

Adversary Instability

DOMINIC CONNOR

LSE_RISK@PROTONMAIL.COM



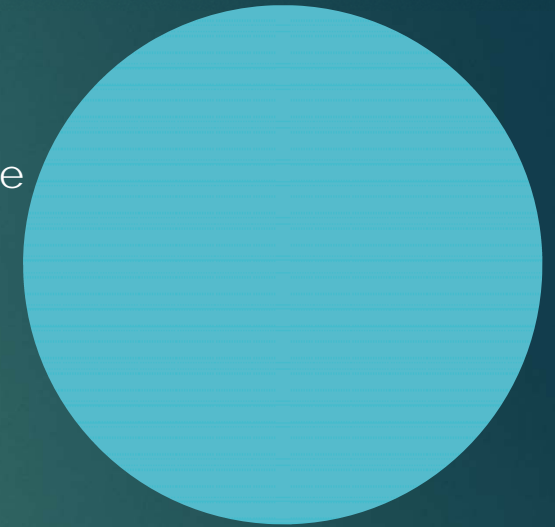
Can we Generate Scenarios ?

- ▶ Strategies
- ▶ Motivations
- ▶ Vulnerabilities
- ▶ Weaponising



Why Generate Scenarios ?

- ▶ We need to prioritise
 - ▶ Requires some function (Probability, Consequence) -> Exposure
- ▶ Systemic risks are:
 - ▶ Individual Low probability
 - ▶ Very low probability for coincident events
 - ▶ Highly uncertain values for probability
- ▶ Hard to allocate resources efficiently
- ▶ Difficult even to acquire resources



Algorithm for Scenario Generation



- ▶ Vary events known to have happened
- ▶ Use techniques and technology generally available
- ▶ Assume Adversary
 - ▶ Interpret known events as if attacks
 - ▶ Flash Crashes
 - ▶ Oli Crises
 - ▶ Storm Crash 87
 - ▶ Suez
 - ▶ 9/11 Airline Put options
 - ▶ Saudi drone attacks
 - ▶ Near misses
- ▶ Adversarial Iteration



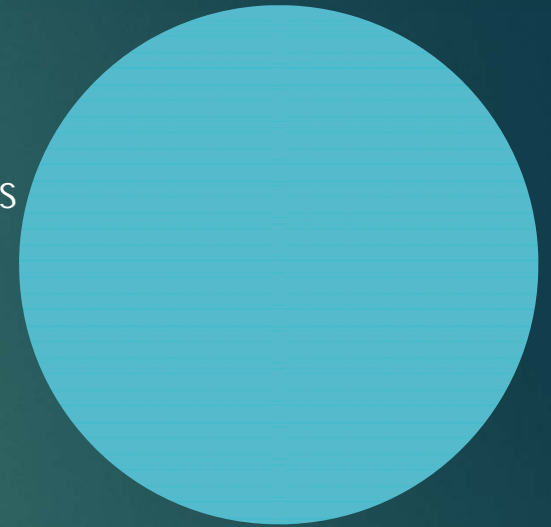
Adversarial Iteration

- ▶ Contemporary Artificial Intelligence
- ▶ Vary attacks
- ▶ Learn which work/fail
- ▶ Highly unintuitive solutions



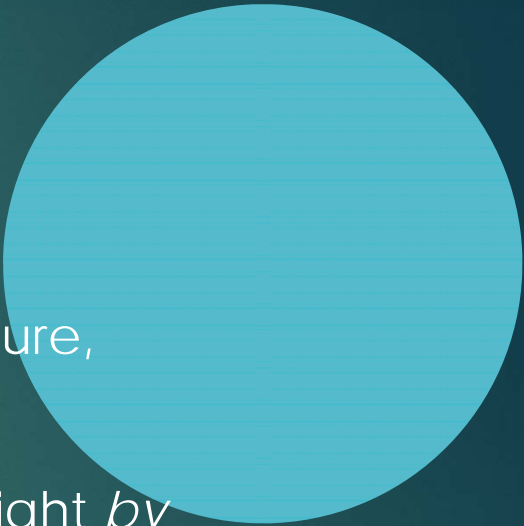
Why Assume Adversary ?

