civilian and military leaders in national and regional defence courses.[34] The courses deepen the understanding of comprehensive security and improves the cooperation between different sectors of society and government institutions.[35]

Adding to this is a marked emphasis on education. Finland boasts one of the most rigorous educational systems in the world and places an emphasis on critical thinking at an early age. Not only does this serve to bolster resilience to disinformation, but the population's ability to adapt to changing social and economic realities if and when required.

Resilience-Building Measures and Capabilities

Measures aimed at ensuring WoS resilience reflect both the nation's emphasis on public-private coordination as well as the need to evolve and adapt to the ever-changing security environment. Finland maintains a modern, well-prepared military. It's possession of a Reserve Army along with its extensive system of national defence courses has helped to ensure the maintenance of a close civil military relationship and a strong understanding of national defence and security issues throughout government and society. It has also worked to facilitate societal support for both the military and defence and security in general. Opinion polls consistently demonstrate a high willingness among Finns to fight for their country and levels of public confidence in the national armed forces which are among the highest in Europe.[36] Civil defence capability is robust as well with the nation currently capable of accommodating approximately 65% of Finland's population within a time frame of 72 hours.[37]

A well-functioning and secure system of supply is also evident and reflects a model of coordination and collaboration between central and local authorities, business and industry. Here, the focus is on ensuring "society's ability to maintain the basic economic functions needed for ensuring the livelihood of the nation's people, the overall functioning and safety of society and the material preconditions for military defence in the event of serious disruptions and emergencies through extensive public-private cooperation in supply chain management."[38]

Involvement in a strong international security cooperation network further bolsters resilience. Bilateral and multilateral cooperation as well as membership in organizations such as the EU, UN, OSCE and NATO provides a significant supplement to resilience-building efforts at home - increasing awareness, dialogue and solutions to emerging threats and challenges as well as the prospects for assistance in the event of threat or crisis. Such involvement has in fact generated considerable advocacy on the part of Finland for placing hybrid threats on the agenda of EU defence and foreign minister meetings[39] as well as the creation in Helsinki of a major center of expertise on lessons learned and know-how on countering hybrid threats.

Meanwhile on the domestic front, concerns over hybrid threats, terrorism and immigration issues have been met with a gradual tightening of internal security. In response to Russian cyber espionage, Finland adopted a Cyber-Security Strategy in 2013. Investments to strengthen the resilience of Finland's information technology (IT) infrastructure and raise public awareness of cyber-security issues have been increased.[40] And the powers of Finland's Security and Intelligence Service (SUPO) have been expanded in the areas of surveillance and intelligence under a new Civilian Intelligence Act.[41]

Collaboration between the Finnish Security and Intelligence Service (SUPO) and the police has also been strengthened, and synergy between the police and the armed forces improved. Moreover, Finland's approach to combating illegal immigration has been modified,[42] and border guards now hold greater powers in a range of areas.[43]

At the same time, both public and private actors have combined to counter challenges stemming from a rise in the conduct disinformation operations targeting the country. At the government level, such action has involved efforts by a special team of experts and officials to identify, analyze and respond to the influencing efforts identified, quickly deny the false information involved, prevent its dissemination and organize training for government officials.[44] It has also involved the Finnish Broadcasting Company YLE who counters disinformation not only through regular production of news but also by fact checking and designing other journalistic actions and content.[45]

Beyond this, government efforts are heavily supplemented by a range of grass roots initiatives comprised of journalists, NGOs and civic engagement. Fakibaari, a Finnish NGO focused on independent journalism, fact-checking and digital literacy information works to support fact-based public debate, digital information literacy and participatory democracy in an effort to strengthen critical thinking and responsible political participation.[46] Various media outlets have issued regular statements condemning the spread of fake news. And campaigns to bolster resilience against misinformation are prominent in Finnish schools as well.[47]

Australia

Resilience and its basic components have been widely practiced at the societal level throughout Australian history. Yet interest in the pursuit of a unified and integrated government strategy for institutionalizing its development and practice has emerged only recently and in somewhat gradual and piece meal fashion.

Notable has been the government's emphasis on resilience building as disaster response, a fact largely based on a concern over the environmental impacts of natural disasters. Initially articulated in Australia`s National Strategy for Disaster Resilience (2011),[48] the initiative involves the adoption of an integrated, whole of nation effort based on four principles: Prevention, Preparedness, Response and Recovery, with the chief focus placed on Prevention and Recovery. Emphasis is placed on "shared responsibility" whereby multiple stakeholders are empowered to directly participate in resilience building and crisis response, including individuals, families, local communities and authorities, the private sector (i.e., small and medium businesses), and state/territory and federal government.[49] So too is the development of enhanced partnerships, sound understanding of the risk environment and disaster impacts, and adaptive and empowered communities capable of acting when necessary.[50]

A capacity to function well under stress, adapt, and practice both self-reliance and social engagement are touted as the strategy's chief objectives**.** And the conduct of risk assessments across social, economic and natural environments, the implementation of consistent methodologies to improve risk management planning, and building strong networks across sectors and regions are all cited as fundamental for its realization.

A highly decentralized structure of governance ensures that much in the way of strategy implementation falls upon the nation's six federated states/territories who hold much of the power and responsibility for crisis management and planning. Yet federal efforts aimed at coordinating resilience-building efforts are numerous. Key initiatives include the 2018 National Strategy for Disaster Resilience, the Disaster Response Plan, and the 2019 National Disaster Resilience Reduction Framework, a framework which guides national, whole-of-society efforts to proactively reduce disaster risk to minimise the loss and suffering caused by disasters. Not only has this led to more coordinated resilience-building across government, but increased awareness of and participation in resilience building initiatives by business and industry, NGOs and Non-Profit Organizations (NPOs), and individual members of local communities nation-wide.

