Working

Paper

October 2020

Author

Dr. Alex Wilner

Cyber Futures: A Preliminary Scanning and Foresight Report

Defence & Security Foresight Group

About the Author

Alex Wilner is an Associate Professor at the Norman Paterson School of International Affairs, Carleton University, where he teaches a graduate course, among others, on strategic foresight in national security. Prior to joining NPSIA Dr. Wilner worked at Policy Horizons Canada, the government's central foresight laboratory. Since 2017, he has provided foresight training and research services to over a dozen government departments and agencies, including the Department of National Defence, Global Affairs Canada, Natural Resources Canada, and the Standards Council of Canada. His books and volumes include Deterring Terrorism: Theory and Practice (Stanford University Press, 2012), Deterring Rational Fanatics (University of Pennsylvania Press, 2015), and Deterrence by Denial: Theory and Practice (Cambria Press, 2020). He lives in Ottawa with his wife and three young daughters.

Funding Acknowledgment

This Working Paper was funded by the Defence and Security Foresight Group which receives funding from the Mobilizing Insights in Defence and Security (MINDS) program designed to facilitate collaboration and mobilize knowledge between the Department of National Defence, the Canadian Armed Forces, and academia and other experts on defence and security issues. Through its Targeted Engagement Grants, collaborative networks, scholarships, and expert briefings, MINDS works and collaborates with key partners to strengthen the foundation of evidence-based defence policy making. These partnerships drive innovation by encouraging new analyses of emerging global events, opportunities, and crises, while supporting a stronger defence and security dialogue with Canadians.

The author also acknowledges the financial support he received from the Department of National Defence's Innovation for Defence Excellence and Security (IDEaS) program as part of his AI Deterrence research project (2019-2021), which helped inform this paper's findings.

Abstract

The objective of this paper is to explore the future of cybersecurity. Using a mix of tools and techniques derived from strategic foresight – including domain mapping, horizons scanning, insight development, and scenario construction – the paper will highlight how social, technological, political, and value-based change might influence cybersecurity in new and novel ways over the coming two decades. Strategic foresight is not used to predict the future, which is impossible. Rather, it provides a set of tools that allow us to better appreciate a range of possible and plausible alternative future scenarios and environments. Strategic foresight allows practitioners, researchers, and decision-makers to systematically contemplate future challenges and opportunities while improving their appreciation for how complex political and strategic issues might evolve. Knowledge of how cybersecurity might unfold provides us with an ability to anticipate change and avoid strategic surprise. The paper discusses where within the Government of Canada foresight is used in policy making, explains the basis and logic of foresight as a method of research, and applies a variety of foresight tools in envisioning alternative future cybersecurity scenarios.

Keywords
Cybersecurity, National Security Policy, Strategic Foresight

Strategic Foresight: A Primer[1]

As a methodology, strategic foresight allows us to do several things. It provides a toolkit for analyzing current developments and anticipating their broader consequences, and for exploring systemic interactions between disparate domains. The goal of foresight in not to predict the future, which is impossible, but rather to pair creative analysis with tailored techniques to avoid strategic surprise (Dator 1995). But while foresight is not a predictive science, it does rely on speculative and creative thinking, providing a collection of tools, techniques, and methods for creatively exploring how emerging trends may shape or alter the future in new, novel, and unexpected ways. As a method, foresight is anticipatory: what might happen, given what we already know? And it relates to organizational planning: given what we think could happen, how might we prepare accordingly? It can be used to contemplate emerging trends and identify where disparate developments may meet and potentially clash. It can be used to explore change within complex social, economic, and political systems. Foresight also provides a lens with which to assess and contemplate alternative futures, which represent possible and plausible alternative processes of change from those most commonly held (i.e. the expected, or baseline, future). Foresight can also be used to test and strengthen our collective and organizational assumptions concerning any number of issues, and can likewise be used to appreciate the nexus between emerging and potentially disruptive technology and socio-economic and security priorities. Finally, foresight provides tools for both anticipating future change, and for responding to future change. Thinking through multiple future scenarios today, allows us to prepare, both mentally and institutionally, for emerging and alternative futures tomorrow (Habegger 2010; Leigh 2003; Missiroli 2013; Bengsten et. al. 2012).

[1]This section borrows from Alex Wilner and Martin Roy, "Canada's Emerging Foresight Landscape: Observations and Lessons," Foresight (Forthcoming, 2020).

As a policy or strategic tool, foresight allows us to anticipate future challenges and opportunities, and tailor our response accordingly (US Office of the Director of National Intelligence 2017; Rademaker 2009; CSIS 2014). The different techniques it provides for acquiring relevant information that portends long-term future change allows government organizations to chart out and anticipate how change might unfold (Schwartz 1991; Bishop and Hines 2012; Padbury 2011; Hiltunen 2008; Harris and Zeisler 2002). As such, foresight relates to the collection and analysis of information and is widely applicable to all functions of government (e.g. health, energy, and environmental policy, economics and trade, etcetera). Moreover, foresight is commonly used by defence planners hoping to avoid strategic surprise in thinking through future security threats and in planning ahead with procurement of materiel and training of personnel (Work and Brimley 2014; Scharre 2014). And intelligence agencies, too, use foresight techniques to identify "the driving forces that may determine future outcomes" (Heuer and Pherson 2011; Caudle and de Spigeleire 2010; US Office of the Director of National Intelligence 2017; Rademaker 2009; CSIS 2014). All told, strategic foresight is not simply an academic curiosity but is rather deeply entrenched in the making and evaluation of government policy and strategy.

As a distinct approach to policy research, foresight is currently being applied across the Canadian federal public service by several government departments and agencies. In fact, since 2015, Canada's foresight landscape has evolved and broadened a great deal. At the center of this emerging ecosystem lies Policy Horizons Canada (Horizons for short), which is Canada's preeminent laboratory and center of excellence on foresight (Ditchburn 2017). First established as the Policy Research Secretariat (within the Privy Council Office) in 1996, it evolved into the Policy Research Initiative, an independent think tank organization within the government, in 2000, and later into Policy Horizons Canada, a center dedicated to foresight research, in 2010. Horizons is a well-known entity in Canada and in various circles internationally, recognized for its rigorous (and prize-winning) methodology and cutting-edge research (Association of Professional Futurists 2018). Horizons' foresight research is meant to assist the Government of Canada in developing future-oriented policies that are resilient to disruption. With a staff of roughly 35, Horizons is by far Canada's largest and most well-established foresight organization. It is deeply entrenched with the international foresight community. Administratively housed within the department of Economic and Social Development Canada (ESDC) – but functionally independent from ESDC – Horizons' mandate spans the entire government. It is governed by a Deputy Minister Steering Committee (DMSC) consisting of 10 Deputy Ministers pulled from across the federal public service, and chaired jointly by ESDC's Deputy Minister and the Privy Council Office's Deputy Secretary to the Cabinet (Plans and Consultations).

Besides Horizons, a number of small Canadian government units and groups have recently been established to conduct foresight research on behalf of their home departments. Some of these initiatives involve the creation of formal foresight units or sub-units like the ones that exist in the Canadian defence and foreign ministries. Other initiatives comprise less structured foresight activities and experiments, conducted by strategic policy planning entities in various departments. Elsewhere, single analysts or small groups of two or three carve out a bottom-up mandate to conduct specific foresight research. Across the federal public service, these small foresight units and teams have been established to better inform Canada's current and future policies into the next decade. The new Foresight Unit at Global Affairs Canada (GAC), for instance, uses foresight to meet its objectives of "challenges assumptions and testing … policy and operational frameworks" (GAC 2017).

