PREFACE

The last few years have seen an incredible increase in the proliferation of false or deceptive information through the information environment—especially through the communication channels provided by social media platforms. While not all false information is promulgated with malicious intent, state and non-state adversaries are actively exploiting the information environment to engage Canada's military, government, public, and institutions to influence their will, attitudes, and behaviours. Several key factors have contributed to the increased importance of the information environment as an "area of operations" for our adversaries. First, engaging with target audiences is made easy when the cyber domain is leveraged to spread false information. Not only is adversaries' reach enhanced by the high level of connectedness Western democracies have to the cyber domain, the generation and sharing of deceptive content can be done quickly and cheaply thanks to algorithms designed to create disinformation intended for online distribution (i.e., "bots"). Second, Canada and its closest allies are democracies that value and promote free speech—a quality that reduces the extent to which access to information within the cyber domain will be put under the control of governments in an effort to reduce exposures to disinformation or even hateful content. The way we use and treat the technologies designed to connect with others not only makes us vulnerable to adversary actions, it has served as an enabler for adversaries and made their operations in the information environment almost inevitable.

This book is about gathering the information Canada needs to begin the development of a framework for devising methods that discourage adversaries' engagement with Canada's institutions and its public. In our view, to successfully deter an actor from engaging us in the information domain, we must have adequate awareness and control of the information environment so that we can shape adversaries' understanding of Canada's readiness and capability to defend itself against psychological and social attempts to manipulate its various institutions.

The first step in creating this book was to hold group sessions in which the critical knowledge gaps were identified in our understanding of the factors that must be considered to discourage adversary attacks in the information environment. The gaps were translated into key issues to be addressed by the chapters. In the next step, we reached out to internationally respected experts across multiple fields to provide us with their perspectives on one or more of the key issues. The editorial team spent long hours over the past year poring over (and chasing after) proposals and manuscripts to create this book. We anticipate that it will have been worth the effort, and that this will serve as an important reference to inform the development and validation of methods and techniques to mitigate the impact of attacks in the cyber domain.

Peter Kwantes, PhD
Chief Scientist, Defence and Research and Development Canada,
Toronto Research Centre