Additional resilience-building efforts have followed with initiatives to support resilience advanced not only in the realm of the environment but also in areas such as cyber security and defence. The 2020 Defence Strategic Update identifies disaster and national resilience as a priority for Australian defence. While the Australian Defence Force (ADF) has long assisted civilian authorities in addressing catastrophic natural disasters, the document underlines the need for integration of resilience considerations in defence planning as well as the need for multi-agency cooperation.[51] It also calls for further efforts to bolster supply chain security as well as the defence of critical national infrastructure, particularly from cyber-threats.[52] A follow-on review released in 2023 extends the focus on resilience further still noting both its significance as a key component of a WoG approach to security and as a central component of credible deterrence.[53] Indeed, the review notes that a high level of resilience not only makes the nation a harder target and less susceptible to coercion, but is key for signalling Australia's resolve to defend itself to potential adversaries.[54]

Australia has also released an updated National Cyber Strategy for developing a multifaceted plan to identify and mitigate cyber-attacks against the country as well as critical infrastructure. The plan, which includes cyber shields, aims to position Australia to manage and mitigate the shifting cyber threat landscape with resilience and efficacy.[55]

Institutions, Players and Processes

Given that Australia is a federal state, state/territory and local authorities hold primary responsibility for resilience and crisis response. Meanwhile, the national government covers roles and functions not otherwise assumed by the lower levels of governance and also retains operational and strategic capabilities which it can provide, upon request, to states/territories in times of crisis.[56] National government support during natural calamities is regulated via the Australian Government Crisis Management Framework. This framework identifies the principal stakeholders involved in the national authority's WoG approach to natural and human-induced crises and resilience building efforts, their duties and responsibilities.[57]

In general, the Ministry Responsible for Disaster Management leads natural disaster response, while the Ministry of Home Affairs assumes the role in cases of threats to internal security or when ambiguity exists regarding which ministry should take the lead.[58] A National Coordination Mechanism is also activated to ensure that the full capabilities of the Australian, state/territory governments, as well as the private sector, are brought to bear during a crisis.[59]

The lead ministry activates the government's Disaster Response Plan which represents the mechanism through which states/territories can request non-financial assistance from the federal government. National level plans are augmented by state/territory plans, some of which are specific to certain types of emergencies[60] (e.g., bushfires, flooding).

Support to disaster impacted communities is handled by the National Recovery and Resiliency Agency (NRRA), a federal government agency under the Ministry of Home Affairs.[61] Deployed NRRA teams assess local needs and provide federally funded financial support across a range of programmes. Identical principles apply at the state/territory level, with a single agency taking the lead. As for risk management, emergency response, and recovery, all are conducted at the lowest level of effective coordination. If required, the provision of Defence Assistance to the Civil Community can be actioned as well. Such support can include the deployment of the ADF personnel to aid local response in combating emergencies or disasters.[62]

Government efforts to encourage societal awareness and training in areas such as emergency preparedness, management and disaster mitigation and relief are relatively widespread. This includes collaboration and cooperation with key industries, businesses (e.g., engineering firms, technology and innovation, construction and infrastructure and supply chain and logistics companies) educational institutions and with NGOs and community organizations.

Resilience-Building Measures and Capabilities

Measures aimed at ensuring resilience are numerous, and reflect both the nation's growing efforts to bolster as well as extend it to help address the challenges of an ever-changing security environment. An emphasis on resilience-building to address the impacts of natural disasters and climate change is especially noteworthy. Not only is this evident in the numerous strategy documents, frameworks, emergency response plans, guidelines and handbooks produced by both the Federal and State/territorial governments over the last decade, but also in the coordinating roles played by bodies such as the National Emergency Management Agency, the National Bushfire Recovery Agency and Emergency Management Australia.

It is also evident in recent efforts aimed at extending and improving capabilities in being. Funding has been increased to enhance Emergency Management Australia's capabilities to improve national disaster preparedness and response. The government has also established a National Recovery and Resilience Agency, an organization tasked with building national resilience and better preparing for future natural disasters. And a range of new Commonwealth programs have been created to fund initiatives to improve the long-term resilience of Australian communities and households and support the ongoing recovery needs of communities impacted by the 2019-20 bushfires.

Elsewhere, and in response to concerns over vulnerabilities in Australia's supply chain prompted by various environmental disasters and COVID-19, the government has launched the Supply Chain Resilience Initiative, an international collaboration between Australia, India and Japan aimed at promoting best practice national supply chain policy and principles in the Indo–Pacific. The initiative seeks to strengthen the supply chains of the participating states through fostering closer interconnectedness of their business.[63]

Progress on ensuring resilient infrastructure is also evident. Activity has included the release of Infrastructure Australia's " Pathway to Infrastructure Resilience," a whole-of-system, all-hazards approach to resilience planning that focuses on strengthening infrastructure assets, networks and sectors, and a new Critical Infrastructure Resilience Strategy which provides a framework for how industry, state and territory governments, and the federal government will work together to mature the security and resilience of critical infrastructure, and anticipate, prevent, prepare for, respond to and recover from all-hazards. All such efforts are facilitated by Australia's Trusted Information Sharing Network (TISN), a platform which provides industry and all levels of government a primary means of engaging to enhance security and resilience.[64]

On the cyber front, policy has been updated to address threats posed by ongoing technological change and international political developments.[65] Widespread concern stemming from a series of significant cyber incidents has resulted in efforts to bolster cyber-resilience, most recently in the form of the 2023-2030 Australian Cyber Security strategy along with an action plan detailing a series of initiatives for implementation over the next several years.

