

# Enhanced Dooley Graphs for Modeling, Analyzing, and Attributing Ransomware Attacks

Physics  
Linguistics  
Biology

ABC Research, LLC

PI: H. Van Dyke Parunak, Ph.D.,  
ABC Research, LLC

[www.abcresearch.org/papers/dooldesn.pdf](http://www.abcresearch.org/papers/dooldesn.pdf),  
[www.abcresearch.org/papers/dooley.pdf](http://www.abcresearch.org/papers/dooley.pdf)

## Ransomware Distinctives:

- Victim knows of attack while in progress
  - Victim and attacker interact deliberately
  - Outcome depends on collaboration
- Compare formalisms for E-commerce

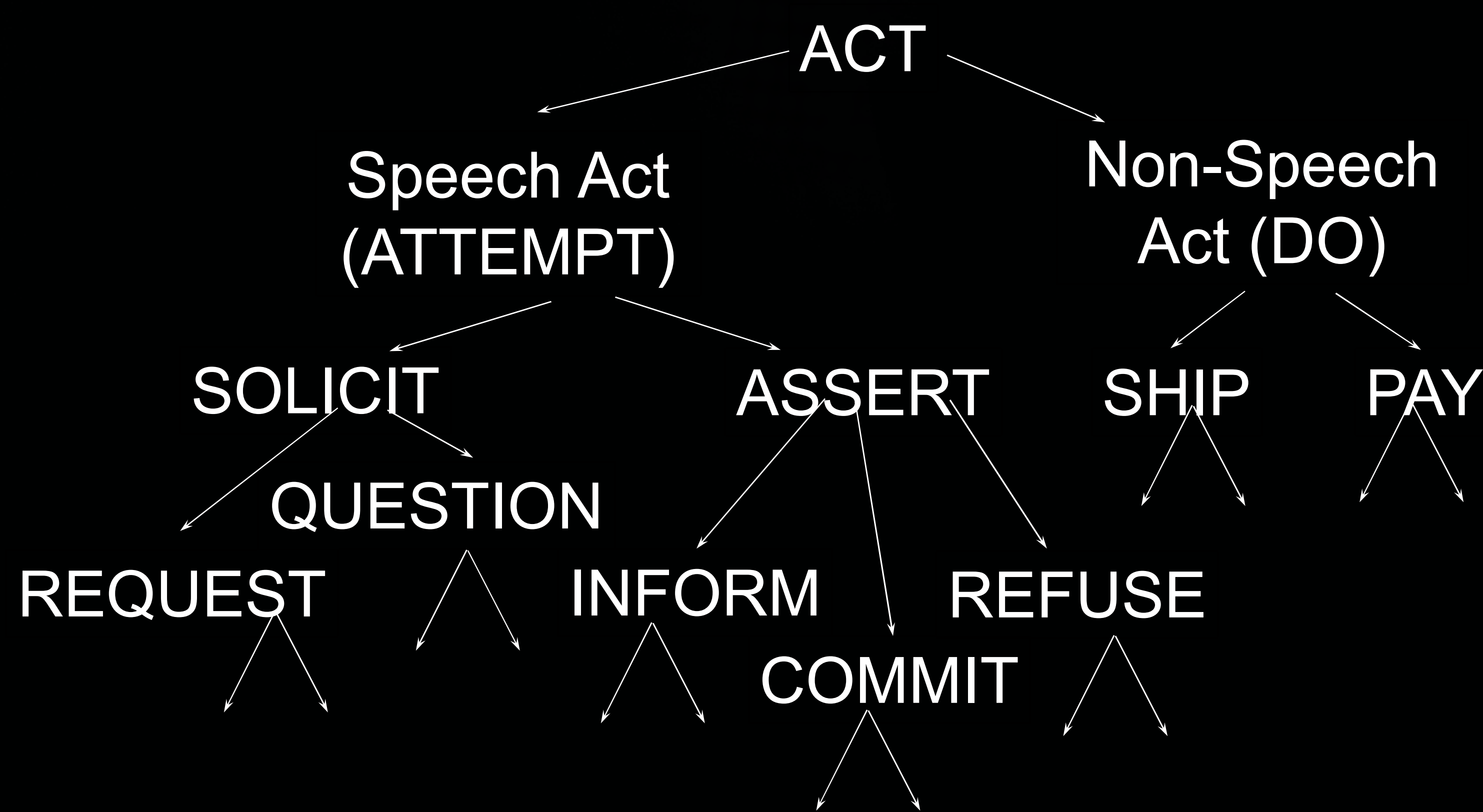
## Requirements:

- Unambiguous, formal model of interaction
- Understandable by human analysts
- Tractable for computer modeling

## Dooley Graphs

- Invented by field linguists to study discourse
- Widely used since 1996 in E-commerce

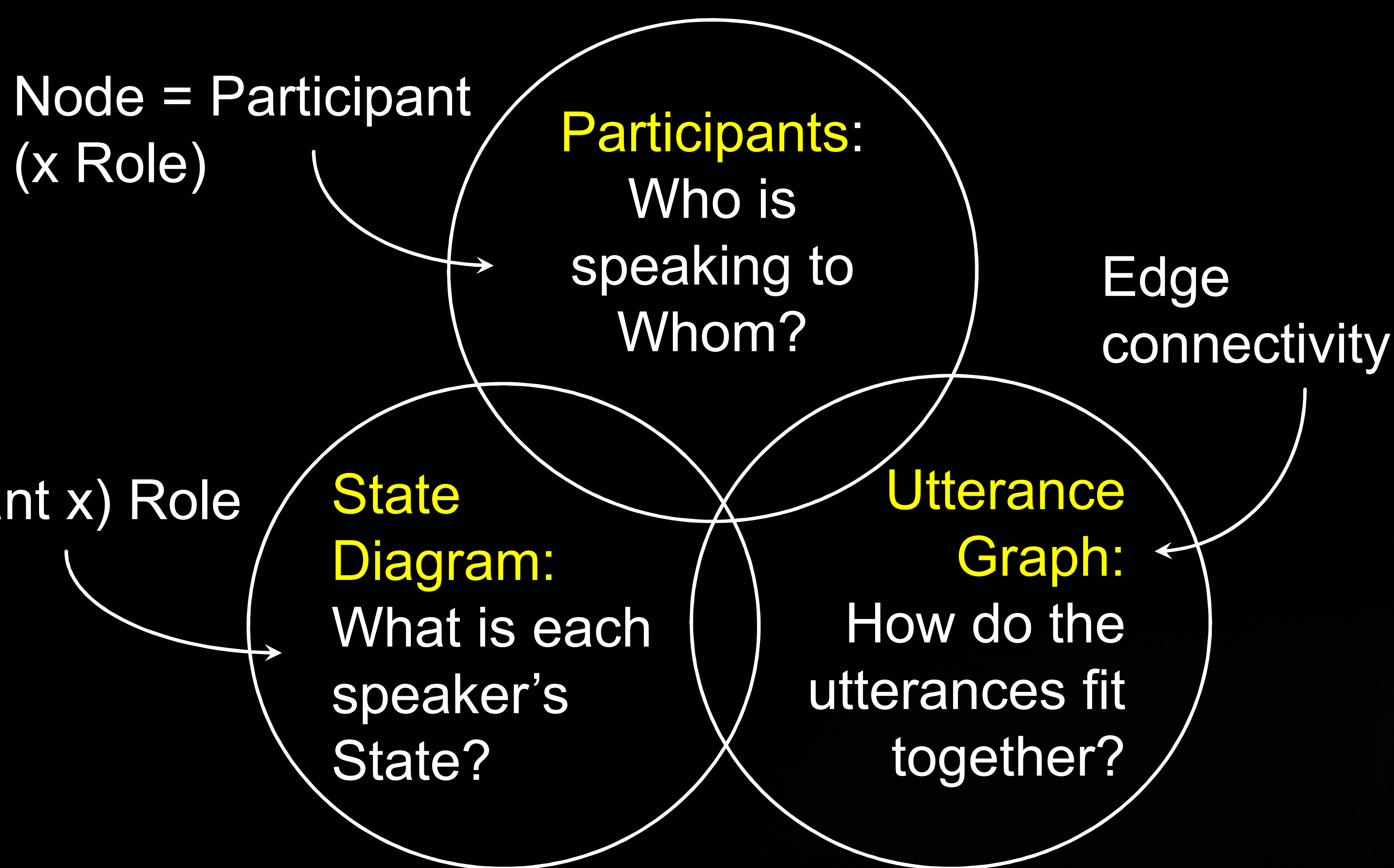
**Speech Act Theory** (Austin 1962; Cohen and Levesque 1995; Parunak 1996)



