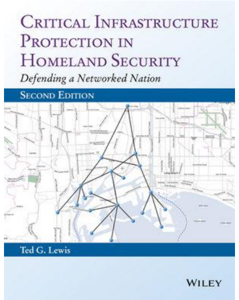
Selected aspects of critical infrastructure security and resilience.

Gkioulos Vasileios
Norwegian Information Security laboratory-NISlab,
NTNU i Gjøvik: Norwegian University of Science and Technology
Department of Information Security and Communication Technology

Theory and foundations



Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation

Ted G. Lewis

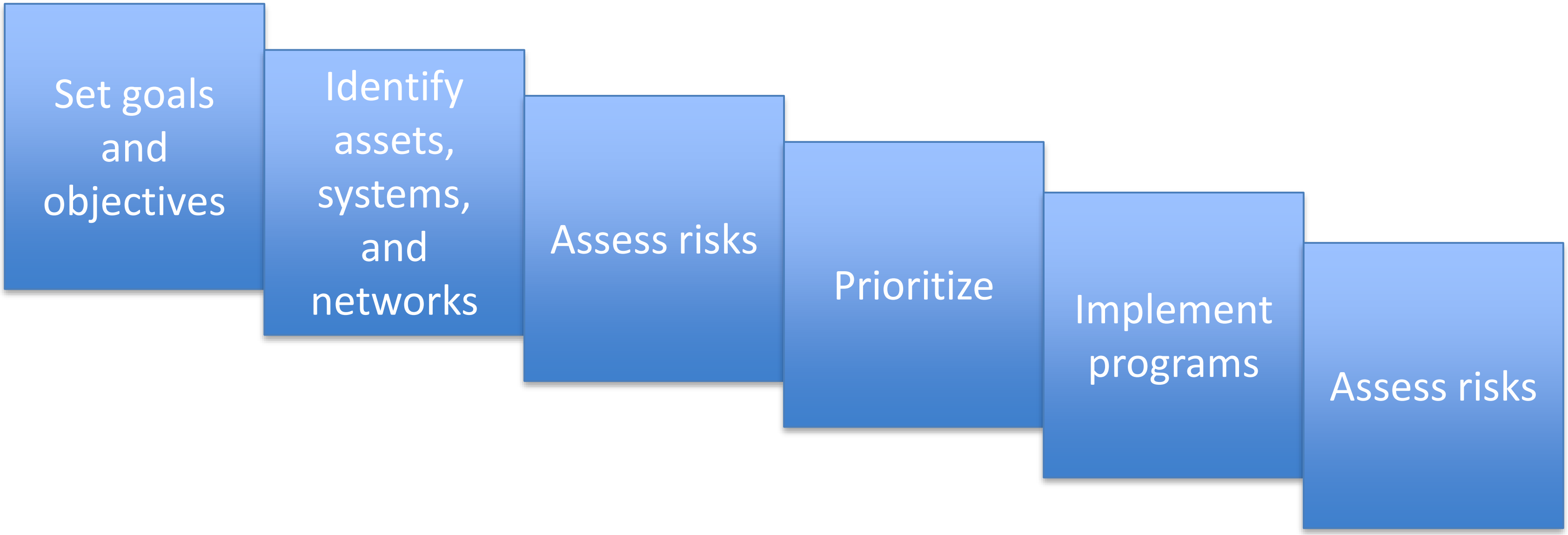
Risk Informed Decision Making

- Given limited resources, how should funding be allocated in order to reduce risk?

  – Risk: The potential of an unwanted outcome resulting from an incident, event, or occurrence, as determined by its likelihood and the associated consequences.

  – Risk informed decision making: The determination of a course of action predicated on the assessment of risk, the expected impact of that course of action on that risk, and other factors.

Continuous improvement feedback



Set goals and objectives

Identify assets, systems, and networks

Assess risks

Prioritize

Implement programs

Assess risks

Continuous improvement feedback

- Set goals and objectives
  - This may range from the reduction of consequences to the elimination of risk.
- Identify assets, systems, and networks
  - Some are easy to identify, but most of the times we are referring to complex systems.
- Assess Risks
  - A variety of methods exists
    - Probabilistic risk assessment:

      Risk=Threat*Vulnerability*Consequence
    - Natural disasters:

      Risk=ProbabilityOfOccurence (based on historical data)*Consequence

Continuous improvement feedback

- Prioritize
  - A variety of methods exist
    - Highest consequence
    - Most vulnerable
    - Highest risk
    - Highest return on investment
    - Highest increase in resilience
- Implement programs
  - The outputs of the previous steps guide the investments that happen here

Continuous improvement feedback

- Measure effectiveness
  - The effectiveness of the investments must be measured and used for future assessments.

$$\text{Return on Investment} = \frac{\text{Risk Before} - \text{Risk After}}{\text{€Investment}}$$