Other measures focus on countering foreign interference, and reflect a whole of nation approach to raising the cost and reducing the benefits to foreign actors interfering in Australian society. Significant steps to detect, disrupt and deter foreign interference activities include: the appointment of a National Counter Foreign Interference Coordinator, who works across government and non-government sectors to strengthen arrangements to counter foreign interference; a Counter Foreign Interference Taskforce to discover, disrupt and investigate foreign interference activity; the passage of legislation criminalizing foreign interference and espionage and increasing transparency around foreign-influence related activities, and the creation of a University Foreign Interference Taskforce to protect the higher education sector from foreign interference threats.[66]

The government is also responding to growing concerns over fake news and disinformation. This has included the creation of a taskforce to address threats to electoral integrity, a social media literacy campaign to address fake news during election campaigns and the introduction of initiatives to promote the development of media literacy skills for all students in the Australian curriculum.[67] Also, in 2023, the government introduced a Communications Legislation Amendment (Combatting Misinformation and Disinformation) Bill that aims to provide the Australian Communications and Media Authority with increased powers to combat online misinformation and disinformation.[68]

As for the defence front, while moves to modernize and augment the nation's military capabilities continue to emphasize the acquisition of hard (i.e., conventional military) power, recognition of WoS resilience as a critical component of deterrence, along with acknowledgement that greater effort be devoted to helping develop national cohesion and public awareness of security issues, indicates a greater appreciation of the need to pursue resilience more broadly. Beyond this, Australia's membership in a number of bilateral and multi-lateral diplomatic and military arrangements works to bolster resilience through cooperative efforts to ensure a stable regional order based on rule of law. For instance, participation in the Quadrilateral Security Dialogue (i.e., the "Quad") with the US, Japan and India aims to build a united front to resist challenges to the rules-based order, particularly in the maritime sphere. And Australian involvement in the Five Eyes intelligence Community provides a means of gaining significant intelligence support on issues of security concern.[69]

Notably, many of the resilience building initiatives underway are accompanied by efforts to promote effective communication and cooperation between governments and society at large. Not only has this involved considerable emphasis on information sharing, but also investment in community-based efforts to foster greater understanding, awareness and development of measures required to ensure societal resilience.

Societal responses to emergencies are not only reflective of the impact of such government initiatives, but also a strong level of NGO-led activity and community volunteerism in Australian society as a whole. During the Australian bushfires (June 2019-May 2020), one report identified a full 42 NGO and community-led initiatives and programs aimed at rapid response, recovery and rebuilding.[70] Nationwide rallies also represented part of the social response to actions taken by the Australian government.[71]

Support for Deterrence

Such resilience building efforts have strengthened the capacity of both Finland and Australia to respond more effectively to the onset of range of natural disaster and human induced disasters and crises. Yet they can also bolster the capacity of each to conduct effective deterrence in both the conventional and hybrid realms.

On the conventional front, active pursuit of initiatives aimed at the development and maintenance of modern, combat ready military forces capable of increasing the costs associated with conventional military aggression has long been evident in both nations. In this regard, measures such as consistent and solid investment in weapon systems and equipment, force structure, force readiness, and Reserve capability stand out as longstanding and key components of robust deterrence of attack by state militaries.

The development and implementation of resilience building measures aimed at hardening key systems (e.g., measures to ensure resilient infrastructure, security of supply, critical infrastructure and secure cyber-systems) offers a similar deterrent effect by reducing their vulnerability to conventional as well as hybrid attack and interference. And the possession of well-established social welfare programs, including progressive taxation and strong education and health care systems offers an additional level of deterrence in each -- potentially reducing the social inequalities and cleavages often targeted for exploitation by actors aiming to generate societal instability.

A capacity to employ resilience as a deterrent against disinformation efforts is also evident in both nations, a fact owing much to the development of initiatives that encourage greater collaboration, cooperation and information sharing between state and society. Here, the participation of personnel from all walks of society in the pursuit of security increases prospects for gaining greater situational awareness of threats which may arise and which government may at times not be fully aware of. And good government-civilian communication and information sharing can also increase prospects for attribution when threats are detected.[72]

In this regard, Australia's efforts to increase citizen awareness of malicious information online are instructive. In fact, such initiatives have been followed by a notable increase in the reporting of such incidents publicly. And similar information campaigns aimed at thwarting recent attempts by China to interfere in Australia's elections, and to spread misleading information regarding the origins of COVID-19 have clearly been launched to produce a deterrent impact.[73] Indeed, in such cases, government action, often aided by collaboration with the media and other public organizations, has involved a concerted effort to delegitimize information content judged as potentially destabilizing both at home and abroad.

Notably, calls for an even greater use of such de-legitimization strategies have been on the rise. General Angus Campbell, Chief of the ADF has recently argued strongly for the use of such public exposure remarking that sunshine is "an extraordinarily powerful disinfectant" against covert activity.[74] Others have concurred, calling for Canberra's use of such an approach more broadly in the Indo-Pacific region as a whole to routinely expose Chinese gray-zone actions.[75]

Resilience building initiatives against disinformation are similarly apparent in Finland, a fact illustrated by Helsinki's cooperation and collaboration with various media organizations in combatting such practice and its support to NGOs and educational groups involved in promoting media literacy and greater public awareness of disinformation campaigns. The impact of such efforts appears to be considerable, and has not only worked to thwart Russian attempts to use public radio to conduct influence activities within Finnish society, but may also have helped to ensure that similar efforts were abandoned altogether by instilling doubt in Moscow that continued attempts to use such methods would succeed.[76]

Other resilience measures promise similar deterrent benefits. Development of mechanisms to track and monitor foreign activities within each country including investment in key industries, the funding of political parties, NGOs and research institutes, as well as anti-corruption measures can provide important tools for generating information for potential use as a means of shaming and delegitimizing instances of hybrid activity if and when it occurs. Indeed, not only can the information gained bolster deterrence by serving to identify threats and fashion effective counters to them but also trust in government providing reassurance that the authorities have a firm grip on challenges faced.

To be sure, the use of such initiatives to enhance deterrence can take time. Their development, institutionalization and practice requires close and sustained cooperation and collaboration between state and society. As such, mutual trust and true partnership are essential to their pursuit and success. That said, pursuit of WoS resilience initiatives in Finland and Australia suggest that the potential benefits both in terms of deterrence in general and the deterrence of hybrid threats in particular can be promising.

Implications for Canada

As cases examined suggest, efforts to develop WoS resilience hold the potential to provide important and useful means for the deterring hybrid threats both generally and in the informational domain. Indeed, by developing a greater capacity both within government and society as a whole to prepare for, respond to and recover from the intended impacts of hybrid actions, resilience can help to increase the prospect that adversaries contemplating such activities will be deterred from their conduct by increasing the likelihood that they will fail to achieve their intended purpose.

