GBA+

Application

July 2020

Author

Andrea Lane

Cyber Futures: A preliminary Scanning and Foresight Report

Defence & Security Foresight Group

About the Author

Originally from Victoria, Andrea holds a BA (Hons) in Political Science from Dalhousie, and an MA in International Affairs from Carleton (NPSIA,) with previous studies in English Literature and Classics. Her MA thesis tested a theory of differential mobilization into non-Islamic terrorism, while her undergraduate thesis explored civil-military tension in the Auditor General's review of defence procurement in Canada. Andrea's research interests include maritime security, military cultures, civil-military relations, defence policy and procurement, gender in security, and Canadian foreign policy. Her dissertation focusses on the impact of service-level cultures on procurement decision-making.

GBA+ Application for: "Cyber Futures: A preliminary Scanning and Foresight Report" b by Alex Wilner

DSFG Thematic Team: North American Security

Gender-Based Analysis Plus (GBA+)

GBA+ is an analytical tool to advance gender equality and diversity outcomes of various policies, programs, and services. This strategy of gender mainstreaming is specific to the Government of Canada, and includes not only gender but also intersectional considerations, such as race and sexuality. In 2016, DND-CAF adopted GBA+ in response to United National Security Council Resolution 1325 and related resolutions, which acknowledges the need for gender perspectives in conflict, post-conflict and peacebuilding processes, and women's participation in decision making. GBA+ training through the Status of Women Canada online course is mandated for most DND-CAF employees and is an important consideration in assessing the most pressing future defence and security issues.

The GBA+ team of the DSF Group has developed a GBA+ toolkit that supports authors of working papers to integrate gender and intersectional considerations in their work from the initial stages of their research to the development of evidence-based findings and recommendations. The GBA+ Toolkit provides a series of key questions for regional teams to consider, such as: "are your concepts conceived in broad and inclusive ways to account for the experiences and perspectives of those not well represented in research and power structures?" or "how does your foresight analysis reinforce or challenge existing power relations?" A gender-liaison from each regional team works in consultation with members of the GBA+ team to develop GBA+ for the working papers. This GA+ application complements the efforts of working paper authors to apply a GBA+ lens to their work.

GBA+ Considerations of "Cyber Futures"

Dr. Wilner's paper presents a comprehensive overview of foresight analysis as a process and then applies it as an example to cyber security. As such, this GBA+ annex will discuss the intersectional considerations both of foresight analysis as a concept and of cyber security as a domain in its own right.

Foresight: Who's in the Room?

Dr. Wilner's description of foresight analysis makes it clear that it is necessary to hear from as diverse a group of people as possible, in order to develop the desired scope and breadth of "possible futures." Particularly in institutions such as DND/CAF, where employees are enculturated into a particular worldview (as is true of all institutions), it is imperative that when foresight analysis takes place, a broad range of participants are included. Institutional worldviews not only produce common "tools" or solution sets, but they develop common problems or questions, as well. This is a fatal limitation to foresight analysis, which is designed to imagine and describe a range of futures from the improbable, but potentially catastrophic, to the most likely. It is in this "baseline/expected future" scenario (described on p. 3) that a lack of diversity in the foresight group will most likely come into play, because the way in which we view our current world—the status quo—informs the manner in which we expect the future to unfold. It is very difficult to envision something you have never even contemplated, and thus the "expected" scenarios will most likely reflect the lived experiences of those doing the brainstorming. The recent international controversy over the "Black Lives Matter" movement is an excellent example of the degree to which even neighbours can disagree fundamentally over the "reality" of the world around them. Capturing perspectival disagreements is essential for genuinely novel foresight analysis.

