SAND2014-16883PE

Behavioral Influence Assessment (BIA)

Modeling of Potential Cyber Behaviors

MIDN Mitchell Pratt

United States Naval Academy

Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.

Purpose of BIA

Informs High Consequence Decisions

- Better understand and anticipate the interplay between specific Individuals, political/social military organizations, and general society in response to potential courses of actions or events

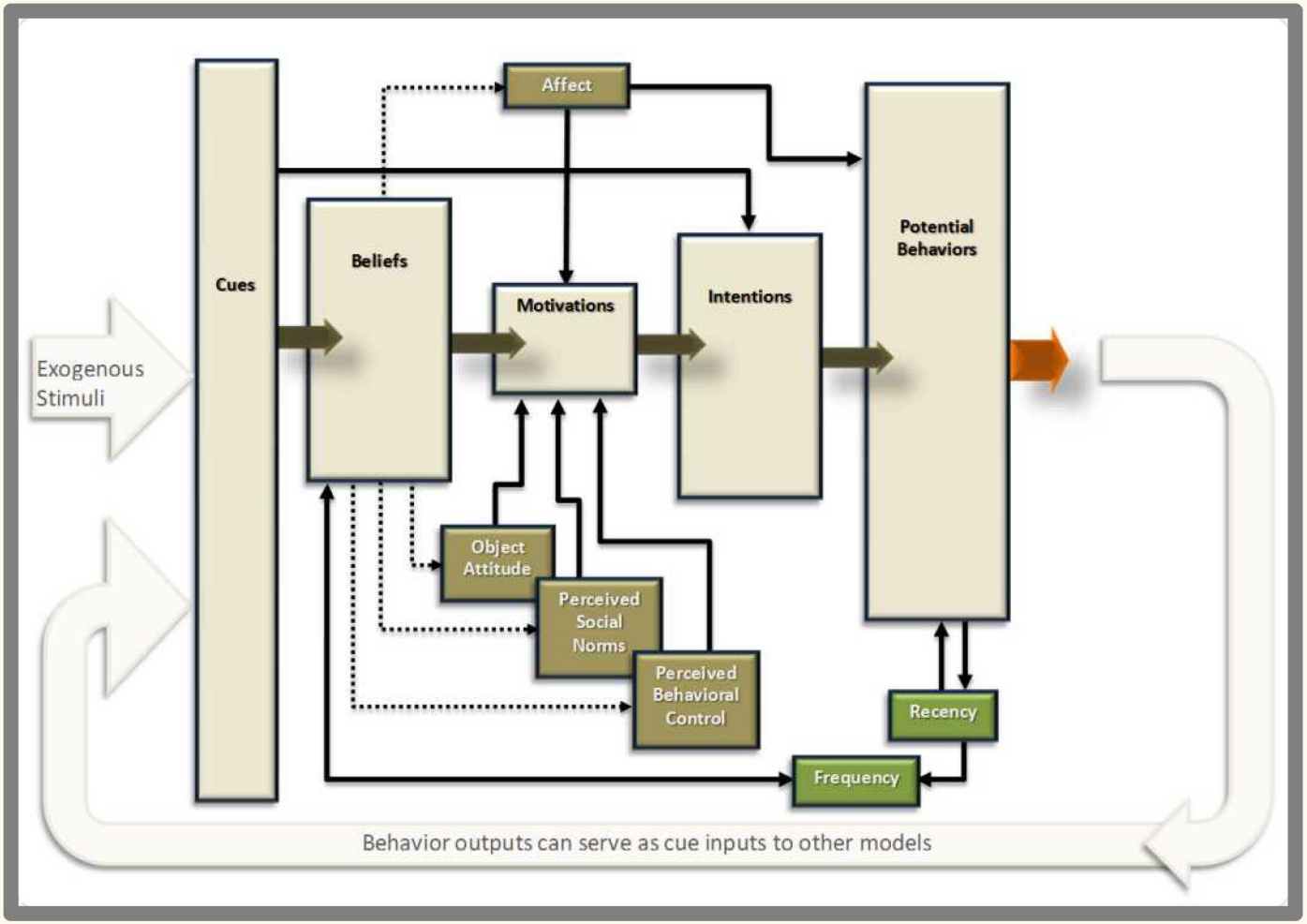
Impacts

- Enables analysts to assess higher-order (cascading) influences and reactions to events, as well as determine the uncertainty that the event will produce the desired results over time