To be sure, the development, character and success of WoS resilience strategies and their contributions to deterrence can owe much to national characteristics as well as the particular geopolitical context which each nation occupies. That said, transnational forces such as ongoing climate change and the spread of information technologies to malign actors underline the fact that significant threats to national security can increasingly transcend the realities of geography and national borders. Indeed, such realities can not only impact nations residing in conflict ridden regions but also those located in regions long regarded as islands of relative stability and security. Today no nation, Canada included, can credibly claim status as a "fire proof house".

In this regard, the pursuit of several broad measures are worthy of consideration. First, to the extent that pursuit of measures aimed at societal resilience are undertaken, they should flow from a broader national security strategy clearly articulating and elaborating the concept and the importance of pursuing it as a key component of the strategy which is advanced. In fact, such an initiative could be loosely based on Finland's CSM, albeit adjusted to accord more fully with the Canadian context. Such an approach would serve to ensure a broad understanding of societal resilience and its importance for national security and increase support for its pursuit. Furthermore, it would also help to integrate any ongoing departmental and agency focused initiatives into a coherent whole.

Second, resilience building initiatives must be undertaken in a spirit of true partnership between state and society. As the development of resilience measures in both nations illustrates, development and implementation of resilience building measures must be informed and pursued through strict adherence to norms of transparency, cooperation and information sharing between government and society. Indeed, such practices are essential for instilling the trust in government necessary for generating the societal support required for the effective pursuit of resilience measures.

Third, consideration should also be given to the development of education and training programs aimed at increasing societal understanding and awareness of hybrid threats, and the steps required to address them. In this regard, such measures could include courses and training in defence and resilience for government officials as well as business and community leaders, the development and promotion of media literacy campaigns perhaps organized and led by NGOs and the creation of courses aimed at the development of critical thinking and media literacy skills for use in both primary and secondary education.[77] While the benefits of such initiatives will likely take time to emerge, efforts to strengthen resilience by providing education and training to citizens in both Finland and Australia indicates that they can yield significant dividends when adequately resourced and pursued in a sustained manner.

Fourth and finally, Canada should give consideration to the creation of a program aimed at providing Canadians with personnel specifically charged with the task of raising awareness of potential security issues that could arise within their communities as well as the resilience building measures required to address them. Indeed, creation of a cadre of such "resilience specialists" perhaps drawn from various government departments and agencies (e.g., Department of National Defence, Emergency Services Canada, Global Affairs Canada) could be particularly useful for addressing the security concerns and challenges that could arise in Canada's remote areas (e.g., Canada's North) providing a resource that would help ensure that such communities received the benefit of on-site knowledge and expertise in resilience building while at the same time generating the trust needed to ensure community understanding and support for any measures that are implemented.

The Reserve Force Contribution to WoS Resilience

Notably, Canada's Reserve Force could play a central role in any Canadian WoS resilience effort. As a component part of Canada's national security infrastructure, the Reserve Force role is to train until placed on active service for operations, to support training and fill institutional needs on a continual or temporary basis. At present, there is high potential for operations to quickly consume the capacity of the standing high-readiness capabilities of the CAF. Reconstitution and modernization efforts are underway to stave of the worst effects of this current and future operating environment. The Reserve Force has an important role to play in this regard. In fact, such a role extends beyond the "twinning" of Reserve Force units, or Reservists, into Regular Force units to the provision of operational capabilities, some which do not exist within the CAF today.[78]

'Enabling Full-Time Capability through Part-Time Service: A New Vision for the Reserve Force' provides the foundation for conceiving new capabilities for the Reserve Force. Indeed, it states that "[t]he ability to quickly mobilize additional capacities and capabilities must become the key overarching Reserve Force focus to ensure CAF resiliency."[79] Moreover, it also goes on to articulate strategic imperatives for the future Reserve Force that can positively contribute to wider national resilience and socioeconomic needs of the communities in which they reside.[80] In fact, one such vision objective is to design and implement new and enhanced roles for Reservists, Reserve Force units and formations between today and 2034. In many cases this capacity can exist in the guise of Reserve units, their equipment and infrastructure to support other whole-of-government efforts, including in underserved, remote regions of Canada.

Such a vision statement provides the necessary backdrop from which to conceive of new capabilities for the Reserve Force and potentially offer a novel perspective in contributing to deterrence of hybrid threats in the grey zone. The pursuit of WoS resilience through a new Reserve Force contribution can provide a traditional military capability that can contribute to a Canadian deterrence strategy but also, due to their part-time military status and civilian employment, Reserve Force capabilities can be harnessed in new ways to contribute to WoS resilience thereby making a complimentary contribution to a deterrence framework.

What the new capabilities for the Reserve Force look like both from a traditional and non-traditional perspective requires greater research and analysis. For example, from a traditional perspective, equipping and training the Reserve Force to provide an initial CAF response to natural disasters (environmental) would go a long way in contributing to societal resilience. Since 2010, Canadian Armed Forces operations in response to natural disasters have roughly doubled every five years.[81] The increase in occurrence and severity such natural disasters should not be underestimated as the past flood, and fire disasters in Canada have aptly demonstrated. Here the Australian case study above and their WoS resilience strategies built around natural disasters is instructive. The Reserve Forces are ideally situated across Canadian communities, including the Arctic with the Canadian Rangers, to contribute in a more meaningful way to this requirement thereby relieving the Regular Force of the task. Indeed, it has been remarked that domestic deployments to natural disasters is negatively affecting operational readiness for warfighting.[82]

In response to hybrid tactics in the grey zone, Reservists are also well situated with communities across Canada to potentially provide a force of resilience specialists charged with the task of raising awareness of potential security issues that could arise within their home communities as well as provide the resilience building measures required to address them. Further, they could be tasked with developing and delivering education and training programs aimed at increasing societal understanding and awareness of hybrid threats, and the steps required to address them. Naturally, the Reserve Force would not be solely responsible for this capability but would ideally work alongside emergency management and public safety agencies. Further, this capability could perhaps be nested within a national security strategy similar to Finland's comprehensive security strategy. As previously noted, the concept of comprehensive security stipulates that all vital functions of society are jointly safeguarded by authorities, business operators, organisations and citizens, and in which there is a readiness to use both military and non-military means to counter both internal and external threats and challenges.[83] The CSM ensures the maintenance of a basic level of understanding of defence, preparedness and self-sufficiency skills throughout society – with training opportunities provided to both civilian and military leaders in national and regional defence courses.[84] Meanwhile defence and security courses serve to deepen the understanding of comprehensive security and improves the cooperation between different sectors of society and government institutions. They also serve to promote a highly cooperative relationship between the military and society as a whole.[85] As the GoC seeks future opportunities to invest in Reserve Force capabilities and capacities to enable strategic readiness and have direct impact on communities across Canada where the Primary Reserve units are located, the Reserve Force offers an innovative approach to building a WoS response to hybrid threats in the grey zone that can equally contribute to Canada's overall deterrence strategy.