Scanning: Breadth, legitimacy, and diversity

"Scanning" is the process whereby extensive research is undertaken to identify all possible "signals" on a topic. This includes websites, newspaper articles, interviews, in-house publications, social media analysis, etc. GBA+ analysis encourages us to recognize the extent to which the resources we choose to include in this "scanning" corpus are heavily influenced by institutional ideas of legitimacy, relevance, and authorial importance, all of which are linked to gender, race, disability, and citizenship status. Particularly in the inclusion of "weak signals" or marginal sources, whose rumours are considered valid, whose esoteric hobby website is considered worth reading, all of these decisions can be subject to the intrinsic biases of the people (and institutions) doing the scanning. Those sources authored or created by women, ethnic minorities, persons with disabilities, people from lower socio-economic classes, and non-citizens are most likely to be ignored or devalued. As an example, the racialized, immigrant women who work in long-term care homes (and their unions and advocates) have been raising the issue of deplorable, unsafe conditions in care facilities for years. Their "signals" had gone unheeded, leaving LTC homes unprepared for the COVID epidemic. Their expertise was discounted, and as a result thousands of Canadian seniors died unnecessarily. When the primarily male, white CAF publicized conditions in the facilities, however, their "signals" were immediately listened to. This example shows that to ensure a productive scanning process, you need analyst diversity, as well as diverse understandings of the topic at hand: "nuclear security" scanning must include anti-nuclear activist zines, or feminist peace activist blogs, even if these sources can seem "crazy" or inconsequential to security analysts.

Cyberfutures: An intersectional understanding

While recognizing the intended Government of Canada audience for this paper, it is important to recognize that for many Canadians, the security "benefits" of the cyber-enabled world described in Dr. Wilner's paper bring with them significant and burdensome downsides, as well. Predictive policing, for example, relies heavily on reported crime statistics, which can be influenced by over-policing of Black and Indigenous communities, or by wealthier residents reporting (and thus criminalizing) harmless activities, such as Black youths playing basketball in Montreal. Artificial Intelligence (AI) and machine learning training have already been shown to be highly replicative of corpus bias and this kind of technological development is no different: if the data is biased, then the predictive policing algorithm itself will be biased.

Finding illicit activities from space (p.10) sounds good, especially when it comes to illegal and destructive extractive activities, or "slavery" as was suggested as an example. But nuances are invisible even at airplane attitude and it is almost impossible that such technological bluntness will not disproportionately affect the already-disadvantaged—for example, artisanal mining is technically illegal, but is a subsistence activity for many. In Canada, such technology could create further tensions if used to criminalize subsistence and ceremonial (but technically "illegal") fishing, hunting, and trapping by Indigenous people on contested land. Such disputes have already led to violence in the past, as at Burnt Church in New Brunswick.

Biotech/nanotech/biohacking (p.11) is another plausible future scenario that urgently needs intersectional analysis. Yes, people can perhaps be modified to be more disease- or fatigue-resistant, but on whom are these technologies being tested? Particularly in the military realm, are nanotechnologies that give soldiers enhanced night vision going to be made mandatory? What about CAF members who object for moral or religious reasons? And if they are mandatory, then what—when soldiers retire, are those implants removed? Or will we have a developing class of bionic citizens, aggravating developing inequities between veterans and non-veterans? In the realm of curing or improving disabilities, many disability advocates rail against existing "curative" technology such as cochlear implants. The questions concerning "fixing" disabilities is a complicated moral and ethical issue with many diverse and opposing viewpoints. Without diligent and cautious intersectional analysis, the voices that are prioritized in these future debates will likely be those with the best access to funds and resources—white, socio-economically well-off, urban, etc.

Discussions of cyberattacks on either state or private industry targets need to include the realization that ultimately, it is "civilians" who end up paying the (oftentimes literal) price, via reduced or collapsed services, taxpayer burden to replace affected services, higher insurance/transaction costs due to bank security investment, etc. While offensive cyber might be necessitated by the state, the impact on the citizenry of "blowback" from attacked states must be taken into account. As always, those most vulnerable and marginalized before any cyberattacks will be disproportionately affected afterwards. Indigenous communities that already struggle with access to clean drinking water are even more vulnerable to cyberattacks that disrupt bottled water supply chains or tanker trucking services. Cyberattacks causing power grid blackouts in summer (or winter) make cramped, multi-family or high-rise living situations even more difficult, affecting those in lower economic strata and urban dwellers disproportionately. The current COVID crisis has already revealed the extent to which system-wide disruption renders the "invisible" inequality in Canada starkly visible; cyber warfare is another such "systems" issue that will cause more harm for the most vulnerable.

