Ministry of Defence

Vulnerability of C2 Networks to Attack: Topology of 11 Dutch Army C2 systems

Tim Grant *, Barend Buizer, & Ron Bertelink

* Netherlands Defence Academy (NLDA)
TJ.Grant@NLDA.nl
Tel: +31 76 527 3261 Mob: +31 638 193 749

Outline

Goal:

- To report the results of measuring the topology of 11 Royal Dutch Army C2 systems, modelled as networks

Overview:

- Motivation
- C2 systems studied
- Modelling C2 systems as networks
- Results of topology measurements
- Conclusions & recommendations

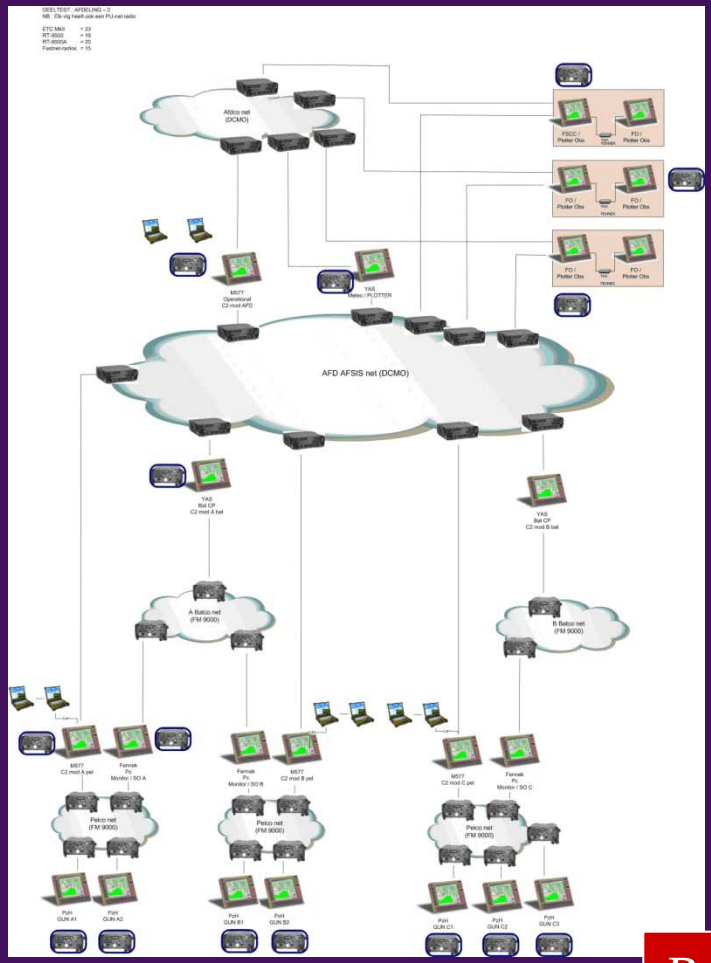
Motivation (1)

Mathematical network theory:

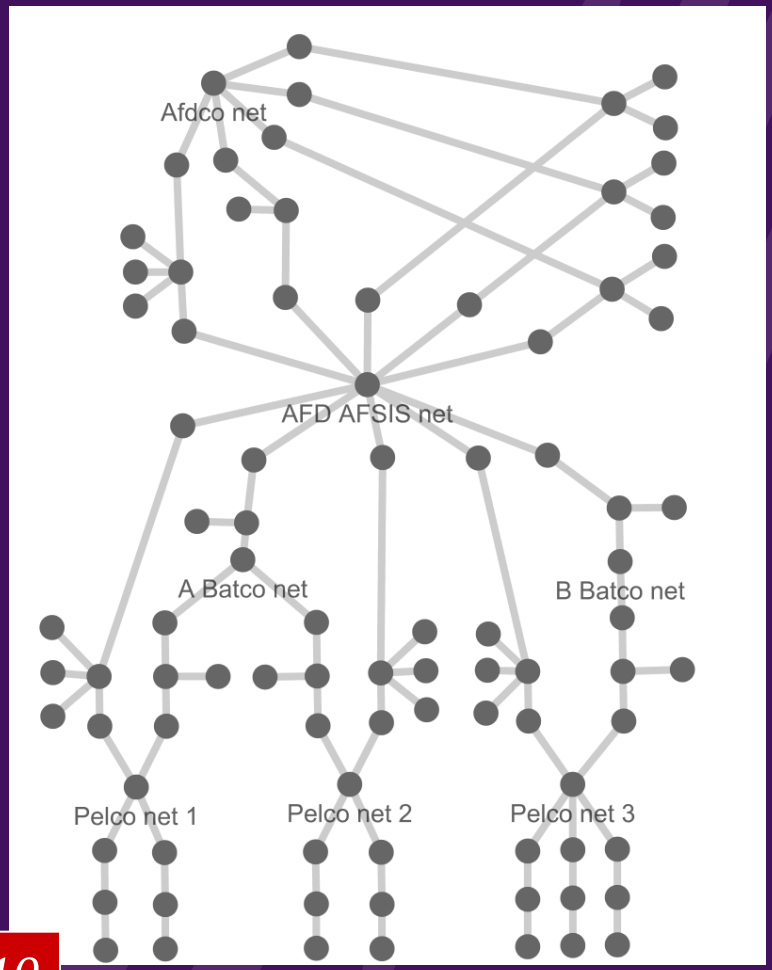
- Biological, social, knowledge, & technical applications
- Network = set of nodes & set of arcs
  - C2 system can be modelled as:
    - Nodes = users, workstations, routers, hubs
    - Arcs = (tele)communications links
- Major theoretical results since 2000:
  - Attacks modelled as removal of nodes
  - Attacks can be random or targeted
  - Types = random graphs, small worlds, scale-free
  - How these 3 types break up after attack

Motivation (2)