Resilience

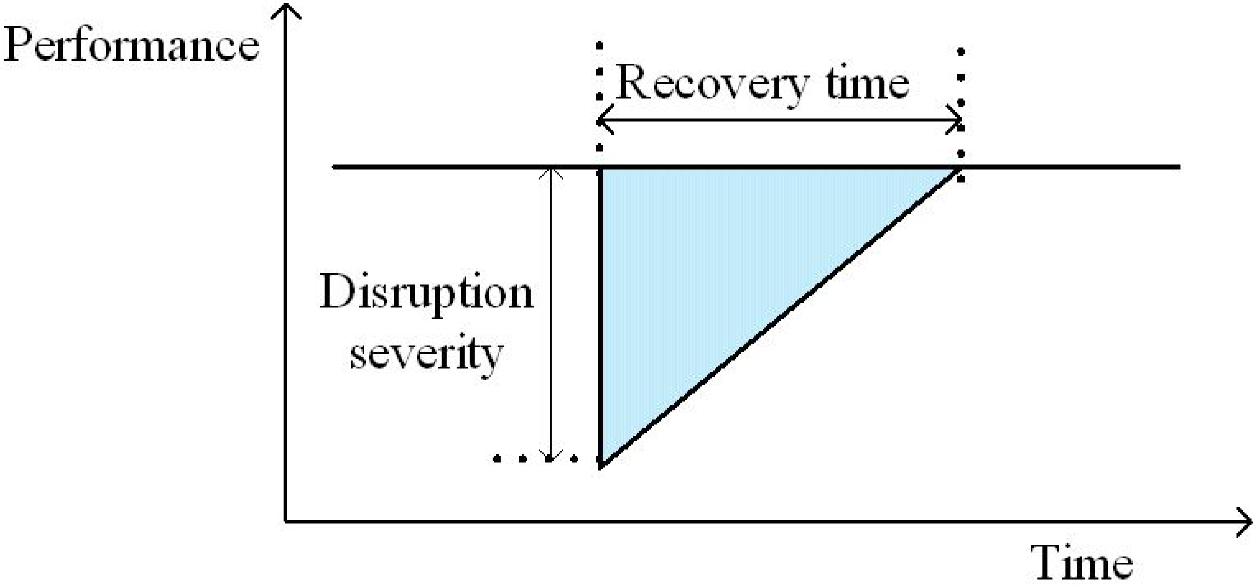
Given the occurrence of a particular disruptive event (or set of events), the resilience of a system to that event (or events), is the ability to efficiently reduce:

1. the magnitude
2. the duration

from targeted system performance levels

Resilience (The triangle)

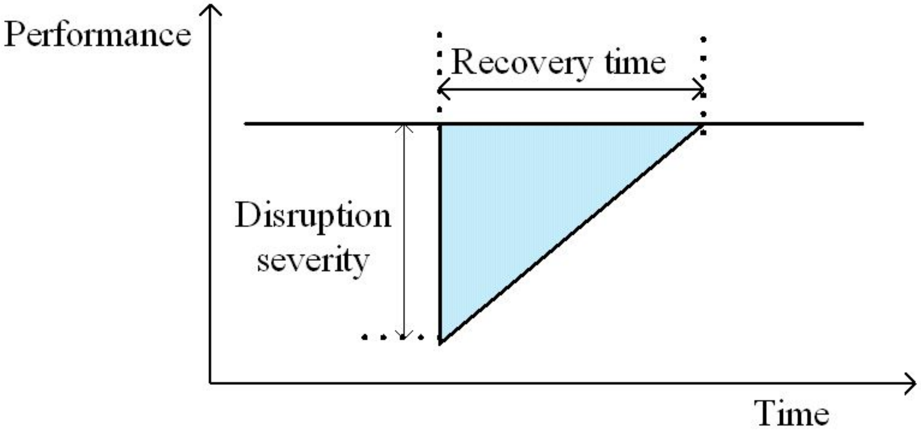
Damage to a system in the form of magnitude and duration, is represented in a triangular (not necessarily!) area across a performance-time diagram.



Resilience (The triangle)

The area of the triangle defines the systems resilience, where smaller area translates to grater resilience. To reduce the area of the triangle:

1. Reduce the recovery time
2. Reduce the drop in performance
3. Reduce both



Resilience (The triangle)

A note of caution!

This is sufficient for single assets or simple systems

BUT

Cannot capture complex interdependent systems such as the power grid or communication networks

Yet another definition for resilience > The ability to resist, absorb, recover from, or successfully adapt to adversity or a change in conditions.

Prevention or response?

How much should we invest to response versus prevention?

Prevention only > spent money to deter and prevent damage

Response only > Invest money in increasing the response capacity

Prevention or response?

We can answer by classifying hazards according to their risk:

- High > As consequence approaches infinity, risk also approaches infinity.
- Low > As consequence approaches infinity, risk approaches zero
- Complex …

NOTE: Consequence can be measured in different units (e.g. money, life etc)

Prevention or response?

The best risk informed strategy might depend on the profile of the hazard

Apply more resources on prevention of high risk hazards, and more resources on response for low risk hazards.

Risk Strategies

- Risk analysis has been developed the past 250 years in order to estimate the potential for financial loss in games of chance.

<u>Core concept</u>

Risk is the expected loss or gain

under uncertainty

Expected Utility Theory / 1738

Daniel Bernoulli (1700-1782)

Risk is the probability of a certain outcome and its consequence

$$R=Pr(c)C$$

Pr(c)= The probability of loosing C euro

C= The loss of C euro

Expected Utility Theory / 1738

When n independent events are possible, risk is the sum of all expected values:

$$Risk=Pr(c1)C1+Pr(c2)C2+\ldots+Pr(cn)Cn$$

Note of caution - 1

Risk is not a probability, and probability is not a risk!

