Counterforce

Real-time detection and mitigation of information warfare

Trust Defence

As a Service

The Big Problem

Truth is not keeping up

By the time we detect false narratives, the damage is already done.

☑ Elections compromised

☑ Evacuations ignored

☑ Vaccines refused

60% of people are exposed to crisis misinformation befofore facts emerger

43% of Canadians were found to be highly susceptible to health misinformation

60% of a false narrative’s recptive audience will be reacghed within 8 hours

The Financial & Human Costs

Total Est. Cost to Global Economy

$76 Billion US

Half of all businesses were victims of deepfake attacks in 2024.

Stock Markets

$13 Billion US

Market volatility, corporate reputation damage, fraud.

Corporate Attacks

$9.5 Billion US

A single false tweet briefly erased $136B from the S&P 500 on April 23, 2013.

Public Health Systems

$8 Billion US

COVID vaccine misinformation cost the US $50M-$300M per day in 2021.

Our Solution

Command-level Control of the Information Domain

First platform to move from observation to operational control

SE

Realtime detection across platfotms

MAP

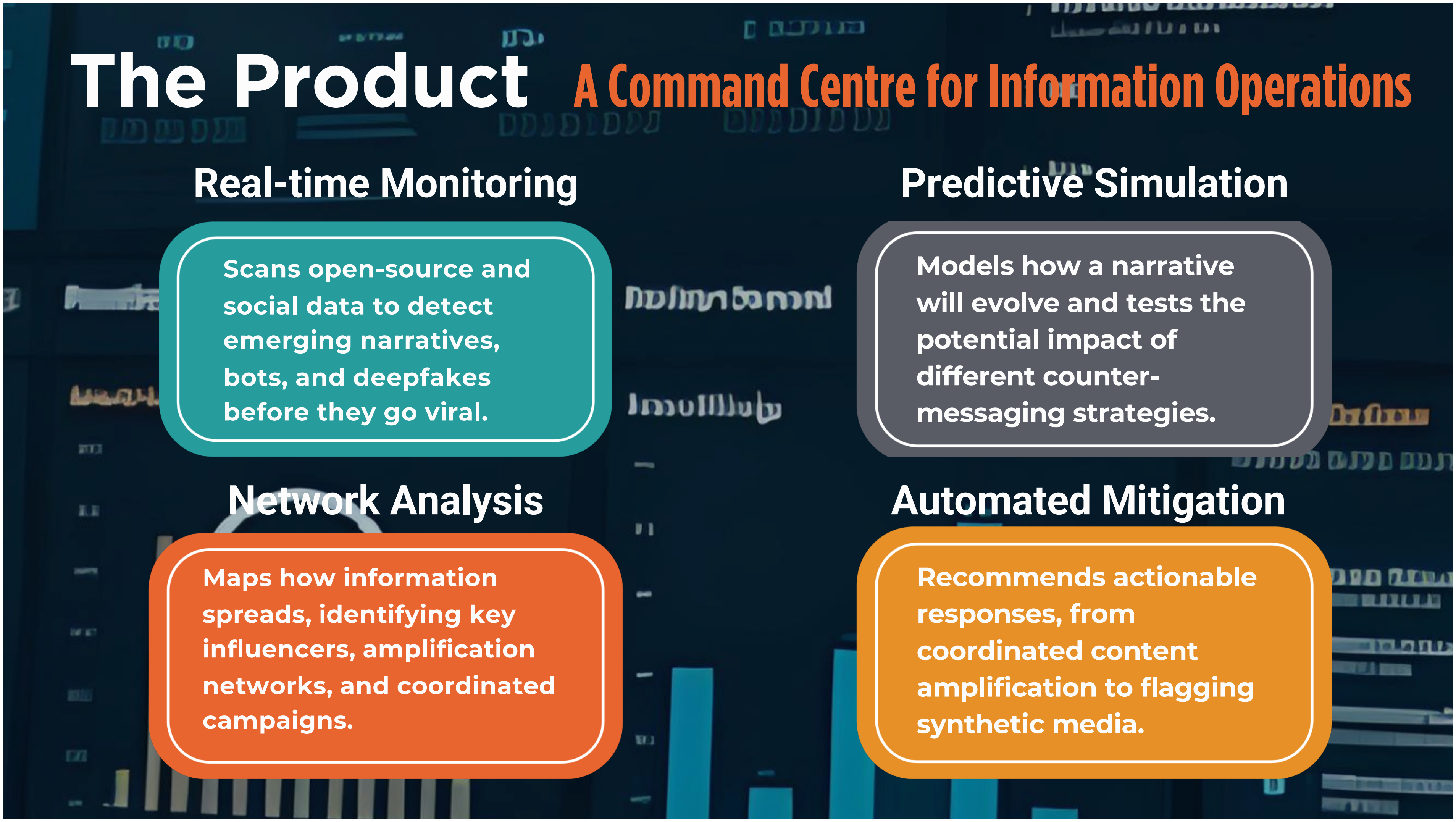
Network analysis of narrative spread