Conclusion

The global security environment is evolving and extant hybrid tactics in the grey zone will continue to threaten western liberal democracies. Concurrently, natural disasters around the world have increased significantly exacting a toll on armed forces' warfighting capacity as states struggle to respond to the natural disasters in a comprehensive a manner. Canada is not immune to either of these threats and must develop new approaches to respond in a more comprehensive manner. Building WoS resilience has emerged as the approach which may leverage extant armed forces capabilities but also open the door for the development of new capabilities that address both of these evolving threats. Finland (state security) and Australia (climate disaster response) can be viewed as global leaders in developing WoS resilience responses.

To be sure, the lessons learned from the study of such cases should not be taken to imply that the resilience-building approach followed in one nation can be fully and easily adopted by another. That said, recent Canadian experience indicates that the threats posed by the use of hybrid tactics and the weaponization of information are on the rise. While Canada may well have enjoyed the advantages bestowed by geography to ensure its national security in the past, such benefits appear far less likely to obtain in the future given the realities of a globalized information environment and an increasingly dangerous world.

Bibliography

Australian Government, 'Countering Foreign Interference', Department of Home Affairs Website. https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/countering-foreign-interference

Braw, E. 'Re-Thinking Deterrence', CHACR Global Analysis Programme Briefing, 16, (2019). https://chacr.org.uk/wp-content/uploads/2020/01/20190201_Issue16_CHACR_GAP_Briefing_Re_Thinking_Deterrence.pdf

Braw, E. 'Countering Aggression in the Gray Zone', *Prism,* Vol. 9, No. 3, (2021). https://ndupress.ndu.edu/Media/News/News-Article-View/Article/2846403/countering-aggression-in-the-gray-zone/

Canada, Department of National Defence, 'Strong, Secure, Engaged, Canada's Defence Policy' (Ottawa: Department of National Defence 2017).

Canada, Department of National Defence. Enabling Full-time Capability through Part-Time Service: A New Vision for the Reserve Force. (Ottawa: Chief of Reserve and Employer Support 2023).

Canada, Department of National Defence, Our North, Strong and Free: A Renewed Vision for Canada's Defence. (Ottawa: Department of National Defence 2024). https://www.canada.ca/en/department-national-defence/corporate/reports-publications/north-strong-free-2024.html

Commonwealth of Australia, '2023-2030 Australian Cyber Security Strategy' (Canberra: Department of Home Affairs 2023).

Commonwealth of Australia, 'Critical Infrastructure Resilience Strategy' (Canberra: Cyber and Infrastructure Security Centre; February 2023). https://www.cisc.gov.au/resources-subsite/Documents/critical-infrastructure-resilience-strategy-2023.pdf

Commonwealth of Australia, 'National Defence: Defence Strategic Review' (Australia: Australian Government 2023). https://www.defence.gov.au/about/reviews-inquiries/defence-strategic-review#:~:text=The%20Defence%20Strategic%20Review%20sets,long%2Dterm%20and%20sustainable%20implementation.

Commonwealth of Australia, 'National Defence: Defence Strategic Update' (Australia: Australian Government 2020). https://www.defence.gov.au/about/strategic-planning/2020-defence-strategic-update

Commonwealth of Australia, 'National Strategy for Disaster Resilience: Building the Resilience of Our Nation to Disasters', (Australia, National Emergency Management Committee 2011). https://knowledge.aidr.org.au/resources/national-strategy-for-disaster-resilience/#:~:text=Released%20in%202011%2C%20Australia's%20National,recover%20from%20emergencies%20and%20disasters

Conference of Defence Societies Institute, "Force Development: The Future of Land Warfare and the Canadian Army Report," (Ottawa 2024). https://cdainstitute.ca/wp-content/uploads/2024/10/Force-Development-Series-Land-Warfare-V1.6.pdf

de Jong, Sijbren, Sweijs, Tim, Kertysova, Katarina and Bos, Roel, "Inside the Kremlin House of Mirrors: How Liberal Democracies can Counter Russian Disinformation and

Societal Interference," Hague Centre for Strategic Studies, (2017). https://www.jstor.org/stable/resrep12585.8

Fife, Robert, Chase, Steven, and Walsh, Marieke, 'Winnipeg Scientist Fired for providing confidential information to China', *Globe and Mail,* 28 February 2024.

Finlay, Lorraine, 'Why Misinformation Bill Risks Freedoms it aims to Protect', Australian Human Rights Commission Website, 24 August 2023. https://humanrights.gov.au/about/news/opinions/why-misinformation-bill-risks-freedoms-it-aims-protect

Government of Canada, 'Canadian Heritage, Digital Citizen Initiative – Online Disinformation and Other Harms and Threats', Canadian Heritage Website, 20 March, 2023. https://www.canada.ca/en/canadian-heritage/services/online-disinformation.html#a1a1

Government of Finland, 'The Security Strategy for Society, Government Resolution 2.11.17' (Helsinki: The Security Committee 2017). https://turvallisuuskomitea.fi/wp-content/uploads/2018/04/YTS_2017_english.pdf

Giegerich, Bastian, 'Hybrid Warfare and the Changing Character of Conflict', *Connections – The Quarterly Journal,* Vol. 15, No. 2, (2016). http://dx.doi.org/10.11610/Connections.15.2.05

Grandi, Marco, 'A Tale of Two Hemispheres: Norwegian and Australian Approaches to National Resilience. A Comparative Analysis', *Security Theory and Practice,* Vol. XLVIII. No. 3, (2022).