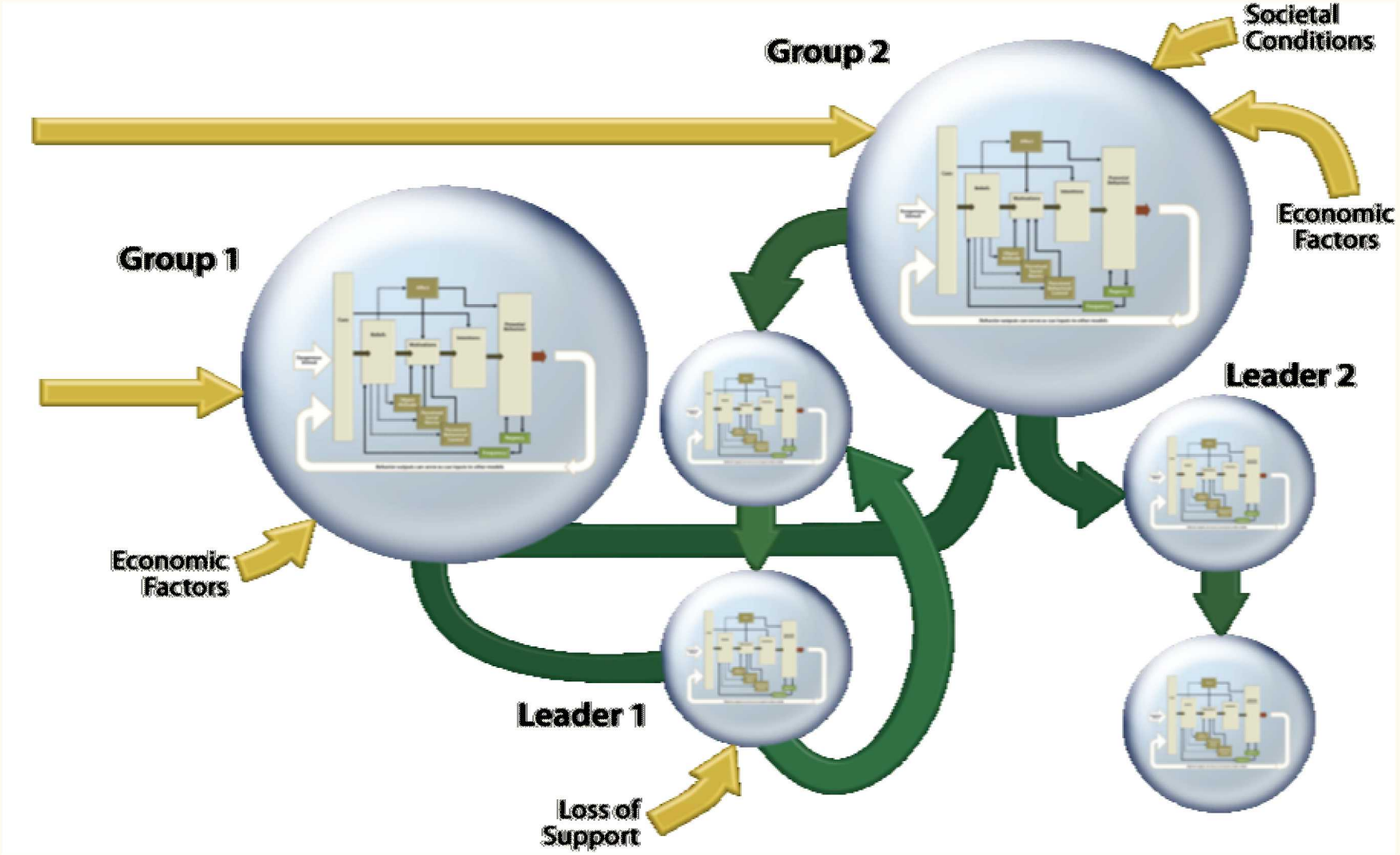
The BIA Philosophy

- Goal: Minimize the likelihood of bad decisions and unintended consequences by assessing risk
  - Often the most likely decision is has undesirable outcomes
- A verified model is superior to business as usual
- We are not interested in point prediction or predictive quantification of magnitude
  - We are interested in:
    - Phenomena
    - Interventions
    - Limits of dynamic repercussions

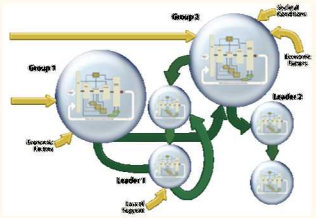
Core Cognitive System Architecture



Systems Dynamics View

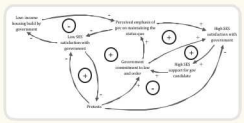


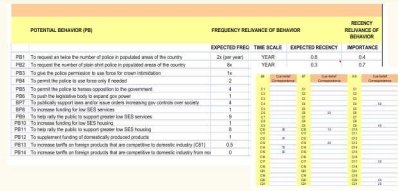
Populating Psychosocial Theoretical Models