(Technical) system

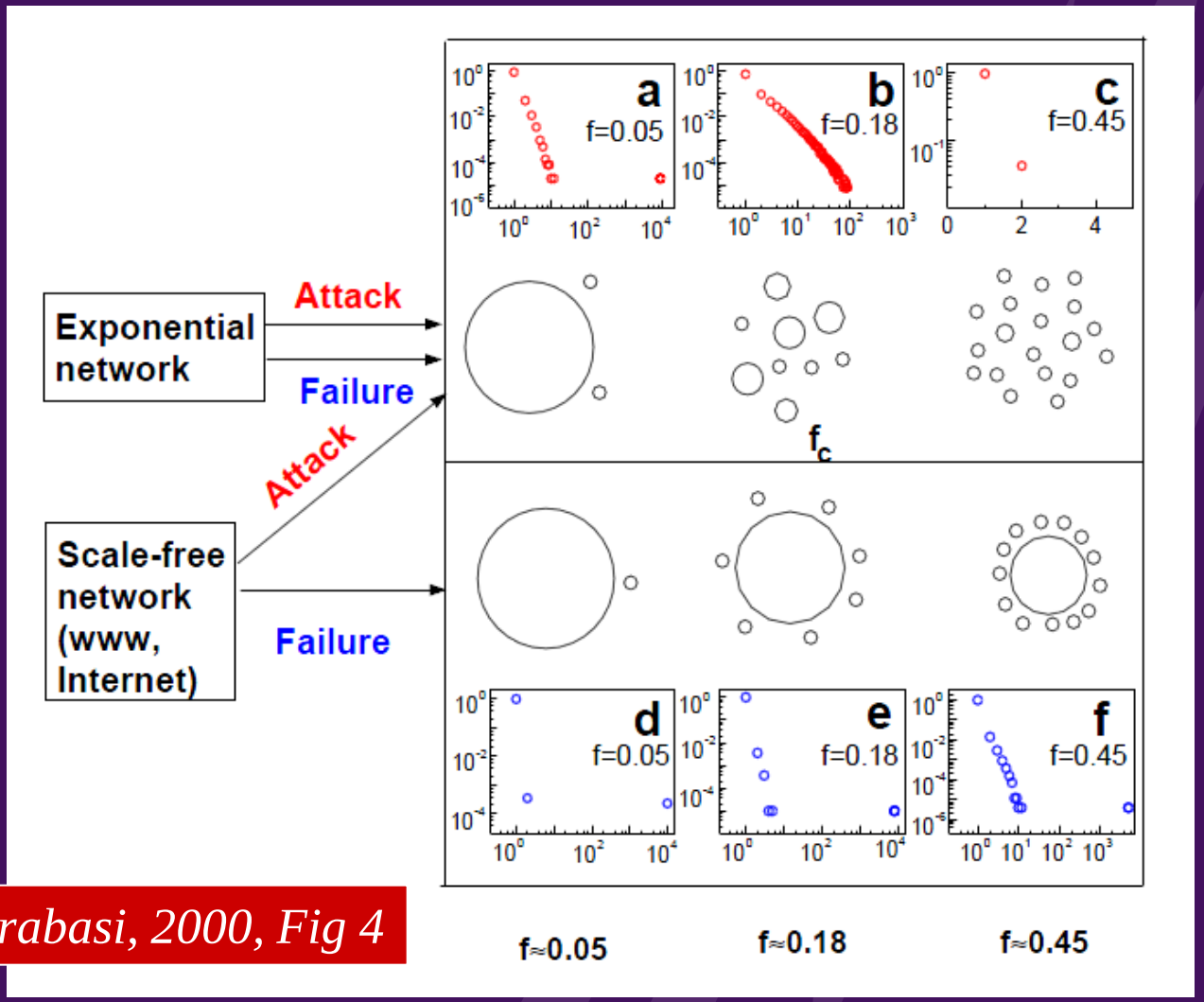


Network model of system



Buizer, 2010

Motivation (3)



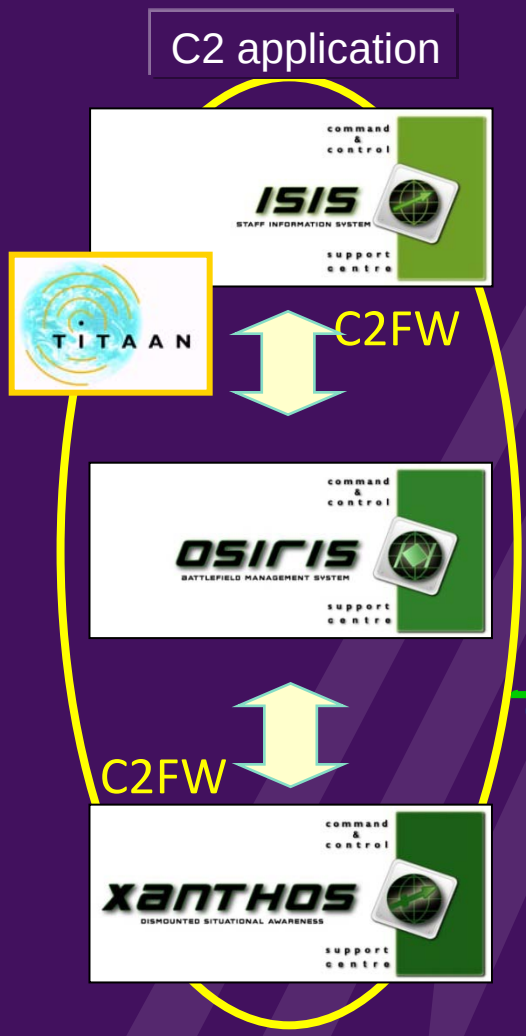
Alberts, Jeong & Barabasi, 2000, Fig 4

C2 systems studied (1)

Deployed

Mobile

Dismounted



C2 systems studied (2)

Network name	Environment	*n*	*m*	<*k*>
FAT 018 strz	Deployed	171	191	2.222
TITAAN v021	Deployed	88	103	2.25
TITAAN41 SYST	Deployed	141	153	2.17
AFSIS 3.2 afd	Mobile	90	96	2.133
AFSIS 3.2 afd man	Mobile	84	88	2.095
AFSIS 3.2 bt	Mobile	76	80	2.105
AFSIS 3.2 man mr	Mobile	79	81	2.051
OSIRIS 3.0 A	Mobile	44	43	1.955
OSIRIS 3.0 B	Mobile	56	58	2.071
BMS 3.1 A	Mobile	94	106	2.191
BMS 3.1 B	Mobile	55	64	2.327

Buizer, 2010, Table 3.1, p.28

Modelling C2 systems as networks

Guidelines adopted for uniform modelling:

- Entity types:
  - Could be routers, hubs, end-user terminals, etc
  - All modelled as nodes, regardless of type
  - Nodes & arcs non-valued
- System boundary:
  - System could have interface(s) to other network(s)
  - Each other network modelled as single node
- End-user terminals:
  - When end-user terminals not shown, 6 assumed
- Wireless “clouds”:
  - Central node to model (jammable) “ether”