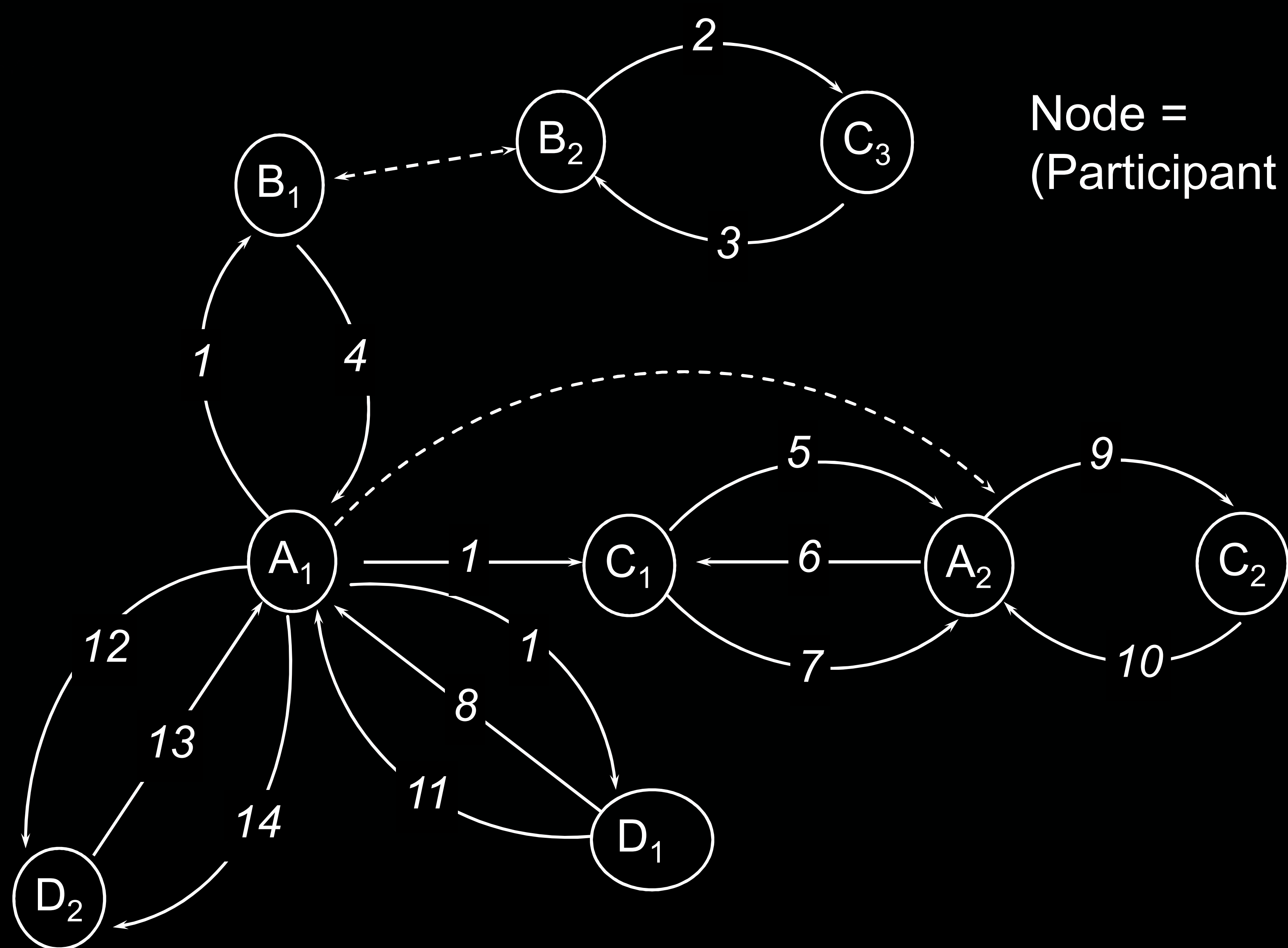
## Building Blocks for Transactions

	Responds	Replies	Resolves	Completes
Example	Any sequence	Any interchange	Question-Answer	Commitment-Execution
Relation	Causal	Causal	Causal + "obeys"	Causal + fulfills
Speakers	Any	Reciprocal	Reciprocal	Same
Control		Undefined	Same	Same

## Dooley Graphs and Other Discourse Formalisms



## Example Dooley Graph in E-Commerce



## Proposal:

- Develop Dooley Graph mapping for ransomware domain
- Construct Dooley Graphs for actual cases
- Identify distinguishing features
- Merge into Dooley Graph of potential interactions
- Demonstrate usefulness for attribution, prediction, and PIR generation