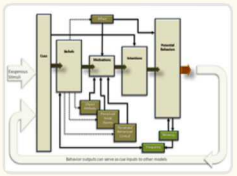


Psychological/group Models

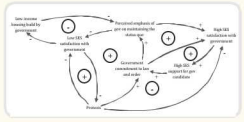
Subject Matter Experts

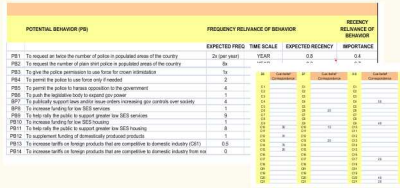


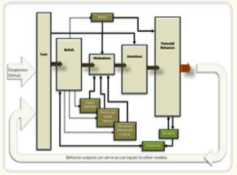




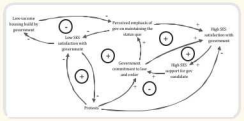
System Models

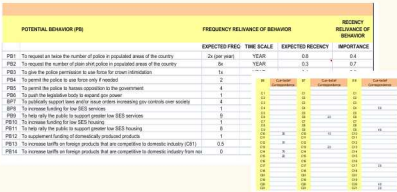


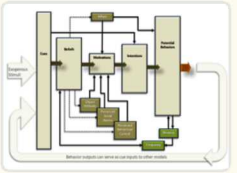


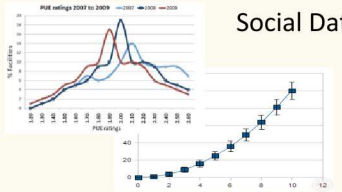


System Models







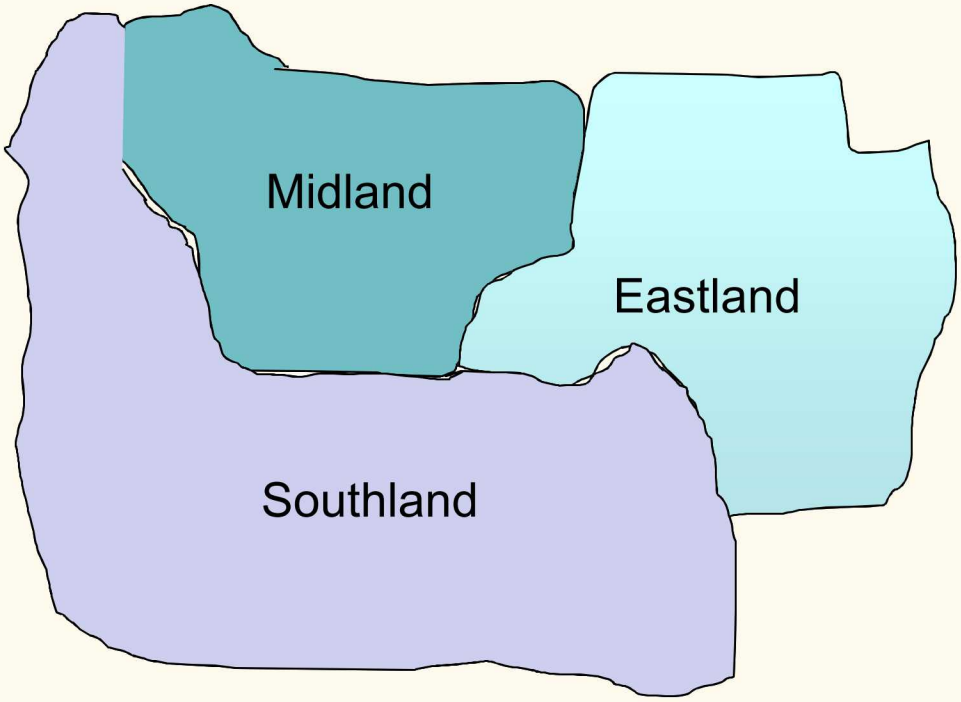


Social Data

Modeling Cyber Behaviors in TracerFIRE

- TracerFIRE is a game developed by SNL to educate cyber defenders.
- Teams work in competition to solve network defense and forensics challenges.
- BIA will begin gathering data from TracerFIRE activities to develop models of cyber behaviors across three fictitious countries
- The cyber models will differ from previous BIA models because attribution is more difficult in the cyber domain

TracerFIRE Scenario



- The new TracerFIRE scenario will be more interactive and dynamic than ever before, with a story revealed through news articles and careful computer forensics.

