Remote WMD Capabilities Assessment

G. Mezzour, M. Kas, W. Frankenstein, Prof. L. R. Carley, Prof. K. M. Carley

Carnegie Mellon University

Biological Weapons (BW)

Research Objectives

- Overarching Problem Addressed
  - Detect offensive WMD programs run by countries
  - Remote detection based primarily on open-source data
  - Early, low-cost detection
- Challenges in BW Area
  - Secrecy & dual-use nature of BW technology
- Approach in BW Area
  - Joint motivation & latent capabilities approach
  - Systematic analysis of all countries

Motivation Assessment

- Motivational Factors
  - BW more attractive to dissatisfied states
  - BW attractive as in-kind deterrent
- Computational Method: Social Influence Model
  - Equation: $y^{(t)} = A\,W\,y^{(t-1)} + (I-A)\,y^{(1)},\ t=2,3,\ \ldots$
    - $y^{(t)}$: countries' motivation at time t
    - A: states' susceptibility to interstate influence
    - W: interstate influence
    - $y^{(1)}$: Initial motivation
  - Parameters
    - A: Based on trade-to-GDP ratio (satisfaction measure)
    - W: International hostilities matrix
    - $y^{(1)}$: Whether states are suspected of having BW

Latent Capabilities Assessment

- Metrics
  - Number of BW papers
  - Trade volume of dual-use biological items
  - Pharmaceutical capability

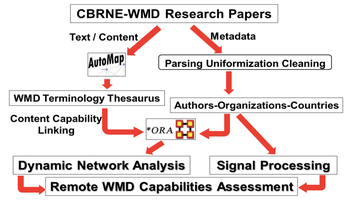
Results

Countries known or suspected to have offensive capability	Countries to watch for
China, Egypt, Iran, Israel, N. Korea, Russia, Syria, Taiwan	India, Pakistan, Taiwan, Georgia, Sudan, Lebanon, Sudan

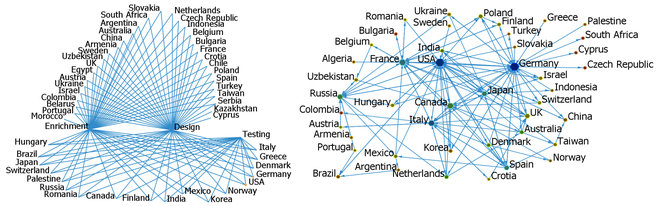
Nuclear Weapons

Expertise Identification & Tracking

- Methodology



- Results



Joint Capabilities & Motivations

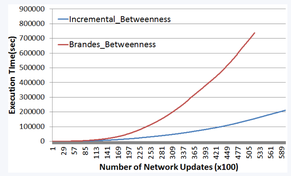
- Motivational Factors
  - Enemy has weapon => increased motivation
  - Ally has weapon => reassurance
- Capabilities based on research & trade

Countries with nuclear weapons	Countries to watch for
US, France, Russia, China, India, UK, Israel, Pakistan, N. Korea	Taiwan, Slovakia

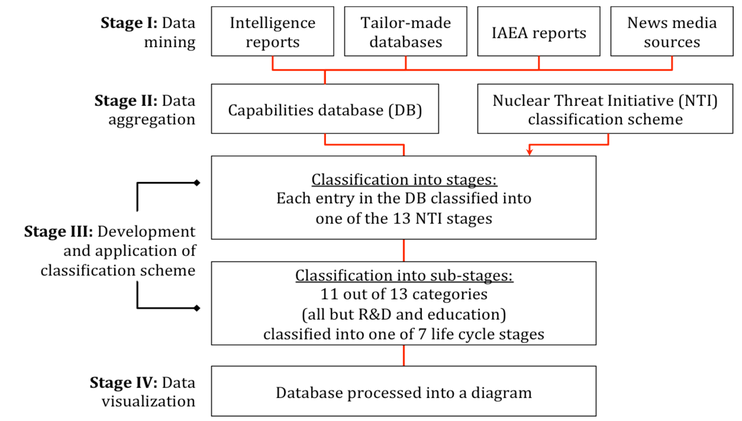
Incremental Computation of Measures

- Motivating example
  - Above networks may be huge, and we want monitor their growth in real time – some measures too complex
  - Incremental computation overcomes complexity barrier
- Approach
  - On network update: e.g., Insert an edge
  - Change only affects part of the network

Results on Facebook-like network



Case Study: Iran's Nuclear Program



- Results
  - Very active nuclear program
  - No unequivocal evidence that Iran is weaponizing its nuclear program

Next Step: Cyber WMDs

- Mining Telemetry Dataset from Symantec
  - 1 billion antivirus submissions & 1 billion intrusion detection submissions
  - Extracting amount of attacks detected in each country
  - Extracting country attack network
    - Source country attribution difficult
- Cyber security papers 2001-2011
- Subject Matter Opinion
  - Cyber capability preparedness of 23 countries obtained by questioning ~ 80 cyber security experts. Source: Cyber-security: The vexed questions of global rules. An independent report on cyber-preparedness around the world, 2011.
  - Cyberwarfare in military doctrine & organization. Source: : Center for Strategic and International Studies. Cybersecurity & Cyberwarfare. Preliminary Assessment of National Doctrine & Organization, 2011.

This work is supported in part by the Defense Threat Reduction Agency (DTRA) under the grant number HDTRA11010102 and by the center for Computational Analysis of Social and Organizational Systems (CASOS). The views and conclusions contained in this document are those of the authors and should not be interpreted as representing the official policies, either expressed or implied, of the DTRA or the U.S. government.