But: The elements of risk are:

1. Likelihood: As measured by a probability
2. Gain /loss: As measured by a concequence

Note of caution - 2

Risk is not a vulnerability or a treat

- Vulnerability is a weakness in an asset that may be exploited in order to cause damage.
    - Can be quantified as a probability but it is not a risk, as it is not an expected gain or loss.
- Threat is a potential to do damage.
    - Can be quantified as a probability but it is not a risk,

      as it is not an expected gain or loss.

A more modern approach

- Threat: Natural or man-made occurrence, individual entity, or action that has or indicates the potential to harm life, information, operations, the environment and/or property.
- Vulnerability: Physical feature or operational attribute that renders an asset likely to fail due to a given hazard-The probability of failure if attacked or subjected to the threat.
- Consequence: The effect of an event, incident, or occurrence-Damages due to a failure, typically measured in money, casualties, or lost time.

A more modern approach

- Threat: Natural or man-made occurrence, individual entity, or action that has or indicates the potential to harm life, information, operations, the environment and/or property.
- Vulnerability: Physical feature or operational attribute that renders an asset likely to fail due to a given hazard-The probability of failure if attacked or subjected to the threat.
- Consequence: The effect of an event, incident, or occurrence-Damages due to a failure, typically measured in money, casualties, or lost time.

A more modern approach

- Threat: Natural or man-made occurrence, individual entity, or action that has or indicates the potential to harm life, information, operations, the environment and/or property.
- Vulnerability: Physical feature or operational attribute that renders an asset likely to fail due to a given hazard- The probability of failure if attacked or subjected to the threat.
- Consequence: The effect of an event, incident, or occurrence-Damages due to a failure, typically measured in money, casualties, or lost time.

A more modern approach

- Accordingly we can compute the risk, and quantify the expected loss due to an event caused by a threat applied to a specific asset, as:

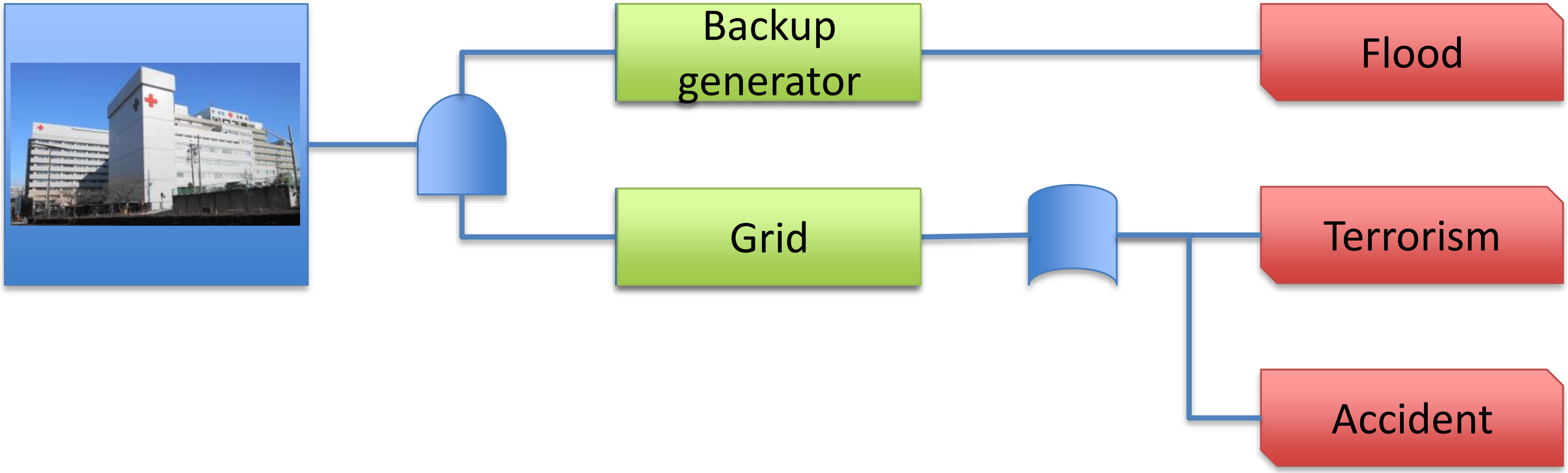
Ri=Ti*Vi*Ci

And for a collection of n threat-asset pairs:

$$R = \sum_{i=1}^{n} Ri = \sum_{i=1}^{n} Ti * Vi * Ci$$

Model Based Risk Analysis

- Note: MBRA assumes exponential diminishing returns.



