FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

A Dynamic Control Scheme for the Secure Operation of Cyber-physical Systems

Erik Miehling — miehling@umich.edu
Department of Electrical & Computer Engineering,
University of Michigan, Ann Arbor, MI, USA

NSF Review Meeting, Arlington, VA — Jan 25-26, 2017

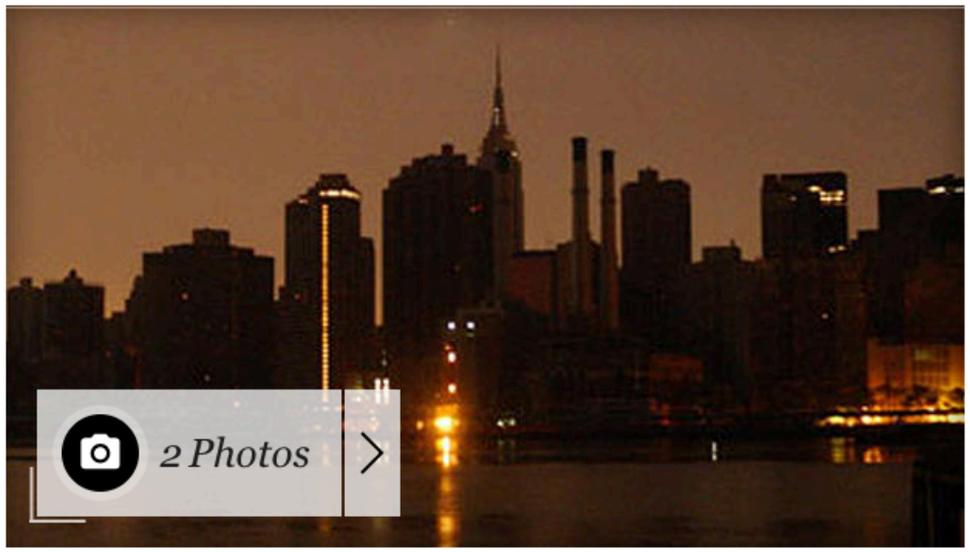
Berkeley UNIVERSITY OF CALIFORNIA
Massachusetts Institute of Technology
NSF
MICHIGAN
VANDERBILT UNIVERSITY

CBS News / CBS Evening News / CBS This Morning / 48 Hours / 60 Minutes / Sunday Morning / Face The Nation / CBSN Log In Search

CBSNEWS Video | US | World | Politics | Entertainment | Health | MoneyWatch | SciTech | Crime | Sports | Photos | More

By **JAIME HOLGUIN** / **CBS/AP** / *August 15, 2003, 7:20 AM*

Biggest blackout in U.S. history



The dark Manhattan skyline, seen from Queens, is silhouetted against a pre-dawn sky Aug. 15, 2003. A widespread power outage hit most of northeastern United States Aug. 14, leaving the city in the dark. / **AP**

Comment / Share / Tweet / Stumble / Email

Power is coming back to some of the 50 million people affected by the blackout which hit Thursday, continued into Friday, and is the biggest power outage in U.S. history.

The outage affected a wide swath of territory in the U.S. and Canada - including New York City, Albany, Hartford, Toronto, Ottawa, Detroit, Cleveland and Ontario

From 60 Minutes


Obama and the 2008 general election


A president and a journalist: 17 interviews


When 60 Minutes first met Barack Obama


Obama and the Democratic 2008 primaries


An Obama family flashback on 60 Minutes

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

CBS News / CBS Evening News / CBS This Morning / 48 Hours / 60 Minutes / Sunday Morning / Face The Nation / CBSN

Log In Search

CBS

By JAIME HOLGUI

Bigg
histo

The dark Manhatta
power outage hit m

Comment /

Power is comi
which hit Thu
history.

The outage af
New York City

NBC NEWS SECTIONS NIGHTLY NEWS MSNBC MEET THE PRESS DATELINE TODAY

BUSINESS > TRAVEL

CONSUMER ECONOMY PERSONAL FINANCE MARKETS

NEWS
AUG 8 2016, 5:41 PM ET

Delta Warns of Chaos After Power Outage, Worldwide System Failure

by ALASTAIR JAMIESON, SHAMAR WALTERS, KURT CHIRBAS and GABE GUTIERREZ

SHARE
Share
Tweet
Share
Email
Print
Comment

Delta flights grounded worldwide due to computer outage
1:26

Tens of thousands of Delta passengers around the world were stranded Monday after a power outage at its Atlanta headquarters caused a global computer failure that halted all flights.

Check-in systems, airport screens and even the airline's website and smartphone apps were affected by the meltdown, which began at 2:38 a.m. ET and lasted six hours.

The airline suspended departures, with airport agents writing out boarding passes by hand. "Our systems are down everywhere," it told customers on Twitter.

Related: After the Glitch: What to Do if You're Flying Delta This Week

The outage ended at about 8:30 a.m. ET, with "limited" resumption of flights. By 1:30 p.m. ET, some 451 flights had been canceled and less than 1,700 of its 6,000 scheduled flights were in operation, the airline said.

CBS News / CBS Evening News / CBS This M

CBS

By JAIME HOLGUI

Bigg
histo

The dark Manhatta
power outage hit m

Comment /

Power is comi
which hit Thu
history.

The outage af
New York City

NBC NE

BUSINESS > TRAV

NEWS
AUG 8 2016, 5:41 PM ET

SHARE
Share
Tweet
Share
Email
Print
Comment

TV RADIO NEWS SPORTS MUSIC LIFE ARTS LOCAL MORE WATCH LISTEN LOG IN

CBCnews | Technology & Science

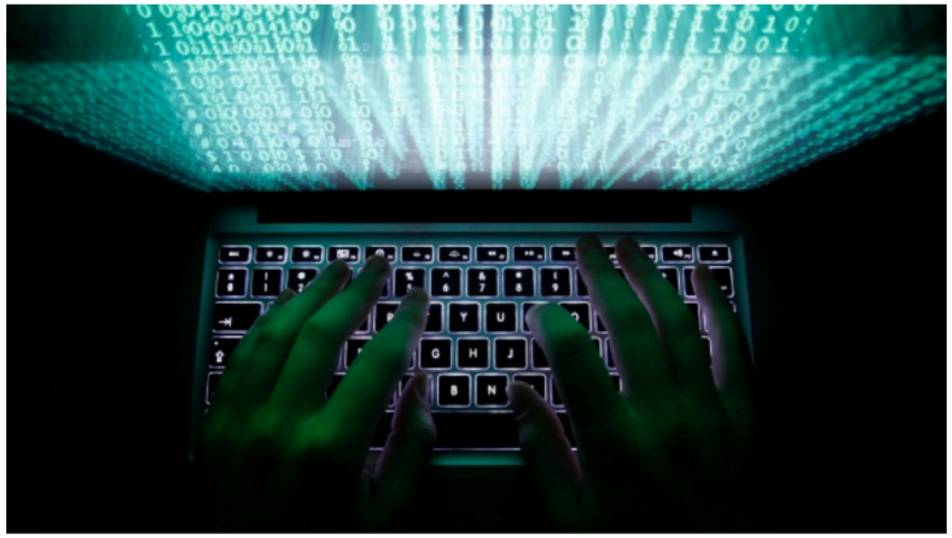
Home | Opinion | World | Canada | Politics | Business | Health | Entertainment | Technology & Science | Video

Technology & Science | Quirks & Quarks Blog | Spark | Photo Galleries

Hackers used 'internet of things' devices to cause Friday's massive DDoS cyberattack

Hackers say the attacks, which affected major sites like Twitter, Netflix and PayPal, were just a dry run

The Associated Press Posted: Oct 22, 2016 3:52 PM ET | Last Updated: Oct 22, 2016 4:15 PM ET



Friday's DDoS attackers now have a secret weapon in the increasing array of internet-enabled household devices they can subvert and use to wreak havoc. (Kacper Pempel/Reuters)

Facebook
Twitter
Reddit

Could millions of connected cameras, thermostats and kids' toys bring the internet to its knees? It's beginning to look that way.

On Friday, epic cyberattacks crippled a major internet firm, repeatedly disrupting the availability of popular websites across North America and Europe such as Twitter, Netflix and PayPal.

Stay Connected with CBC News

Mobile Facebook Podcasts Twitter Alerts Newsletter

Top News Headlines

- Porter Airlines grounds all flights, citing system outage
- In facing the public, will Trudeau go beyond talking points?: Aaron Wherry 906
- Here's what really happens to all those gifts you return to the store 277
- Jennifer Holliday latest to pull out of Trump inauguration amid overwhelming backlash
- 'Apartheid system' of reserves to blame for Innu suicides: Quebec coroner

Latest Technology & Science News Headlines

- Scientists call for tri-national conservation

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

CBS News / CBS Evening News / CBS This M

CBS

By JAIME HOLGUI

Bigg
histo

The dark Manhatta
power outage hit m

Comment /

Power is comi
which hit Thu
history.

