

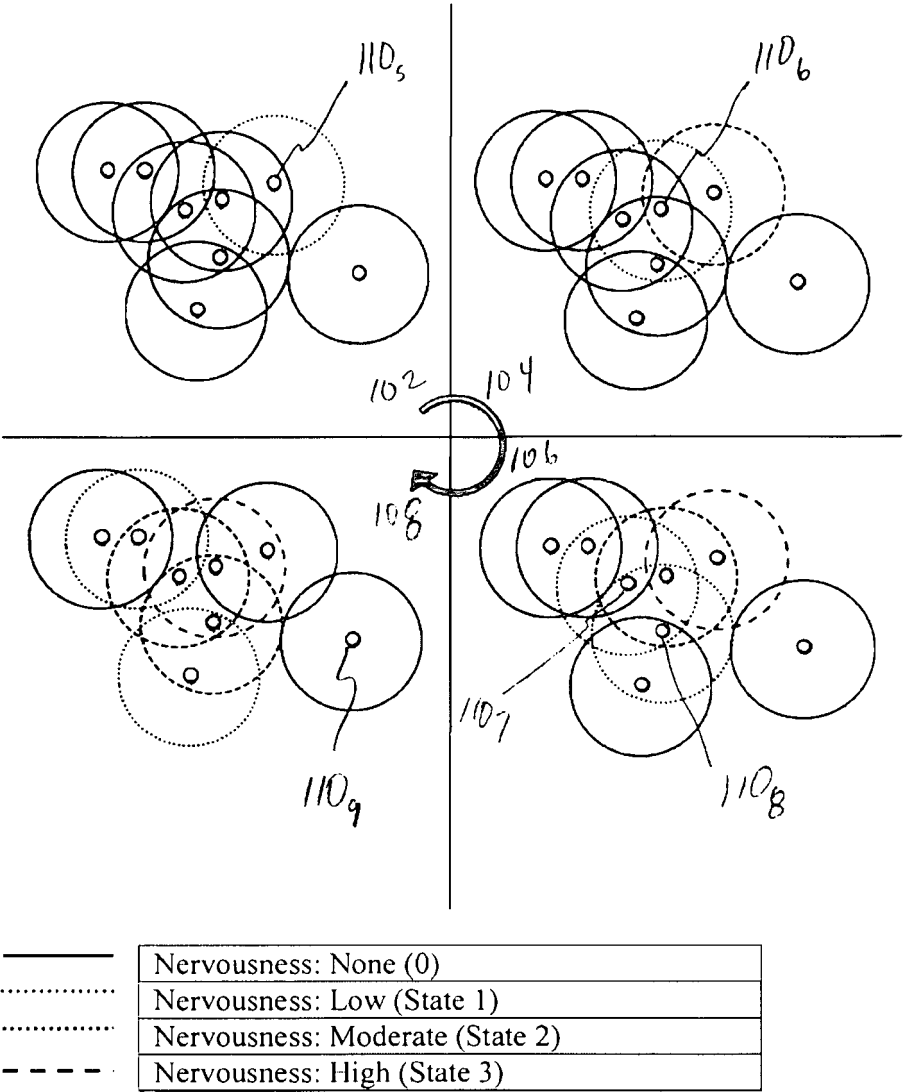


Figure 1: Network Nervousness Assessment

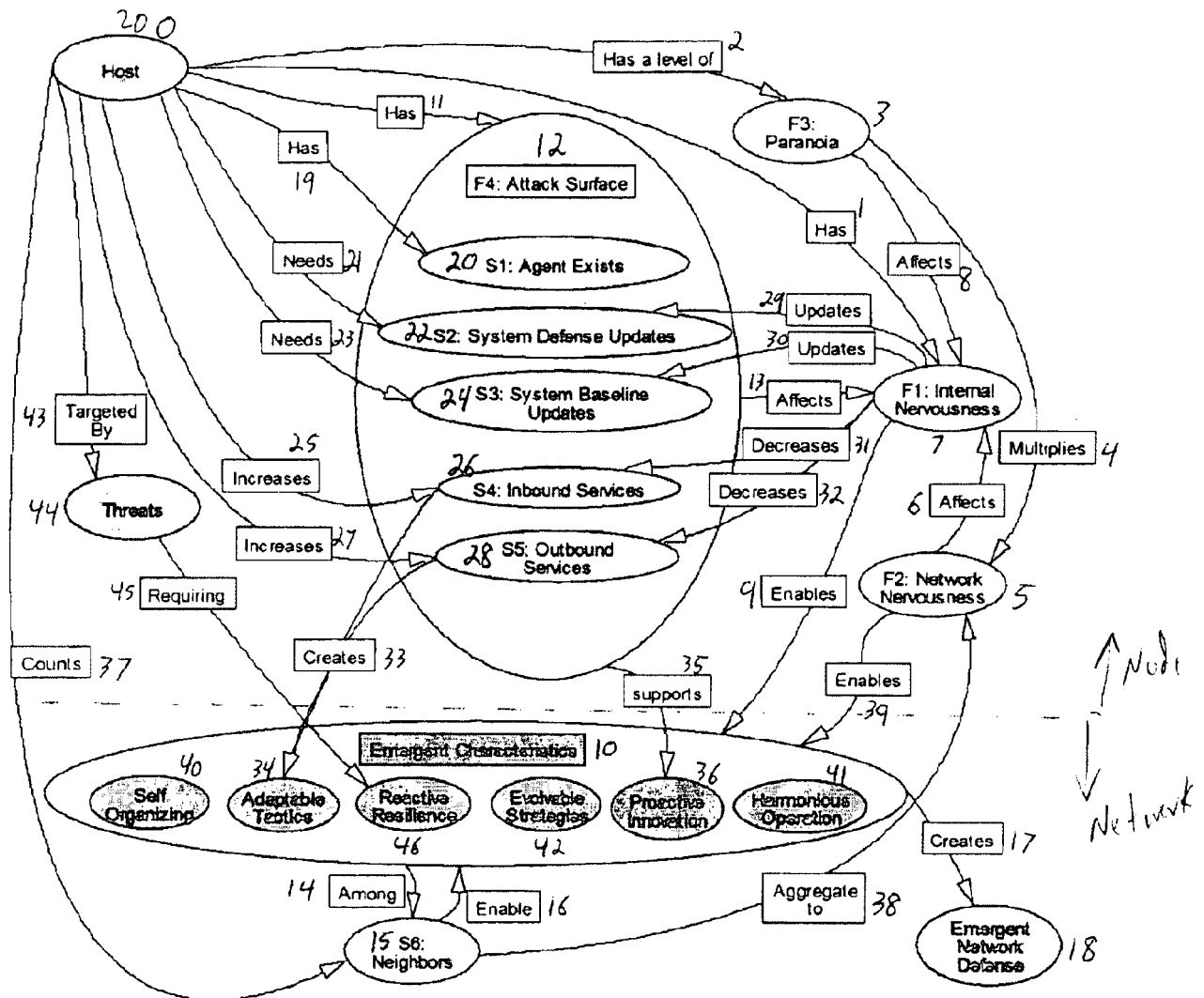