Model Based Risk Analysis

Initial inputs and risk				
Threat	T(%)	V(%)	C	Elimination cost
Flood	50	50	1.000.000	100.000
Terrorism	50	50	2.000.000	1.000.000
Accident	50	50	1.000.000	200.000
Initial risk	1.000.000			

T, V = 50% representing maximum uncertainty

Initial risk =
(0,5)(0,5)1000000+(0,5)(0,5)2000000+(0,5)(0,5)1000000=
250000+500000+250000=1.000.000

Model Based Risk Analysis

Results of investment of 125.000 for securing the power infrastructure			
Threat	Allocation	Reduced V(%)	Reduced risk
Flood	44.000	8.95	44.730
Terrorism	28.500	44.70	447.300
Accident	52.550	17.90	89.460
Reduced risk	581.490	(41,85% reduction)	

$$\text{Return on Investment}=\frac{\text{Risk Before }-\text{Risk After}}{\text{€Investment}}=3{,}35\text{€/€}$$

Theories of catastrophe

Studying security of critical infrastructures, requires an understanding of the relationship between complexity and failure.

Normal Accident Theory

Extreme events occur when two or more failures occasionally come together in an unexpected way, are accelerated and increased in severity if the system is tightly coupled, while they grow to catastrophic proportions when the system has catastrophic potential.

…Domino theory.. where the size of the dominoes increases as they fail

Punctuated Equilibrium Theory

Per Bak, Chao Tang, and Kurt Wiesenfelt

Observed catastrophic collapses of a hypothetical sand pile, as a metaphor of simple systems that behave in complex ways.

Concluded that:

Incidents impacting complex systems are bursty, as they occur according to long-tailed probability distributions.

This is attributed to the systems building up self-organized criticality.

Self Organized Criticality

It generally builds up by:

Increasing efficiency and optimizations of performance, that eliminate redundancy and surge capacity.

Tragedy of the Commons

The system contains its own seed of destruction due to non-linearities, which become evident only when the system comes under stress.

TOC: The system may not be sustainable if the actions of a self-interested predator overwhelms the capacity of an underlying commons.

Collapse comes unexpectedly because of the inherent non-linear relationship between the load places on the system and the carrying capacity.

Paradox of Enrichment

A complex system becomes unstable due to an enrichment that exceeds the organic carrying capacity of the commons and destabilizes the balance between predator and prey.

Although initially such an enrichment appears to enhance the system, it ultimately leads to its collapse.

Competitive Exclusion Principle

Competitive ecosystems tend to eliminate all but one competitor, leading to a monopoly which reduces redundancy and diversity.

This can lead to reduced redundancy, as monopolies build optimized organizations and systems

Preferential Attachment

Self organization build upon and further strengthening:

1. Competitive Exclusion Principle
2. Self Organized Criticality

This creates:

1. Concentrations of assets
2. Bottlenecks
3. Single Points of Failure

Note of Caution

Accidents and minor incidents happen all the time …

…most of them are soon forgotten…

…Yet, some propagate through a system of interdependent components and magnify in intensity or severity as they spread.

Note of Caution

Therefore:

Linkages among sub-systems can be more critical that the individual sub-systems.

As two or more failures that are not destructive in isolation can come together with catastrophic results.

What is Critical Infrastructure? - EU

- Critical infrastructure means an asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions.

COUNCIL DIRECTIVE 2008/114/EC

of 8 December 2008

on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection

What is Critical Infrastructure? - USA

- The nation's critical infrastructure provides the essential services that underpin American society and serve as the backbone of our nation's economy, security, and health. Overall, there are 16 critical infrastructure sectors that compose the assets, systems, and networks, whether physical or virtual, so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof.

Source: https://www.dhs.gov/what-critical-infrastructure

What is Critical Infrastructure? - Norway

- Critical infrastructures are those constructions and systems that are essential in order to uphold society's critical functions which in time safeguard society's basic needs and the feeling of safety and security in the general public.

Norges offentlige utredninger 2006: 6**,** **"**Når sikkerheten er viktigst. Beskyttelse av landets kritiske infrastrukturer og kritiske samfunnsfunksjoner"

What is Critical Infrastructure? - Norway

Critical Infrastructure

- Electric Power
- Electronic communications
- Water supply and Sewage
- Transport
- Oil and Gas
- Satellite-based infrastructure

Critical Societal Functions

- Banking and Finance
- Food Supply
- Health Services, Social Services and Social Security Benefit
- Police
- Emergency and Rescue Services
- Crisis Management
- Parliament and Government
- The Judiciary
- Defense
- Environmental Surveillance
- Waste Treatment

Complex Critical Infrastructure and Key Resources Systems

CIKR

- A collection of assets that are:
  - Interrelated
  - Interdependent
  - Linked through multiple connections

They evolve over long periods of time shifting from simple structures, towards greater orders of complexity and self organization, due to adapting to efficiency and optimization forces.

CIKR as networks

- Can be represented as networks

$$G = \{N, M, F\}$$

Where:

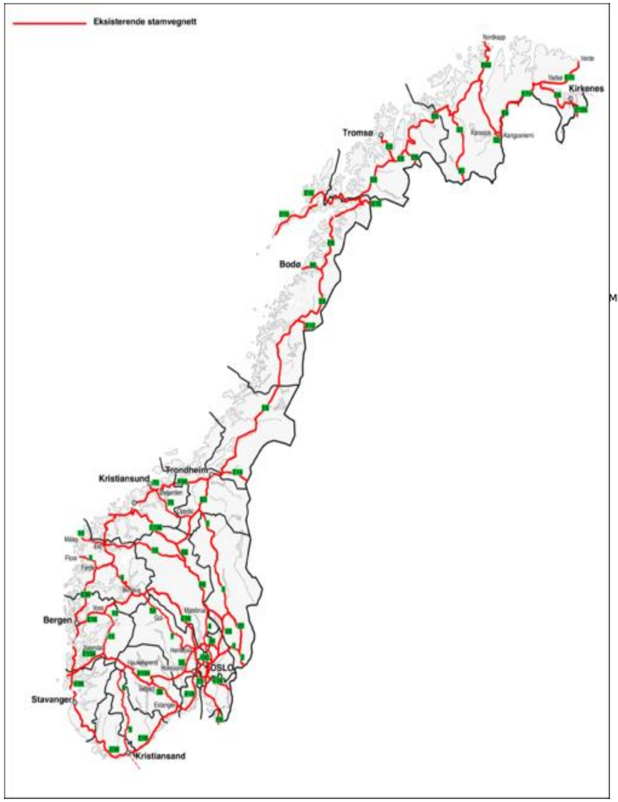
- N= A set of nodes
- M= A set of links
- F= A mapping function that defines how node pairs are connected

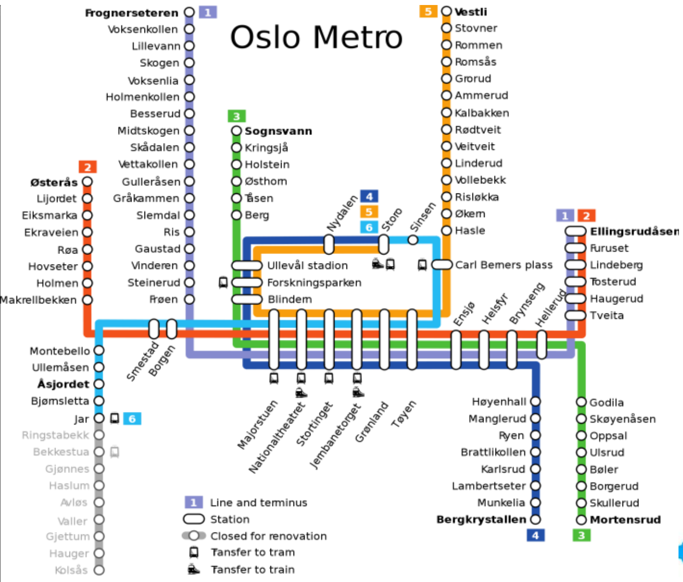
$$N = \{n_0 + n_1 + \cdots + n_{n-1}\}$$
$$M = \{l_0 + l_1 + \cdots + l_{n-1}\}$$
$$F = \begin{Bmatrix} f_{0,0} & f_{0,1} & f_{0,2} \cdots & f_{0,n-1} \\ f_{1,0} & f_{1,1} & f_{1,2} \cdots & f_{1,n-1} \\ \cdots\ldots & \cdots\ldots & \cdots\ldots & \cdots\ldots \end{Bmatrix}$$

CIKR as networks

Nodes? : Internet switches, hospitals, airports, people …

Links? : Roadways, pipes, wires, power lines …





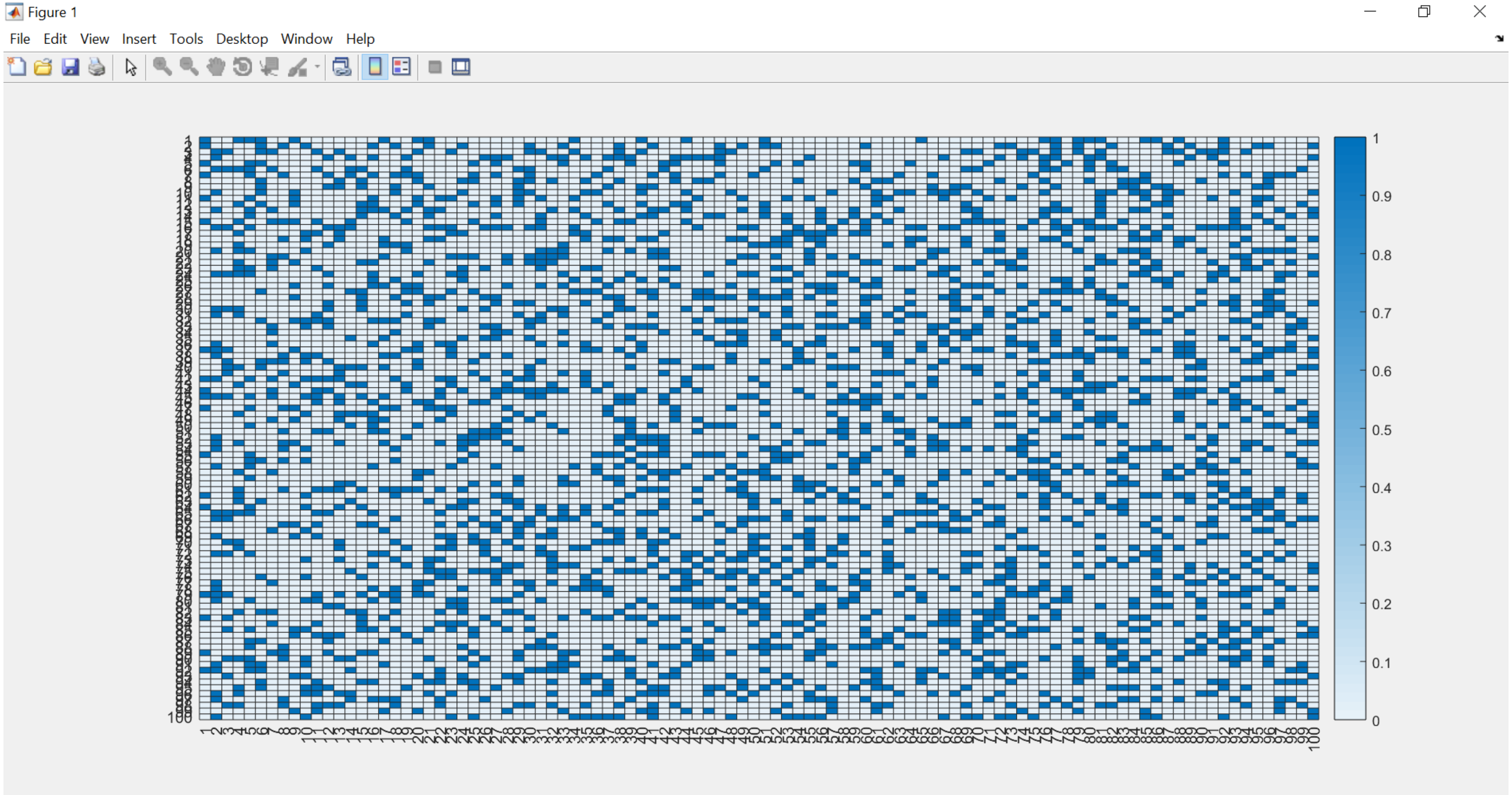
CIKR as networks (Core concepts)

