Predicting Cyber Attacks in the Entangled Cyberspace

Ruth Ikwu
Digital Economy & Cyber Security
research group, Brunel University London

RITICS Showcase, 18th October 2018
Nova South, London

E: Ruth.Ikwu@brunel.ac.uk

INTRODUCTION

- A proactive framework to predicting cyber-attacks.
- The cyber analytics space is currently dominated by mono-dimensional linear analysis.
- Our framework conceptually fuses multiple sources of evidence across cyberspace to predict events in subsequent stages of the kill-chain.
- Current techniques are limited in their ability to understand the dynamics of entanglements related to cyber-incidents.
- We provide a multi-dimensional phased analysis of the traditional kill-chain model using structural vector auto-regressive models.

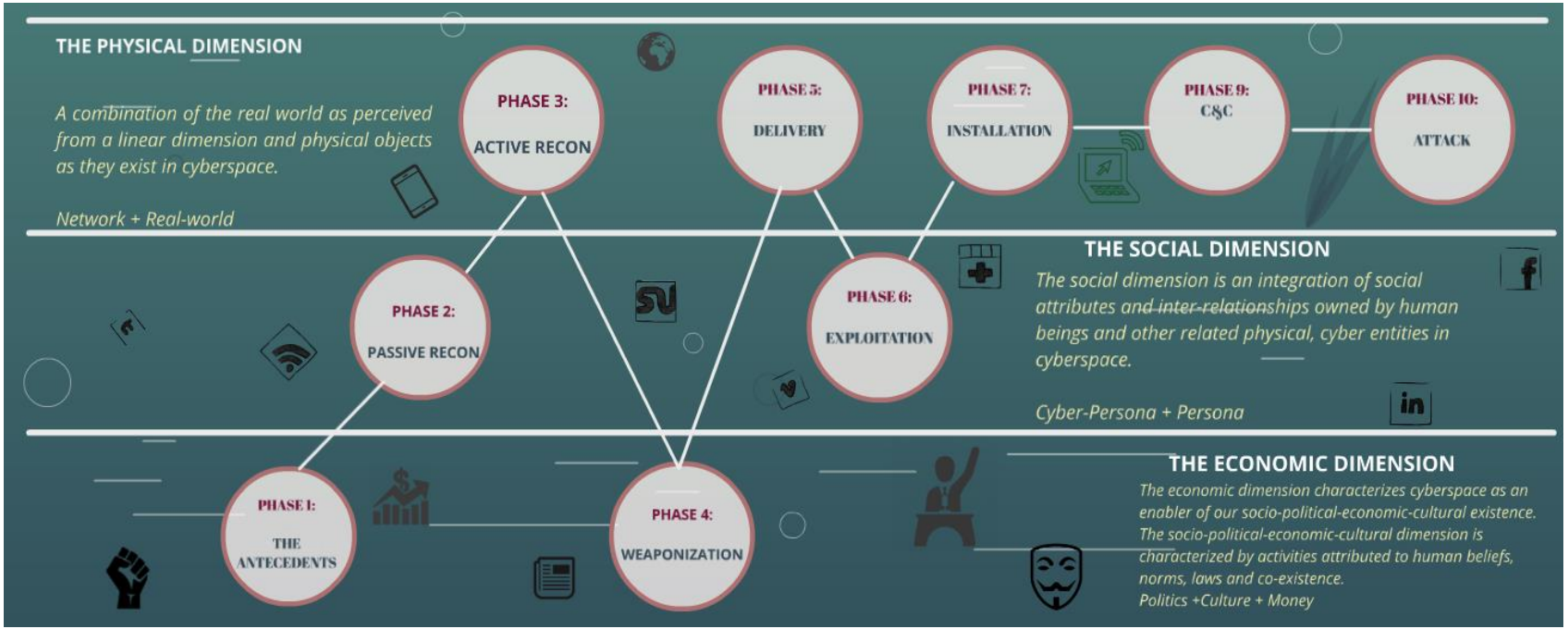
CONCEPTUAL FOUNDATIONS

- The entangled cyberspace is a seamless integration of evidence sources across cyberspace to predict stages of the kill-chain.