- ▶ Overcome defensive reactions
- ▶ Adversaries have explainable and predictable objectives
- ▶ Behaviour unlike actors for gain or blunder
- ▶ Engineering Discipline
- ▶ System set up to guard against thieves and blunders
- ▶ There exist hostile actors



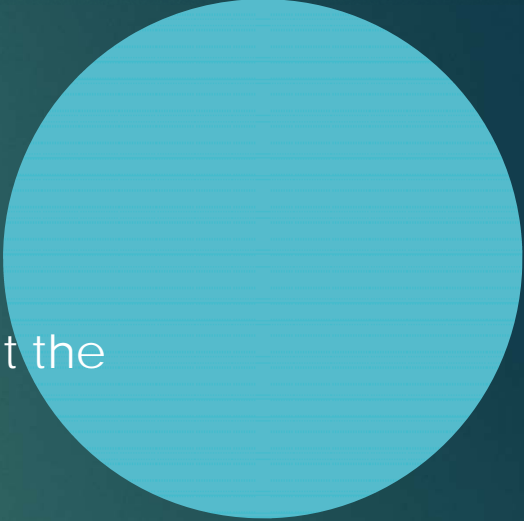
Generated Scenarios are more general



- ▶ Apply adversarial techniques to each scenario
 - ▶ Vary Targets
 - ▶ HFT, MIM, Force Multiplication, Market Microstructure, Liquidity, Politics
 - ▶ Chances of the right (wrong) effect happening slight *by accident, but Adversary will choose more damaging*
 - ▶ Upgrade contagion from a coincidence to a plan
- 


Benefits



- ▶ Patterns and vocabulary
 - ▶ Recognise attack
 - ▶ What happens next
 - ▶ Form a narrative that makes thinking and reasoning about the problem easier
 - ▶ Allow for preparation and detection
 - ▶ More cost effective
- 

Strategic Objective: Phase Change



- ▶ Market Crashes exhibit jump in correlation
 - ▶ Equity markets often have negative correlation with debt
 - ▶ Reduce Trust
 - ▶ How to keep important markets in desired phase ?
 - ▶ Brute Force expensive, unreliable, undeniable
 - ▶ Chinese Snow
- 

Force Multiplication

- ▶ Modern definition of market is information exchange
- ▶ Nation State level actors have access to information before the market
 - ▶ Norway
 - ▶ Developing Nations
 - ▶ Large nation states play fair because it is rational



9/11 Put Options

- ▶ Allegedly for financial gain
 - ▶ Exfiltration Difficulties
 - ▶ Exonerated
- ▶ Different observable behaviours in Adversary
 - ▶ Gains not primary objective
 - ▶ Short Term goals
 - ▶ Not risk averse
 - ▶ ...but that is end game only
 - ▶ temptation



Variations

- ▶ Drone attack on Saudi refinery
 - ▶ Massive spike in prices
 - ▶ No observed use of weaponised financial techniques\
- ▶ Directional Variant
 - ▶ Systemically important energy companies
 - ▶ Many energy firms state owned or integral



Amplification

- ▶ Flash Crashes now known to be frequent
- ▶ Continuous time finance useful model, but inadequate



High Frequency Trading

- ▶ Source of short term instabilities
- ▶ But medium term stability
- ▶ Producing Techniques and Technologies
- ▶ Gaming the system



Pessimax

- ▶ Market Impact Modelling
 - ▶ Integral component of HFT systems
 - ▶ Optimise for minimal impact
 - ▶ Mature base of skills and practice
- ▶ Optimise to find most impact for a given ability to trade
- ▶ Excellent tools for targeted and general attack



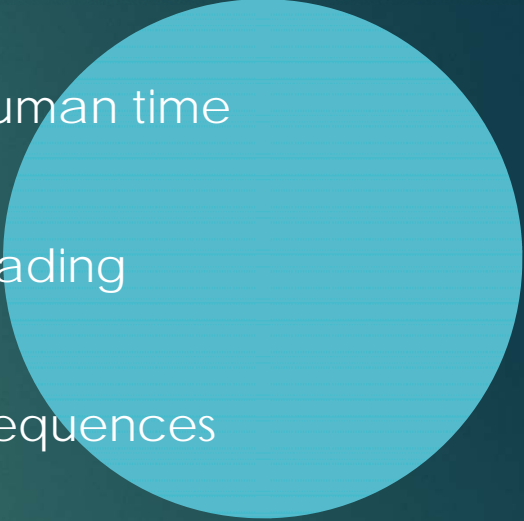
Barriers to entry

- ▶ MIM not trivial
- ▶ Maximisation is classic AI problem
- ▶ Tensorflow, toolkits, Cloud, new generation hardware
- ▶ Arms race



Not so Brute force



- ▶ 2010 Flash Crash took place in both machine (<1s) and human time
 - ▶ Humans believed Greek default was imminent
 - ▶ When systems misbehaved, at first thought to be insider trading
 - ▶ Crash amplified an imaginary event
 - ▶ Regulators pressured into decisions with longer term consequences
 - ▶ Scale large enough for politicians to be aware
- 