Besides GAC, over a dozen other foresight units have recently been established, with major initiatives undertaken at the Canadian Forest Service (CFS) at Natural Resources Canada (NRCan), Employment and Social Development Canada (ESDC), Immigration, Refugees, and Citizenship Canada (IRCC), Canadian Heritage, the Department of National Defence (DND), the Bank of Canada, the Standards Council of Canada (SCC), the Bank of Canada, the Canadian Revenue Agency (CRA), among other departments and agencies. Organizations at other levels of government, from the emergency management division at the City of Calgary to the Ontario Provincial Police (OPP), are likewise exploring the use and utility of foresight for purposes of planning and governance. Like Horizons, these federal units and groups share a dedication to using a systematic and rigorous approach to foresight research, often in step with Horizon's own approach (i.e. the "Horizons Foresight Method") (Horizons 2016). But unlike Horizons, these new foresight entities are specifically tasked by management to produce tangible outputs derived from foresight that are meant to directly inform specific departmental or institutional processes, including annual and strategic plans, risk profiles, and transition advice for new governments.

Understanding where and how foresight is used within Canada to improve policy and strategy provides an appropriate conceptual backdrop for the paper itself. The primary objective of this paper is to provide Canadian policy-makers with an exploration of the future of cybersecurity. The intention is to help Canadians avoid strategic surprise by contextually broadening the way they think about probable and possible cybersecurity futures. The paper has several secondary objectives as well, including providing readers from all backgrounds with a better understanding of how foresight works in practice, and popularizing how foresight is currently used within the Government of Canada. The intention here is to further extend the use of foresight across the federal public service and among other levels of government across Canada.

Relying a mix of foresight tools and techniques used by Canadian federal departments and agencies, the paper will highlight how social, technological, political, and value-based change might influence cybersecurity in new and novel ways over the coming decades. The paper is organized in three sections. The current section provides a broad overview of foresight and of its use by the Government of Canada. Section two provides a summary of the specific conceptual building block upon which foresight is built. And section three uses three foresight techniques – domain mapping, scanning and insight development, and scenario construction – to explore the future of cybersecurity.

Conceptual Building Blocks: From Future (*singular*) to Futures (*plural*)

> **"As a set of tools, strategic foresight provides different techniques for acquiring relevant information that portends future change, and for thinking through what that change might mean for an organization."**

Strategic foresight is the study of societal change. It is not predictive science, but rather a thought exercise, a way of thinking creatively about how emerging trends may help shape and alter the future in new, novel, and unexpected ways. As a set of tools, strategic foresight provides different techniques for acquiring relevant information that portends future change, and for thinking through what that change might mean for an organization. Strategic foresight, as its name implies, is focused on long-term dynamics.

Systemic change can be subdivided into three conceptual timeframes (Bishop and Strong 2010). Immediate change is short-term change that spans hours, days, and weeks. Operational change occurs over months and years. Strategic change is longer-term, measured in years and decades. Public policy foresight – at least in Canada – ordinarily sits in the last of these time horizons, looking ahead between three and 15 (or more) years. Another way to think about strategic foresight is to approach it from a policy surprise framework. Figure One provides the visual context. Some future developments, given current trends and expectations, can be anticipated. That anticipation also establishes a certain degree of awareness among decision makers (and the general public). The greater the awareness of a possible future, the more likely its eventual development will have a more limited impact on a system; awareness creates pressure to plan ahead in anticipation of change.

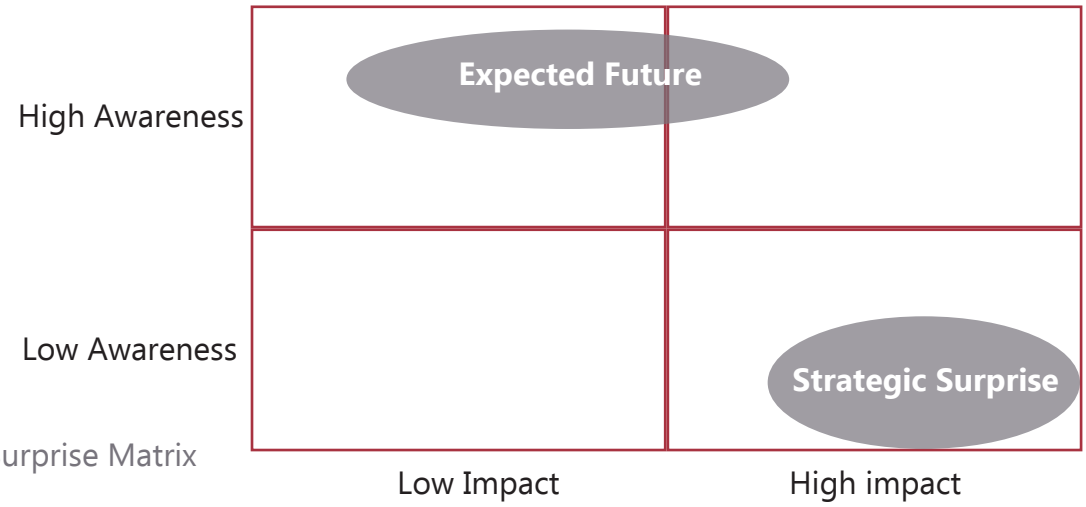


Figure 1: Surprise Matrix

Other future developments, however, are less easily anticipated. Here, trends are not well understood, or the interaction among disparate trends and developments within and beyond the system being evaluated, are not fully considered. Either way, possible alternatives to the expected future are missed; there is low awareness of what might occur. And with low awareness comes high impact events that serve as episodes of strategic surprise. For planning purposes, the goal of strategic foresight is to avoid strategic surprise. As an exercise, it sits most comfortably within the lower right-hand quadrant of Figure One, where low awareness meets high societal impact.

> **“Strategic Foresight is rooted to a number of conceptual building blocks. The first, and perhaps most important, is the idea that the future is not singular.”**

Strategic Foresight is rooted to a number of conceptual building blocks. The first, and perhaps most important, is the idea that the future is not singular. As Peter Schwartz explains, “the future is plural” (Schwartz 1991/1996). Many possible futures – rather than only one future – are possible. The cornerstone of foresight is the idea that there are a range of plausible developments and interactions that feed an equally diverse set of alternative futures. Instead of thinking of time as one single line emanating outwards from today and into tomorrow, picture a river delta with various braids and branches, each representing a different path that leads to a different alternative future. If we think in terms of only one stream and one future, we risk strategic surprise.

But if we think about a set of different possible streams and futures, we cover our strategic bases more thoroughly: we can envision many different alternative futures for ourselves and plan accordingly. The point is not that each branch of the river delta will eventually emerge to represent the present, but only that they represent what is possible in the future. Thinking through multiple alternative futures allows us to avoid strategic surprise. As will become evident in the next section of the paper, this concept of alternative futures is perhaps best captured in scenario planning. A second concept of foresight is the cone of plausibility (Figure Two). Conceptually, the cone does three things. First, it represents the relationship between past, present, and future, highlighting how possible alterative futures are whittled down over time as the present approaches. Second, moving into the future from the present, the cone illustrates how the array of alternative futures broadens the further out one goes. And third, the cone delineates between what is plausible in the future and what is implausible. Whatever rests outside the cone is considered implausible, perhaps interesting to think about but exceptionally unlikely to occur.