The outage af
New York City

NBC NE

BUSINESS > TRAV

NEWS
AUG 8 2016, 5:41 PM ET

SHARE
Share
Tweet
Share
Email
Print
Comment

TV RADIO

CBCnew

Home Opinion
Technology & Scien

Hacker
massiv

Hackers say the
The Associated Pres

Friday's DDoS attack
they can subvert and

Facebook
Twitter
Reddit

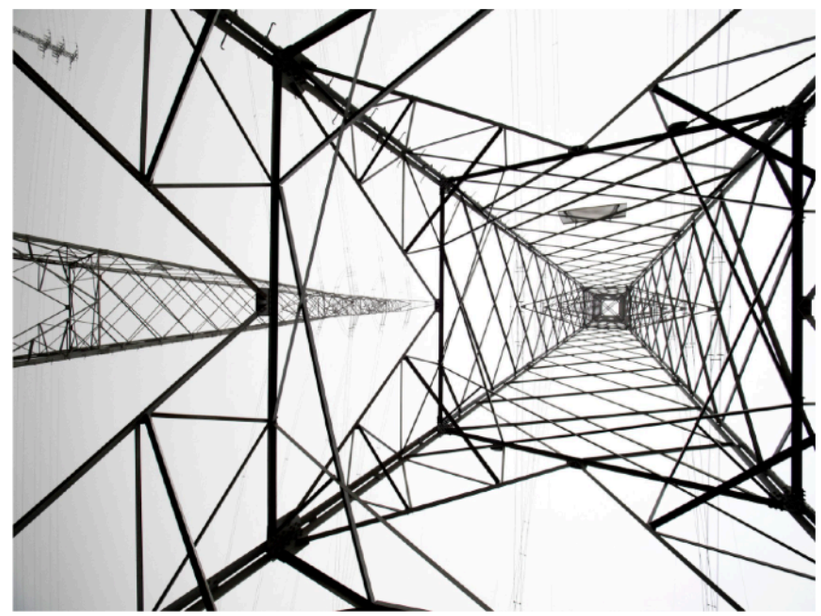
WIRED Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid SUBSCRIBE

BUSINESS CULTURE DESIGN GEAR SCIENCE SECURITY TRANSPORTATION

SHARE
SHARE 1232
TWEET
PIN 2
COMMENT 97
EMAIL

KIM ZETTER SECURITY 03.03.16 7:00 AM

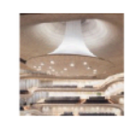
INSIDE THE CUNNING, UNPRECEDENTED HACK OF UKRAINE'S POWER GRID



JOSE A. BERNAT BACET/GETTY IMAGES

IT WAS 3:30 p.m. last December 23, and residents of the Ivano-Frankivsk region of Western Ukraine were preparing to end their workday and head home through the cold winter streets. Inside the Prykarpattyaoblenergo control center, which distributes power to the region's residents, operators too were nearing the end of their shift. But just as one worker was organizing papers at his

MOST POPULAR



ARCHITECTURE
What Happens When Algorithms Design a Concert Hall? The...
2 DAYS

GAMING
Nintendo's Boss Promises the Switch Won't Have the NES Classic's Supply...
22 HOURS

WIRED OPINION
How America Can Beat Russia in Cyber War, Despite Trump
11 HOURS

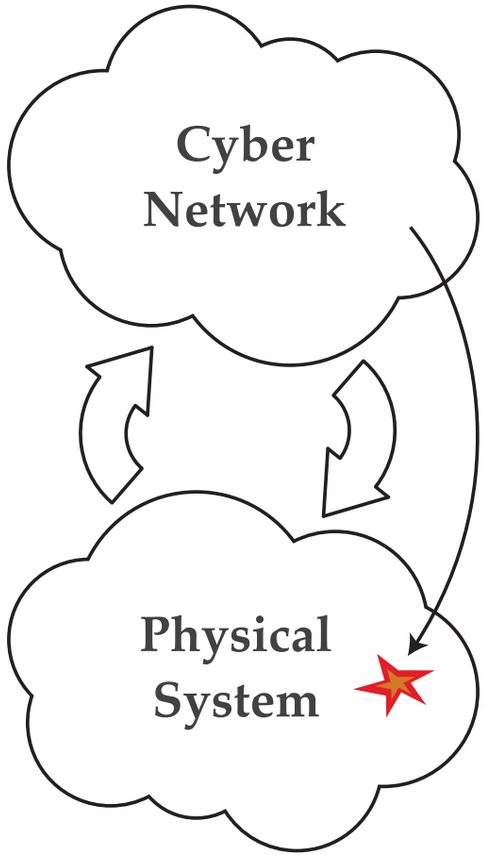
MORE STORIES

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Objective

- We propose a model for the ***graceful degradation*** of **cyber-physical systems** while subject to persistent attacks from an adversary

We are interested in modeling, and defending against, **cyber attacks that trigger physical contingencies.**



FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

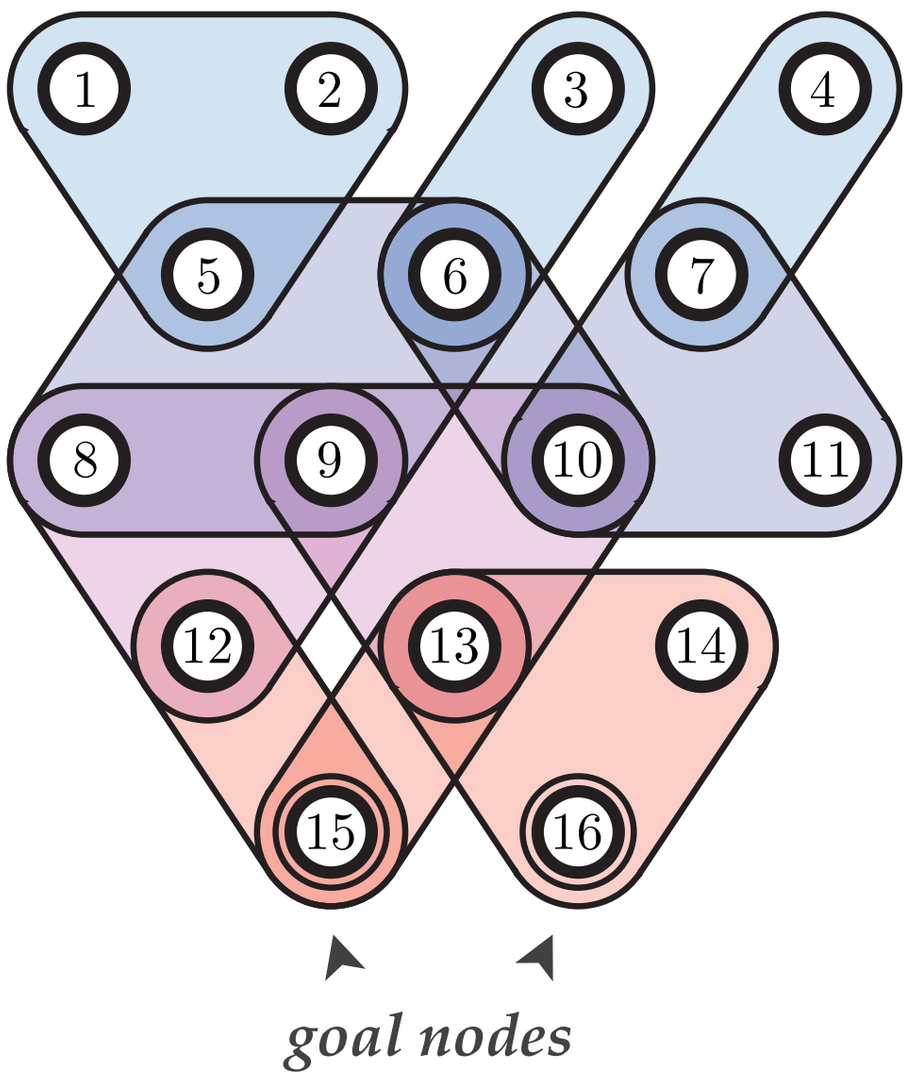
Cyber-physical Systems

1. **Cyber network**
   - Forms the computational, comm., and control structure of the system
2. **Physical infrastructure**
   - Represents the physical network of connections, switches, and sensors
   - Dynamics of the (continuous) **physical state** x_t are dictated by laws of nature

tightly integrated at all time-scales and levels

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

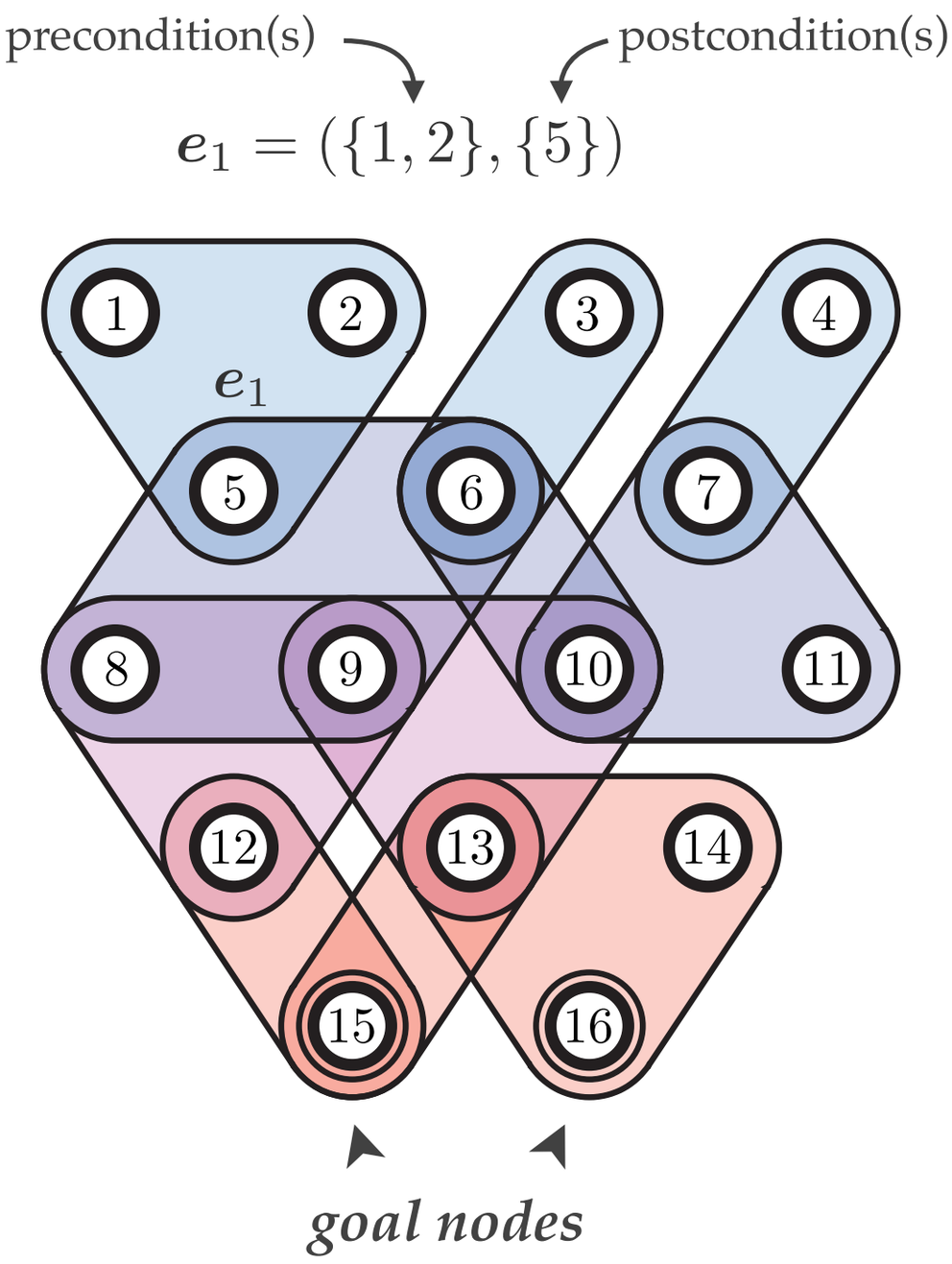
Cyber Layer



- Attacks are modeled using a dependency graph
  - **Nodes:** attacker capabilities
  - **Edges:** exploits