- **Unidirectional links:** Carry a commodity only in one direction.
- **Bidirectional links:** Carry a commodity in both directions.
- **Degree (of a node):** The number of the node’s connections.
- **Hub:** The node with the highest degree.
- **Betweenness:** The number of paths running through a node or link from all other nodes to all other nodes.
  - Nodes with high betweenness are more critical!
- **Diameter:** The maximum number of hops along a chain of links from one node to another, needed to travel from any node to any other node.
- **Cluster coefficient:** A measure of how many neighbors of nodes are connected to one another.

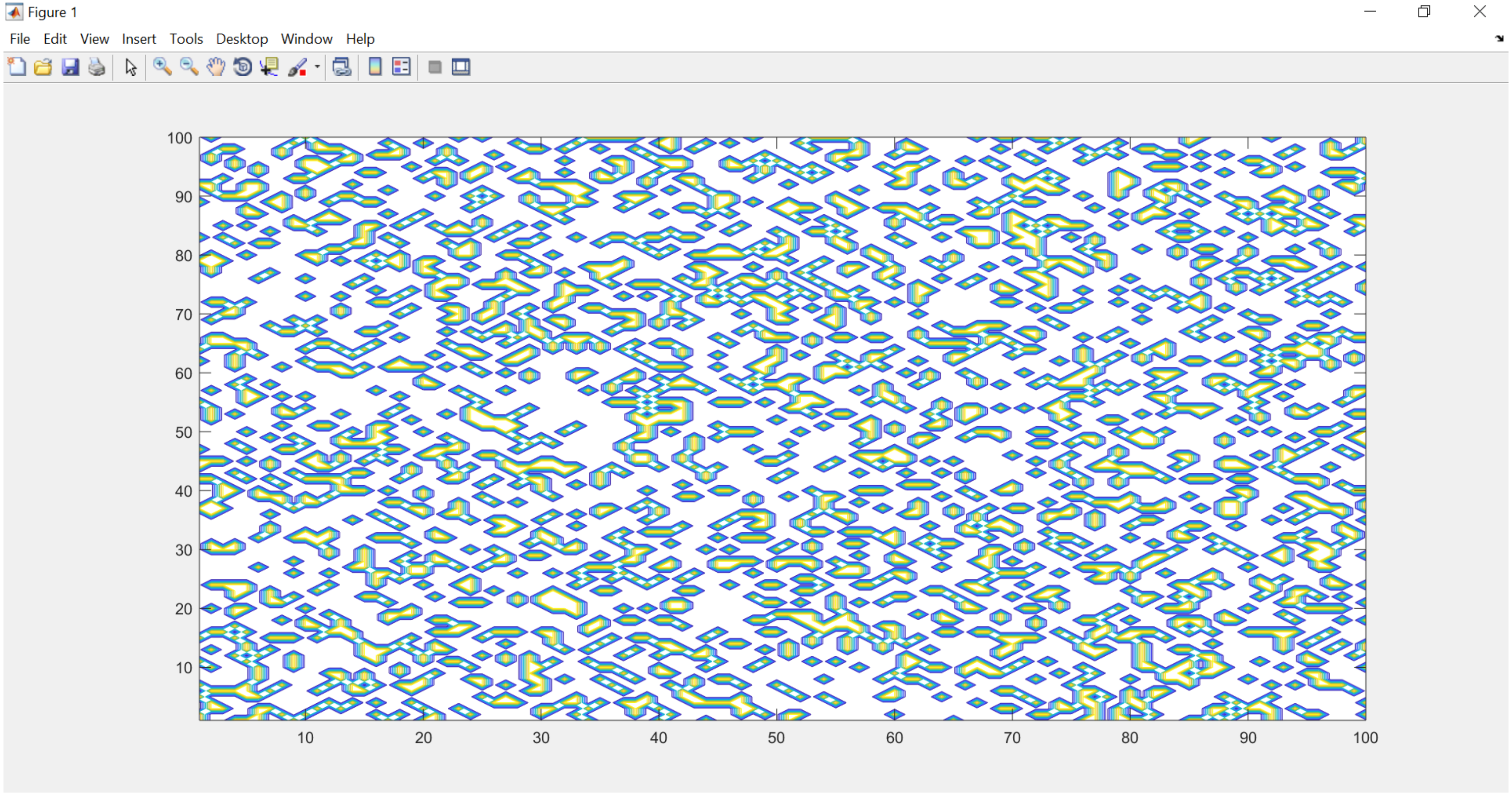
CIKR as networks

- Types of networks:
  - **Random networks**: Formed by randomly connecting pairs of nodes.
  - **Scale free networks:** Contain a hub with many connections, and many nodes with few connections each.
  - **Clustered networks:** Have no particular link distribution, but the nodes are more tightly connected to one another in local clusters.

CIKR as networks (Random)



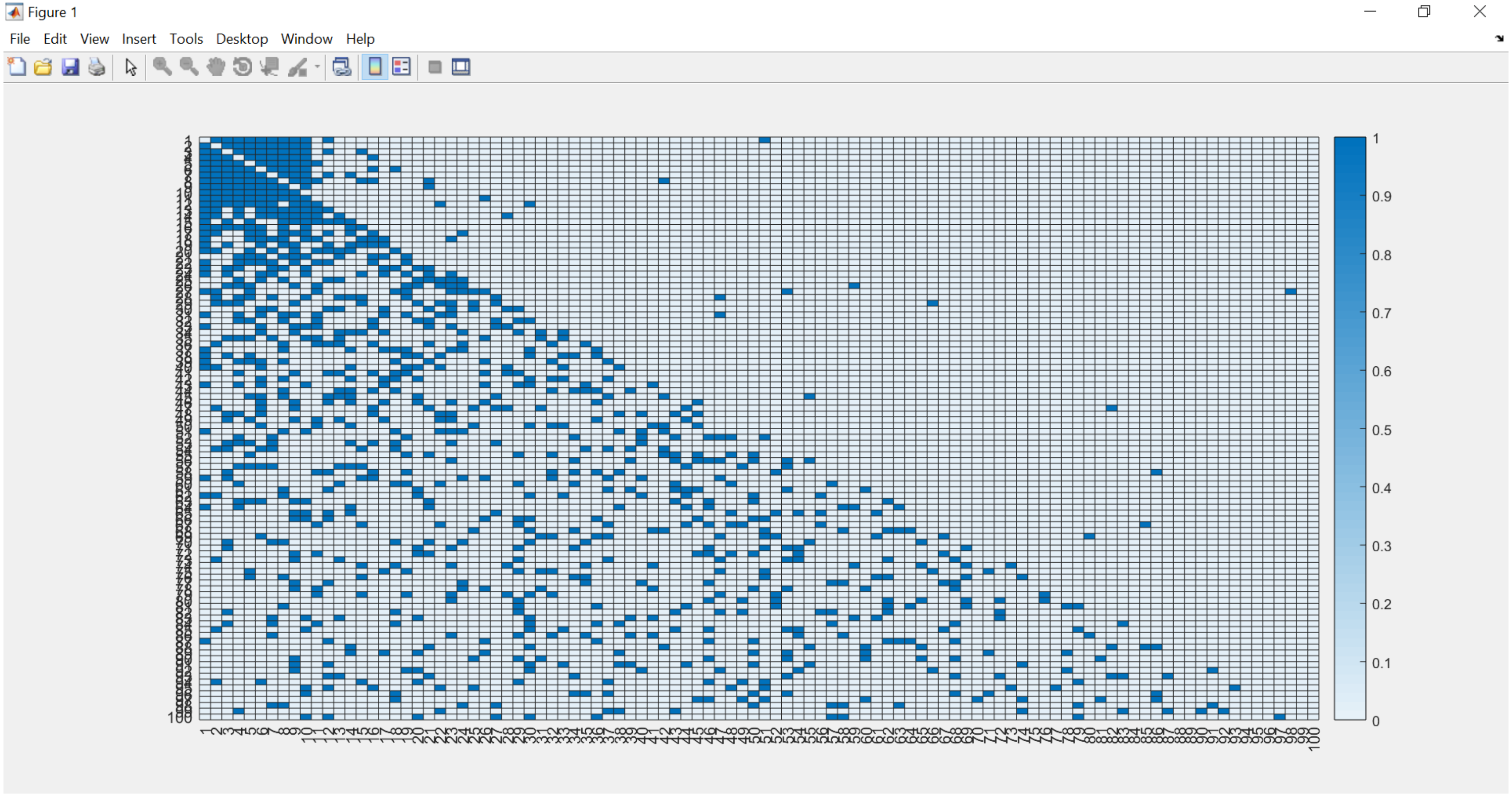
CIKR as networks (Random)