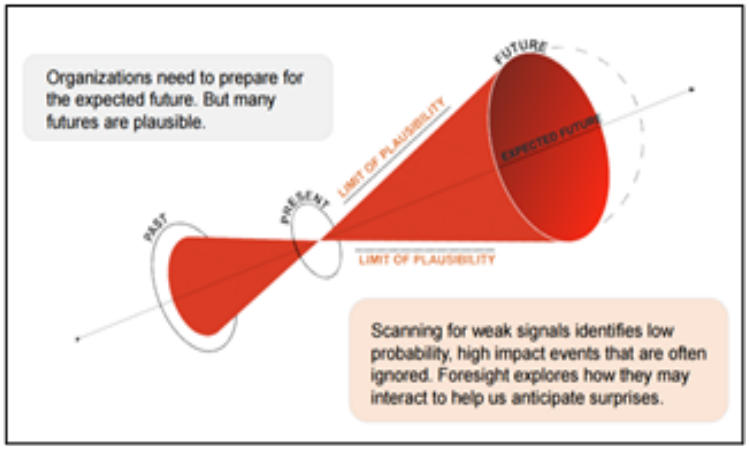


Figure 2: The Cone of Plausibility, Policy Horizons Canada, 2017

At the mouth of the cone of plausibility, travelling outwards into the future from the center, is a line, the expected, or baseline, future. This is the future we expect to happen given current trends, and – all things being equal – are on track to experience. For illustration: the expected future holds that military and security operations will continue to rely on human analysts. Analyzing and predicting short-term change or immediate developments is a subfield of research in itself, perhaps best captured by probabilistic science, forecasting, and prospection (i.e. prospective cognition) (Tetlock and Gardner 2015; Tetlock et. al. 2017; Meller et. al. 2015a; 2015b; Barnes 2016; Mallard and Lakoff 2011; Gilbert and Wilson 2007). Other tangentially related scholarship explores how organizations think about, anticipate, preempt, and prepare for low-probability (but highly impactful) future events and developments (Taleb 2007; Perrow 1999; Anderson 2010; de Goede and Randalls 2009).

However, if you analyze only contemporary trends based on historical data, then the only future you are truly exploring is the most likely and expected one, which is a fine exercise and valuable in itself, but does not properly prepare you for less-expected developments further out in the distance. Foresight corrects this deficiency by introducing a set of other alternative futures. Figure Three provides a visualization. Besides the expected future, the next most likely are the probable futures. These are "likely" to happen; these futures may be familiar to us. For illustration: one probable future holds that Artificial Intelligence and Machine Learning (AI/ML) are likely to augment intelligence collection and analysis.

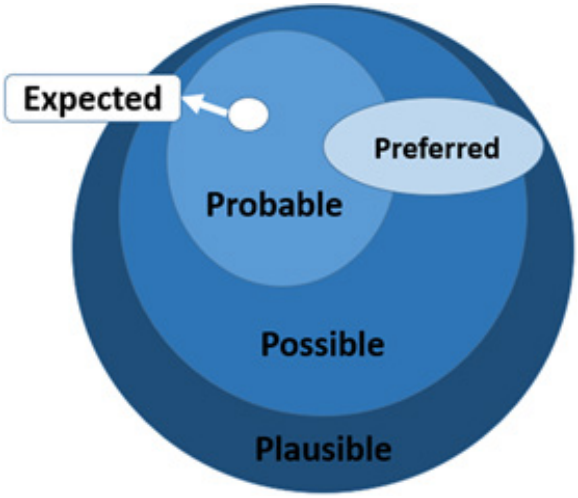


Figure Three: Alternative Futures Schematic

A third level are the possible futures. These "could" happen: they make intuitive sense given what we already know, but they are sufficiently different from what we might ordinarily expect. For illustration: one possible future holds that AI/ML could dictate and direct (rather than simply augment) security and military operations. The fourth level are the plausible futures; they include everything we can imagine. These futures "might" happen, even though they may rely on knowledge or technology humanity does not yet possess. Joseph Voros points to Star Trek's warp drive as an example of a plausible future: we don't have the technology to achieve it yet, but we've envisioned what it might look like (Voros 2001). For illustration: one plausible future that might occur is that AI-haves enslave AI-have nots in all domains of business, society, and warfare. The line between probable, possible, and plausible is fluid. For example, 25 years ago, autonomous robotics was a plausible future, but today it is a probable one. And 25 years from now, it may be a baseline or expected future. One final alternative future is the preferred one. This is a subjective or normative future, what "should" happen, or what we wish "would" happen. Former US President Barack Obama's Global Zero initiative to rid the world of nuclear weapons might be considered a preferred future. Other examples include Glenn Paige's vision for a society free of killing more broadly (Paige 2009).

A third concept important to strategic foresight is systems thinking. The premise is that all socio-political and economic phenomena are systems, made up of subsystems, actors, and relationships that connect to one another (Bishop and Hines 2012; Leonard and Bear 1994). Systems and parts of systems interact with each other in countless and complex ways. Strategic surprise is the result of that novel interaction. Systems thinking is a core philosophical underpinning of strategic foresight. It is not a tool, per se, but rather a lens with which to explore the possibility of alternative futures. Foresight, then, uses systems thinking to uncover potential interactions between and within systems in order to better appreciate alternative futures. A somewhat related and helpful concept is the acronym STEEP-V, which stands for Society; Technology; Environment; Economics; Politics; and Values. The system is exceptionally divers, best captured if one thinks of it as an amalgamation of different and distinct areas. Approaching systems thinking from a STEEP-V perspective ensures that we accept as broad a view as possible in our foresight research. As will become evident in the following section, the notion of STEEP-V is perhaps best captured by the Domain Map, which helps captures the scope of the foresight project itself.

The Future of Cybersecurity: Domain Map, Scanning & Insights, and Scenarios

What follows is an exploration of the future of cybersecurity based on three foresight tools and techniques that are commonly used within the Government of Canada, include domain mapping, horizons (or environmental) scanning and insight development, and scenario planning.

Domain Mapping: Exploring the Contours of Cybersecurity

A domain is any topic that serves as the focus of a foresight exercise. The domain can be a geographic region (e.g. Ottawa; Canada; North America), an organization (e.g. Global Affairs Canada; NATO), or an institution (e.g. education, policing, governance). The domain often also relates to time – how far into the future is the project meant to explore? Domain mapping is the process of conceptually and visually framing the scope of a given topic, of identifying and binding its conceptual parameters. Ideally, a domain map will incorporate elements captured from each of the distinct STEEP-V categories. Doing so ensures the subsequent foresight research will properly explore and contemplate important forces of change emanating from different and distinct areas of research, including areas that might not be ordinarily associated with the topic at hand. Developing a robust domain map at the beginning of a foresight exercise can help clarify how the foresight process will unfold.

Figure Four provides an domain map for "cybersecurity."[4] The map captures an array of traditional and less-traditional aspects associated with cybersecurity, including the actors involved in cyberspace, the emerging technologies and threats that influence cybersecurity, environmental, regulatory, and finance-based aspects of cybersecurity, and issues involving resilience and digital identity. The domain map provides us with a guideline for conducting the next phase of the foresight project: scanning and insight development.