Hunter, Edward H and Christie, Kristine Berzina, 'NATO and Societal Resilience: All Hands-on Deck in an Age of War', The German Marshall Fund of the United States (GMF). https://www.coe-civ.eu/kh/nato-and-societal-resilience-all-hands-on-deck-in-an-age-of-war

Hurst, Daniel, 'Australian Defence Chief Says War between China and Taiwan Would Be Disastrous', *The Guardian*, 15 April 2021. https://www.theguardian.com/world/2021/apr/16/australian-defence-chief-says-war-between-china-and-taiwan-would-be-disastrous

Moilanen, Panu, Hautala, Miriam and Saari, Dominic, 'Disinformation Landscape in Finland', EU Disinfo Lab, May 2023.

Nye, Joseph, 'Whatever Happened to Soft Power?, *The Strategist,* Australian Strategic Policy Institute, 19 January, 2022. https://www.aspistrategist.org.au/whatever-happened-to-soft-power/

Osinga, F. and Sweijs, T (eds.), 'Conclusion: Insights from Theory and Practice', Deterrence in the 21st Century, *NL ARMS Netherlands Annual Review of Military Studies* (The Hague: Asser Press 2021).

Parliament of Australia, Australia's Security Relationships. Parliament of Australia Website. https://www.aph.gov.au/About_Parliament/Parliamentary_departments/Parliamentary_Library/pubs/BriefingBook47p/AustraliaSecurityRelationships.

Persson, Ed, 'Whole of Society Preparedness: Finland's Approach' (UK: National Preparedness Commission 2021). https://nationalpreparednesscommission.uk/2021/10/whole-of-society-preparedness-finlands-approach/

Phua, Royston, 'Improving Government Supply Chain Resilience', *GovTech Review*, 28 July 2023. https://www.govtechreview.com.au/content/gov-tech/article/improving-government-supply-chain-resilience-789291497

Prior, T. "Resilience: 'The 'Fifth Wave' in the Evolution of Deterrence', in Thränert, O., and Zapfe, M.,(eds.), *Strategic Trends 2018: Key Developments in Global Affairs* (Zürich: Center for Security Studies (CSS) 2018). https://doi.org/10.3929/ethz-b-000317733

Raitasalo, Jyri, "Finnish Defense 'Left of Bang'" *Prism,* Vol 10. No. 2 (Washington D.C.: National Defense University 2023). https://ndupress.ndu.edu/Media/News/News-Article-View/Article/3323928/societal-security-and-total-defense-the-swedish-way/

Szymanski, Piotr, 'New Ideas for Total Defense: Comprehensive Security in Finland and Estonia' (Warsaw: Centre for Eastern Studies 2020). https://aei.pitt.edu/103309/1/OSW-Report_New-ideas-for-total-defence_net_0.pdf

Valtonen, Vesa, and Branders, Mina, 'Tracing the Finnish Comprehensive Security Model', in Larsen, Sebastian and Reinhard, Mark, (eds.), *Nordic Societal Security: Convergence and Divergence* (London: Routledge 2020).

van Doorn, Cees, and Theo Brinkel, 'Deterrence, Resilience, and the Shooting Down of Flight MH17', in Osinga, F. and Sweijs, T.,(eds*.), NL ARMS Netherlands Annual Review of Military Studies 2020: Deterrence in the 21st Century—Insights from Theory and Practice* (The Hague: T.M.C. Asser Press 2021).

Wigell, Mikael, 'Democratic Deterrence: How to Dissuade Hybrid Interference', *Washington Quarterly,* Vol. 44, No. 1 (Spring 2021).

Wigell, Mikael, Mikkola, Harri, and Juntunen, Tapio, 'Best Practices in the Whole of Society Approach in Countering Hybrid Threats' (Brussels: European Union 2021).

Williams, A.M., 'Evolution of Australia's Cyber Warfare Strategy', *Journal of Information Warfare*, Vol. 20, No. 1 (Winter 2021).

Wilner, A. S., 'Deterrence by Delegitimization in the Information Environment: Concept, Theory and Practice', in Ouellet, E., D'Agata, M., and Stewart, K., (eds.), Deterrence in the 21st Century: Statecraft in the Information Environment (Calgary: University of Calgary Press 2024).

Wilson, Samuel, Sivasubramaniam, Diane, Farmer, Jane, Aryani, Amir, De Cotta, Tracy, Kamstra, Peter, Adler, Viktoria, and Knox, Jasmine, 'Everyday Humanitarianism During the 2019/2020 Australian Bushfire Crisis' (Victoria: Social Innovation Research Institute, Swinburne Institute of Technology 2020). https://www.researchgate.net/publication/341135752_Everyday_Humanitarianism_Bushfire_Report

Wyeth, Grant, 'Why Did Australia Push Out a Chinese Communist Party-Linked Billionaire?', The Diplomat, 9 February 2019.'https://thediplomat.com/2019/02/why-did-australia-push-out-a-chinese-communist-party-linked-billionaire/

Endnotes

[1] Bastain Geigerich, 'Hybrid Warfare and the Changing Character of Conflict", Connections, The Quarterly Journal, Vol. 15, No. 2, (2016), 68-69.

[2] Canada, Department of National Defence, 'Strong, Secure, Engaged: Canada's Defence Policy' (Ottawa: Department of National Defence 2017), 53.

[3] Canada, Department of National Defence, 'Our North, Strong and Free: A Renewed Vision for Canada's Defence' (Ottawa: Department of National Defence 2024), 10. https://www.canada.ca/en/department-national-defence/corporate/reports-publications/north-strong-free-2024.html.

[4] See Robert Fife, Steven Chase and Marieke Walsh, 'Winnipeg Scientist Fired for providing confidential information to China', Globe and Mail, 28 February 2024. https://www.theglobeandmail.com/canada/article-winnipeg-scientists-fired-for-providing-confidential-information-to/

[5] Canada, Department of National Defence, 'Strong, Secure, Engaged' (Ottawa: Department of National Defence 2017), 53.