CIKR as networks (Random)

- Rarely found in practice
  - Resilient against single node/ link failures and attacks

CIKR as networks (Scale free)

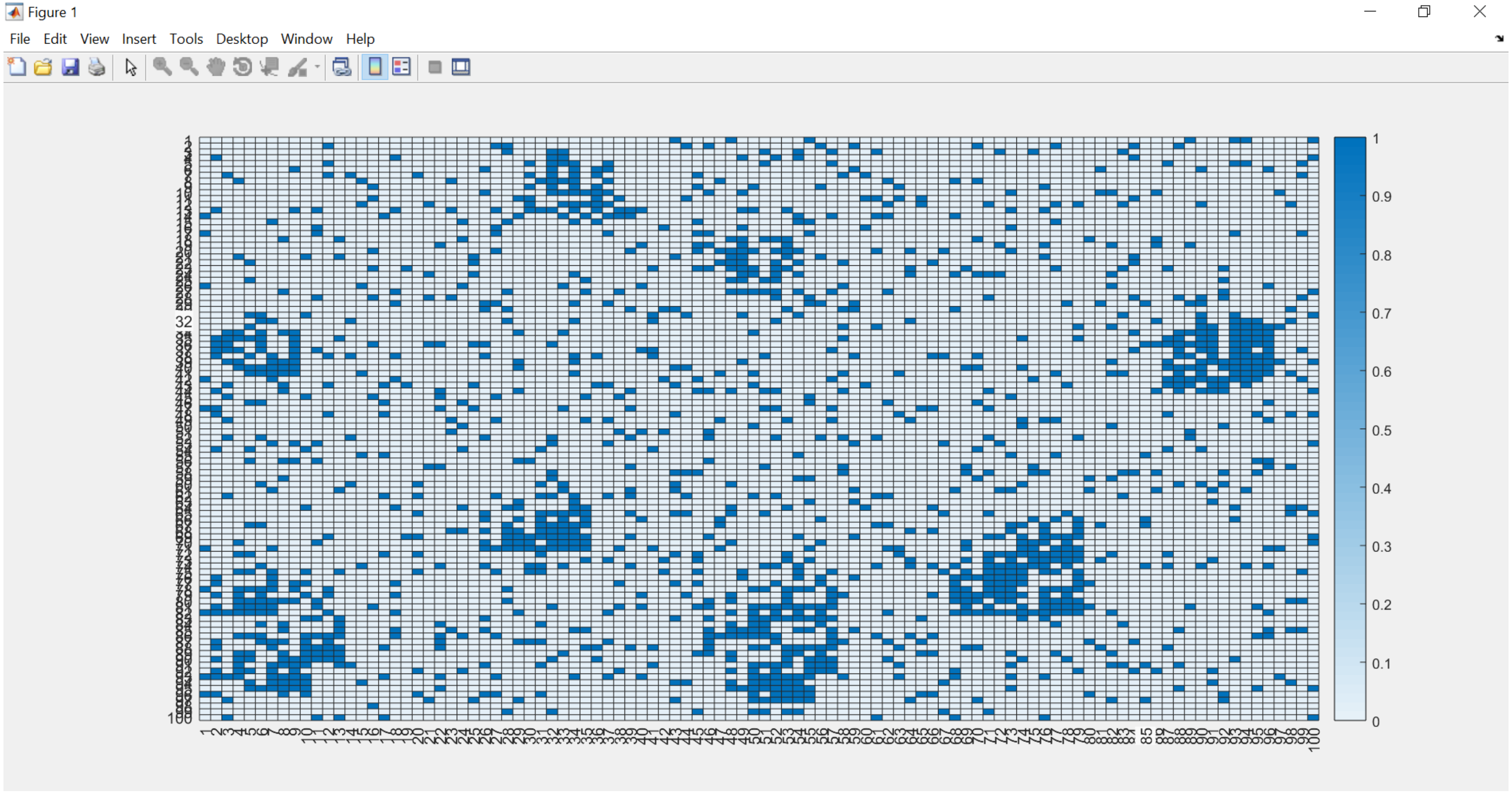


CIKR as networks (Scale free)

- More resilient in general
  - Resilient to random attacks and failures

- Less resilient in particular
  - Vulnerable to targeted attacks

CIKR as networks (Clustered)



CIKR as networks (Clustered)

- Somewhere between random and scale free networks
  - Nearly as resilient as random networks
  - Yet! Can be easily separated into isolated clusters

CIKR and self organization

- Networks are inclined to build self-organization and transition from random to scale-free or clustered networks.
  - It is an emergence that builds from the bottom up based on minor or major operational changes arising due to:
    - Threats
    - Efficiency
    - Regulation
    - Costs
    - Demand
    - Not in My Backyard Phenomenon (NIMBY)

CIKR: Targeted attacks

- Critical nodes with high degree act as “super-spreaders”
  - Magnifying consequences!

- Critical links with high betweenness can reduce resilience
  - High probability that they break under stress!

Targeted attacks can transform a network from error prone to catastrophe prone!

CIKR: Robustness

- A network is robust when it withstand damage to nodes and links while remaining in one piece.

  – Robustness is a measure of how many nodes and links can be removed before breaking a connected network into disconnected components or islands.