Finally, an intersectional approach allows us to see that surveillance is never neutral. A general recognition that increased surveillance by both the state and industry is "bad" is insufficient—intersectional analysis reveals the extent to which racialized, impoverished, disabled, and non-citizen residents are already viewed as deviant, and increased surveillance tech will only magnify this. Enhanced biometric measures for ID cards, for example, will immediately disadvantage the homeless or temporarily housed, who will have even greater difficulty accessing the "paper trail" required for advanced ID requirements. Lower-income citizens might require assistance in paying fees attached to enhanced IDs. Care must be taken that any biometric information retained in such ID cards or databases does not serve to further stigmatize or marginalize people with disabilities, especially those whose disabilities have a hereditary or genetic component, which could be revealed/stored by DNA tests. Brainwave scanning offers unique challenges for people living with mental illness, some of whom might be concealing their condition from their employer. The potential of almost unlimited data being available to savvy hackers means women and children who have fled abusive partners are at even greater risk of detection and harm. Revenge porn, doxxing of ex-partners, and other online gender-based crimes will potentially be even more harmful, due to the sheer volume of personal information at risk. Given the sex ratio disparity in the computing and cybertechnology worlds, it can be expected that women will continue to be at disproportionate risk of such crimes.

The lack of female cyber experts means that such GBA+ considerations are unlikely to be "backed in" to any commercially-developed applications, so government agencies will have to carefully vet any product or system they acquire for gender-based disparities or vulnerabilities, to ensure they do not increase women's marginalization via their use.

Recommendations for DND/CAF

1. Above all else, diversity is required in any foresight cell, at every stage of the analysis. "Diversity" here includes not only gender, language, ethnic origin, and regional diversity, but also cognitive diversity: participants from different socio-economic and educational backgrounds, from different occupations (and the un- and under-employed) and from various political affiliations. This poses difficulty for very specialized agencies like DND/CAF, which requires their foresight to be specific and focussed on military eventualities. Therefore, some combination of outside analysts with in-house Subject Matter Experts (SMEs) to advise—but not inhibit—the outside analysts is suggested as a workaround. Care must be taken that the future scenarios envisioned by non-traditional security experts are not classified as "normative" or "aspirational," and thus dismissed.

2. The same recommendations apply for the scanning stage of foresight: ensure the broadest possible corpus of signals by enlisting the assistance of researchers far beyond the usual stable of consultants and employees. In some cases, especially on security-related matters, it would be especially useful to consult with groups traditionally viewed as antagonistic to the state security apparatus: peace groups, anti-racist activists, 'anarchists,' etc. This ensures that signals that go against the government's expected or preferred future outcome are heeded to and incorporated in any scenario analysis. This is similar to the way the information domain is being viewed as part of the CAF's evolving Pan-domain Force Employment Concept (PFEC), in which a broad range of public opinion "signals" are collected in order to fully understand the operating environment. As in Dr. Wilner's descriptive scenario, anti-cyber sentiment is an important aspect of any imagined cyber future, so understanding that opposition before making any cyber-related policy is crucial. You can't adequately imagine or prepare for political opposition without engaging with that community's FaceBook posts, pamphlets, blogs, etc. However, as the above-referenced story of CAF signal-gathering illustrates, this scanning must be undertaken with sensitivity and transparency, to avoid the implications of the state "spying on" citizens or viewing them as adversaries, which can exacerbate a group's oppositional posture.

3. Recognize and plan for the extent to which "impact on civilians" requires intersectional analysis from the very beginning. If a likely futures scenario involves disruption to public services, for example, research and analysis of the disproportionate impacts on racialized, Indigenous, female, indigent, homeless or disabled people must be a part of any discussion of scenario mitigation from the very beginning. This avoids the possibility of proposed mitigation solutions causing unintended harm to the most vulnerable. Again, the COVID pandemic provides ample illustration of these unintended effects: while quarantine/lockdown was necessary to control the spread of the virus, homeless people suffered as a result of the concomitant closure of public toilets, for example, and isolation has exacerbated many people's mental health issues.