AC

Automated response and mitigation

The Product

A Command Centre for Information Operations



Real-time Monitoring

Scans open-source and social data to detect emerging narratives, bots, and deepfakes before they go viral.

Predictive Simulation

Models how a narrative will evolve and tests the potential impact of different counter-messaging strategies.

Network Analysis

Maps how information spreads, identifying key influencers, amplification networks, and coordinated campaigns.

Automated Mitigation

Recommends actionable responses, from coordinated content amplification to flagging synthetic media.

Technology & IP

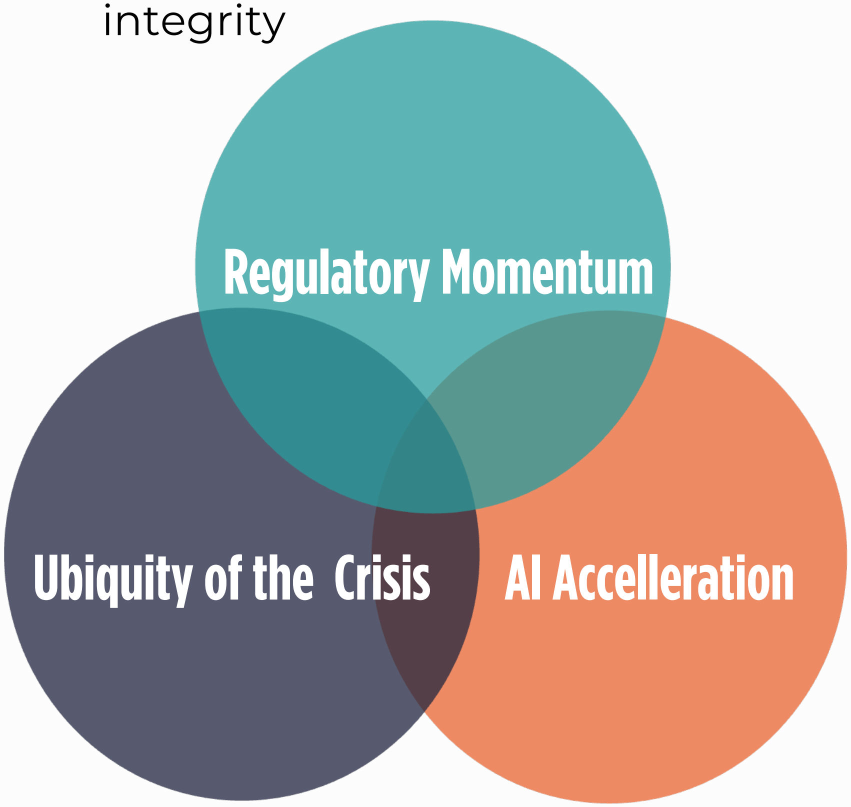
Proprietary Stack of Models & Tools

Technology	Description
NLP Modules	Fine-tuned transformers identify manipulative language and sentiment across multilingual datasets.
Graph Neural Networks	Detect coordinated inauthentic behaviour and botnets that simpler tools miss.
Agent-based Simulation	Forecasts narrative spread and models intervention outcomes, enabling strategic response planning.
Equity-driven Metrics	Integrates social trust and fairness indicators to ensure accuracy in diverse communities.

Why Now?