Figure Four: Domain Map of Cybersecurity

[4]The Domain Map was created by Professor Wilner's graduate students: Jenn Spencer, Marion Agier, Veronica Driscoll, and Wesley Dionne, "The Future of Cyber Security," Strategic Foresight in International Security, NPSIA, Carleton, December 2019

Scanning: Building Insights on the Future of Cybersecurity

Scanning forms the basis of good foresight. It is the practice of systematically exploring a domain and the larger system's environment to better appreciate the nature of change within that environment. It is a process of identifying new and emerging issues and trends that could portend a future development, shift, or change (Hines and Bishop 2006; Hiltunen 2008; Harris and Zeisler 2002). Scanning can involve reading hard and online information, interviewing experts and laymen alike (e.g. Delphi approach), canvasing scientific data, and so on. Scanning aims to better understand the system under consideration by providing a bird's eye view of emerging developments. It tries to flush out individual signals and indicators of low probability but high impact that may lead to significant change within and beyond the system. In one sense, then, scanning is the collection of data relevant to the future. Scanning usually emphasizes technology-based signals because the emergence of a new technology often drives change in other categories. But scanning less tangible topics, like values, ethics, or governance, can also prove informative. A "scanning hit," or "weak signal," is an early sign of a potentially disruptive development. A hit is often a single point of data. It provides a glimpse of an alternative future, a sign that significant change could be under way. As a tool, scanning can prove a fast and effective way to build a repository of weak signals and other relevant information on a specific system or topic (Jackson 2013). A collection of related weak signals can be shaped into a higher-level insight or change driver. Here, individual scanning hits are combined and synthesized into a larger, more robust and impactful finding. Change drivers can cause significant change throughout the entire system under study (Policy Horizons 2017). And when two or more change drives interact between different systems, they can lead to unique and surprising events. In sum, scanning is the process of identifying and collecting scanning hits, which can be coalesced into insights or change drivers, which improve our understanding of a system's current and future state of change.

What follows is scanning material and high-level insights relevant to cybersecurity developed by Professor Wilner's graduate students at the Norman Paterson School of International Affairs (NPSIA), Carleton University. Five insights comprising several dozen weak signals are offered.

Insight 1: Data-mapping Adversarial Behaviour[5]

Artificial Intelligence, social media, and augmented reality will change how state authorities find, track, and catch criminals, spies, and other malicious actors. The ability to predict and preempt unwanted adversarial behavior may become a reality.

> **"The ability to predict and preempt unwanted adversarial behavior may become a reality."**

[5]This insight is derived from Professor Wilner's graduate student researchers: Gabriella Colavecchio, Mutasem Abu Hammad, Laurence Desforges-D'Aoust, Albert Johnson and Nathan Patterson, "The Future of Crime," Strategic Foresight in International Security, NPSIA, Carleton, December 2019.

> *Crime data is analyzed live by way of digital streaming services.* Twitch is a live video streaming platform owned by Amazon. Popular with gamers, it is also used by criminals and terrorists to live stream their activities and attacks. Other platforms, including Twitter, Streamable, and Telegram are used to similar ends. Authorities will have the ability to surreptitiously track and monitor these platforms for unwanted criminal behavior, shortening the time they may need to intervene.

> *Physical events are digitized for perpetual virtual investigation.* Augmented reality technology will provide investigators with the ability to revisit exact replicas of crime, terrorism, or battle scenes in fully immersive digital settings. These digital scenes can be continuously revisited, extending the longevity and "freshness" of the event itself. The data could allow for greater inter-agency, inter-jurisdictional, and international cooperation among enforcement and intelligence communities.

> *Open-sourced satellite data facilitates international investigations.* Paired with AI, satellite imagery can allow investigators to spot evidence of slavery from outer space. Illegal mines and kilns, and transient fish processing camps, can be identified from space, spurring international action and further physical intervention. Some malicious actors, unable to hide their criminal behavior form prying satellites, might change their behavior and forgo certain activities.

> *Predictive policing goes live.* Data is used to shape where, when, and why security and police patrols take place. Determining which individual is most likely to commit a future crime may follow, providing authorities with the means to counter and preempt crime and other attacks before they take place.

Insight 2: Upending the Conventional Security Paradigm[6]

Several inter-related developments in technology, politics, and society are providing new opportunities for weak states, malicious non-state actors, and criminals to achieve their strategic goals, potentially re-writing conventional assumptions embedded in contemporary statecraft, diplomacy, and warfare. Traditionally strong actors may find themselves with less power and fewer meaningful capabilities.

"Traditionally strong actors may find themselves with less power and fewer meaningful capabilities."

> *Emerging technology spurs multiple, novel arms races.* Nanoweapons, "nano-poisons," miniature drones, and the synthesis between cyberspace and biological space – the "biodigital convergence" – spur new competition between states seeking to leverage a fleeting competitive advantage over rivals. Existing concepts of dual-use technology, research ethics, and export control may expand as a result.

> *The weaponization of living things.*[7] The natural mechanisms inherent to plants, marine mammal behaviour, and even robotic bee drones are used to enhance surveillance capability.

[6]This insight is derived from Professor Wilner's graduate student researchers: Muna Osman, Jenn O'Rourke, Andreas Arvanitis, Piotr Dobrzynski, and Andrew Barker, "Bank of Canada Strategic Outlook 2030: A Foresight Exercise," Capstone in National Security Policy, NPSIA, Carleton, Summer 2018
[7]This insight is derived from Professor Wilner's graduate student researchers: Gant Croker, Hannah Diegel, Jenna McMahon, and Sean Murphy, "The Future of Weaponry," Strategic Foresight in International Security, NPSIA, Carleton, December 2019.

Elsewhere, other technology is being developed to genetically manipulate insects to spread viruses that attack specific genomic attributes. Tampering with genetic code can likewise lead to new methods of genocide or the eradication of entire species (e.g. "gene drive"). And human beings can be genetically enhanced to heal faster, regulate neurological processes, and learn new skills more quickly.

> *Autonomous warfare comes of age*. Developments in AI, robotics, and sensors threaten to permit machines to choose whether or not to kill a human being. These weapons can come in various shapes and sizes, can strike or observe with unprecedented precision, allow a military to operate without risking human lives, upend traditional notions of deterrence and coercion, and are vulnerable to proliferation should they become easier and more cost effective to produce. At the same time, there is no consensus within the international community on limiting or banning the use of autonomous weapons systems.

> *Cyberwarfare goes viral*. Cyberattacks are becoming more pervasive and prominent across both the public and private sectors. As critical and basic infrastructure becomes more reliant on digital networks, cyber weapons may become simultaneously cheaper and more effective. Greater computer literacy has the potential of creating a large supply of technological experts, which may use their skills for nefarious purposes. Major powers, including the US, remain relatively acquiescent regarding offensive cyber intrusions, unwilling to risk conventional escalation in the face of cyber intrusions. Conversely, rising powers, like China, appear willing to ensure their cyber attacks are deliberately noisy to illustrate both the depths of their newfound capability and the weaknesses of their adversaries. In response, traditional institutions, including banks, have accepted the inevitability of cyberattacks, altering their strategies accordingly.

> *The commodification of cyber weapons.*[8] In 2013, a group called the Shadow Brokers, managed to gain access to the National Security Agency's cyber weapons. Some of the stolen tools were made publicly available in 2017, and proved useful for gaining access to cyber infrastructure, for launching ransomware attacks, for surveillance operations, and for extracting, damaging, or deleting data from targeted systems. Since then, other developments have led to the emergence of black-market sales of cyber weapons, augmenting the cyber capability of traditionally weak actors. Non-experts can hire or purchase sophisticated cyber weapons for use in personalized attacks without having the matching technological knowhow.

Insight 3: The World goes "Smart" [9]

Several emerging technologies provide ever greater interconnectivity within society, providing the means for the constant monitoring of behaviour. With an individual's information connected to everything else, new and incredibly nuanced surveillance tactics could emerge, along with an endless exploitation of digital vulnerabilities. The result could lead to a world where truth is hard to ascertain, and profiling systems reign supreme.

> *We become data; the data become us*. Internet of Things (IoT) devices support "smart" living, intimately connecting our lives to the devices we own.