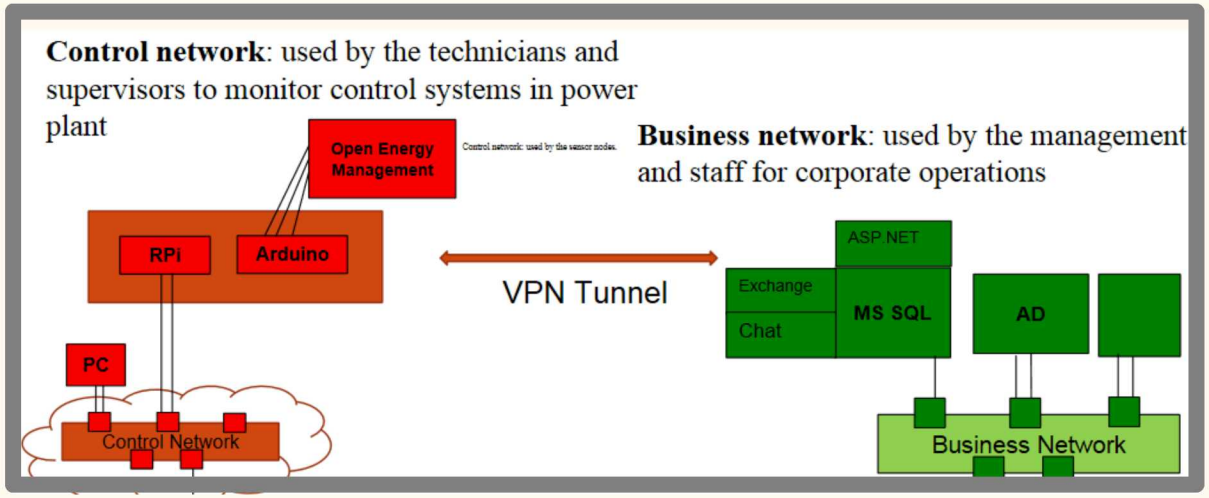
Fictitious Scenario

- Years ago, a civil war split the country of Midland in half to form Midland and Eastland. An uneasy truce continues, but no lasting peace.
- Southland has ambitions of taking over both and will weaken the countries by agitating conflict between them.

TracerFIRE Scenario

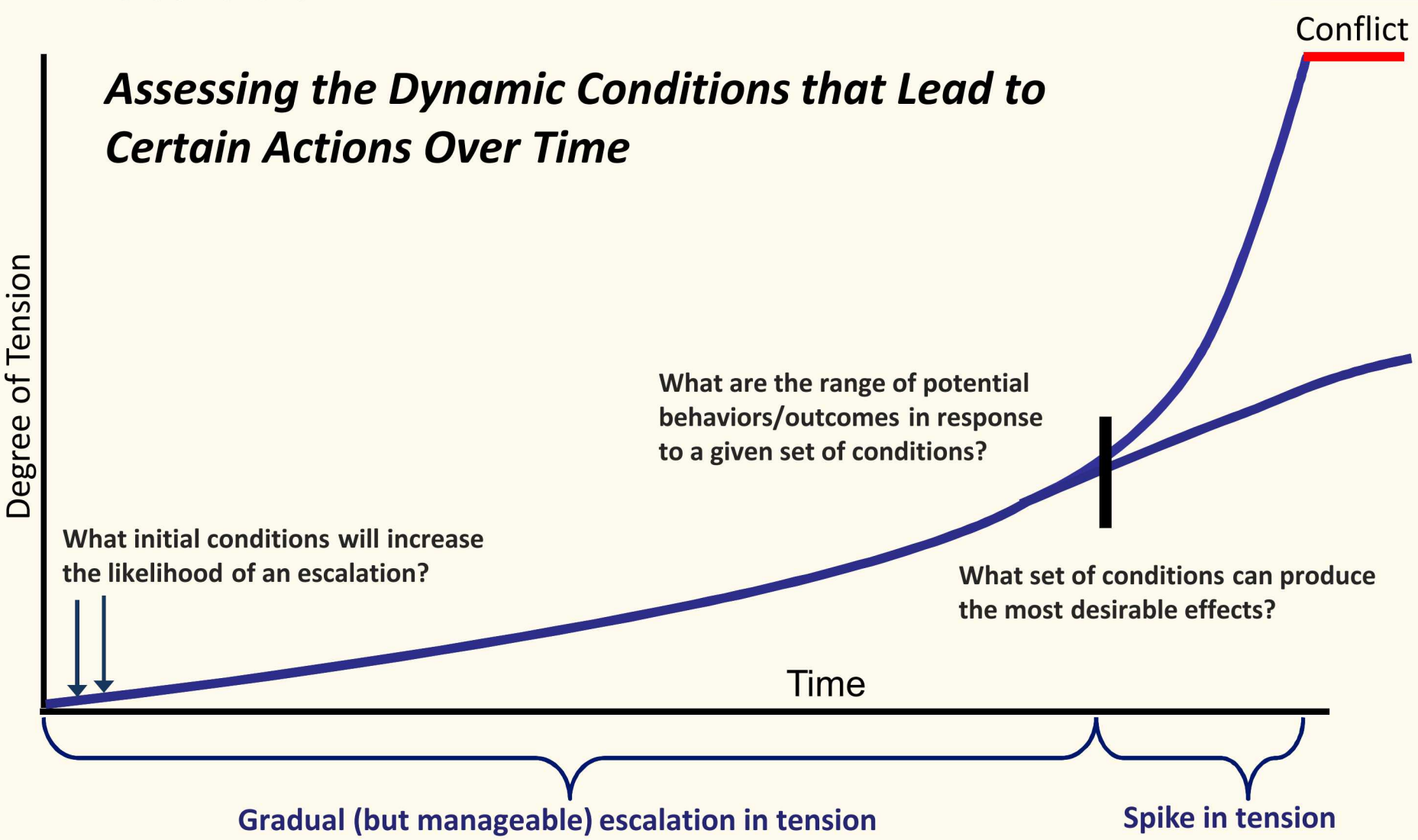
Cyber Exchange Between:
Midland and Eastland