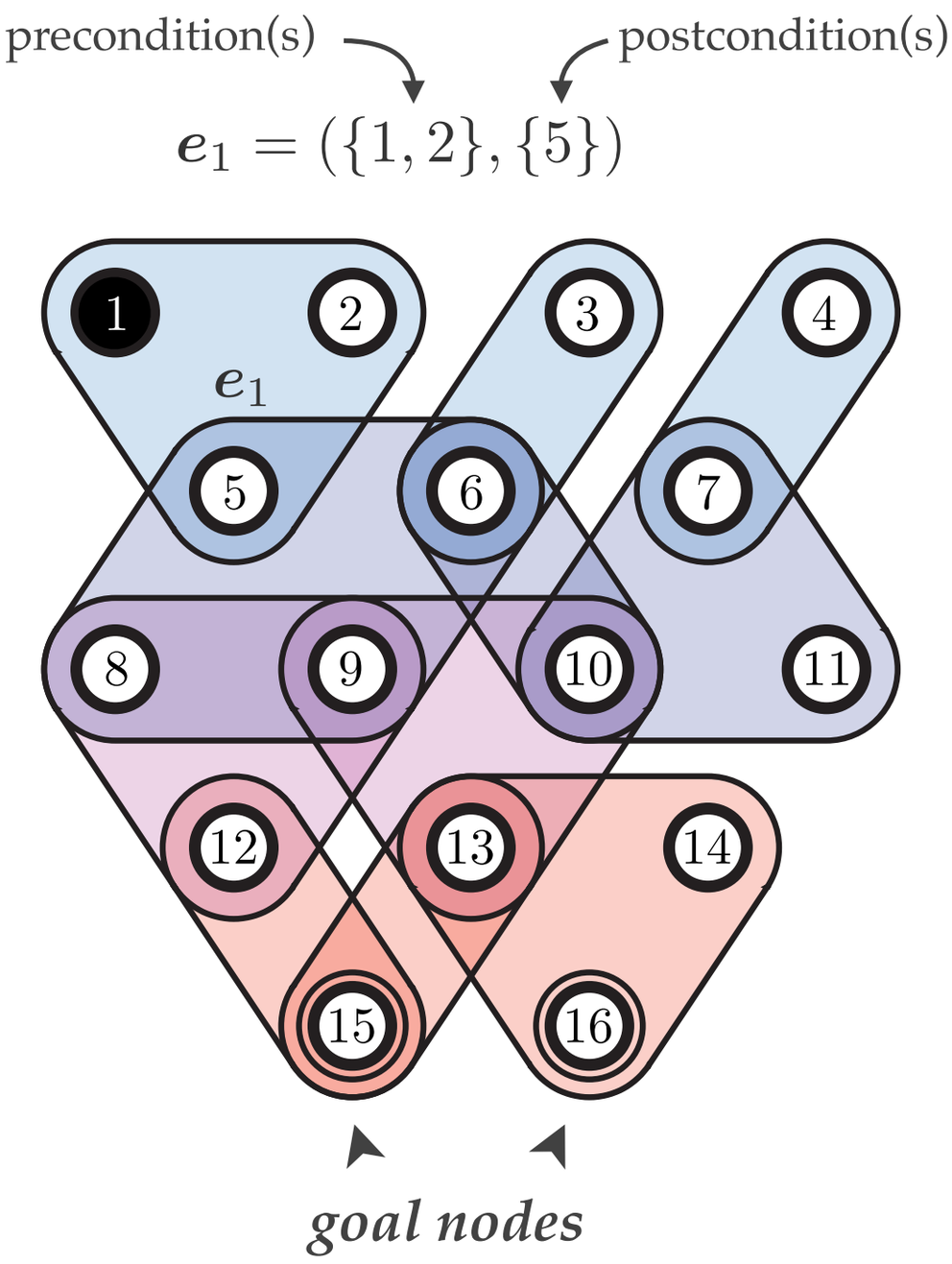
FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Cyber Layer



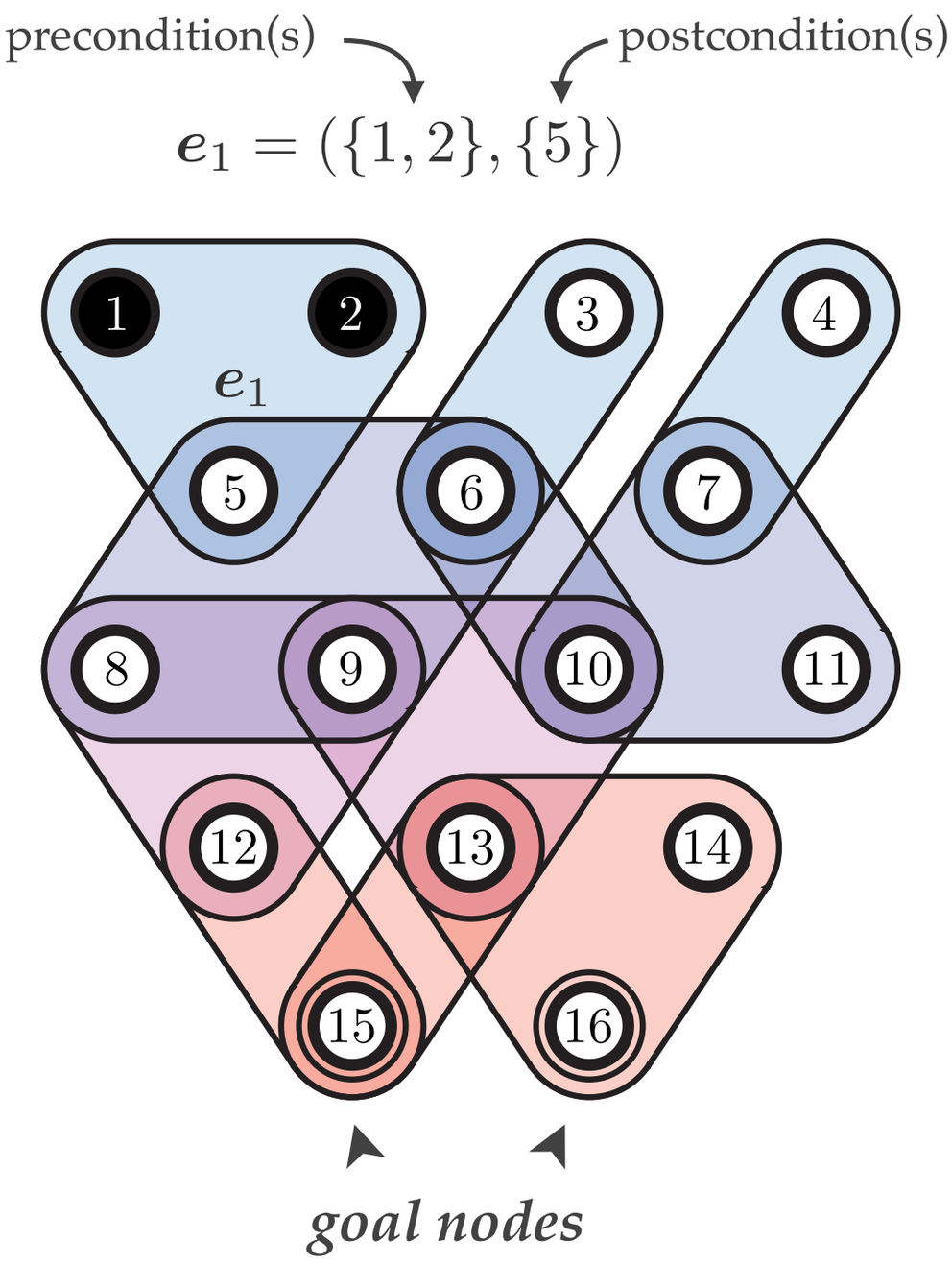
- Attacks are modeled using a dependency graph
  - **Nodes:** attacker capabilities
  - **Edges:** exploits

