

Wave-Based Cybersecurity

*A New Paradigm for Attack,
Defense and Military Cyber Doctrine*

Adapting de Broglie-Schrödinger Wave Formalism
to Network Security and Information Warfare

Abdelkader Bousabaa

Second Edition · 2026

SEVEN LIONS EDITIONS

Contents

Contents	v
Preface	ix
Mathematical Notation	xi
1 Mathematical Foundations	1
1.1 The Cyber Wave Function ψ_c	2
1.1.1 The Born Rule for Cyber Events	4
1.1.2 Real and Imaginary Components	4
1.2 The de Broglie Relation for Data Packets	5
1.3 The Cyber Schrödinger Equation	7
1.3.1 The Momentum and Kinetic Operators	9
1.3.2 The Defensive Potential $\hat{V}_c$	9
1.4 The Fundamental Role of the Imaginary Unit i	10
1.4.1 Polar Decomposition and the Phase Gate	11
1.5 Superposition and Wave Interference	11
1.6 The Cyber Uncertainty Principle	13
1.7 The Cyber Wigner Function	14
2 Defense by Destructive Interference	19
2.1 Conditions for Perfect Cancellation	20
2.2 The Wave-Cancelling Firewall (WCF)	22
2.3 The Phase Synthesis Engine (PSE)	22
2.3.1 Online Phase Estimation via Extended Kalman Filter	23

2.3.2	Latency Constraint	23
2.4	Phase Trap Nodes (PTN) — Active Wave Lures	24
2.5	The Self-Hardening Potential (SHP)	25
2.6	The Wave Cancelling Response Protocol (WCRP)	26
2.7	Failure Modes and Theoretical Limits	28
3	Coherent Attacks by Wave Superposition	33
3.1	Taxonomy of Coherent Attacks	34
3.2	Quadrature-Phase Attack	35
3.2.1	Covert Channel Capacity	35
3.3	Cyber Tunnel Effect	36
3.4	Wave-Packet Offensive Attack (WOPA)	37
3.5	Coherent Spoofing — Phase Cloning	38
3.6	The Wave APT — Slow Accumulation Attack	39
3.7	Anti-WCF Chirp Attack — PSE Saturation	40
3.8	Attack-Counter-Measure Correspondence Table	41
4	Military Applications: Doctrine and Operations	45
4.1	Resilient C2 Architecture — The $\hat{H}_{C2}$ Model	46
4.1.1	Wave Handover Protocol (WHO)	47
4.2	Inter-Service Communications in Hilbert Space — HCIP	48
4.2.1	HCIP vs. Link 16 — Comparative Analysis	48
4.3	Wave-Based Electronic Warfare (WEW)	49
4.3.1	Electronic Attack Cyber (EAC) — Jamming by Potential Inflation	49
4.3.2	Ghost Wave Deception (GWD)	50
4.3.3	Cyber SIGINT via Phase Measurement	50
4.4	Defense of Critical Military Infrastructure (DCMI)	51
4.5	Cyber Wave Engagement Doctrine (CWED)	52
4.6	NATO Standards Integration	53

Preface

This book was born from a deceptively simple question: *what if network traffic behaved like a wave?*

In 1924, Louis de Broglie asked an equally audacious question about matter. Two years later, Erwin Schrödinger gave it a mathematical answer, and modern physics was never the same again. The formalism they developed does not merely describe quantum particles — it fundamentally re-frames what it means to “know” a physical system, introducing superposition, interference, and irreducible uncertainty as first-class citizens of reality.

We contend that network security is ripe for an analogous revolution. Classical cybersecurity thinks in terms of *signatures, rules, and perimeters*. It is reactive by design — naming what it recognises, blocking what it identifies. This is Newtonian mechanics applied to information: deterministic, local, causal. It has served us well, and it has failed us systematically.

This book develops, chapter by chapter, a new language for cybersecurity — one borrowed from wave mechanics and extended to the information domain. We define a *cyber wave function* ψ_c , write its equation of motion, introduce the imaginary unit i as the engine of interference, and derive from first principles the conditions under which an attack can be *cancelled* by a precisely engineered counter-wave.

The result is not merely theoretical. It yields:

- a concrete defensive architecture — the *Wave-Cancelling Firewall* (WCF) — with sub-millisecond response times;
- a taxonomy of six classes of *coherent attacks* that are structurally invisible to classical detection;
- a military doctrine (*DECO*) and command-and-control architecture ($\hat{H}_{C2}$) grounded in the formalism;
- a vision for a next-generation internet — the *Quantum Wave Internet* (QWI) — in which defense is a protocol primitive, not an afterthought.

Who this book is for. This text is addressed simultaneously to cybersecu-

rity engineers who want rigorous new tools, to military planners who need a doctrine for the coming era of information warfare, and to researchers who suspect that the physics of information has more to offer than current frameworks acknowledge. A working knowledge of calculus and linear algebra is assumed; familiarity with quantum mechanics is helpful but not required — the necessary concepts are developed from scratch.

How to read this book. Each chapter is self-contained and includes a summary box at the end. Chapters 1 and 2 form the mathematical and defensive core. Chapter 3 presents the adversarial perspective — essential for building effective defenses. Chapter 4 applies the framework to military operations and NATO doctrine. The concluding chapter 5 sketches the long-term vision: a fundamentally attack-resistant internet.

I have resisted the temptation to make this book longer than it needs to be. The obvious extensions — a reference implementation of the Phase Synthesis Engine, measured values of h_c on production networks, a formal security proof for the QWI handshake — are precisely the material that cannot be written from an armchair. They belong to whoever builds the thing first.

A word, then, on the numbers. The latencies, efficiencies and thresholds quoted throughout are *indicative design targets* — derived from the formalism and from plausible hardware, not measurements of a system that exists. They are stated precisely on purpose: a figure one can argue with, and disprove, is worth more to a young field than a hedge. If this book proves useful, it will be because someone read Chapter 2 as a specification rather than as an argument: treat phase as real, and see what breaks.

Abdelkader BOUSABAA
August 2026

Classical cybersecurity is losing the arms race — and the reason is architectural, not tactical.

Every new defensive layer is eventually circumvented, every perimeter eventually breached, because our defences are *added onto* a protocol never designed to carry them. This book proposes a departure. Borrowing the de Broglie–Schrödinger formalism that reshaped physics in the 1920s, it treats network flows as complex wave functions ψ_c carrying not only amplitude but phase, coherence and interference structure — the half of the signal classical monitoring throws away. From that foundation a complete architecture follows:

- The **Wave-Cancelling Firewall**, which neutralises an attack by emitting its exact negative in under $200\ \mu\text{s}$.
- **Six coherent attack classes** — quadrature, tunnel, WOPA, APT, spoofing, anti-WCF — structurally invisible to amplitude-only detection, each with its matching defence.
- The **Cyber Wave Engagement Doctrine**, a five-level ROE ladder tied to measurable wave indicators, with a NATO integration roadmap.
- The **Quantum Wave Internet**, a network in which defence is a protocol primitive rather than an afterthought.

Written for cybersecurity engineers, military planners and researchers, the book assumes calculus and linear algebra, and develops the physics from scratch.

Abdelkader Bousabaa works at the intersection of quantum physics, information theory and applied cybersecurity, on translating structural analogies between wave mechanics and information security into deployable, standards-ready architectures.