[8]Derived from Spencer, Agier, Driscoll, and Dionne, "Future of Cyber Security," Carleton, December 2019.
[9]Derived from Osman, O'Rourke, Arvanitis, Dobrzynski, and Barker, "Bank of Canada Strategic Outlook 2030," Carleton, Summer 2018.

Almost every product available to consumers – from cars to toothbrushes – has an IoT model. Traditional computer technology companies, like Nvidia, have partnered with traditional vehicle manufacturers, like Volkswagen and Audi, to enhance their product's ability to make use of developments in AI and ML. Other companies, like Mercedes Benz, are developing autonomous public transit vehicles. Alphabet, parent company of Google, is building mini smart cities in urban areas. Taking the IoT one step further, individuals are implanting devices into their bodies: employees of a vending machine company volunteered to have microchips implanted into their skin that could serve as security access cards and allow them to make purchases at work.

> *Super-profiling.* Emerging technologies are used to profile individuals in new ways. In China, facial recognition systems, which pair AI and biometrics, are used to arrest fugitives in public gatherings, and to track an individual's movements around restricted areas. China uses these and other emerging technologies in its social reputation and "morality scoring" systems, which provide individuals with a rating, influencing their access to financial and other services, and restricting their freedom of mobility and travel.

> *Fact equals fiction.* Discerning fact from fiction may become increasingly difficult in an interconnected world. Live video and audio can be superficially augmented. AI generated deepfakes might overwhelm "real" content online. Already, social media platforms are rife with bot accounts that influence narratives and public perceptions. Moreover, the transformation of the traditional media ecosystem, declining trust in public institutions, and low media literacy rates, have left the digital realm ripe for information and narrative control and manipulate.

Insight 4: Validating Digital Identity[10]

Most private and public sector engagements rely on identity verification to provide individuals with access to restricted networks, information, and services. Flaws within this process can lead to unauthorized access to digital systems, leading to significant security breaches, fraud, and loss of data. New forms of biometric data feeding newly established national digital identification systems provide possible solutions.

> *Upgrading verification.* Cybersecurity may require the continuous development of new methods for improving identify verification. Traditional biometric data, including fingerprints, blood and iris samples, voice or heartbeat recognition, and hair or DNA samples, may be combined with tokenized representations or ID Chip cards to verify the identity of an individual online when using private or public sector services. For illustration, Singapore's new public service app, SingPass, uses two-factor identification of either fingerprints, facial recognition, or 6-digit password to provide individuals with digital services provided by over 60 agencies.

> *Fooling face readers.* Smartphone facial recognition systems are not as impenetrable as some believe; new manufacturing techniques can fool the technology. Using several dozen cameras, a reporter was able to capture an especially detailed digital scan of his own face and head.

[10]This insight is derived from Professor Wilner's graduate student researchers: Jenn Spencer, Marion Agier, Veronica Driscoll, and Wesley Dionne, "The Future of Cyber Security," Strategic Foresight in International Security, NPSIA, Carleton, December 2019.

He then transferred the data to physical space using additive manufacturing technology (3D printing), creating a replica of his head able to trick the facial recognition software protecting his data. 3D printed biometric masks create problems for contemporary biometric identification processes.

> *Brainwaves as security*. An individual's unique brain print might be used as a biometric password. Brainwaves can be recorded and matched with an individual's specific thought process. These data assess how an individual reacts to a particular stimulus, a picture or phrase, for instance. The signal created by the stimulus will diverge between individuals based on unique physical characteristics and learned or experienced behavior, creating a complex interaction difficult to compromise or duplicate.

Insight 5: AI, Not Just Fancy Math

Much of society conceives of Artificial Intelligence, Machine Learning, and related technology from a position of data analytics: AI is simply (but not simple) advanced analytics and pattern recognition through big data.[11] But increasingly, AI is also finding its creative and cultural side, potentially changing the way individuals, communities, and societies relate to, and engage with, one another.

> *AI wins a Nobel Prize in Literature*. Artificial Intelligence is creating artistic content and ideas. Algorithms have been paired with cultural data in order to create new and novel art, a task once thought reserved to the human mind and to human creativity. AI has written original scores for Sci-Fi movies (staring David Hasselhoff, no less) and pop songs, created renaissance paintings, played piano, and generated original (but admittedly bad) jokes. And, in digital space, AI is generating new strategies for playing and winning multi-player computer games that simulate warfare.

> *AI personalizes climate change*. In much of the global north, in the relatively wealthy societies of North America, Europe, and parts of Asia, climate change is not (yet) personally felt. AI is being used to counter that, adopted to help visualize the effects of climate change on a local scale in areas where the actual effects of climate change are not commonly felt. ClimatPix is a free App that allows users to upload and share pictures of climate change, like wildfires, flooding, extreme weather, crop failure, locusts, and so on. The AI then uses these pictures to simulate the different climate change effects on other, local streetscapes, including those in wealthy major urban centers. The goal is to change local perception of and narrative around climate change by allowing wealthy populations to visualizing its personal and intimate effect.

Insights, weak signals, and scanning material provide the foresight process with the data needed to creatively (but realistically) envision a future landscape. The next step in the foresight process usually entails developing alternative scenarios of the future. What follows are two scenarios for the future of cybersecurity based on the scanning material synthesized here.

[11] Author interview, Anonymous, GCHQ Mathematician, London, UK, March 2020. Conducted as part of the author's IDEaS project on AI Deterrence.

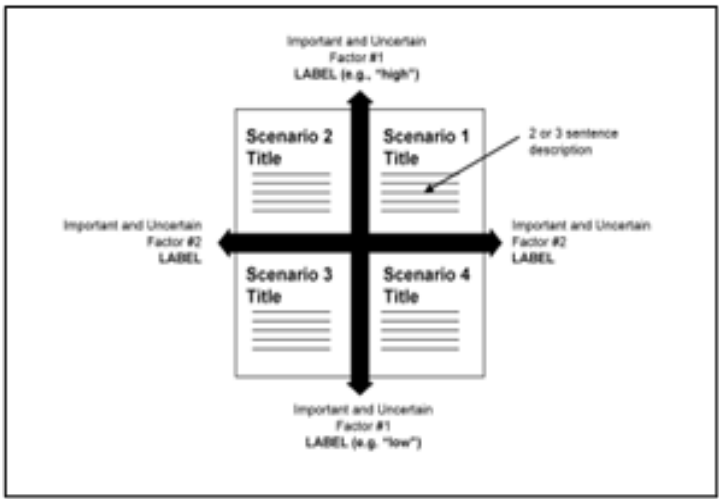
Scenarios: Imagining the Plausible

Scenarios are widely used and popular among serious futurists and non-experts alike (Singer and Cole 2015; Hanson 2016; Wittes and Blum 2015). Scenarios incorporate scanning material to establish and tell a fictionalized story that is interesting and plausible, and relevant for exploring a topic's or system's potential future (Lindgren and Bandhold 2003; Ringland 2010; Ogilvy 2002). They are used to describe the plausible futures that could arise when signals, change drivers and the system itself interact together. They offer us a way to imagine how future change will be felt and addressed. They help us visualize and think about how a system or domain might evolve. And they allow us to reduce complexity of the future states. Importantly, scenarios are easy to pitch to skeptical audiences who do not necessarily buy into foresight more broadly. After all, most individuals think through alternative scenarios in their own day-to-day activities – should I walk to work, take public transport, or Uber? – so it is not a giant leap to suggest and illustrate how organizations might use scenarios in their own long-term planning. When multiple, contrasting scenarios are used at once, diverging alternative futures can be visualized and explored side-by-side. Each scenario is unique and qualitatively different, forcing us to think in different and divergent directions. This helps us think through the unthinkable, to anticipate surprising plausible events and environments, and to contemplate the strengths and weaknesses of our, and our organization's, contemporary assumptions about the future. Finally, scenarios allow us to pick a time and space well into the future to explore without having to necessarily predict the specific path of actually getting to that future environment. Unlike trend analysis and forecasting, which project a trend into the future in the scale of days, weeks, or months using historical and contemporary data, scenarios are not necessarily path-dependent. Trend analysis identifies the path of change; scenarios skip that altogether in order to explore a set of future changes that are plausible, but not determined by any specific event or string of events. Likewise, because there are countless possible futures, the goal is not to explore them all – that would be tedious if not impossible. Rather, the goal with scenarios is to capture a slice of possible futures in a selected series of scenarios, each covering a different range of possible future outcomes and environments. The more points in the future you cover, the more likely you will be prepared to live that future if and when something like it occurs. You can prepare for it now, accordingly, by exploring what that space might look like for you, your organization, your policies, and so on.