A Synergy of 3 Important Events Make Now Opportune

- Nearly every organizations now affected so more treat information integrity as a core resilience requirement
- Generative AI amplifies narrative manipulation at scale, increasing frequency and sophistication of campaigns
- Regulatory frameworks are maturing around information integrity

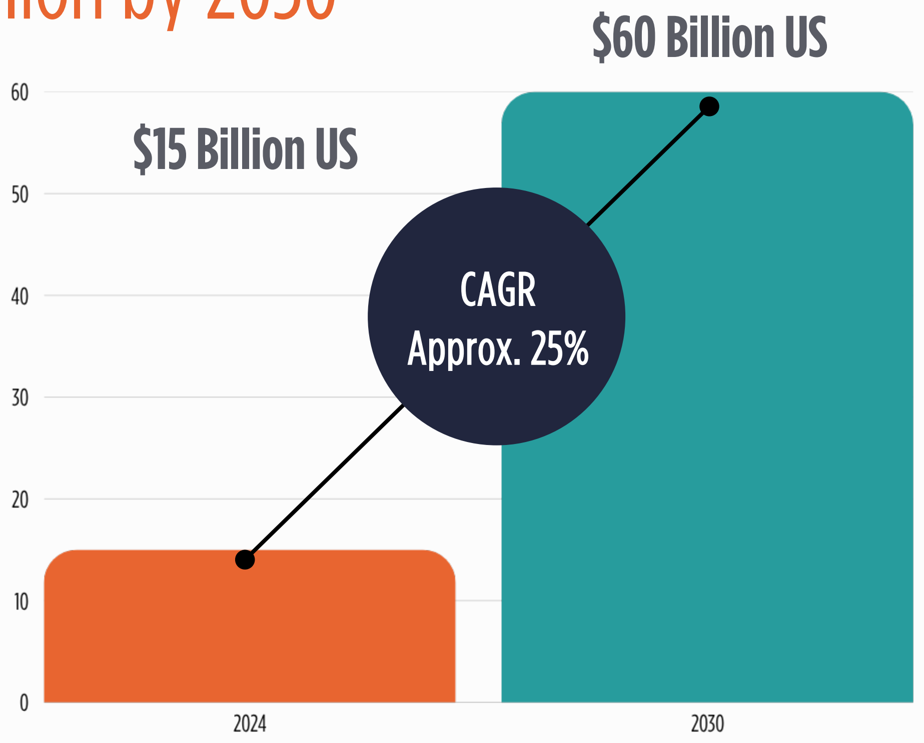


The Market Opportunity

$15 Billion Climbing to $60 Billion by 2030

Primary Target Markets:

- NATO/EU Defense: Annual information defense budgets exceeding €1.5B.
- Canadian National Security: Annual budgets over $800M for cyber and information integrity.
- Global Health Security: An additional $2-3B global opportunity in public health misinformation.



Go-to-Market A 3 Phase Strategy

1

- **Target**: Existing consulting clients (WHO, Health Canada, DND partners).
- **Action**: Convert high-value consulting relationships into paid pilot deployments of the TDaaS platform.
- **Goal**: Secure 2-3 flagship contracts with key defense, public health, and emergency management agencies.

Phase 1: Co-Development & Pilots

2

- **Target**: Expand across NATO/Five Eyes defense agencies and provincial/state health authorities.
- **Action**: Build a small, specialized direct sales team. Establish partnerships with major defense contractors and systems integrators.
- **Goal**: Achieve scalable, repeatable sales process.