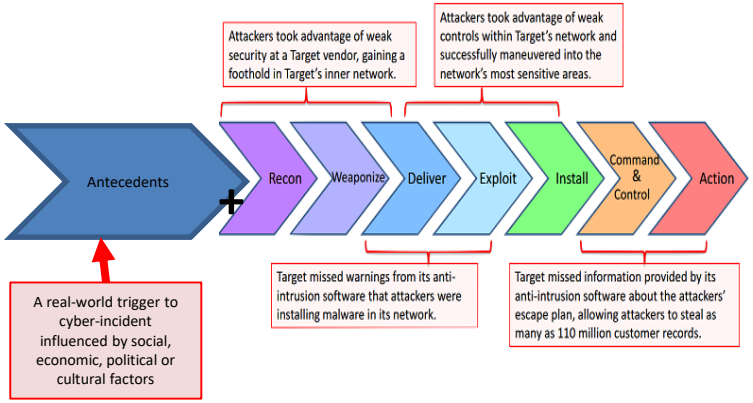
- The entangled cyberspace in theory is the fusion of three conceptual foundations:

  - A sequential phased model for perpetrating cyber-attacks.
  - A multi-dimensional characterization of cyberspace.
  - A structural model for integrating and simultaneously analysing multiple sources of evidence.