- Cyber group has gained a foothold on both of Midland and Eastland's networks



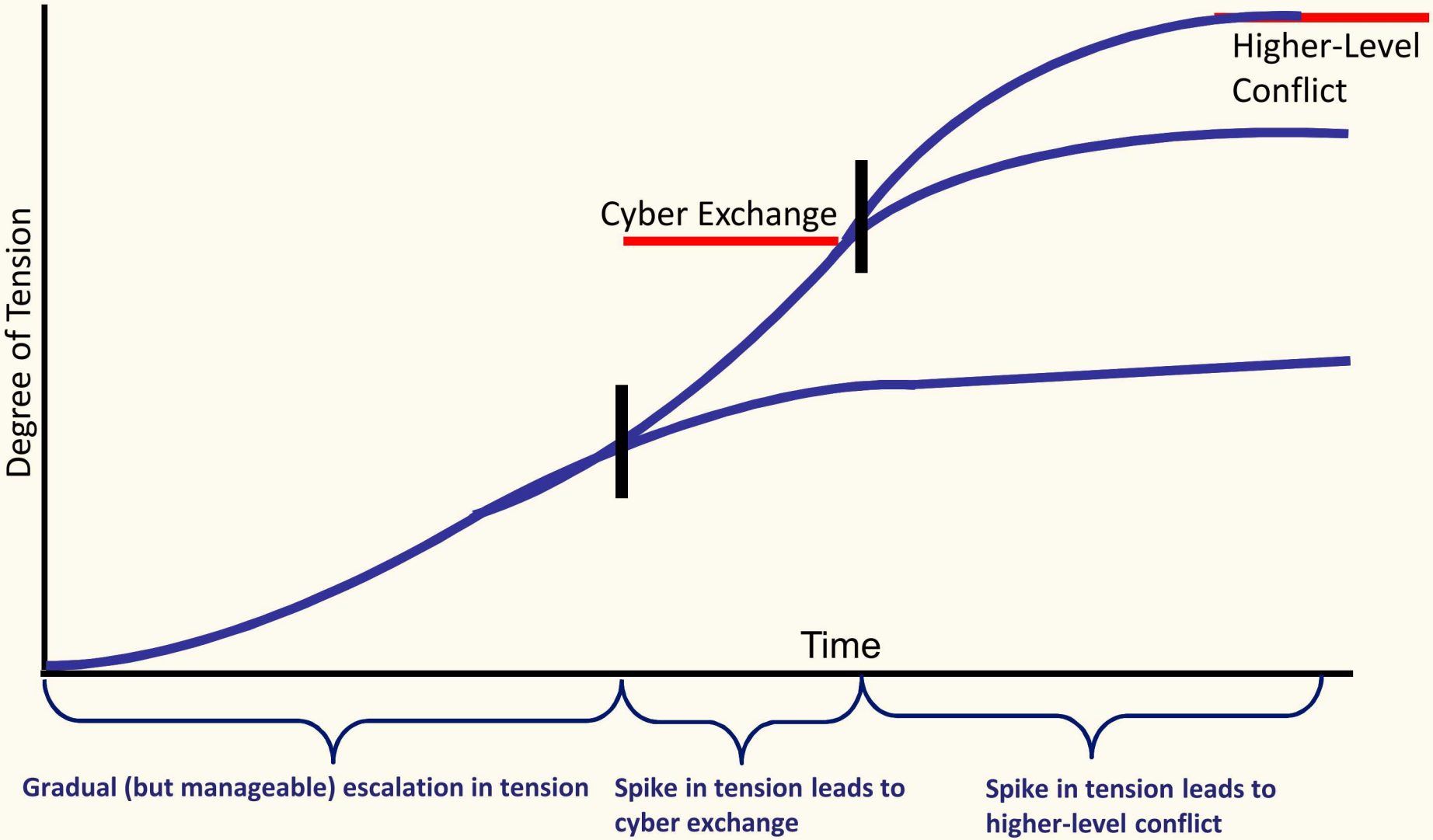
- Participants will notice the blackout and will be tasked to find the cause
- The challenges will get progressively harder, and the best cyber defenders will unravel the conspiracy.