Phase 2: Direct Sales & Channel Partners

3

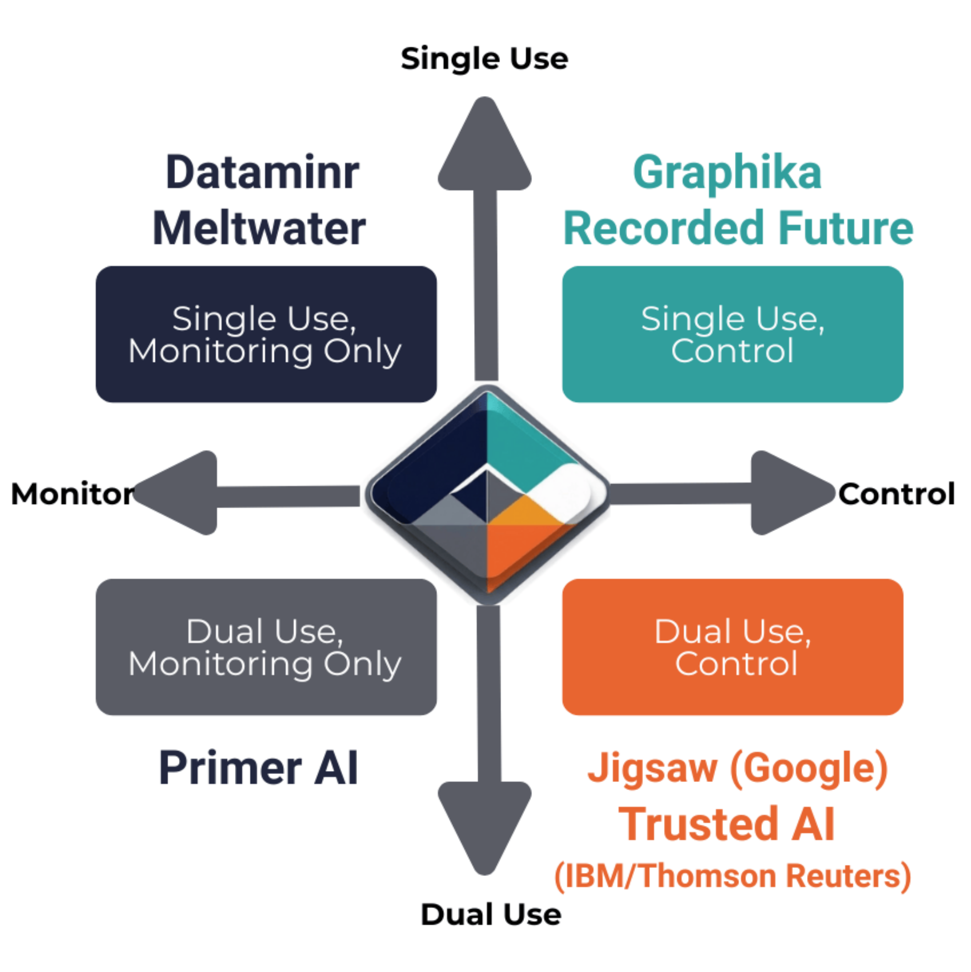
- **Target**: Critical infrastructure (pharma, energy, finance), insurance.
- **Action**: Develop industry-specific modules for corporate reputation and threat defense.
- **Goal**: Become the dominant platform for trust intelligence across public and private sectors.

Phase 3: Industry Expansion

Competitive Analysis

Market Positioning by Breadth and Depth

- Competitive landscape mapped by use scope and intervention capability.
- Vertical axis: single-use to dual-use offerings.
- Horizontal axis: monitoring-only to control-oriented solutions.
- Dataminr and Meltwater: single-use, monitoring-only tools.
- Graphika and Recorded Future: single-use with intervention controls.
- Primer AI: dual-use, primarily monitoring.
- Jigsaw/Trusted AI (IBM/Thomson Reuters): dual-use with control capabilities.*



- There are no comparative companies we could identify from this quadrant, but these initiatives of larger non-competitor corporations are working in this space

Impact Monitoring & Risk Mitigation

Measuring Performance While Safeguarding Trust

Evaluation Metrics

Real-World Outcome Metrics:
Reduction in Misinformation Reach, Time to Containment, Evacuation Compliance / Health Behaviour Uptake, Sentiment/Trust Restoration: Change in public sentiment or trust

User/Customer Adoption Metrics:
Analyst/Operator Productivity, False Positive & False Negative Detection Rates

Security & Compliance Metrics:
System Uptime & Reliability, Incident Escalation Rate, Adherence to Data Privacy & Ethical Guidelines

Business/Customer Value Metrics:
Annual Recurring Revenue (ARR), Net Revenue Retention (NRR), Customer Satisfaction/Net Promoter Score, Churn Rate

Ethical Guardrails

- **Strong Data Governance:** Counterforce AI implements strict access controls, regular audits, and complies with ISO 27001 and public-sector security frameworks.
- **Respect for Data Sovereignty:** Client data is processed according to specified jurisdictions to adhere to residency and privacy laws.
- **Principles of Data Minimization:** Only essential personal information for threat detection is collected, with regular reviews to eliminate excess data.
- **Community Oversight & Monitoring:** Community advisory panels and transparent reporting support ongoing oversight, promoting cultural safety and equity for all groups affected.