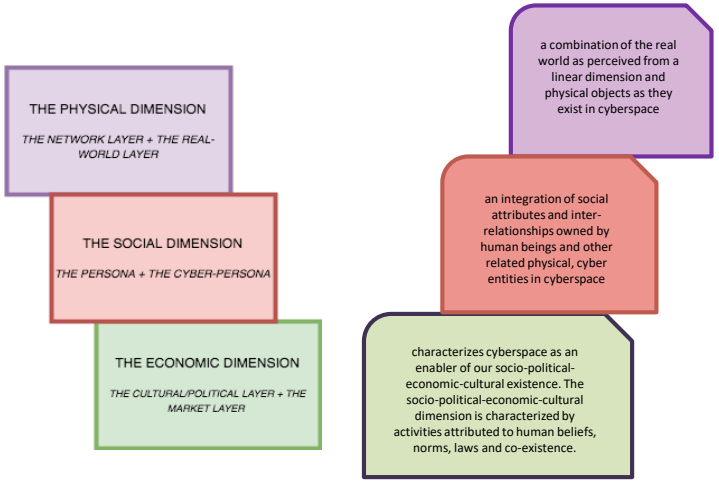
THEORETICAL FRAMEWORK



CF I & CF II

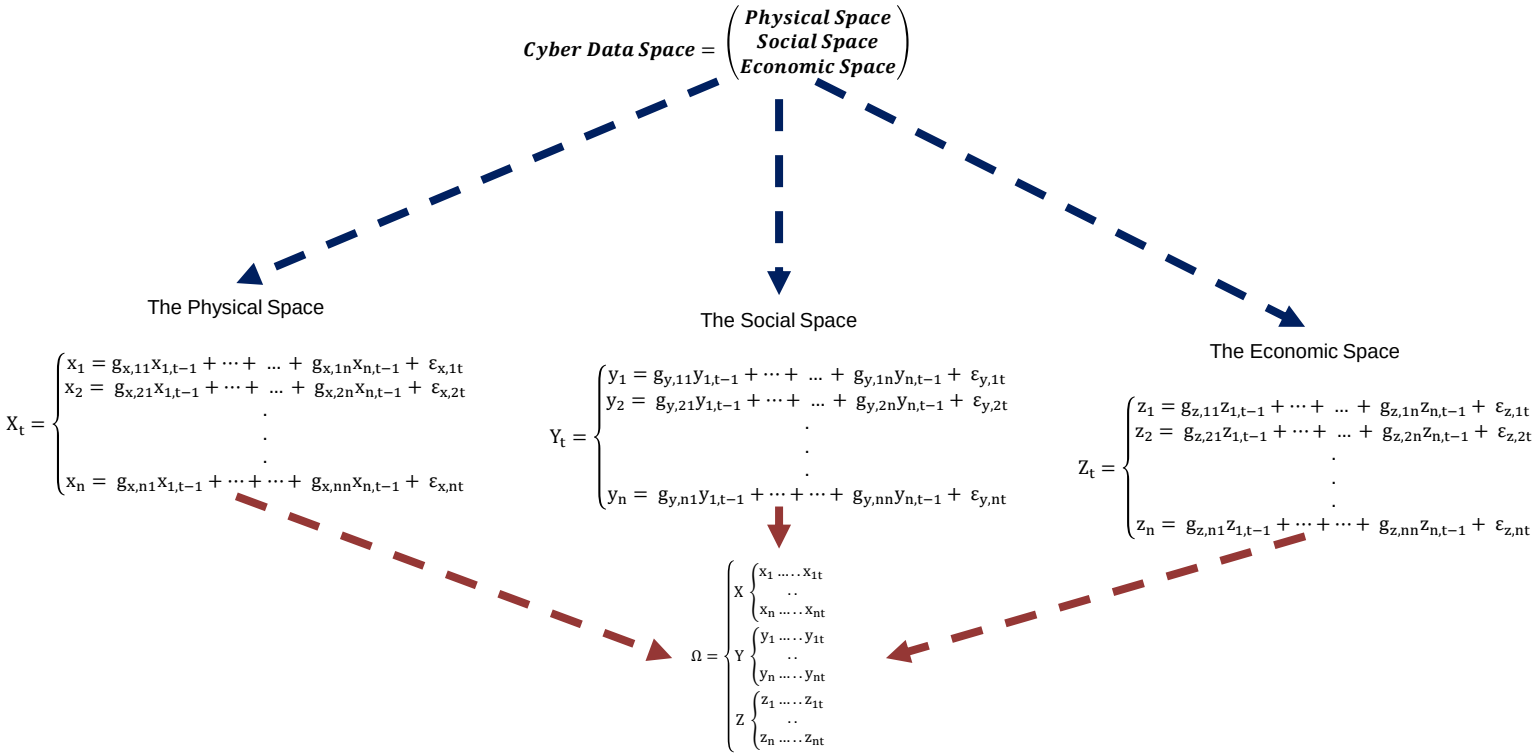