Figure 2: Systemigram for Emergent Network Defense

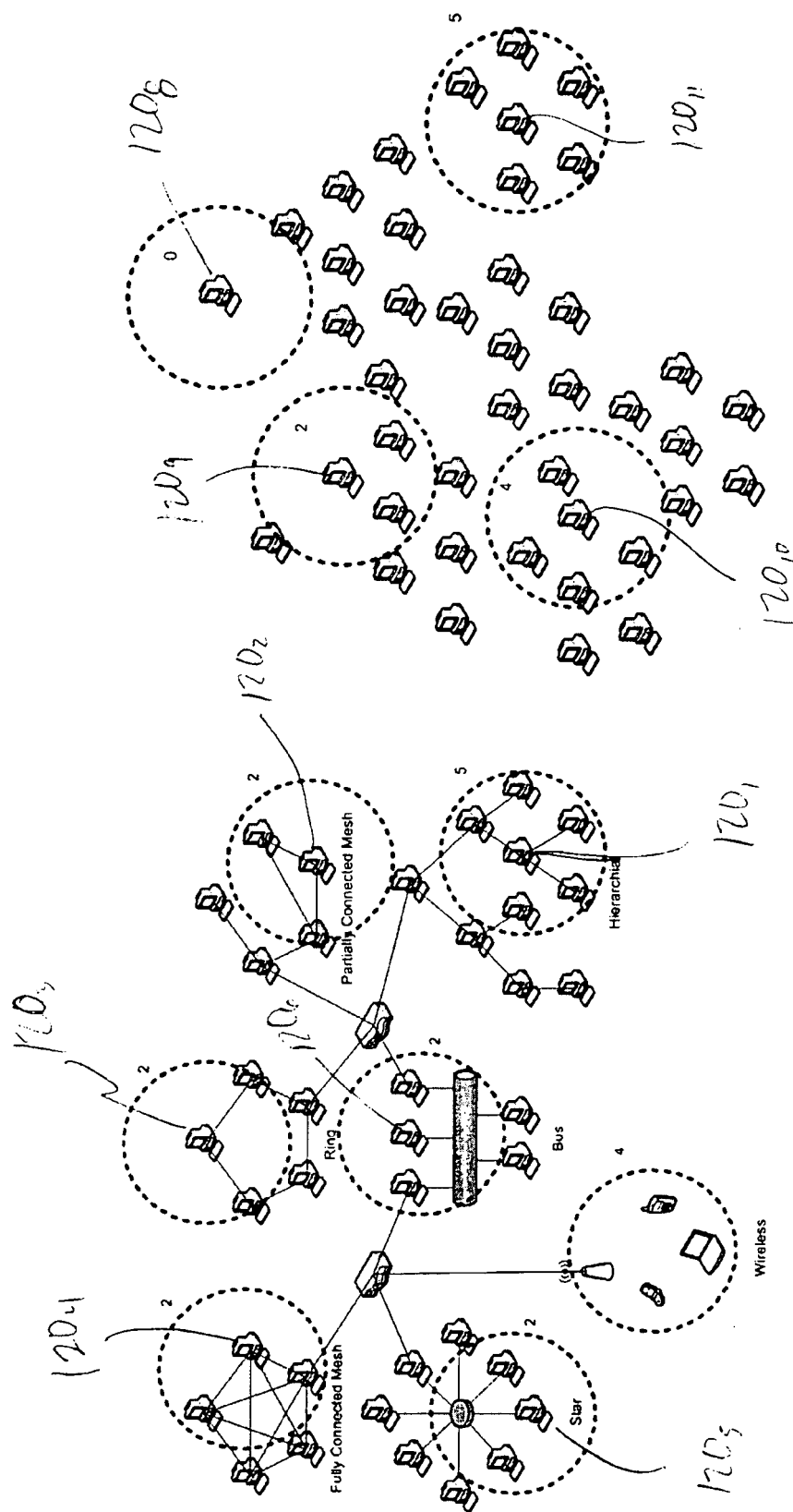


Figure 3: Nearest Neighbor Abstraction