Cyber Layer



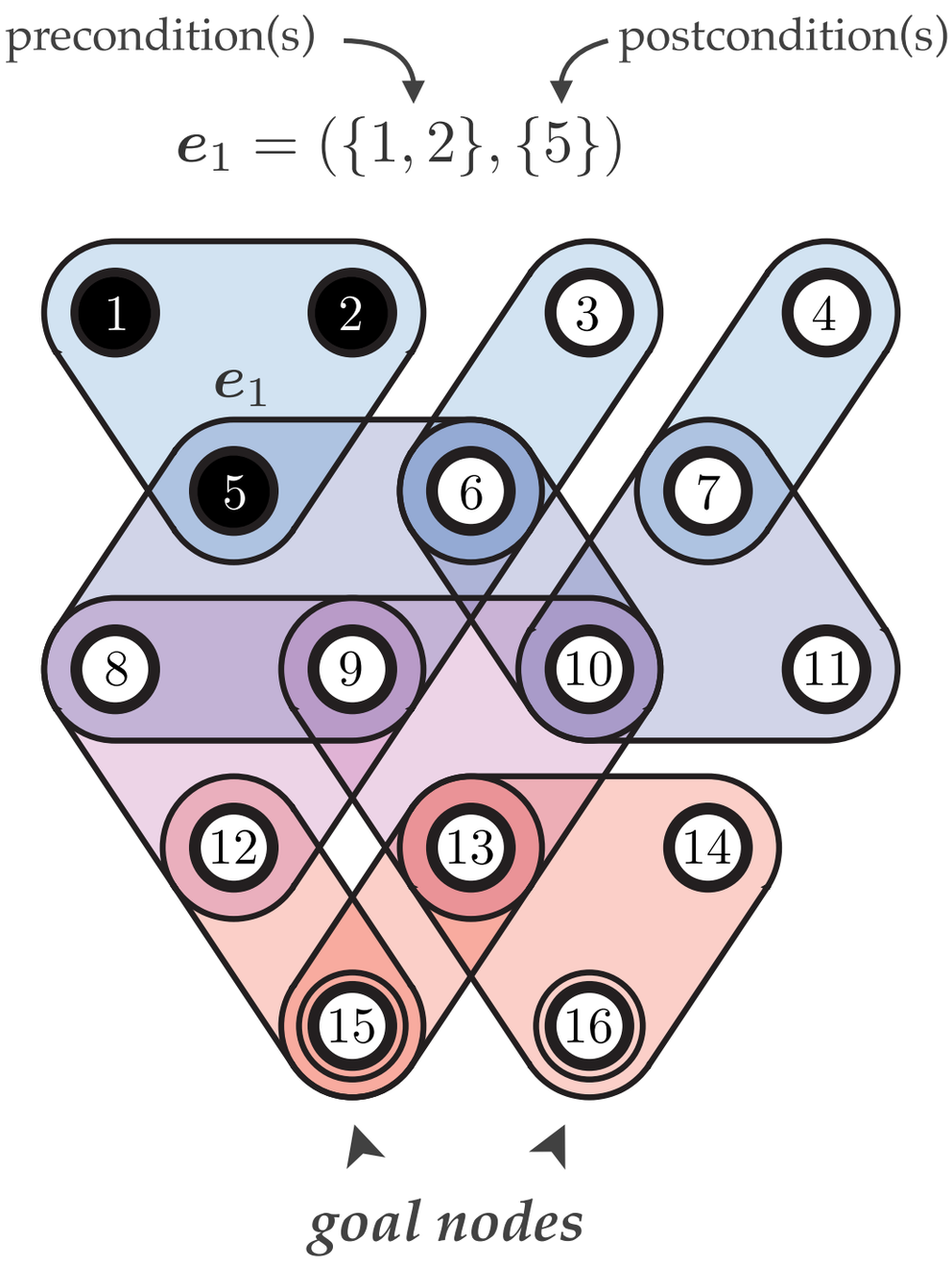
- Attacks are modeled using a dependency graph
  - **Nodes:** attacker capabilities
  - **Edges:** exploits

Cyber Layer



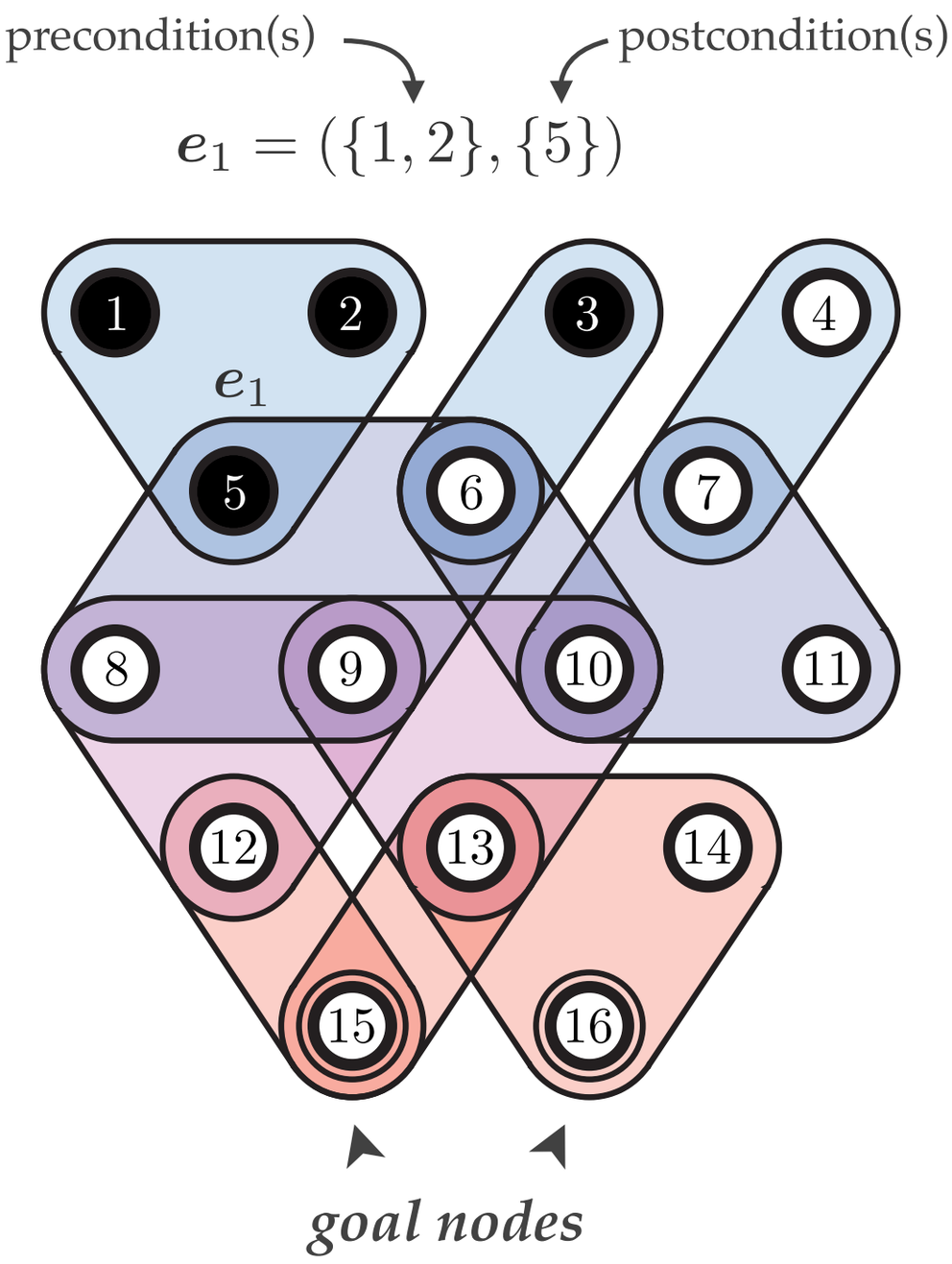
- Attacks are modeled using a dependency graph
  - **Nodes:** attacker capabilities
  - **Edges:** exploits

Cyber Layer



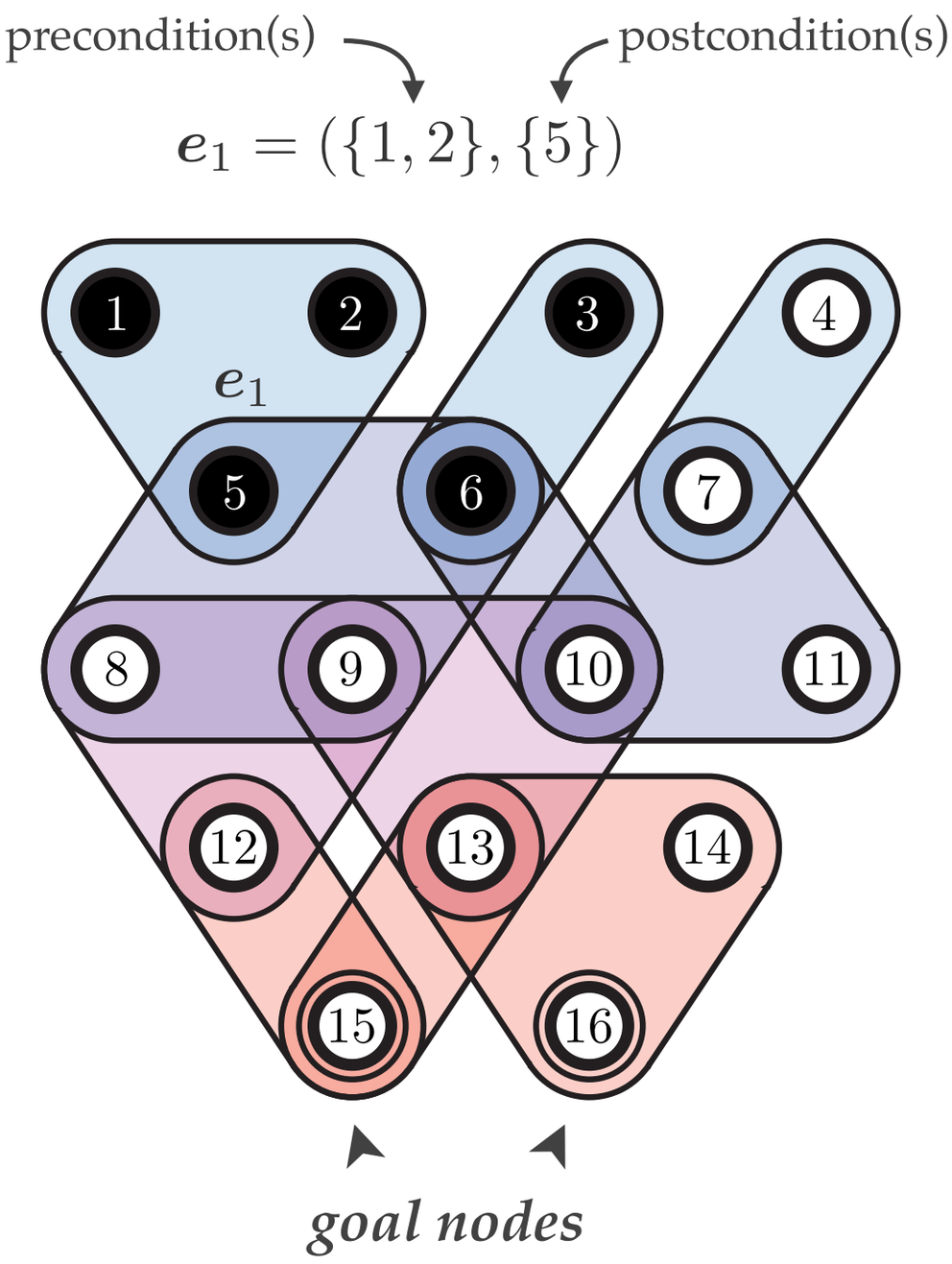
- Attacks are modeled using a dependency graph
  - **Nodes:** attacker capabilities
  - **Edges:** exploits