The Attack Kill-Chain



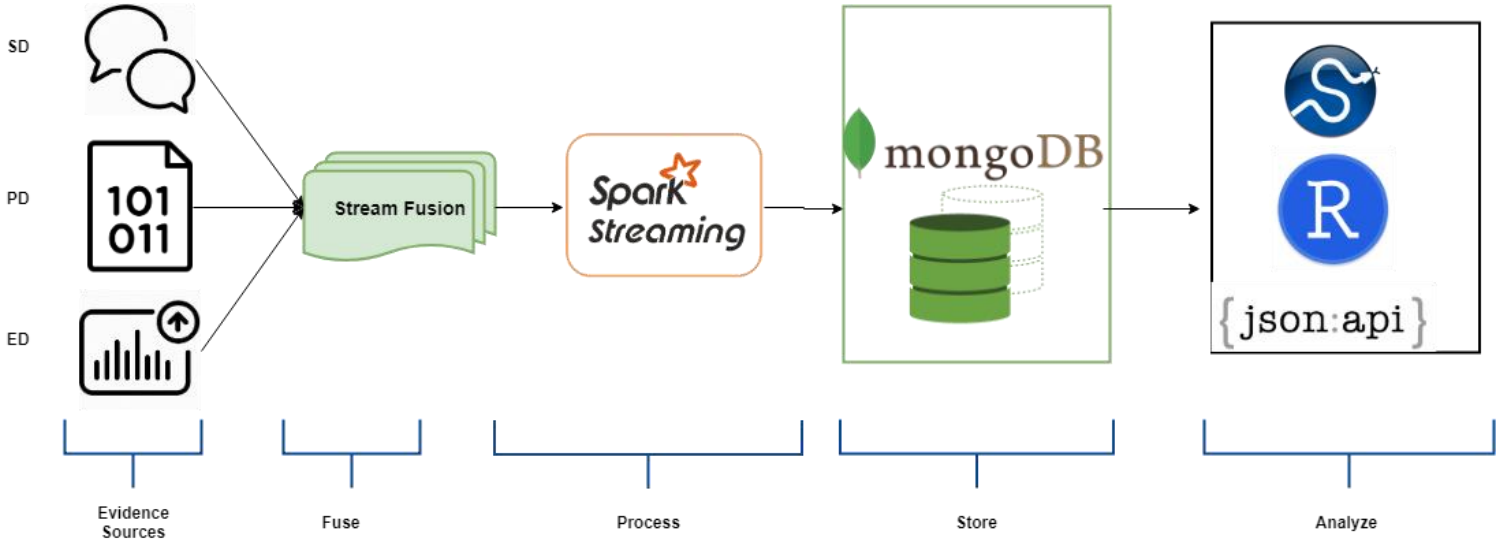
The Multi-Dimensional Cyberspace

CF III: VECTOR AUTO REGRESSIVE