There are dozens of ways, techniques, and methodologies for creating scenarios (Bishop, Hines, and Collins 2007; Policy Horizons 2017). Choosing a technique can depend on what the scenario's purpose is: Predictive scenarios explore *What will happen*?; exploratory scenarios ask *What can happen*?; and normative scenarios answer *How can we get to a specific future?* (Borjeson et. al. 2006). Scenarios can adopt thematic and archetypal formats. Policy Horizons Canada's *MetaScan 4: The Future of Asia* (which the author helped research and write) for instance, uses four archetype scenarios – expected, decline, progress, and transformative scenarios – that provide the fictional scaffolding upon which information derived from scanning, insights, and change drivers is hung. (Policy Horizons 2015a; 2015b.) Each archetype covers a range of plausible futures captured within a distinct but internally congruent narrative.

Another approach to scenario development relies on a matrix. Figure Five provides a graphical representation. Here, two major driving forces of change previously identified by scanning processes, are paired, one along the X-axis, the other on the Y-axis. At all four points of the intersection, the change driver is purposefully pushed to an extreme.

Figure Five: Matrix Scenario Construction (Heuer and Pherson 2011)



For example, in thinking through the Future of NATO, US *Leadership* might be placed along the X-axis, expressed as *Strong Leadership* at the far left and *Weak Leadership* at the far right. On the Y-axis, a second driver of change, perhaps European Domestic Support for NATO can be added, with *Strong Support* pointing upwards and Weak Support pointing downwards. We now have the making of four contrasting future scenarios with which we might explore multiple plausible futures for NATO. For illustration, at the bottom-left quadrant, NATO suffers as a result of both weak US leadership and weak European support. At the top-right, by contrast, a muscular NATO emerges as a result of strong US and European support. The matrix approach to scenario creation provides a clever way to explore deeply contrasting future scenarios that are nonetheless rooted to current events. A serious limitation, however, is that a 2 X 2 construct only captures two change drives, placing a significant limit on how much scanning material can be packaged into the exercise.

Although scenarios are only plausible descriptions of potential future events, and are inherently fictional in nature, they provide a context against which to explore and test our contemporary assumptions and policies. Scenarios provide us with the creative license to explore and consider future policy challenges and opportunities. What follows are two alternative scenarios for the future of cybersecurity, derived with assistance from Professor Wilner's graduate students: *Cyborg Security and Return to Analog.*[12]

Scenario One: Cyborg Security

The year is 2035. Following decades of escalating cyber intrusion and attack, Canadian businesses, communities, and citizens have demanded more innovative solutions from their governments. In response, government funding has led to spectacular breakthroughs in biometrics, leading to the development of related technology able to actively synthesize an individual's genome DNA into a digital footprint. The bio-digital technology is comprised of a small device – roughly the size and width of a postage stamp – that is embedded (painlessly) under the skin, usually around a person's wrist or forearm. Because the device fuses seamlessly into the body, cybersecurity experts have dubbed its development "cyborg security".

[12]Derived from Spencer, Agier, Driscoll, and Dionne, "The Future of Cyber Security," Carleton, 2019.

Every citizen's genome DNA has been articled into a database, the Canadian Identity Hub (CIH). The Hub, for short, is an infallible bio-digital network and storage system that is continuously updated and monitored using artificial intelligence combined with quantum computing. The encryption of the network changes and evolves at speeds far faster than a zeptosecond, robbing cybercriminals and hackers sufficient time to breach the system. The active DNA footprint from each individual's embedded device is used to verify an individual's identity online. The DNA verification device is continuously connected and paired to the Hub through Canada's National 6G Network (N6N) and serves as a means to log in and identify an individual on the internet. This biometric device cannot be stolen, mimicked, or defrauded because only one unique active genome ID can be connected to the network at any time, and an individual's connection is permanently active. This technological breakthrough has essentially eliminated online identity fraud and allowed the field of cybersecurity to guarantee identities for online public and private sector services.

As a result of these developments, a rapid consolidation of traditional identity markers has taken place. An individual's passport, drivers' licenses, Health Card, Social Insurance Number, federal Personal Record Identifier (PRI), banking credentials – even their Netflix-Disney+ accounts – and dozens of other services, Apps, and platforms are now combined into a single genome identity. The Hub provides umbrella security to these disparate pieces of information and data, all of which can now be accessed by all participating entities and organizations, providing new services and benefits to the individual.

Canada's bio-digital verification standard and technology was adopted by members of the Group of Thirty-Three (G33), which represents three-quarters of the world's population and 93 percent of gross world product. Almost immediately, rates of international cybercrime drop back to 2015 levels. The arrangement also provides G33 governments with the ability to leverage the system's AI to help identify genome IDs that conduct illicit cross-border activity, both on and offline. In keeping with the 2025 *Tbilisi Protocol for the Ethical Use of AI*, the person's identity is not revealed to international law enforcement until a human agent verifies the flag for accuracy and judgement. If illicit activity is indeed identified and confirmed by a human agent, an international investigation is conducted, and the genome identity is revealed and disseminated to the necessary authorities. In less than three months following its inauguration, the G33 system has all but extinguished international cybercrime.

> **"At long last, the bio-digital industry has lived up to its hype, providing infallible cybersecurity that promises to generate countless further innovations in society, the economy, and good governance. The pillars of a true cyber civilization appear on the horizon."**

A welcome, but initially unintended, secondary social effect of the new global verification system is that individuals and groups begin to be more conscientious, courteous, and civil in their online interactions. The rate of vitriol drops precipitously: misinformation, cyber-misogyny, and racialized content, for instance, begin to disappear. A new culture of online trust takes hold, strengthening democratic discourse. At long last, the bio-digital industry has lived up to its hype, providing infallible cybersecurity that promises to generate countless further innovations in society, the economy, and good governance. The pillars of a true cyber civilization appear on the horizon.

Scenario Two: Regression to Analog

The year is 2035. Following decades of escalating cyber intrusion and attack, most governments and all major private sector actors have started the process of "cyber regression," actively pulling critical services, platforms, and industries offline. Cyberspace is simply too risky: the narrow and limited benefits the Internet provided society during its first two decades are now far outweighed by the social, economic, privacy, security, and governance costs it has generated.