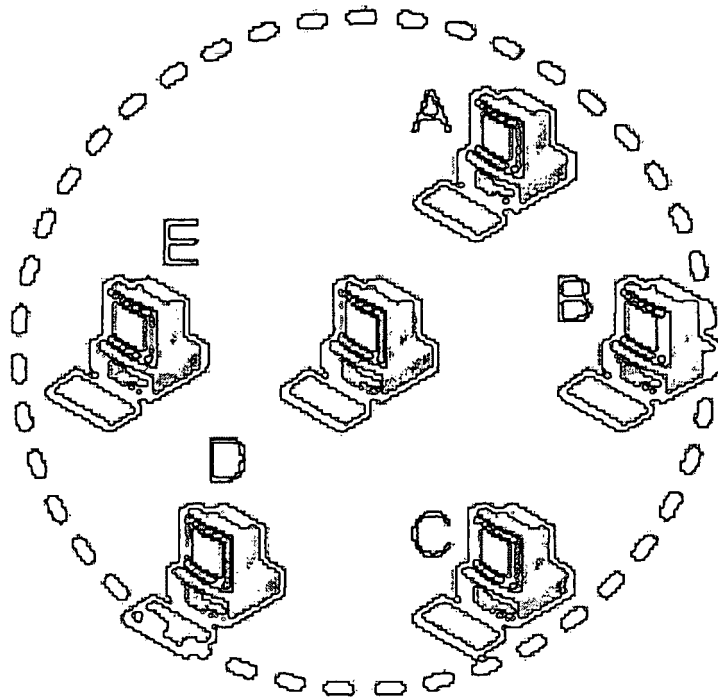


Figure 4: Nervous Example

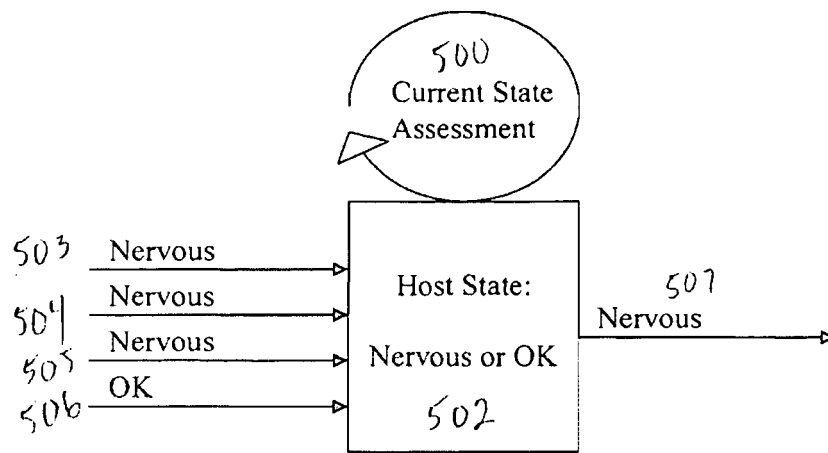


