Foreword

When Martín presented me with the content of his book, *Digital Security for Celebrities*, and asked me to write the foreword, I was surprised. At first, I thought he was joking, but his earnest Germanic eyes blinked at me, much like a computer *prompt*, simply waiting for the user's response. He was serious. My job requires me to quickly evaluate situations and make decisions, so I instinctively set about finding answers. Why me? What could I possibly contribute? Clearly, I'm no celebrity. While I do have a certain media presence due to my responsibilities, it's typically because of the institution I work for or the importance of the individual whose news I'm sharing. Nor am I a cybersecurity expert. I don't belong to that generation born with a mobile device in hand—the digital natives—yet the digital world is a constant in my professional and personal life. And then it became clear: I am what a less charitable person might label a "technological dinosaur," but whom Martín's analytical mind identifies as a typical reader who could benefit from this book—someone with a certain level of responsibility, corporate or otherwise, who, therefore, needs at least a basic awareness of cyberdefense. I am also someone who navigates the digital ecosystem daily without the necessary training to fully understand digital signs and clues, much like confident vacationers sailing with their family on board, oblivious to how a drop in the barometer, a shift in wind, or the formation of certain cloud types can presage a squall. For those who, to any extent, identify with this profile, I can tell you now that, just as it did for me, this book will be a game-changer.

This is a book that simply *had* to be written. Written in accessible, yet precise and professional language, it analyzes across five parts the environment we navigate (the digital ecosystem); the physical (devices) and digital (digital identity) means we use; how we employ those means (activity); and, finally, it answers the key question: What does all of this mean for *me*? (operational security). And this answer isn't academic, theoretical, or difficult to apply. It provides details through examples of real-world incidents and hypothetical scenarios tailored for various profiles. Furthermore, its structure allows for isolated, selective reading of specific chapters or parts of interest, without having to start from the introduction and finish with the epilogue. It is, therefore, an ideal reference book. As a final notable aspect, I must mention its enduring relevance. While certainly not a timeless book independent of future technological developments, it has been written in such a way that its tenets, proposals, and recommendations will remain relevant for a long time. What you read here will accompany you and strengthen your personal cyberdefense for many years to come.

Believe me, this book will turn many of the digital convictions we uncritically follow as axioms completely on their head; it will largely change your perceptions or eliminate ill-founded clichés and common misconceptions. How many times have we heard that passwords should never be written down? Or that they must be changed periodically? Who hasn't heard that large companies systematically activate mobile phone microphones to eavesdrop on user conversations? Or that cyberattacks will only succeed if we make mistakes in the digital environment? You will discover that many behaviors we *believe* strengthen our cyberdefense are, in fact, enablers for malicious actors.

By the time you finish reading this page, you'll probably check your social media on your mobile device, look at your corporate email on your work computer, or browse the internet for a while from your laptop at home. You'll still be immersed in that digital ecosystem from which we neither want nor can escape. This book

will teach you how to read the barometer and other signs to know if a squall is coming—and how to prepare for it.

Remember, as the great strategist Sun Tzu said, "invincibility lies in defense"—in our case, in having a sound operational security strategy. This book will enable you to understand the strategy *you* need.

Pedro Cardona Suanzes
Spanish Navy Captain