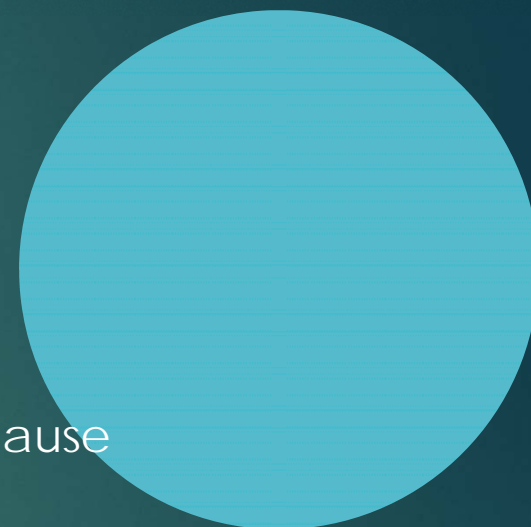
Toxic Order Flow

- ▶ Market Makers and Liquidity providers dislike:
 - ▶ Volatility
 - ▶ Asymmetric information
 - ▶ Toxic counterparties
 - ▶ Narrow spreads



Variations

- ▶ Move currency to unacceptable levels
- ▶ Distract political policy makers
- ▶ Cause financial instability, reducing ability to respond
- ▶ Divide and Conquer
- ▶ Most ambitious, perhaps draw target into positions that cause structural harm



Deniability

- ▶ Spectrum of actors in markets
- ▶ We observe that several nation states prefer even limited and less credible deniability
- ▶ Easy to build an attack fund
 - ▶ Tomorrow ?



Bond Markets

- ▶ Market much larger than Equities
 - ▶ Over 100 Trillion in *simple* bonds, also FRNS etc
- ▶ Price (X) $\rightarrow F(\text{Price(Gilt)}, \text{Price BAE} + \text{VR}, \text{S/D})$
- ▶ Inbuilt transmission mechanism for contagion
- ▶ In crisis, debt markets are critical



Stabilising Factors

- ▶ Resilient
- ▶ Large and dispersed
- ▶ Bond holders often take longer term view, for instance pension funds
 - ▶ Pension funds, make market more and less resilient
- ▶ Exist Mark Makers



Contagion and Destabilisation



- ▶ Flash Crashes already observed
- ▶ Oct 2014 US Treasuries, still disputed
- ▶ Direct transmission mechanism to wide range of bond prices
- ▶ Market Makers may stop if volatility becomes high

Market Makers

- ▶ Obligated to quote hard two way prices
 - ▶ Within spread
 - ▶ Up to certain volume
- ▶ Risks Include
 - ▶ Volatility
 - ▶ Toxic Order flow
 - ▶ Counterparty, capital and risk limits
- ▶ Market Makers retreat from market when it gets tough
- ▶ Drop in liquidity



Trust and Risk

- ▶ Operational
 - ▶ Technical and human failures
- ▶ Compliance Risk
 - ▶ Rules Complex
 - ▶ Retroactive Action
- ▶ Model Risk
 - ▶ Diversity of Models
 - ▶ Well built models systemically dangerous
- ▶ Volatility
 - ▶ Variance



Fake News

- ▶ Bloomberg has started quietly generating stories based on market data and “AI”
- ▶ Many streams of data
 - ▶ Few aggregators
- ▶ Relatively resilient



History is Bunk


- ▶ Volume of financial data is now in petabytes
- ▶ Moving to Cloud
 - ▶ Fewer Cloud providers
- ▶ Innovation in financial models has severely declined
 - ▶ Off the shelf and cloud software

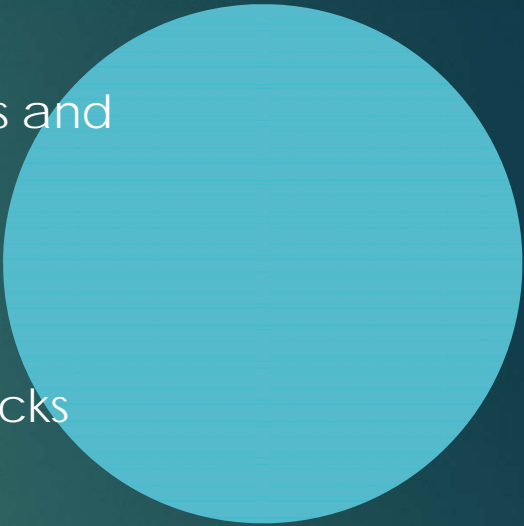


Breaking Trust

- ▶ If N banks share historical data
 - ▶ Compromise data
- ▶ Leave to cook
- ▶ Two possibilities
 - ▶ Discovered
 - ▶ Disclosed
- ▶ Value of current positions is now unknown
- ▶ Value of counterparty positions is unknown
- ▶ Could happen accidentally




$$\int_0^{\infty} \text{fear}(x)$$

- ▶ Existing Techniques enable hostile actor to disrupt markets and attack specific critical firms
 - ▶ New technology lowering the barrier to entry
 - ▶ Attack surface enormous
 - ▶ Response: Generate patterns to detect and counter attacks
- 

Future Work

- ▶ Pensions
 - ▶ Large
 - ▶ Politically sensitive
 - ▶ Find linkages to drive political mistakes
- ▶ Economic Sanctions
 - ▶ Building
 - ▶ Busting
- ▶ Find more tools to weaponise
- ▶ Develop an Adversary