Cyber Layer



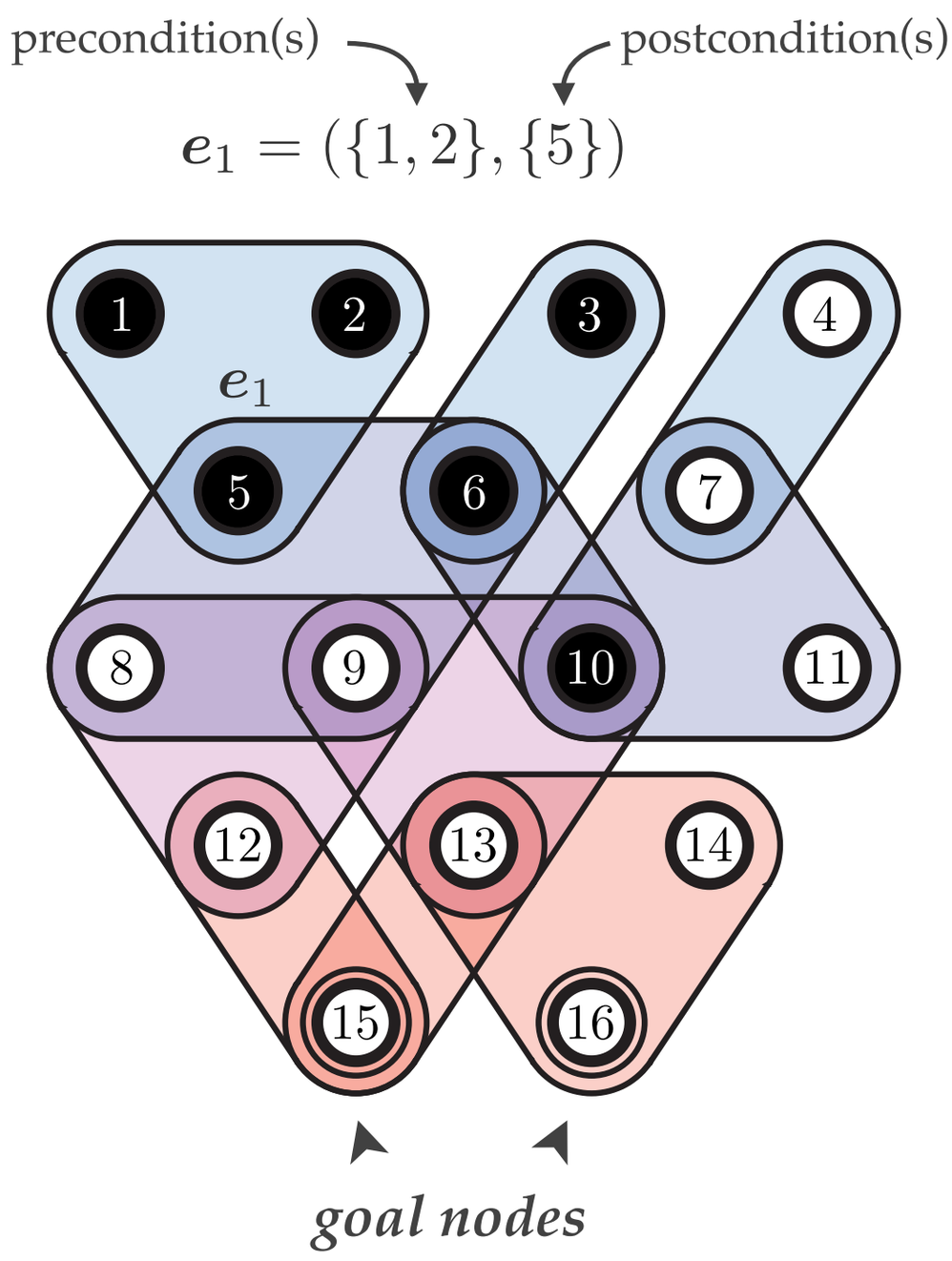
- Attacks are modeled using a dependency graph
  - **Nodes:** attacker capabilities
  - **Edges:** exploits
- Successive exploits allow the attacker to progress through the network, captured by the **security state,** s_t

Cyber Layer



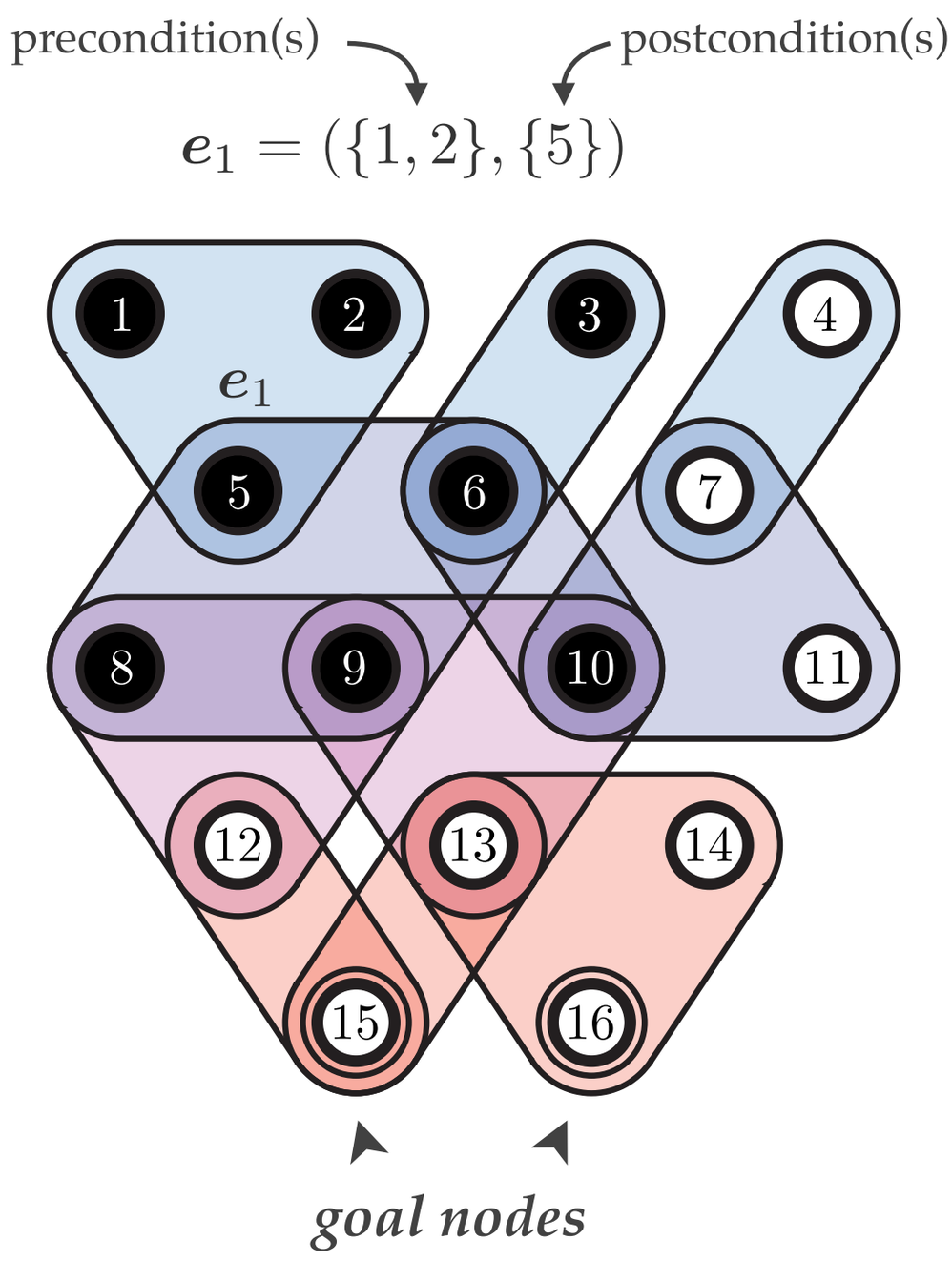
- Attacks are modeled using a dependency graph
  - **Nodes:** attacker capabilities
  - **Edges:** exploits
- Successive exploits allow the attacker to progress through the network, captured by the **security state,** s_t