Watershed moments in cybersecurity – which in another era would have been the defining event of the decade – cascade into each other on a semi-regular basis. The 2032 simultaneous hack of all e-Yuan trading platforms hosted in mainland China led to the theft of an estimated ¥150 trillion CNY ($200 trillion USD); the People's Bank of China, which guaranteed the e-Yuan, ceased functioning for six weeks as a result. The 2033 cyber attack on the Nogent Nuclear Power Plant in France – with its catastrophic nuclear fallout – devastated Europe; much of Paris, Brussels, and Amsterdam remain uninhabitable. And the 2034 data breach of the My Social Security portal – resulting in the identity theft of over 90 percent of all American citizens – continues to ripple through the United States; the Senate recently failed to pass a bill that would have provided a short-term replacement to compromised Social Security Numbers, once again stalling the delivery of social benefits and provisions. Other major cyberattacks continue apace, fed by the widespread development and proliferation of sophisticated cyber weapons, readily available for purchase, rent, or hire on the Dark Web.

In response to these cascading concerns and developments, the Government of Canada's cyber regression strategy entails a radical and rapid technological shift to analogue in critical infrastructure, national defence, governance, and social service provision. The new Prime Minister, whose anti-tech Altruist Party of Canada swept last year's federal election, has a popular – some say populist – mandate to take her "de-teching" plans even further: the removal of all sensitive digital information from Canadian hospitals, banks, universities, and major industries. Political rumours swirl that a total ban on e-commerce is in the making. Most other governments around the world are similarly reluctant to rely on technology in their own operations. Some institutions have resorted to using L-LANs (Limited Local Area Networks) for transferring sensitive information within their immediate organization; any system or device containing sensitive data is not permitted to connect to any wider network. When information has to be transferred off-site, it is moved using confidential (and usually armed) physical couriers which transport data using 1 petabyte c-drives.

The wider, and global, implication of cyber regression are evident across society. Major insurance providers no longer offer cybersecurity coverage of any sort. Bitcoin and Ether both trade at less than an American nickel. Global online retail sales have dropped precipitously, to below 2015 levels. Tech-free communes and sanctuary cities proliferate. Social distrust – even fear – of cyberspace and other related technologies is commonplace. Some scholars equate the counter-tech epoch as a counter-revolution; others see the making of a new quasi-religious identity. Either way, most individuals significantly limit their time spent online. So called "dumb phones" are now the new smart phones. Social Media interactions give way to traditional friendships and physical experiences. Both Facebook and Twitter file for bankruptcy protection within weeks of each other, and WeChat, TikTok, and Weibo are forcibly shut down by Chinese regulators.

To a large degree, people consider cyberspace a lost cause; unsalvageable. "I f*cking quit" is how one prominent Japanese cybersecurity expert put it in his now-legendary speech to the UN General Assembly. There has been a marked shift away from trying to actually improve cybersecurity, to rebuilding and bolstering traditional and classical sectors of industry, including brick and mortar retail, tourism, manufacturing, clean energy, bio-ethical agriculture, asteroid mining, physical rather than digital services, drone shipping, and vertical real estate. As a result, new employment opportunities emerge in areas of the market that had largely been replaced by the tech sector decades ago. Unemployment rates in most countries have dropped to a respectable 10 percent. Civilization's turbulent experiment with cyberspace may be ending, but the simple life is providing its own rewards.

Concluding Thoughts

While strategic foresight is ultimately about researching the future, the end goal of the research itself is about informing the present. As Martin Roy and I explain: "Foresight is all about making decisions today, not tomorrow. … While foresight involves the exploration of possible and plausible alternative futures, its main focus is about making the best possible choice today to withstand whatever may come next" (Wilner and Roy 2020). This report, combining a series of foresight tools derived from the Government of Canada, provides a preliminary investigation of plausible alternative cyber futures, suggesting avenues for exploring and improving current policy.

The domain map illustrates why a narrow perspective of cybersecurity invites strategic surprise: important change to cybersecurity might come from sub-domains not ordinarily associated with cybersecurity. Taking a broad view of the subject forces us to think more creatively about where the forces of change might emerge. Launching off the domain map, next steps might entail broadening the scope of the subject matter experts and community and private sector stakeholders invited to the table to discuss and plan Canada's cybersecurity future. Ethicists, anthropologists, psychologists, religious scholars, and others not currently or traditionally involved in cybersecurity policy should be sought out, expanding the frame with which we presently view the topic.

The scanning material highlights elements of change currently taking place within the domain. Some of the scanning hits and insights, depending on whether and how they interact with the larger system at hand in the coming years, may lead to monumental change in the way we think about and approach cybersecurity. They provide us a glimpse of what is possible and plausible, further forcing us to think creatively about the future of cybersecurity. And yet, the scanning material provided here is far from exhaustive; it is but an introduction to (or snapshot of) current developments. Moreover, scanning is a continuous and ongoing process of building better awareness of the forces of change within a domain. Accordingly, next steps might involve using the scanning material presented here as an impetus to developing more robust, nuanced, and dedicated scanning capacity within the federal government with a particular focus on cyber futures. Existing (or newly convened) scanning networks dedicated to cybersecurity could then routinely meet to share their scanning material, much as Horizons, NRCan, SCC, and other federal entities do today with their own scanning research. Cybersecurity scanning reports and briefs should likewise be regularly published and disseminated within the government (and, perhaps, with the public, too), just as GAC, the Canadian Forest Service, and the Canadian Nuclear Safety Commission have done with their own material (GAC 2018; CFS 2020; CNSC 2018).

The end result would be a public service more keenly aware of the forces of change, better able to adapt and respond.

And finally, the two scenarios – which capture contrasting "progress" and "decline" storylines for the future of cybersecurity – thematically extrapolate and combine the scanning material in ways that allow us to envision alternative futures for ourselves. From a policy perspective, the scenarios can be used to creatively reflect on the continued strengths of the assumptions embedded within contemporary cybersecurity strategy and decision-making, and on the continued long-term utility of existing polices, programs, and regulations. Next steps might involve convening cybersecurity stakeholders for a series of tabletop or experiential exercises where current cybersecurity assumptions can be identified and tested against these (and other similar) scenarios. The goal should be to identify weak current assumptions that are embedded within existing Canadian cybersecurity priorities, programs, and policies. These weak assumptions do not properly reflect the future of cybersecurity; corresponding government policies might therefore fail to accomplish their intended future effect. Using scenarios to determine the strengths and weaknesses of current assumptions can help improve and bolster government policy in ways that resonate with future plausible developments.

References

Anderson, Ben, "Preemption, Precaution, Preparedness: Anticipatory Action and Future Geographies," Progress in Human Geography 34:6 (2010).

Association of Professional Futurist, "2018 MSFW Award Winners," October 9, 2018
Barnes, Alan, "Making Intelligence Analysis More Intelligent: Using Numeric Probabilities", Intelligence and National Security 3:31 (2016).

Bishop, Peter Bishop and Andy Hines, Teaching about the Future, Palgrave Macmillan: 2012).
Bishop, Peter, Andy Hines, and Terry Collins, "The current state of scenario development: an overview of techniques", Foresight 9:1 (2007).

Bishop, Peter and Kay Strong, "Why Teach the Future?", Journal of Future Studies 14:4, (2010), 101.
Bengston, David, et. al., "Strengthening Environmental Foresight: Potential Contributions of future Research," Ecology and Society 17:2 (2012).

Borjeson, Lena, et. al., "Scenario Types and Techniques: Towards a User's Guide", Futures 38 (2006).
Canadian Forest Service, Snapshots of Canada's Forests in 2035 (2020 draft).

Canadian Nuclear Safety Commission, EScan 2018, (2018 draft).

Canadian Security Intelligence Service, "Of Threats and Opportunities: Exploring Canada's National Security Interests in 2025", (2014).

Caudle, Sharon and Stephan de Spiegeleire, "A New Generation of National Security Strategies: Early Findings from the Netherlands and the United Kingdom", Journal of Homeland Security and Emergency Management 7:2 (2010).

