Introduction

Disinformation in its international form, often referred to as Foreign Information Manipulation and Interference (FIMI), is considered one of the oldest and most natural phenomena in social history. Throughout history, there have been numerous examples of communication techniques and processes that were built on lies, both spontaneously and in an organized manner (Frankfurt, 2005). And with advancements in technology and society, these communication techniques have become modern tools of politics and marketing (Phillips, 2019). Disinformation arises from the cognitive weaknesses, habits, and limitations inherent in the brain's natural physiology that controls information processing. These weaknesses are sometimes exploited consciously and deliberately by states in information operations to gain an advantage over the target of such actions.

An in-depth analysis of the international discussion on the phenomenon in question led the authors to propose an "operational" definition of disinformation, namely: *a doctrine and practice employed by states and non-state actors to deliberately use manipulated or falsified information in order to induce a desired change in a specific audience within a planned area of influence. Disinformation is intended to harm the recipients and is used as part of information and propaganda operations involving techniques of influence and psychological manipulation during times of peace, crisis, and war*. In Chapter 3, the authors outline various approaches to defining the phenomenon and explore alternative synonyms for conceptualizing it.

Disinformation is of interest as a subject of research in many scientific disciplines. Often, however, these disciplines are confined to methodological particularisms and a narrow spectrum of interests. For example, political scientists will look at disinformation as a tool of state and international policy; they will examine its goals and justifications and analyze the impact it has on society and individual and collective decisions. At the same time, a foreign relations scholar will study the place of this phenomenon in the foreign policy arsenals of modern countries. When addressing issues around the politicized impact of disinformation on democratic societies and their resilience, both academics may seek the support of a psychologist or sociologist in understanding the dynamics of social change and the limitations of cognitive processes. They may be assisted in this by a linguistic scholar focused on language and communication. Strategic studies researchers may view disinformation as a "peacetime and wartime weapon" and analyze the threats it poses. In the area of media studies, disinformation may be investigated through the lens of the

evolution of the entire information ecosystem, the technology boosting the news production and accelerating its circulation. These varied methodological approaches all contribute value within their individual disciplines but have left the study of disinformation disjointed and in need of a broader interdisciplinary framework – one that understands disinformation both as a social phenomenon and a tool of politics.

International disinformation, which is the focus of this book, adds to the foreign policy arsenals of modern states. Some states rely on it more heavily than others in their international activities, thereby becoming a paragon for other zealous states. However, what distinguishes this disinformation from other types of truth falsifications in human communication is, apart from its goals, the intensity and scale of means used to target wider groups. In a sense, state disinformers are like traveling salespeople trying to sell a certain message or narrative. However, unlike dishonest traders, they target not individuals but whole foreign societies, or large factions within them, seeking to control their behavior and decisions.

Disinformation, regardless of its motives and manifestations, poses a significant threat to security due to its increasingly harmful impact on communication and cooperation among the international community, both at the individual and interstate levels. True information is essential for individuals to satisfy their needs and function properly. The foundation of this process is trust, which is the recipient's belief that a source and its information are credible. The way information is perceived is sometimes conditioned by emotions, the appeal of the medium, or cognitive traps. It is therefore not difficult to imagine the potentially catastrophic consequences of automatic trust that is not supported by control mechanisms or sufficient critical thinking. It is essential that truthfulness of information be verified (McIntyre, 2018).

Contemporary technological developments, and in particular the rise of the internet and so-called new media, have resulted in an unprecedented production of information that circulates more quickly than ever before. Modern communication tools not only allow for access to various online services but also provide opportunities to store and develop knowledge, reduce communication costs, globalize messages, change social relations, and diversify forms of communication by combining words, pictures, sounds, and other content. As a result, modern opinion leaders are no longer solely entities legitimized by democratic choice (e.g., politicians) or public authority (e.g., ethical scientists or media journalists), but can also include any individual producer of disinformation.

These new technological tools also help to test the vulnerability of small niche interest groups and micro-target them more effectively as a result. This creates new opportunities to affect multiple social targets at the same time,

using various narratives within a strategic disinformation campaign implemented by a given state actor. In such operations, however, diverse content and ways of communicating that content – tailored to the specific nature of the target audience – also involve a shared intent and digital tools. Modern recipients of information, equipped with technologies, can independently choose what sources and information they want to access. However, these choices often contribute to the growth of "information bubbles" operating in competition. Such bubbles compete for the attention of recipients, striving to increase the "clickability" of their own content. To improve customer satisfaction, they will often simplify or falsify information to better correspond to their target demographics' identified or influenced needs, tastes, and emotions. In business, manipulating information translates itself into customer acquisition and, ultimately, financial profit. However, in interstate relations, manipulating information brings rewards of much greater value.

In this book, we look at the specific dimensions of this phenomenon, namely disinformation carried out by modern states and other international actors, sometimes used by states as proxies. From the earliest forms of inter-state relations, disinformation based on fabricated data has been a policy tool used by states in times of war and peace with the goal of gaining an advantage. It has been used to blur and disrupt opponents' recognition of the environment, therefore making it difficult to overcome uncertainty around decision-making.