Cyber Layer



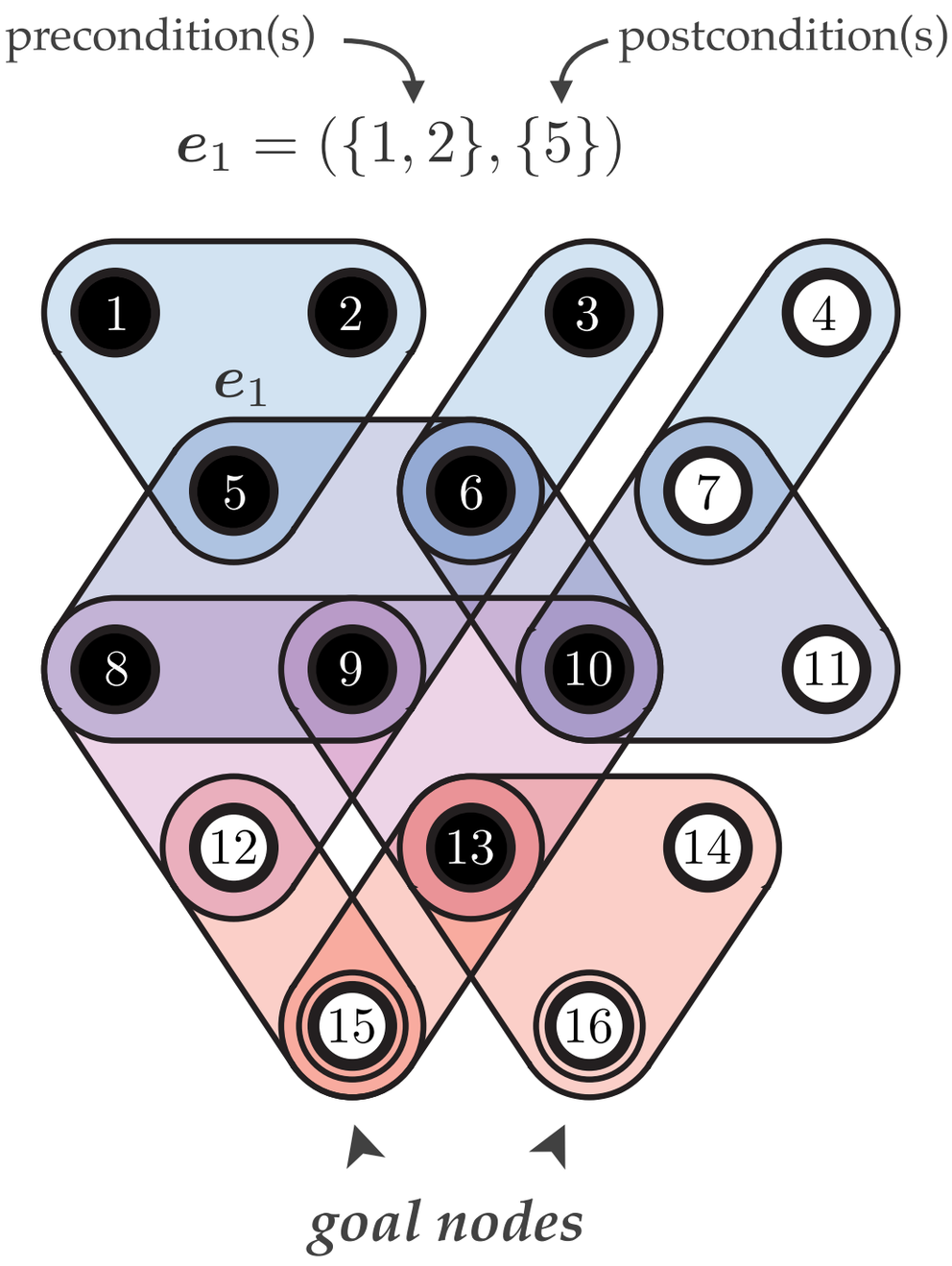
- Attacks are modeled using a dependency graph
  - **Nodes:** attacker capabilities
  - **Edges:** exploits
- Successive exploits allow the attacker to progress through the network, captured by the **security state,** s_t

Cyber Layer



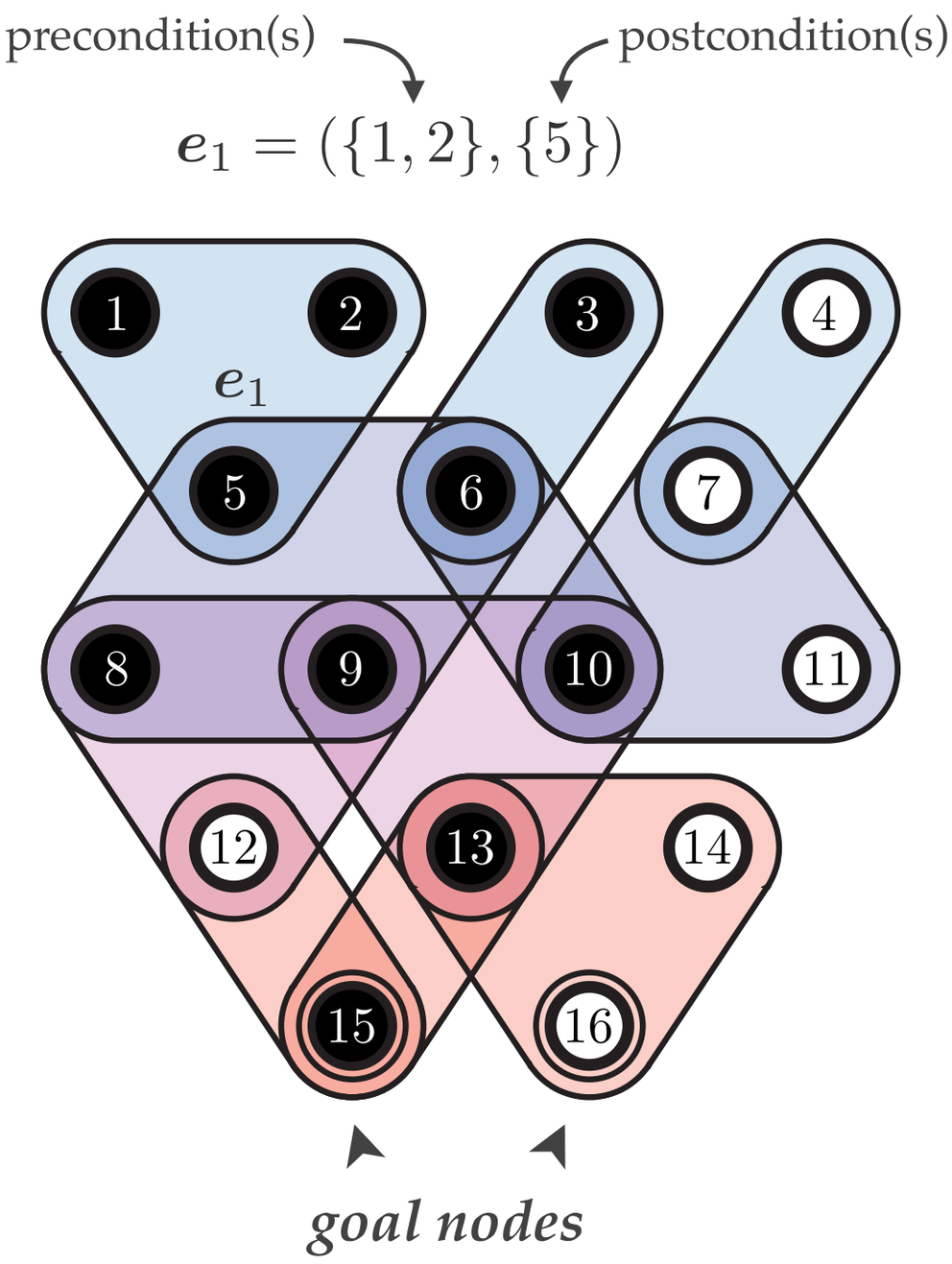
- Attacks are modeled using a dependency graph
  - **Nodes:** attacker capabilities
  - **Edges:** exploits
- Successive exploits allow the attacker to progress through the network, captured by the **security state,** s_t

Cyber Layer



- Attacks are modeled using a dependency graph
  - **Nodes:** attacker capabilities
  - **Edges:** exploits
- Successive exploits allow the attacker to progress through the network, captured by the **security state,** s_t

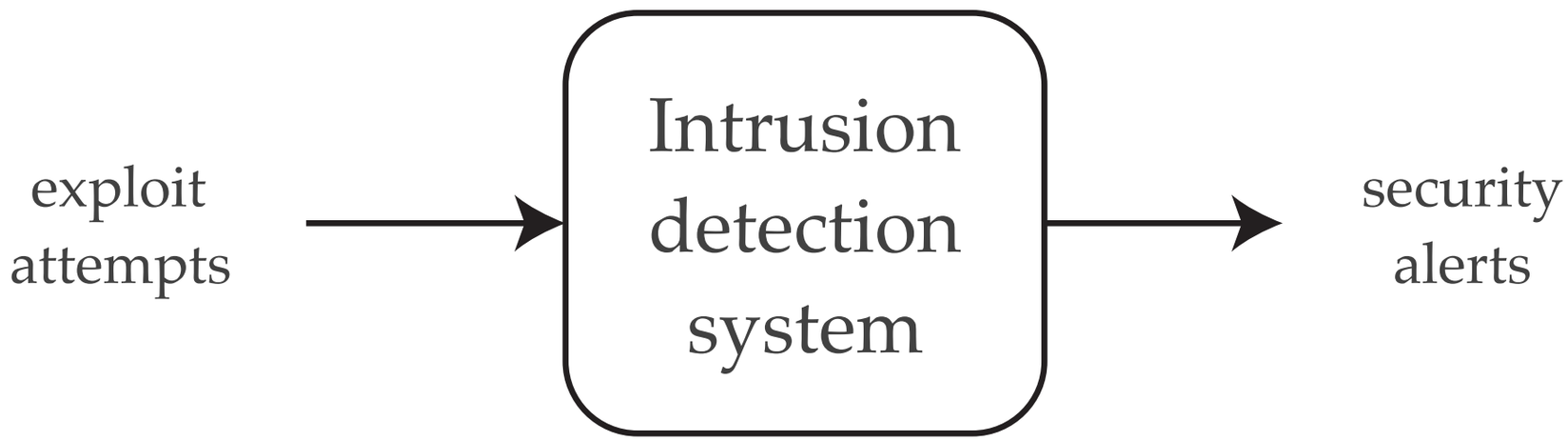
Cyber Layer



- Attacks are modeled using a dependency graph
  - **Nodes:** attacker capabilities
  - **Edges:** exploits
- Successive exploits allow the attacker to progress through the network, captured by the **security state,** s_t

