

Ignoring Antagonistic Information Threats

Evidence from Ukraine

**Liubov Tsybulska
Stockholm
February 2026**

Antagonistic information threats operate across 4 layers

Cognitive —
perception, threat
interpretation,
identity



Institutional —
trust in government,
elections, expertise

Informational — narrative
dominance, agenda-setting

Behavioral — voting, protest,
compliance, policy pressure

The goal is to reduce a society's capacity for coherent decision-making.

Crimea 2014

Information operations before occupation:

- “Russian speakers under threat”
- Delegitimizing Kyiv
- Manufactured local support
- “Little green men” bring no harm
- Media saturation



MH-17: Information chaos functioned as a strategic shield



- 30+ competing explanations circulated
- coordinated state & proxy amplification
- high-volume narrative flooding across media ecosystems

Objectives:

- delay clear attribution
- fragment international consensus
- politicize investigation
- slow coordinated response

Russia's full-scale invasion of Ukraine 2022



Information objectives:

- panic
- leadership delegitimization
- international fatigue
- alliance fragmentation

Nord Stream 2: energy leverage exposed as geopolitical tool

- “Purely commercial project”
- Russian gas as reliable & apolitical
- Critics framed as ideological or anti-business
- energy interdependence = stability
- state messaging & proxy experts
- Lobbying & policy influence ecosystems
- business-media narrative alignment

Nord Stream pipelines from Russia



Source: Gazprom

BBC

Dehumanisation as preparation for violence

Ukrainians

- “Nazis”, “traitors”, “subhuman” framing
- denial of Ukrainian statehood & identity
- portrayal as existential threat



Europe & the West

- “decadent”, “hostile civilization”
- moral degradation narratives
- war framed as civilizational defence

Function of dehumanisation:

- normalize extreme violence
- reduce moral constraints on soldiers
- sustain domestic support for war
- justify prolonged conflict

Cognitive warfare: society as the central battlespace

Cognitive warfare shifts the primary target from territory → to perception

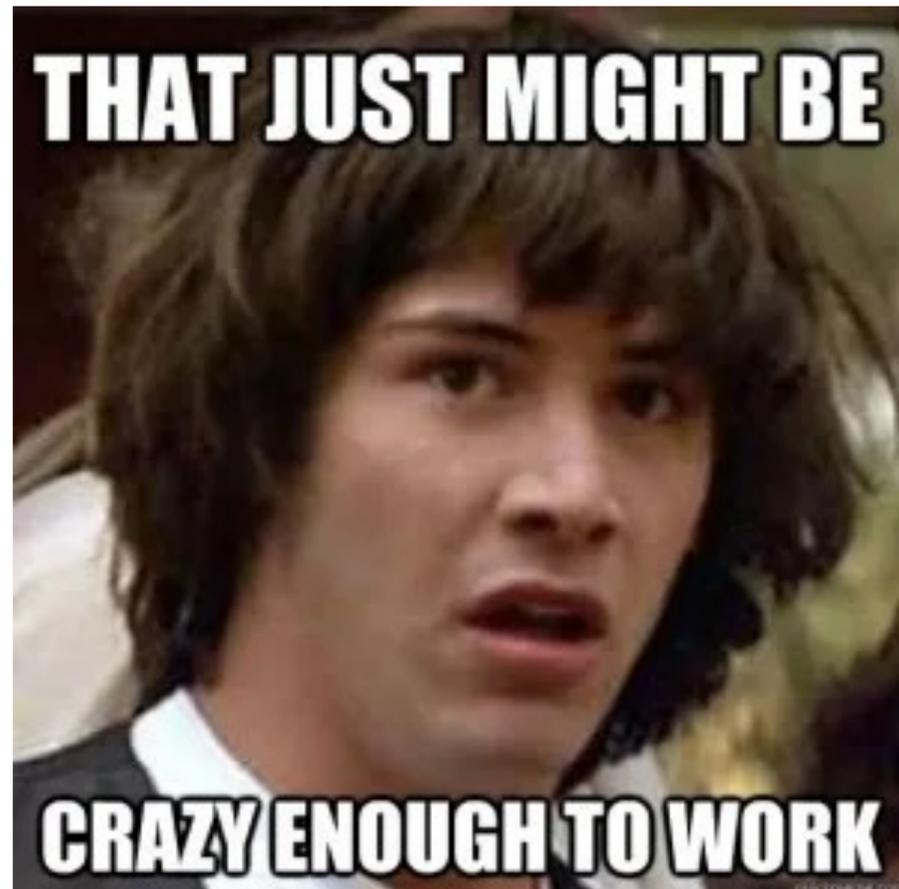
Operations aim to influence:

- how people interpret reality
- whom they trust
- how they make decisions
- whether they act collectively



Trust becomes the critical vulnerability — and the core defence asset

What works?



- Information resilience must be integrated into Total Defence concept
- Treat information threats as security & economic risk
- Develop policy frameworks toward malign actors
- Civil society + state coordination
- Strategic communication
- International coordination

Thank you!