Escalation

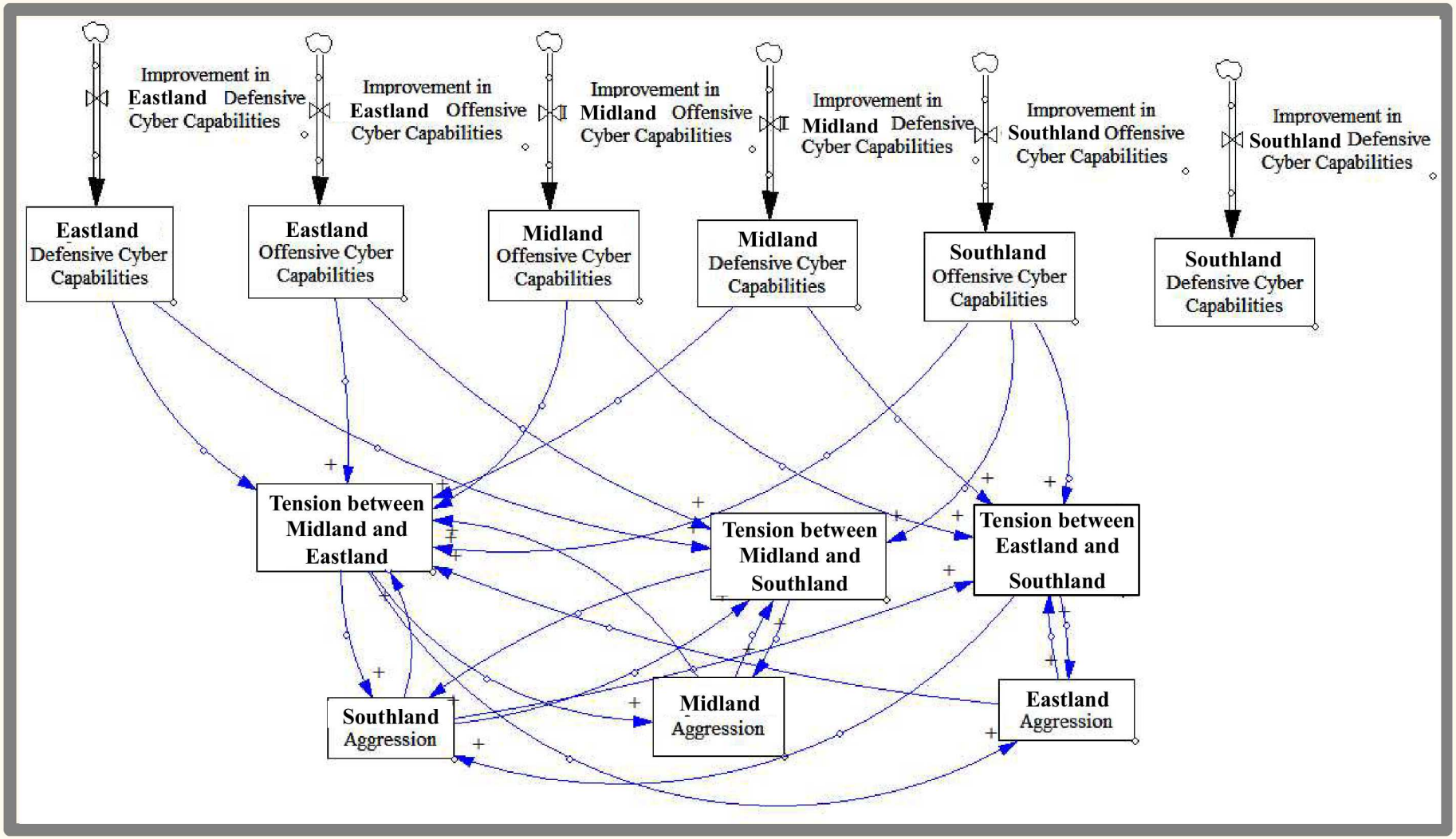


What are the immediate and long-term effects of a COA on different groups/countries?

Escalation in the Cyberspace Domain



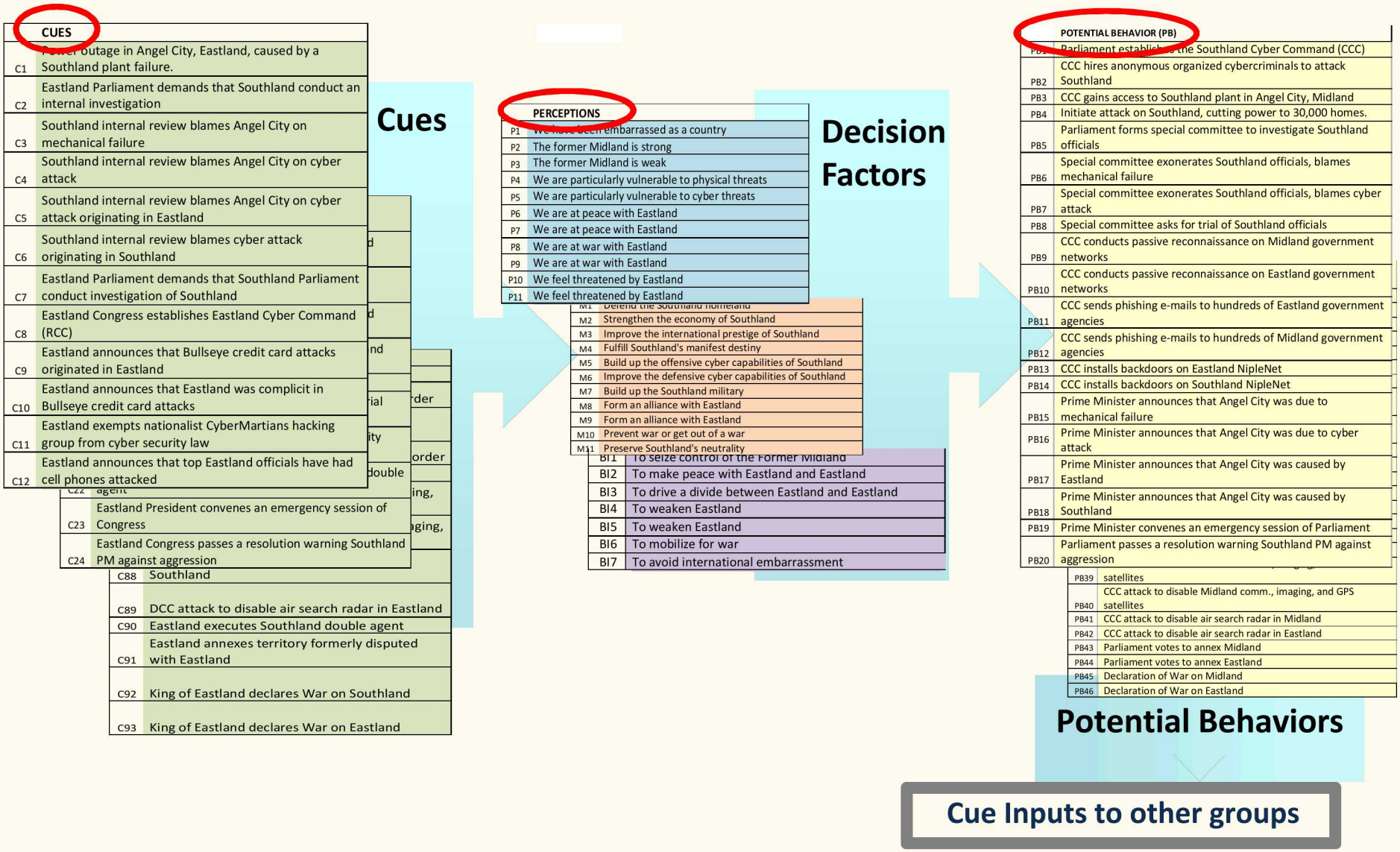
The Systems Dynamics Level



The Cognitive Level

- Each society (Southland, Midland, and Eastland) is modeled at the cognitive level to simulate behavior.
- Dozens of cues for one society lead to dozens of potential behaviors, which become cues for another society.
- Data from TracerFIRE will help determine how likely a society is to pick up on certain cyber-related cues.