Defender's Information

- The defender does not know the **security state,** s_t, with certainty

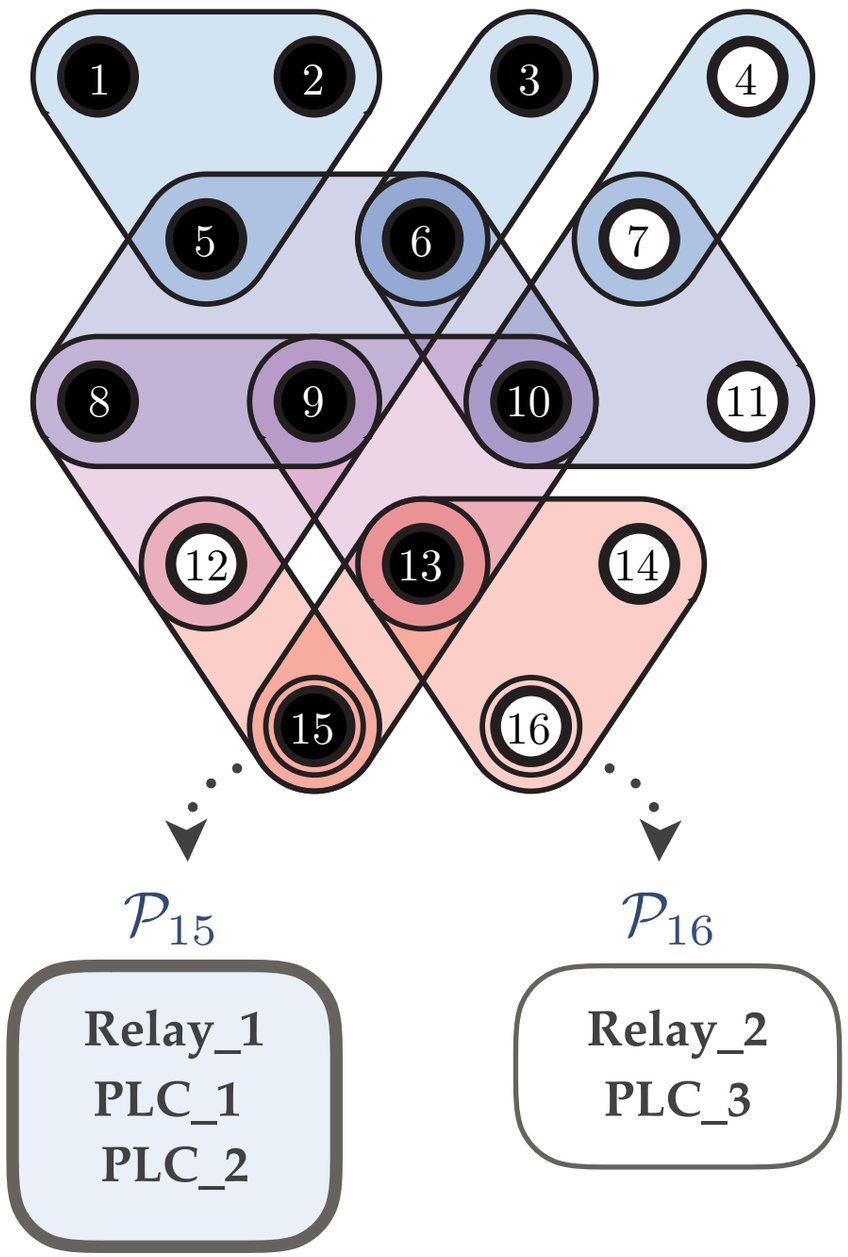


- Furthermore, the defender must estimate the **physical state,** x_t, using data from sensors

Goal Nodes

- Enabled goal conditions give the attacker **physical capabilities**

$\mathcal{P}_i$: **physical elements that the attacker can influence from i**

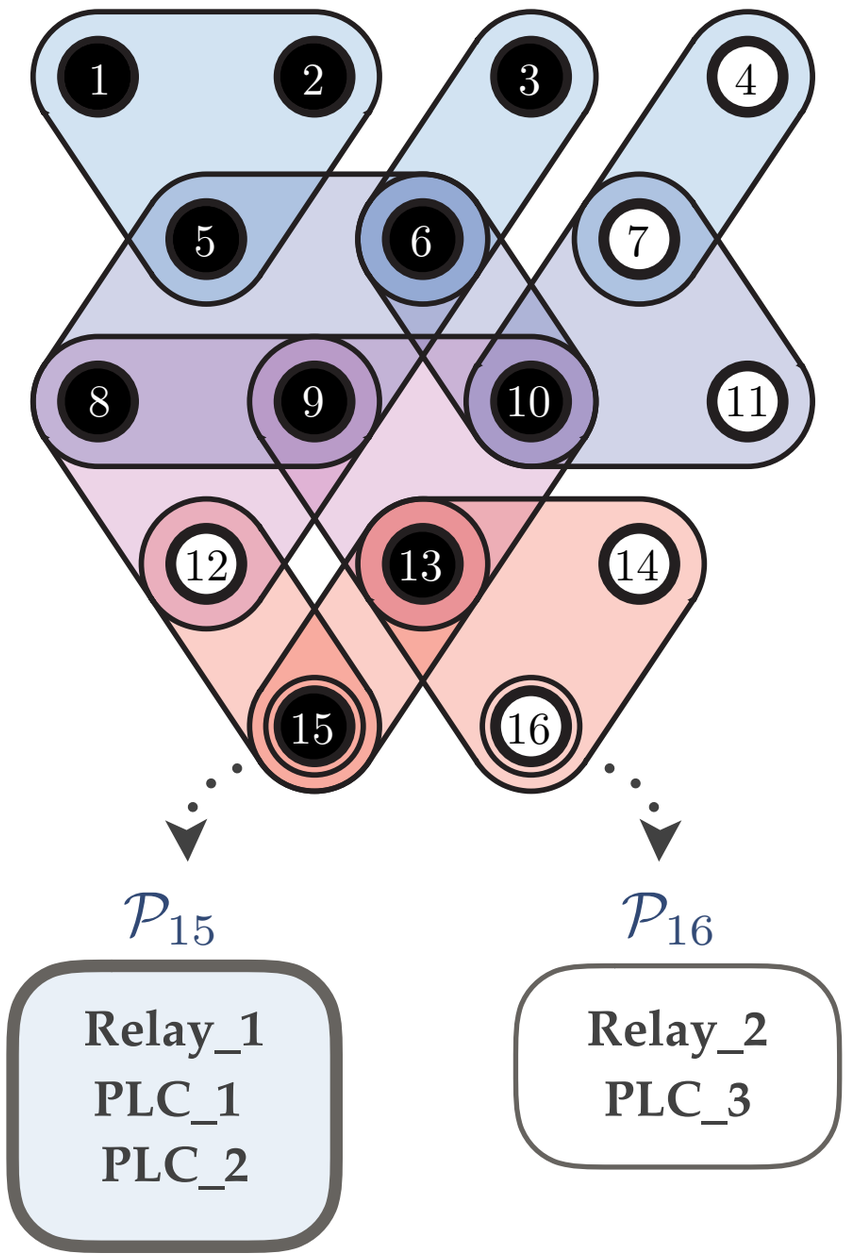


Goal Nodes

- Enabled goal conditions give the attacker **physical capabilities**

  $\mathcal{P}_i$: **physical elements that the attacker can influence from i**

- Attacker can then trigger **physical failures**
  - Severity is dependent upon the current **physical state, x_t**



FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Operating Modes

- The defender wishes to continue to operate the system, at reduced performance, while it is under attack
- Define set of **operating modes,** $\mathcal{M}$,
- Each operating mode $m \in \mathcal{M}$ defines a structure for:

cyber network

- port connectivity, active services, trust relationships

$\xRightarrow[\text{analysis}]{\text{vulnerability}}$ dependency graph

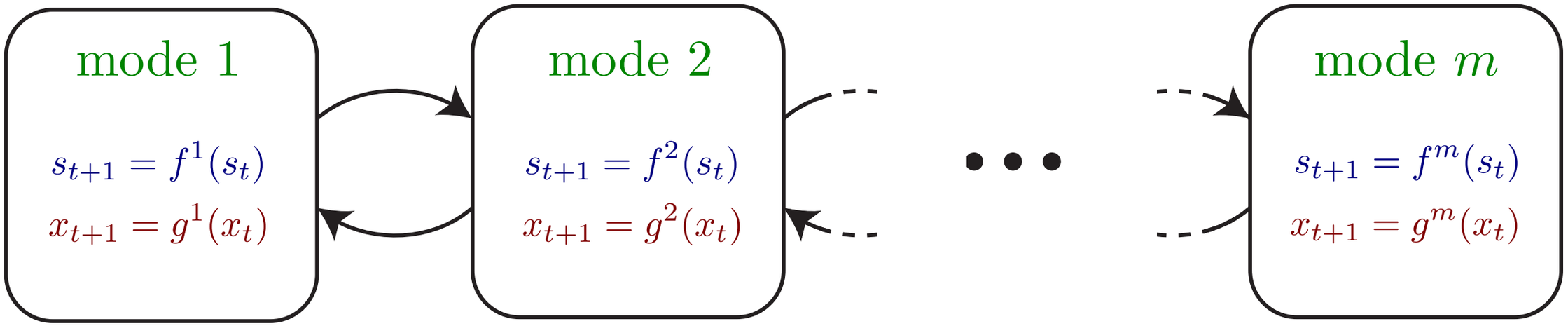
physical network

- status of relays, breakers, sensors, valves

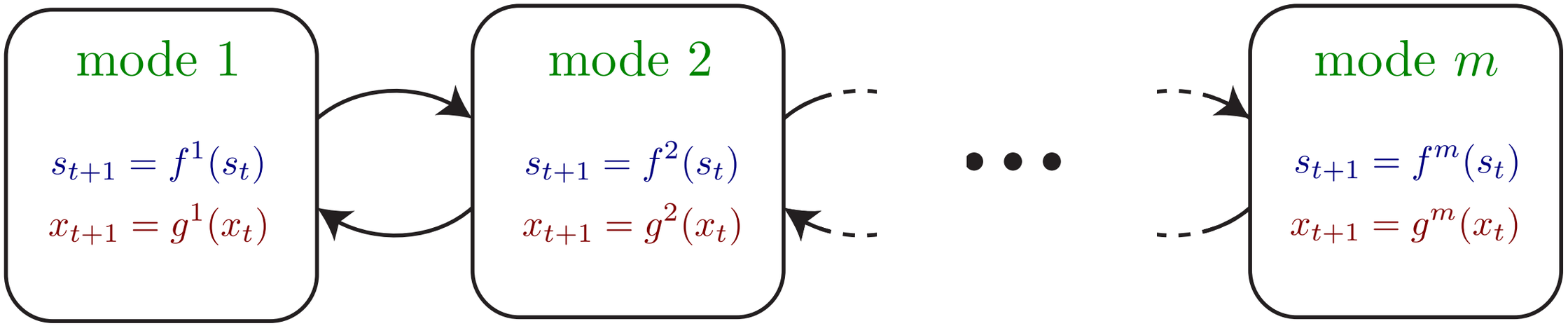
$\Rightarrow$ physical network topology

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Operating Modes



Operating Modes



- **Defense Problem:** The defender uses its belief of (s_t, x_t) to **control** the transitions between **operating modes**
  - The defender is attempting to maximally interfere with the progression of the attacker while maintaining functionality of the network