[6] Edward H Hunter, and Christie, Kristine Berzina, 'NATO and Societal Resilience: All Hands-on Deck in an Age of War', The German Marshall Fund of the United States (GMF), 3. https://www.coe-civ.eu/kh/nato-and-societal-resilience-all-hands-on-deck-in-an-age-of-war.

[7] Cees van Doorn, and Theo Brinkel, 'Chapter 19 Deterrence, Resilience, and the

Shooting Down of Flight MH17', in Frans Osinga and Tim Sweijs, (eds.), NL ARMS Netherlands Annual Review of Military Studies 2020: Deterrence in the 21st Century—Insights from Theory and Practice (The Hague: T.M.C. Asser Press 2021), 370.

[8] Mikael Wigell, 'Democratic Deterrence: How to Dissuade Hybrid Interference', Washington Quarterly, Vol. 44, No. 1, (Spring 2021), 55.

[9] Elizabeth Braw, 'Countering Aggression in the Gray Zone', Prism, Vol 9, No. 3, (2021), 63. https://ndupress.ndu.edu/Media/News/News-Article-View/Article/2846403/countering-aggression-in-the-gray-zone/

[10] Mikael Wigell, 'Democratic Deterrence: How to Dissuade Hybrid Interference', Washington Quarterly, Vol. 44, No. 1, (Spring 2021), 55.

[11] Mikael Wigell, Harri Mikkola, and Tapio Juntunen, 'Best Practices in the Whole of Society Approach in Countering Hybrid Threats'(Brussels: European Union 2021), 21-2.

[12] T. Prior, 'Resilience: The 'Fifth Wave' in the Evolution of Deterrence', in O. Thränert and M. Zapfe

(eds.), Strategic Trends 2018: Key Developments in Global Affairs. (Zürich: Center for Security Studies 2018), 70. https://www.research-collection.ethz.ch/handle/20.500.11850/317733.

[13] Mikael Wigell, 'Democratic Deterrence: How to Dissuade Hybrid Interference', 53.

[14] Ibid.

[15] T. Prior, 'Resilience: The 'Fifth Wave' in the Evolution of Deterrence', 69-70.

[16] Ibid., 74.

[17] According to Joseph Nye, soft power derives from a nation's culture, political values and policies and is based on the idea that a government can exert its influence – both at home and abroad -- by the way it behaves. See Joseph Nye, "Whatever Happened to Soft Power?, The Strategist, 15 January 2022. https://www.aspistrategist.org.au/whatever-happened-to-soft-power/

[18] Elizabeth Braw, 'Re-Thinking Deterrence', CHACR Global Analysis Programme Briefing, (2019), 4.

https://chacr.org.uk/wpcontent/

uploads/2020/01/20190201_Issue16_CHACR_GAP_Briefing_Re_Thinking_Deterrence.pdf

[19] Past waves have varied regarding their analytical focus, with the first wave focused on the implications of the development of the atomic bomb for international relations, the second on how to defend the nation and attain political objectives in a nuclear armed world while at the same time controlling the risks of nuclear war, a third wave focusing on the appropriate balance between nuclear and conventional forces in securing effective deterrence and a fourth examining how to deter rogue leaders and non-state actors. For a useful summary of the five waves of thinking on deterrence, see Frank Osinga and Tim Sweijs, 'Conclusion: Insights from Theory and Practice', in F. Osinga and T. Sweijs, (eds.), Deterrence in the 21st Century, NL ARMS Netherlands Annual Review of Military Studies (The Hague: Asser Press 2021), 526.

[20] Alex Wilner, 'Deterrence by Delegitimization in the Information Environment: Concept, Theory and Practice', in Deterrence in the 21st Century: Statecraft in the Information Age. Eric Ouellet, Madeleine D'Agata, and Keith Stewart, (eds.), (Calgary: University of Calgary Press 2024), 72-3.

[21] Ibid., 73.

[22] Ibid., 71-2.

[23] Ibid., 72.

[24] See Government of Finland, 'The Security Strategy for Society, Government Resolution 2.11.17' (Helsinki: The Security Committee 2017). https://turvallisuuskomitea.fi/wp-content/uploads/2018/04/YTS_2017_english.pdf.

[25] Jyn Raitasalo, 'Finnish Defense "Left of Bang', Prism, Vol. 10, No. 2 (Washington D.C.: National Defense University 2023), 79. https://ndupress.ndu.edu/Media/News/News-Article-View/Article/3323928/societal-security-and-total-defense-the-swedish-way/

[26] Ed Persson, 'Whole of Society Preparedness: Finland's Approach' (UK: National Preparedness Commission 2021). https://nationalpreparednesscommission.uk/2021/10/whole-of-society-preparedness-finlands-approach/

[27] Ibid.

[28] Ibid.

[29] Vesa Valtonen, and Mina Branders, 'Tracing the Finnish Comprehensive Security Model', in Sebastian Larsen and Mark Reinhard, (eds.), Nordic Societal Security: Convergence and Divergence (London: Routledge 2020), 94.

[30] Perrson, 2021.

[31] Ibid.

[32] Ibid.

[33] Ibid.

[34] Ibid.

[35] Ibid.

[36] Piotr Szymanski, 'New Ideas for Total Defense: Comprehensive Security in Finland and Estonia' (Warsaw: Centre for Eastern Studies 2020), 25.

[37] Ibid., 27.

[38] Ibid., 28.

[39] Ibid., 24.

[40] Ibid., 66.

[41] Ibid., 30.

[42] Ibid., 29.

[43] Ibid.

[44] Ibid., 34-5.

[45] Panu Moilanen, Miriam Hautala and Dominic Saari, 'Disinformation Landscape in Finland' (Brussels: EU Disinfo Lab 2023), 7. https://www.disinfo.eu/wp-content/uploads/2023/05/Finland_DisinfoFactsheet.pdf.

[46] Ibid., 7.

[47] Szymanski, 2020, 35.