Figure 5: Theoretical Context Diagram for Block One

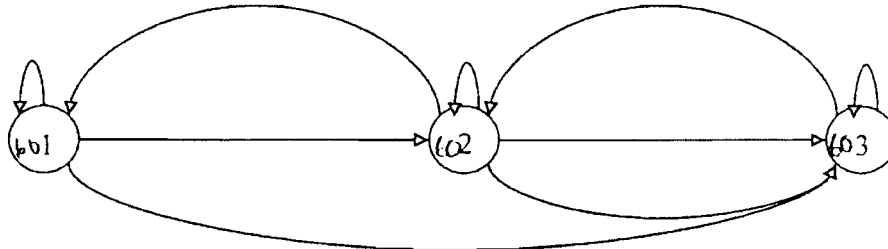
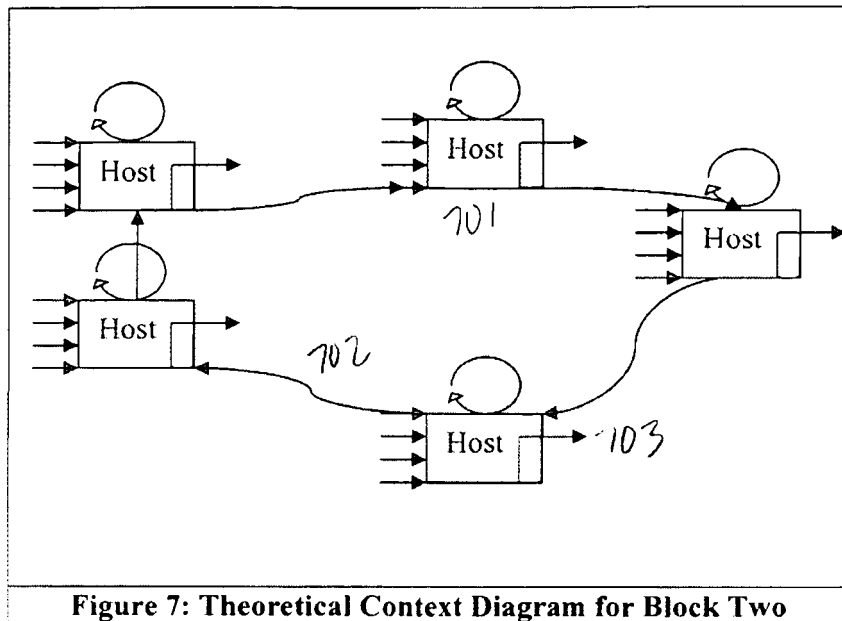