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Ongoing Work

- Past work on the **defense of cyber networks**
  - *E. Miehling, M. Rasouli, and D. Teneketzis.* **Optimal Defense Policies for Partially Observable Spreading Processes on Bayesian Attack Graphs** (MTD Workshop — CCS 2015)
  - *E. Miehling, M. Rasouli, and D. Teneketzis.* **A POMDP Approach to Autonomic, Dynamic Defense of Large-Scale Cyber Networks** (to be submitted to IEEE Transactions on Information Forensics and Security)
- Current work is focused on **integrating the physical system**

Summary

- The model allows us to relate attacker capabilities to spatial regions of the physical infrastructure
- The **security state** tells us likely physical contingencies and, coupled with the **physical state**, the severity of the potential damage
- Controlling the **operating mode** decreases the chances that the attack will succeed ***and*** ensures that the system is prepared for any contingencies

Acknowledgments

- Special thanks to the following funding sources

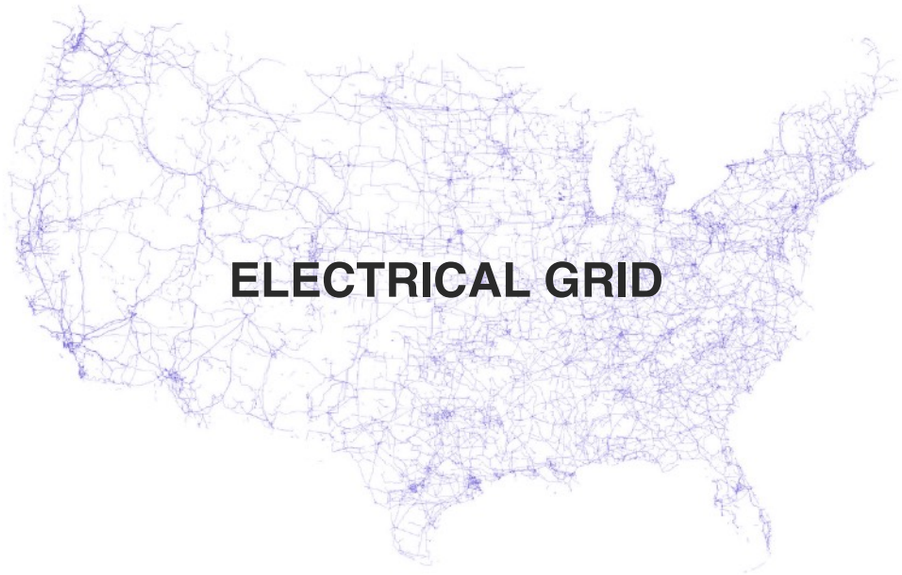
- **NSF —** Foundations Of Resilient CybEr-physical Systems (FORCES)

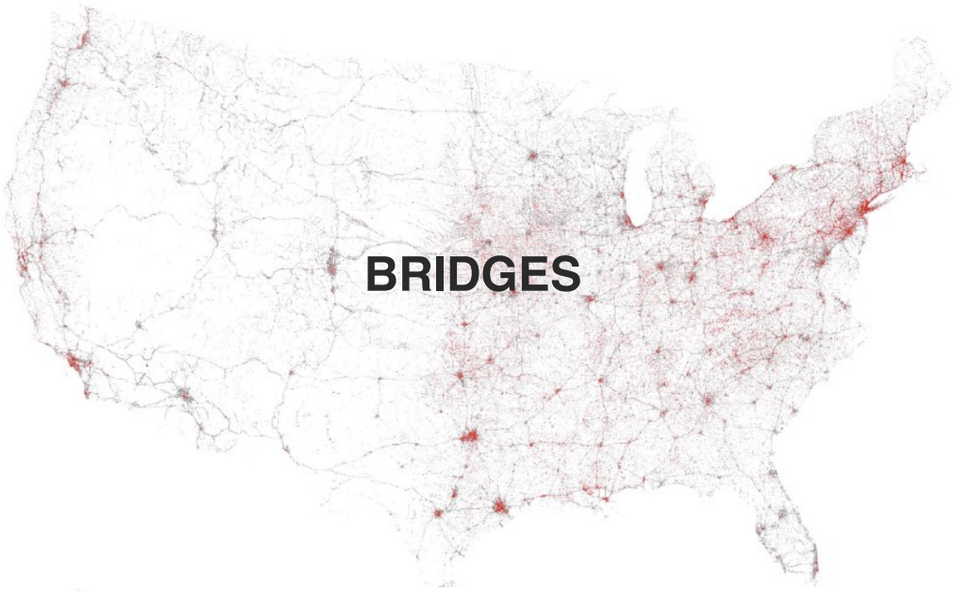
  Grant: CNS-1238962

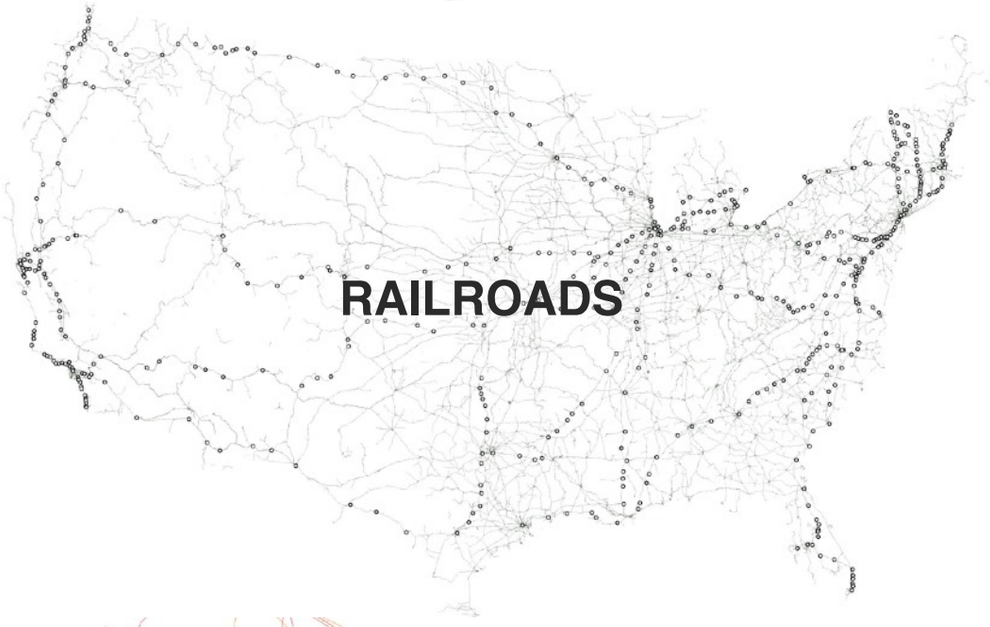
- **ARO MURI —** Adversarial and Uncertain Reasoning for Adaptive Cyber Defense: Building the Scientific Foundations

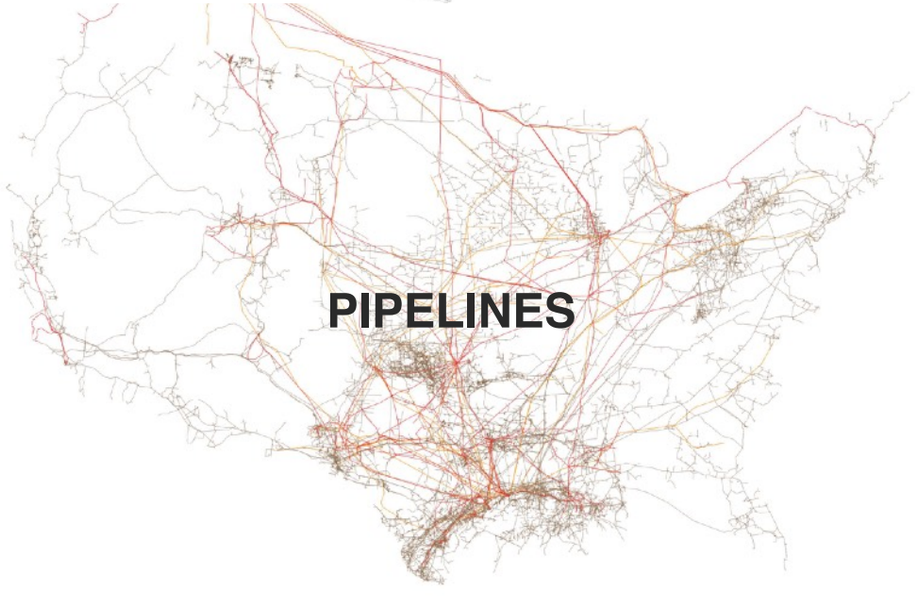
  Grant: W911NF-13-1-0421

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS









Tim Meko, “Six maps that show the anatomy of America’s vast infrastructure,” The Washington Post, 2017