REPRESENTATION OF CYBERSPACE



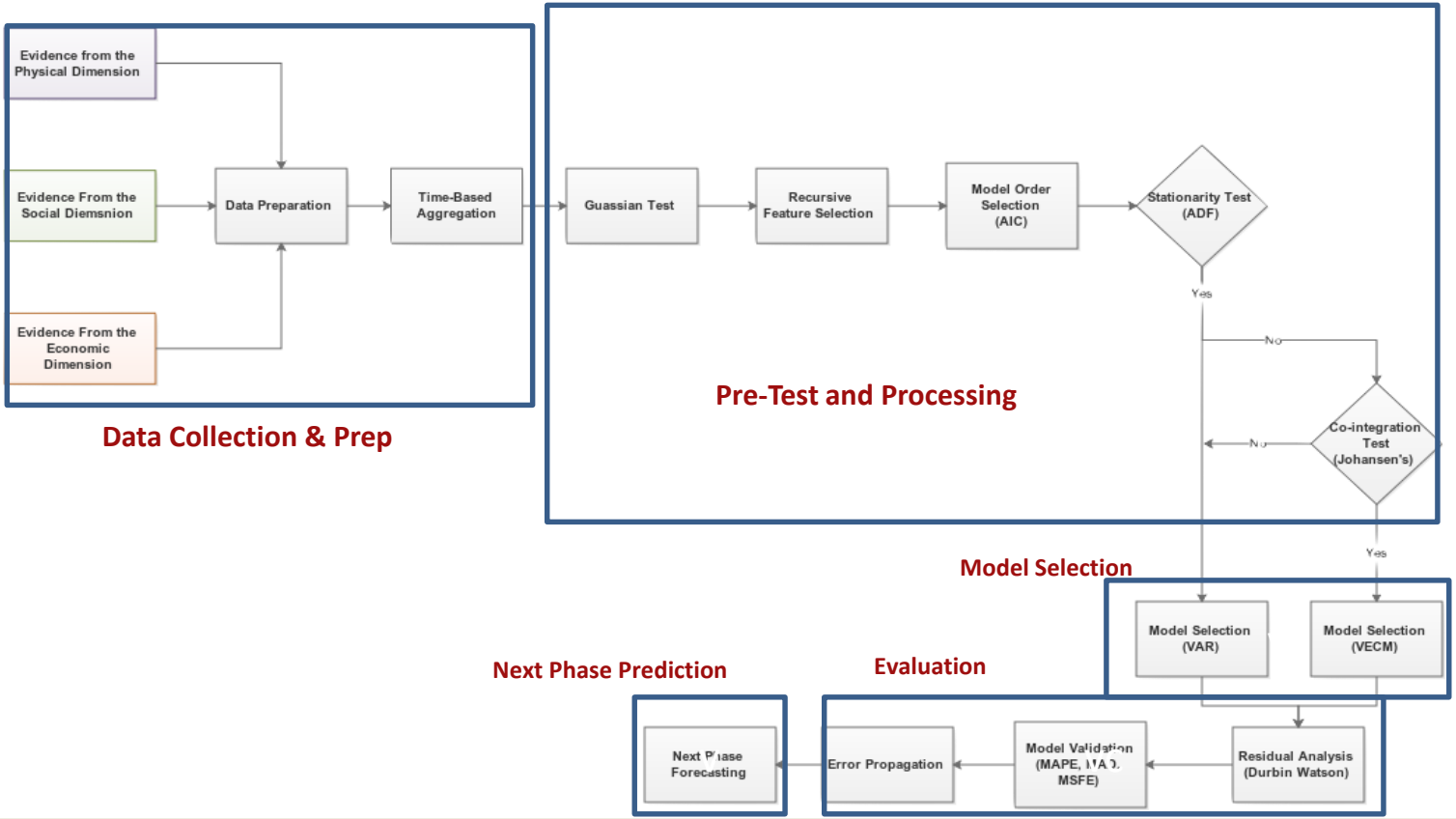
*An **n X n** VAR for each identified dimension of cyberspace*