Team

Combined 40+ Years of Frontline & Respected Thought Leadership

Chief Executive Officer

Dr Meaghan Thumath, DPhil, MPH, RN

Assistant Professor, School of Nursing, Faculty of Applied Science,
University of British Columbia

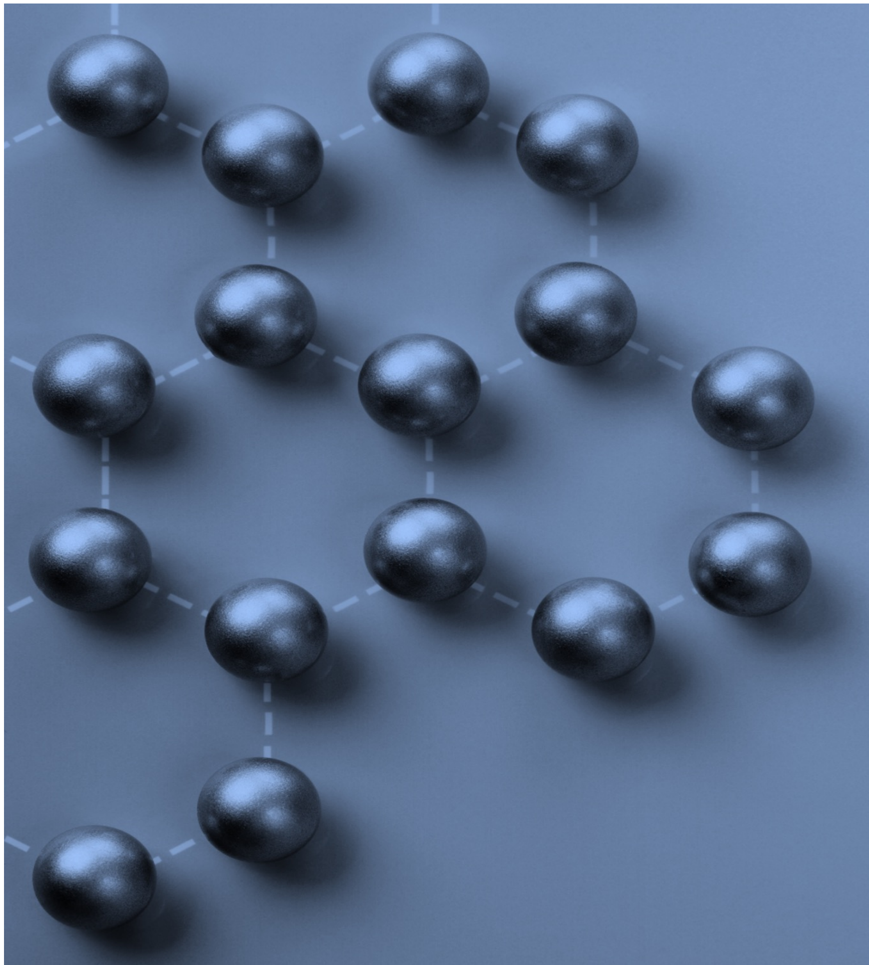
Health Policy & Leadership, Emergency Response, Health Communication, Health Equity, Clinical Care

Chief Information & Technology Officer

Dr Jamie Forrest, PhD, MPH

Scientific Director, Health Equity & Resilience Observatory,
University of British Columbia

Digital Health, Artificial Intelligence in Health, Network Analytics, Clinical Research Methods



THE VISION

Empowering societies to safeguard trust and act with confidence—enabling truth to overcome the harms of manipulation.

Our Ask

We are seeking **$1,500,000** in seed capital to accelerate the development and deployment of Counterforce AI—empowering societies to defend trust in a rapidly evolving information battlespace.

Allocation	% of Funds	Key Milestones
Product Development (2-3 Engineers)	50%	Complete working prototype (Q1 2026), build enterprise-grade features
Go-to-Market & Pilots (1 sales lead)	30%	Secure 3–5 paid pilot contracts; $500K ARR target
Governance & Operations	20%	Achieve Controlled Goods registration, legal/compliance, staff training

Join us in building the operational shield for truth—and ensure societies worldwide can act with confidence in the face of modern threats.

Counterforce

CONTACT

Dr. Meaghan Thumath, DPhil, MPH, RN
Chief Executive Officer, Counterforce

Assistant Professor, University of British Columbia, Faculty of Applied Science

meaghan.thumath@ubc.ca