In each case, these activities have specific justifications and contexts, but their general ambition seeks to improve the disinformer's position in the world and achieve specific short- or long-term benefits. Such benefits are often the opposite of cooperation and reflect a zero-sum game, measured by the resulting influence, power, and control the disinformers have over decisions and social processes in foreign countries. A well-known example of such consequences of disinformation is Russian influence over presidential campaigns in the U.S. and the weaponization of disinformation during the COVID-19 pandemic (Allcott & Gentzkow, 2017, pp. 211–236; Collins, 2021). Disinformers view information operations as a cheap tool of influence based on state power and facilitated by modern technology. However, the consequences of such operations are deep and destructive for democratic societies, whose resilience continues to be tested as means of counteraction remain relatively limited and often delayed.

This book addresses several research issues concerning three distinct groups of problems related to disinformation, which are:

1. The origins and characteristics of disinformation as a security problem for modern states.
2. Ways to identify disinformation and operational schemes of international disinformation actors.

3. Countering the threat of disinformation through methods that make societies more resilient and promote media education.

The community of democratic states is increasingly aware of disinformation threats, which has encouraged their societies, governments, international organizations, and technology companies to reflect on educational and protective measures. The key to successfully countering contemporary forms of disinformation is by making individuals and societies more resilient. Resilience is the ability to recognize and solve problems, assess a situation, and react to it appropriately. It also depends on the ability to respond to false, manipulated, or incorrectly prepared and disseminated information in a systematic manner.

The authors of this book took up the challenge of gathering in one place previously scattered knowledge on how to understand, recognize, and combat disinformation. We aim to offer readers a publication that, in a scientifically yet concise and reader-friendly manner, guides them through the meanders of this issue. To this end, the book has been divided into three parts, each consisting of four chapters and a short summary in the form of answers to the ten most relevant questions related to the topics discussed.

The first part of the book is devoted to the concept of disinformation, its intellectual and political origins, and its broader social context. The opening chapter discusses issues related to the evolution of the international security environment in recent years and how disinformation has developed into one of its principal threats. Chapter 1 also discusses the issues of the information ecosystem of modern countries, including the phenomena of post-truth and information science. Chapter 2 introduces the intellectual tradition related to the philosophical and legal dimensions of lies, as well as the foundations of strategic thought, which is the premise of the process known as the "weaponization of information". Chapter 3 contains a conceptual framework and a critical review of the definitions of disinformation in science and documents produced by states and international organizations. In this chapter, we also formulate our own working definition for the term. Chapter 4 describes the basic tools used in disinformation activities and their main development trends, covering the process of disinformation as a learning system; derivatives of the development of modern digital technologies like artificial intelligence; and the characteristics of China as a powerful state actor in the field of international disinformation that uses social media effectively and has a huge track-record of exploiting other media types for its propaganda and disinformation activities.

The second part of the book looks at recognizing and analyzing disinformation. Chapter 5 discusses the impact of disinformation on a state's information security in the theoretical, practical, and legal dimensions. In addition to a discussion of the general characteristics of information manipulation, its

specialized forms, which include intelligence disinformation and military disinformation, are also presented. Chapter 6 identifies methods and techniques of disinformation as well as the goals pursued by political actors using this tool. The following section, Chapter 7, discusses methods and techniques of information analysis available to internet users, including critical thinking, fact-checking, and open-source intelligence. This chapter contains a set of useful tools that can be used to verify information and its sources. In Chapter 8, special attention is paid to the information and psychological operations utilized by Russia, which constitutes the foremost threat to the information security of NATO and European Union members.

The third part of the book covers issues related to counteracting disinformation and building resilience, ranging from the roles of individual participants in the information community to those of state authorities and international organizations. In this context, chapter 9 then offers a general characteristic of the challenges facing modern democratic societies. Chapter 10 points to the role of media education as a key instrument for counteracting disinformation and reflects comprehensively on national models and practices as well as relevant recommendations of the European Union. It also contains an overview of methods of combating disinformation at the level of individual internet users. Chapter 11 outlines the activities of tech companies and social media platforms that propel the circulation of information, such as Facebook, Twitter and YouTube. It analyzes how they react to omnipresent misinformation, offers recommendations on what more could be done to reduce it, and evaluates the expectations of users, regulators, and research and journalism communities towards these companies. It also examines the role of civil society in counteracting disinformation. The last section of the book, Chapter 12, is devoted to the responses of states and the international community, primarily the European Union and NATO.

We intend for this book to be both a contribution to and strong proponent for interdisciplinary research on disinformation. However, it is itself embedded in research methods and areas of interest in strategic and security studies. The bibliography contains a variety of source texts, monographs, scientific articles, and analytical materials produced by international organizations.

The main part of this book was written before Russia's war of aggression against Ukraine began on February 24, 2022. When possible, we have endeavored to analyze related issues.

The research and writing of this book have been greatly facilitated by a generous scientific grant offered by the EU's Horizon Europe program (HORIZON-CL2–2023-DEMOCRACY-01–01, Secure Automated Unified Framework for Exchange – SAUFEX).