Figure 6: State Change



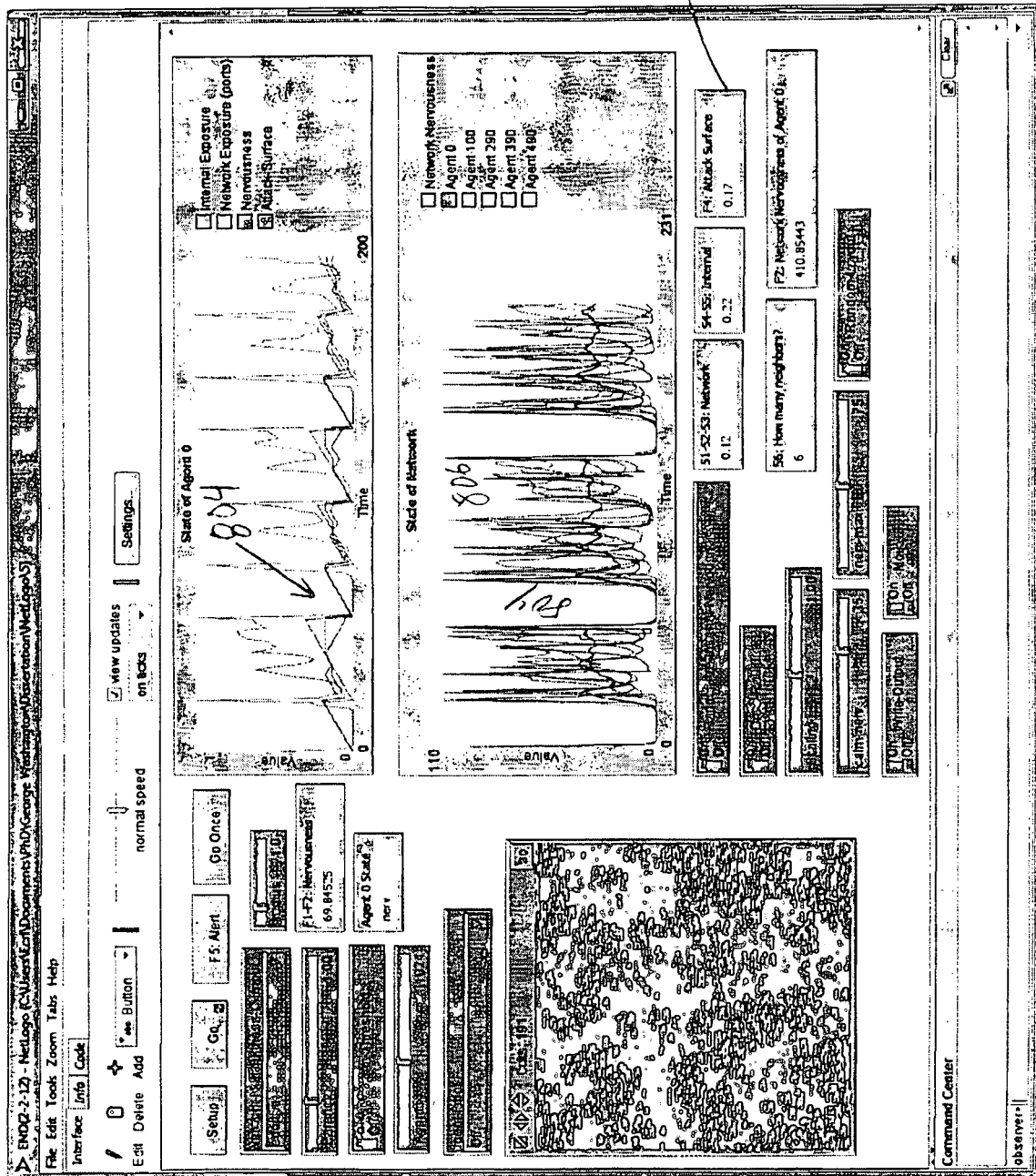


Figure 8: Three Alerts Demonstrate Emergent Behavior

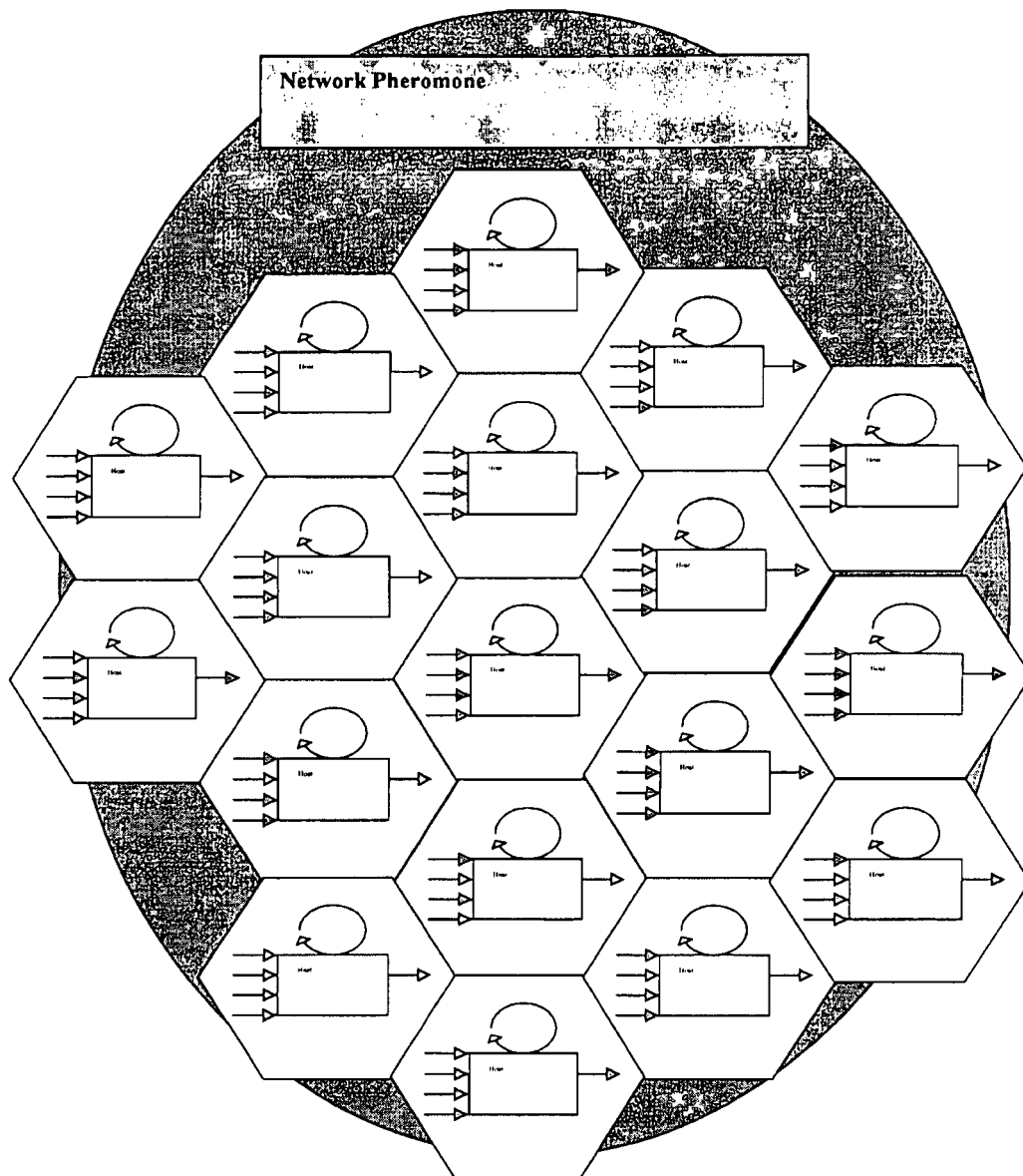


Figure 9: Theoretical Context Diagram for Block Three

Feedback Data:	State Data:
F1: Level of Internal Nervousness F2: Level of Network Nervousness F3: Level of Paranoia F4: Attack Surface	S1: Agent exists on node S2: System Defenses (HBSS, AV, IDS) at latest signature level S3: System Baseline (OS, Applications) at latest patch/configuration level S4: Inbound services restricted (services disabled, ports blocked) S5: Outbound services restricted (blocked IP, subnets, URLs) S6: Number of Neighbors

	F1: Level of Internal Nervousness	F2: Level of Network Nervousness	F3: Level of Paranoia	F4: Attack Surface	S1: Agent exists on node	S2: System Defenses at latest signature level	S3: System Baseline at latest patch/configuration level	S4: Inbound services restricted	S5: Outbound services restricted	S6: Number of Neighbors
Block One: Endpoint attack surface characteristics				X	X	X	X	X	X	
Block Two: Endpoint nodes share security states through "nervous network"	X	X	X		X					X
Block Three: Node systems change their attack surface and node nervous state based on inputs	X	X	X	X	X	X	X	X	X	X

Figure 10: Required Data Elements