

Info-

## Graphic

July 2020

### Author

Dr. Alex Wilner



# The (Cyber) Future of Procurement

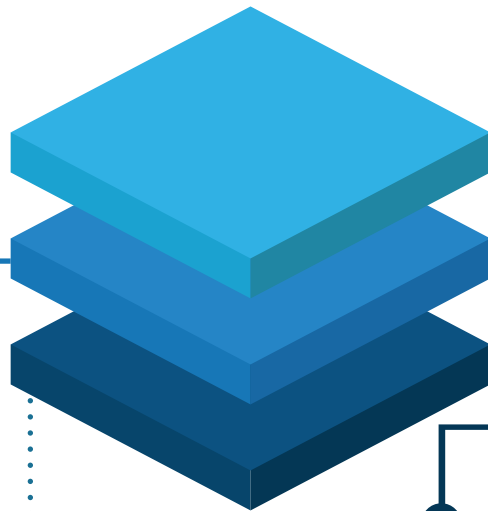
# CYBER FUTURES

## A PRELIMINARY SCANNING AND FORESIGHT REPORT

Cybersecurity is an ever-evolving landscape. Foresight tools—derived from the Government of Canada—can aid in the preliminary investigation of plausible alternative futures.

Strategic foresight is the study of societal change.

STRATEGIC FORESIGHT IS ROOTED TO 3 CONCEPTUAL BUILDING BLOCKS.



### 1. THE FUTURE IS NOT SINGULAR

Instead of thinking of time as one single line emanating outwards from today, picture a river delta with various braids and branches, each representing a different path that leads to a different alternative future.

### 2. THE CONE OF PLAUSIBILITY

If you analyze only contemporary trends based on historical data, the only future you are truly exploring is the most expected one. Foresight corrects this deficiency by introducing a set of alternative futures.

- » **PROBABLE FUTURE:** artificial intelligence (AI) and machine learning (ML) support intelligence operations.
- » **POSSIBLE FUTURE:** AI and ML direct security and military operations.
- » **PLAUSIBLE FUTURE:** AI enslaves humankind for its own security and military operations.

### 3. SYSTEMS THINKING

All socio-political and economic phenomena are systems, made up of subsystems, actors, and relationships that connect to one another. 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.

### STEEP-V

A helpful concept is the acronym STEEP-V: Society; Technology; Environment; Economics; Politics; and Values. Approaching systems thinking from a STEEP-V perspective ensures that we accept as broad a view as possible in our foresight research.

### SCANNING

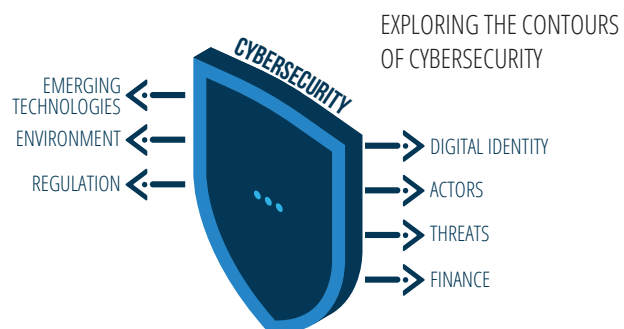
Scanning involves reading information, interviewing experts, and examining data to form a picture of emerging threats by identifying different signals (areas of potential disruption) consolidated as insights or change drivers.

### POTENTIAL INSIGHTS ON THE FUTURE OF CYBERSECURITY

1. Data-mapping adversarial behavior to preempt it.
2. Conventional security paradigm shifts.
3. Smart technology maximizes surveillance opportunities and increases vulnerabilities.
4. Digital identity validation.
5. The emerging pre-eminence of AI intelligence.

### DOMAIN MAPPING

Domain mapping identifies an issue's scope and demarcates the parameters of connections between concepts. Ideally, a domain map will incorporate elements captured from each of the STEEP-V categories.



### SCENARIOS

Analysts develop alternative scenarios of the future to visualize how systems or domains might evolve and to discover how to reduce complexity through predictive, exploratory, and desired scenarios.

Two scenarios – which capture contrasting “progress” (*Cyborg Security*) and “decline” (*Return to Analog*) storylines for the future of cybersecurity – thematically extrapolate and combine the scanning material.