Colavecchio, Gabriella, Mutasem Abu Hammad, Laurence Desforges-D'Aoust, Albert Johnson and Nathan Patterson, "The Future of Crime," Strategic Foresight in International Security, NPSIA, Carleton, December 2019.

Conference Board of Canada, Energy Futures for Canada (2012).

Croker, Gant, Hannah Diegel, Jenna McMahon, and Sean Murphy, "The Future of Weaponry," Strategic Foresight in International Security, NPSIA, Carleton, December 2019.

Dator, Jim, "What Futures Studies is, and is Not", Hawaii Research Center for Futures Studies, 1995.
De Goede, Marieke and Samuel Randalls, "Precaution, Preemption: Arts and Technologies of the Actionable Future," Society and Space 27:5 (2009).

Department of National Defence, The Future Security Environment 2008-2030 (January 2009).

Ditchburn, Jen, "The Coolest Government Org You've Never Heard Of," Policy Options, 2017.

Gilbert, Daniel and Timothy Wilson, "Prospection: Experiencing the Future," Science 317:5843 (2007).

Global Affairs Canada, "The Missing Link Between Present & Future," Martin Roy presentation to Ottawa Workshop on Strategic Foresight, Ottawa, November 2017.

Global Affairs Canada, "A (de)Globalizing World? Environmental Scan 2017-18," (2018).

Habegger, Beat, "Strategic Foresight in Public Policy: Reviewing the Experiences of the UK, Singapore, and the Netherlands," Futures 42 (2010).

Harris, Dyer and Steven Zeisler, "Weak Signals: Detecting the Next Big Thing," Futurist 36:6 (2002).
Heuer and Pherson, Structured Analytics Techniques for Intelligence Analysis (2011).

Hiltunen, Elina, "Good Sources of Weak Signals: A Global Study of Where Futurists Look for Weak Signals," Journal of Futures Studies 12:4 (2008).

Hines, Andy and Peter Bishop, Thinking about the Future: Guidelines for Strategic Foresight, (Washington, DC: Social Technologies 2006).

Hanson, Robin, The Age of Em: Work, Love, and Life when Robots Rule the World, (Oxford University Press, 2016).

Global Affairs Canada, "The Missing Link Between Present & Future," Martin Roy presentation to Ottawa Workshop on Strategic Foresight, Ottawa, November 2017.

Global Affairs Canada, "A (de)Globalizing World? Environmental Scan 2017-18," (2018).

Habegger, Beat, "Strategic Foresight in Public Policy: Reviewing the Experiences of the UK, Singapore, and the Netherlands," Futures 42 (2010).

Harris, Dyer and Steven Zeisler, "Weak Signals: Detecting the Next Big Thing," Futurist 36:6 (2002).
Heuer and Pherson, Structured Analytics Techniques for Intelligence Analysis (2011).

Hiltunen, Elina, "Good Sources of Weak Signals: A Global Study of Where Futurists Look for Weak Signals," Journal of Futures Studies 12:4 (2008).

Hines, Andy and Peter Bishop, Thinking about the Future: Guidelines for Strategic Foresight, (Washington, DC: Social Technologies 2006).

Hanson, Robin, The Age of Em: Work, Love, and Life when Robots Rule the World, (Oxford University Press, 2016).

Jackson, Michael, Practical Foresight Guide (Shaping Tomorrow, 2013), chapter 3.
Leigh, Andrew, "Thinking Ahead: Strategic Foresight and Government," Australian Journal of Public Administration 62:2 (2003).

Leonard, Allenna and Stafford Bear, "The Systems Perspective: Methods and Models for the Future", AC/UNU Millennium Project, 1994.

Lindgren, Mats, and Hans Bandhold, Scenario Planning: The Link between Future and Strategy, (Palgrave: 2003).

Mallard, Gregoire and Andrew Lakoff, "How Claims to Know the Fugure are used to Understand the Present Techniques of Prospection in the Field of National Security," in Camic, Gross, and Lamont (eds.) Social Knowledge in the Making (University of Chicago Press, 2011).

Meller, Barbara., et., al., "The Psychology of Intelligence Analysis: Drivers of Prediction Accuracy in World Politics", Journal of Experimental Psychology 21:1 (2015).

Meller, Barbara, et. al., "Identifying and Cultivating Superforecasters as a Method of Improving Probabilistic Predictions", Perspectives on Psychological Science 10:3 (2015).

Missiroli, Antonio, "Strategic Foresight – and the EU", European Union Institute for Security Studies, Brief Issue 13, 2013.

Ogilvy, Jay, Creating Better Future: Scenario planning as a tool for a better tomorrow, (Oxford 2002).

Osman, Muna, Jenn O'Rourke, Andreas Arvanitis, Piotr Dobrzynski, and Andrew Barker, "Bank of Canada Strategic Outlook 2030: A Foresight Exercise," Capstone in National Security Policy, NPSIA, Carleton, Summer 2018.

Padbury, Peter, "Next Stop: Scanning and Foresight", Policy Horizons Canada, 2011.

Paige, Glenn, Nonkilling Global Political Science, (Center for Global Nonkilling, 2009).

Perrow, Charles, Normal Accidents: Living with High-risk Technologies, (Princeton University Press, 1999).

Policy Horizons Canada, "An Overview of the Horizons Foresight Method," Module 1 (2016).

Policy Horizons Canada, Module 5: Change Drivers, 2017.

Policy Horizons Canada, "Introduction to Foresight," Module 1, 2017.

Policy Horizons Canada, MetaScan 4: Future of Asia (2015).

Policy Horizons Canada, Geostrategic Cluster Findings: The Future of Asia, December 2015.

Policy Horizons Canada, "Exploring Biodigital Convergence," February 11, 2020.

Policy Horizons Canada, "Scenarios in the Horizons Foresight Methods," Module 6, 2017.

Rademaker, Michel, "National Security Strategy of the Netherlands: An Innovative Approach," Information & Security 33:1 (2009).

Ringland, Gill, "The Role of Scenarios in Strategic Foresight", Technological Forecasting and Social Change 77 (2010).

Scharre, Paul, "Robotics on the Battlefield Part II: The Coming Swarm", Center for a New American Security, 2014.

Schwartz, Peter, The Art of the Long View (Doublday, 1991/1996).

Singer, PW, and August Cole, Ghost Fleet: A Novel of the next World War, (Harcourt, 2015).

Spencer, Jennifer, Marion Agier, Veronica Driscoll, and Wesley Dionne, "The Future of Cyber Security," Strategic Foresight in International Security, NPSIA, Carleton, December 2019.

Taleb, Nassim Nicholas, Black Swan: The Impact of the Highly Improbable (Random House, 2007).

Tetlock, Philip and Dan Gardner, Superforecasting: The Art and Science of Prediction (London: Random House, 2015).

Tetlock, Philip et. al., "Bringing Probability Judgements into Policy Debates via Forecasting Tournaments", Science 355 (2017).

UK Government Office for Science, "The Futures Toolkit," November 2017.

US Office of the Director of National Intelligence, Global Trends: Paradox of Progress, January 2017.

Voros, Joseph, "A Primer on Futures Studies, Foresight and the Use of Scenarios," Prospect 6 (2001).

Wilner, Alex and Martin Roy, "Canada's Emerging Foresight Landscape: Observations and Lessons," Foresight, (forthcoming 2020).

Wittes, Benjamin and Gabriella Blum, The Future of Violence: Confronting a New Age of Threat, (Basic Books, 2015).

Work, Robert and Shawn Brimley, "20YY: Preparing for War in the Robotics Age," Center for a New American Security, 2014.