IMPLEMENTATION

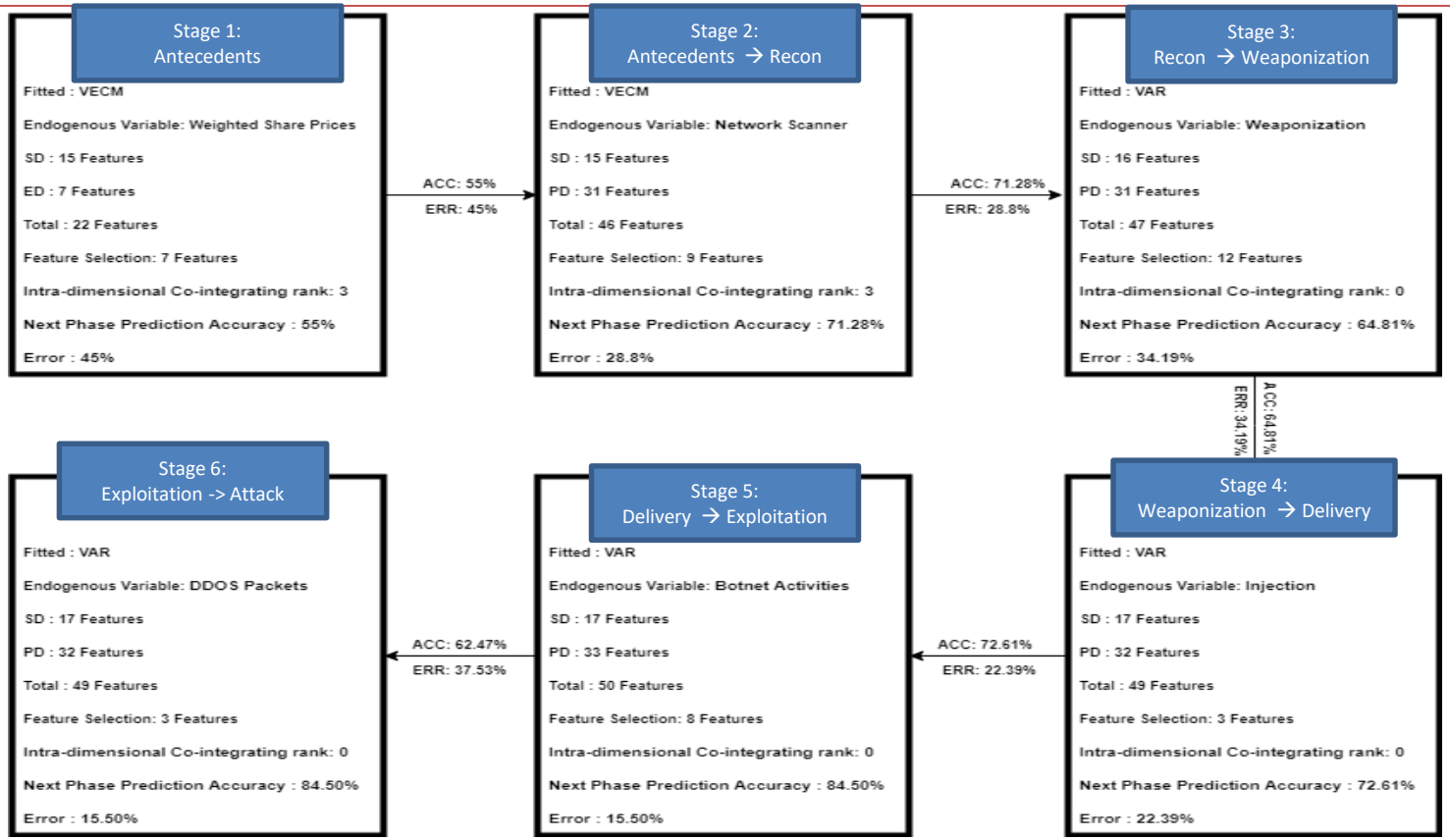


Timeline Integration

PHASED ANALYTICAL APPROACH



RESULTS


Stage 1:
Antecedents
Fitted : VECM
Endogenous Variable: Weighted Share Prices
SD : 15 Features
ED : 7 Features
Total : 22 Features
Feature Selection: 7 Features
Intra-dimensional Co-integrating rank: 3
Next Phase Prediction Accuracy : 55%
Error : 45%
ACC: 55%
ERR: 45%
Stage 2:
Antecedents → Recon
Fitted : VECM
Endogenous Variable: Network Scanner
SD : 15 Features
PD : 31 Features
Total : 46 Features
Feature Selection: 9 Features
Intra-dimensional Co-integrating rank: 3
Next Phase Prediction Accuracy : 71.28%
Error : 28.8%
ACC: 71.28%
ERR: 28.8%
Stage 3:
Recon → Weaponization
Fitted : VAR
Endogenous Variable: Weaponization
SD : 16 Features
PD : 31 Features
Total : 47 Features
Feature Selection: 12 Features
Intra-dimensional Co-integrating rank: 0
Next Phase Prediction Accuracy : 64.81%
Error : 34.19%
ERR: 34.19%
ACC: 64.81%
Stage 4:
Weaponization → Delivery
Fitted : VAR
Endogenous Variable: Injection
SD : 17 Features
PD : 32 Features
Total : 49 Features
Feature Selection: 3 Features
Intra-dimensional Co-integrating rank: 0
Next Phase Prediction Accuracy : 72.61%
Error : 22.39%
ACC: 72.61%
ERR: 22.39%
Stage 5:
Delivery → Exploitation
Fitted : VAR
Endogenous Variable: Botnet Activities
SD : 17 Features
PD : 33 Features
Total : 50 Features
Feature Selection: 8 Features
Intra-dimensional Co-integrating rank: 0
Next Phase Prediction Accuracy : 84.50%
Error : 15.50%
ACC: 62.47%
ERR: 37.53%
Stage 6:
Exploitation -> Attack
Fitted : VAR
Endogenous Variable: DDOS Packets
SD : 17 Features
PD : 32 Features
Total : 49 Features
Feature Selection: 3 Features
Intra-dimensional Co-integrating rank: 0
Next Phase Prediction Accuracy : 84.50%
Error : 15.50%

FINDINGS

- Findings
  - Analytical Characterization of the kill-chain.
  - Analytical proactivity in cyber situational awareness.
  - Integration of predictive feature scope beyond the network layer.
  - Antecedents of cyber-incidents.
  - Multi-source data fusion implementation cyber analytics.

IMPACT

- Implementing Proactive controls for protection of industrial control systems.
- Understanding the dependencies of entities and events within the cyber-operating environment.
- Enhancing Situational awareness by understanding the dynamics of these entanglements in a multi-dimensional, multi-level cyberspace.

- THANK YOU FOR YOUR TIME!!