The Cognitive Level



	CUES
C1	Power outage in Angel City, Eastland, caused by a Southland plant failure.
C2	Eastland Parliament demands that Southland conduct an internal investigation
C3	Southland internal review blames Angel City on mechanical failure
C4	Southland internal review blames Angel City on cyber attack
C5	Southland internal review blames Angel City on cyber attack originating in Eastland
C6	Southland internal review blames cyber attack originating in Southland
C7	Eastland Parliament demands that Southland Parliament conduct investigation of Southland
C8	Eastland Congress establishes Eastland Cyber Command (RCC)
C9	Eastland announces that Bullseye credit card attacks originated in Eastland
C10	Eastland announces that Eastland was complicit in Bullseye credit card attacks
C11	Eastland exempts nationalist CyberMartians hacking group from cyber security law
C12	Eastland announces that top Eastland officials have had cell phones attacked
C23	Eastland President convenes an emergency session of Congress
C24	Eastland Congress passes a resolution warning Southland PM against aggression
C88	Southland
C89	DCC attack to disable air search radar in Eastland
C90	Eastland executes Southland double agent
C91	Eastland annexes territory formerly disputed with Eastland
C92	King of Eastland declares War on Southland
C93	King of Eastland declares War on Eastland

	PERCEPTIONS
P1	We have been embarrassed as a country
P2	The former Midland is strong
P3	The former Midland is weak
P4	We are particularly vulnerable to physical threats
P5	We are particularly vulnerable to cyber threats
P6	We are at peace with Eastland
P7	We are at peace with Eastland
P8	We are at war with Eastland
P9	We are at war with Eastland
P10	We feel threatened by Eastland
P11	We feel threatened by Eastland

M1	Defend the Southland homeland
M2	Strengthen the economy of Southland
M3	Improve the international prestige of Southland
M4	Fulfill Southland's manifest destiny
M5	Build up the offensive cyber capabilities of Southland
M6	Improve the defensive cyber capabilities of Southland
M7	Build up the Southland military
M8	Form an alliance with Eastland
M9	Form an alliance with Eastland
M10	Prevent war or get out of a war
M11	Preserve Southland's neutrality
BI1	To seize control of the Former Midland
BI2	To make peace with Eastland and Eastland
BI3	To drive a divide between Eastland and Eastland
BI4	To weaken Eastland
BI5	To weaken Eastland
BI6	To mobilize for war
BI7	To avoid international embarrassment

	POTENTIAL BEHAVIOR (PB)
PB1	Parliament establishes the Southland Cyber Command (CCC)
PB2	CCC hires anonymous organized cybercriminals to attack Southland
PB3	CCC gains access to Southland plant in Angel City, Midland
PB4	Initiate attack on Southland, cutting power to 30,000 homes.
PB5	Parliament forms special committee to investigate Southland officials
PB6	Special committee exonerates Southland officials, blames mechanical failure
PB7	Special committee exonerates Southland officials, blames cyber attack
PB8	Special committee asks for trial of Southland officials
PB9	CCC conducts passive reconnaissance on Midland government networks
PB10	CCC conducts passive reconnaissance on Eastland government networks
PB11	CCC sends phishing e-mails to hundreds of Eastland government agencies
PB12	CCC sends phishing e-mails to hundreds of Midland government agencies
PB13	CCC installs backdoors on Eastland NipleNet
PB14	CCC installs backdoors on Southland NipleNet
PB15	Prime Minister announces that Angel City was due to mechanical failure
PB16	Prime Minister announces that Angel City was due to cyber attack
PB17	Prime Minister announces that Angel City was caused by Eastland
PB18	Prime Minister announces that Angel City was caused by Southland
PB19	Prime Minister convenes an emergency session of Parliament
PB20	Parliament passes a resolution warning Southland PM against aggression
PB39	satellites
PB40	CCC attack to disable Midland comm., imaging, and GPS satellites
PB41	CCC attack to disable air search radar in Midland
PB42	CCC attack to disable air search radar in Eastland
PB43	Parliament votes to annex Midland
PB44	Parliament votes to annex Eastland
PB45	Declaration of War on Midland
PB46	Declaration of War on Eastland