[48] See Commonwealth of Australia, National Strategy for Disaster Resilience: Building the Resilience of Our Nation to Disasters. (Australia, National Emergency Management Committee 2011). https://knowledge.aidr.org.au/resources/national-strategy-for-disaster-resilience/#:~:text=Released%20in%202011%2C%20Australia's%20National,recover%20from%20emergencies%20and%20disasters.

[49] Marco Grandi, 'A Tale of Two Hemispheres: Norwegian and Australian Approaches to National Resilience. A Comparative Analysis', Security Theory and Practice, Vol. XLVIII. No. 3, (2022), 259.

[50] Ibid.

[51] See, Commonwealth of Australia, 'National Defence: Defence Strategic Update' (Australia: Australian Government 2020), 16. https://www.defence.gov.au/about/strategic-planning/2020-defence-strategic-update.

[52] Ibid., 27-28, 35.

[53] See Commonwealth of Australia, 'National Defence: Defence Strategic Review' (Australia: Australian Government 2023), 37-8. https://www.defence.gov.au/about/reviews-inquiries/defence-strategic-review#:~:text=The%20Defence%20Strategic%20Review%20sets,long%2Dterm%20and%20sustainable%20implementation.

[54] Ibid, 38.

[55] See Commonwealth of Australia, '2023-2030 Australian Cyber Security Strategy' (Canberra: Department of Home Affairs 2023).

[56] See Grandi, 2022, 257-73. On this point, see 260.

[57] Ibid.

[58] Ibid.

[59] Ibid.

[60] Ibid., 261.

[61] Ibid., 262.

[62] Ibid.

[63] Royston Phua, 'Improving Government Supply Chain Resilience', GovTech Review , 28 July 2023. https://www.govtechreview.com.au/content/gov-tech/article/improving-government-supply-chain-resilience-789291497.

[64] Commonwealth of Australia, 'Critical Infrastructure Resilience Strategy' (Canberra: Cyber and Infrastructure Security Centre 2023), 10-11. https://www.cisc.gov.au/resources-subsite/Documents/critical-infrastructure-resilience-strategy-2023.pdf.

[65] See A.M. Williams, 'Evolution of Australia's Cyber Warfare Strategy', Journal of Information Warfare, Vol. 20, No. 1, (Winter 2021), 1-16.

[66] See Australian Government, 'Countering Foreign Interference', Department of Home Affairs Website. https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/countering-foreign-interference

[67] See Lorraine Finlay, 'Why Misinformation Bill Risks Freedoms it aims to Protect'' Australian Human Rights Commission Website, 24 August 2023. https://humanrights.gov.au/about/news/opinions/why-misinformation-bill-risks-freedoms-it-aims-protect.

[68] Ibid.,

[69] Parliament of Australia, 'Australia's Security Relationships', Parliament of Australia Website. https://www.aph.gov.au/About_Parliament/Parliamentary_departments/Parliamentary_Library/pubs/BriefingBook47p/AustraliaSecurityRelationships.

[70] Samuel Wilson, Diane Sivasubramaniam, Jane Farme and Amir Aryani, 'Everyday Humanitarianism During the 2019/2020 Australian Bushfire Crisis' (Hawthorn: Social Innovation Research Institute Swinburne University of Technology, 2020). https://www.researchgate.net/publication/341135752_Everyday_Humanitarianism_Bushfire_Report

[71] Ibid.

[72] Ibid.

[73] Grant Wyeth, 'Why Did Australia Push Out a Chinese Communist Party-Linked Billionaire?', The Diplomat, 9 February 2019. https://thediplomat.com/2019/02/why-did-australia-push-out-a-chinese-communist-party-linked-billionaire/

[74] Daniel Hurst, 'Australian Defence Chief Says War Between China and Taiwan Would Be Disastrous', The Guardian, 15 April 2021. https://www.theguardian.com/world/2021/apr/16/australian-defence-chief-says-war-between-china-and-taiwan-would-be-disastrous.

[75] Ibid.,

[76] On this point see Sijbren de Jong, Tim Sweijs, Katarina Kertysova and Roel Bos, 'Inside the Kremlin House of Mirrors: How Liberal Democracies can Counter Russian Disinformation and Societal Interference', Hague Centre for Strategic Studies (2017), 30. https://www.jstor.org/stable/resrep12585.8

[77] Some initial efforts to develop such capability are already evident. In 2019-20, as part of Canada's approach to protecting its democracy, Canadian Heritage contributed $7 million over 9 months to 23 projects delivered by Canadian civil society stakeholders that strengthened citizens' critical thinking about online disinformation, their ability to be more resilient against online disinformation, as well as their ability to get involved in democratic

processes. The Digital Citizen Initiative (DCI) provided funding for civic, news, and digital media literacy, ranging from awareness sessions and workshops to the development of learning materials. These projects have reached more than 12 million Canadians from coast to coast to coast including youth, seniors, minority communities, official languages minority communities, etc. The initiative was delivered through the Canada History Fund, Collective Initiatives – Canada Periodical Fund and Youth Take Charge. See Government of Canada, Canadian Heritage, Digital Citizen Initiative – Online Disinformation and Other Harms and Threats. Canadian Heritage Web Page, 20 March, 2023. https://www.canada.ca/en/canadian-heritage/services/online-disinformation.html#a1a1

[78] Canada, Department of National Defence, 'Enabling Full-time Capability through Part-Time Service: A New Vision for the Reserve Force' (Ottawa: Chief of Reserve and Employer Support 2023),11,14.

[79] Ibid., 5.

[80] Ibid., 11.

[81] Canada, Department of National Defence, 'Our North, Strong and Free: A Renewed Vision for Canada's Defence' (Ottawa: Department of National Defence 2024), 3.

[82] Conference of Defence Societies Institute, 'Force Development: The Future of Land Warfare and the Canadian Army Report' (Ottawa, 2024), 7. https://cdainstitute.ca/wp-content/uploads/2024/10/Force-Development-Series-Land-Warfare-V1.6.pdf.

[83] Persson, 2021.

[84] Ibid.

[85] Ibid.