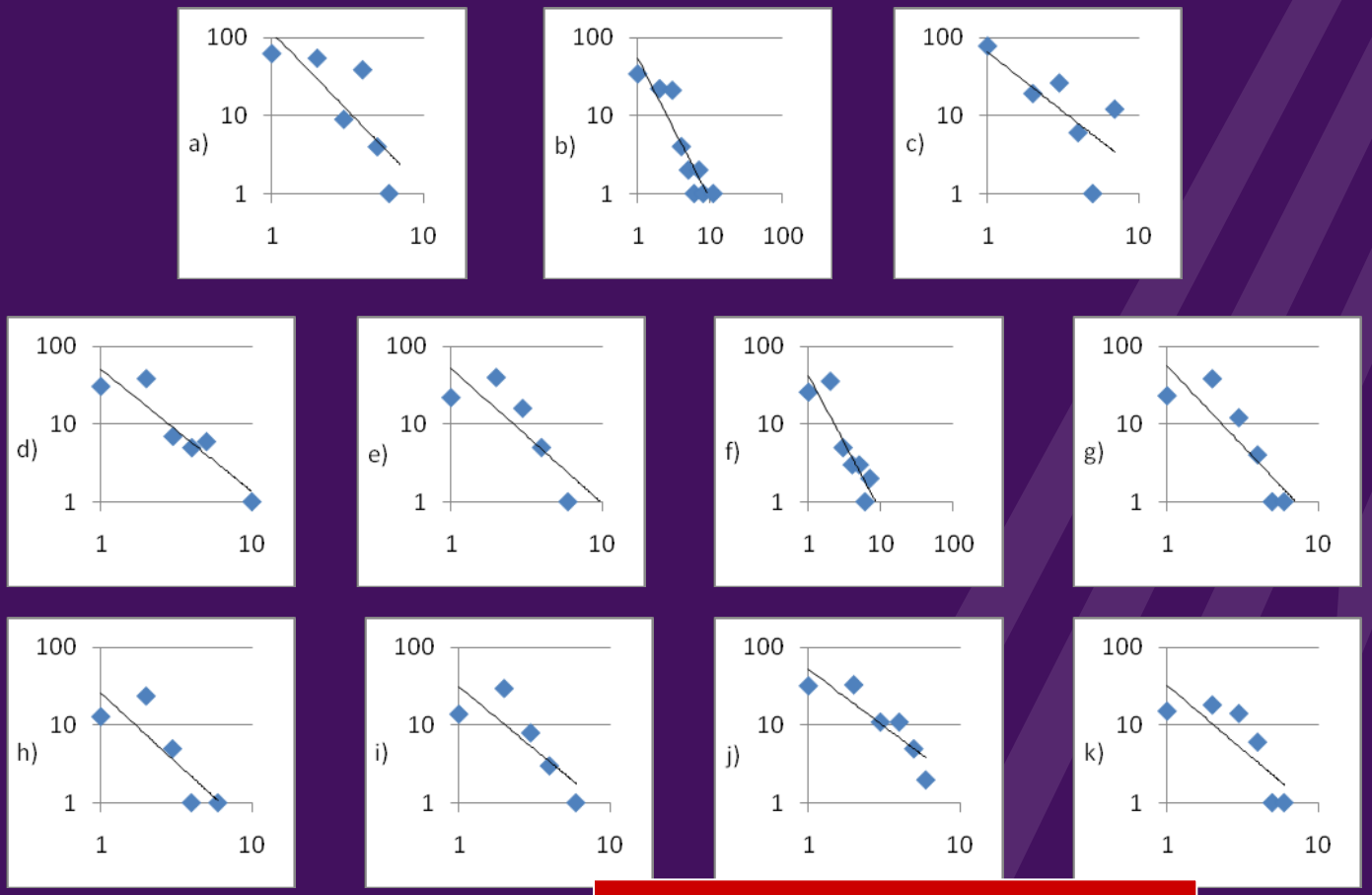
Results of topology measurements (1)

Network name	Power	Real length	Rand length	Real coeff	Rand coeff
FAT 018 strz	1.996	9.723	6.440	0.034	0.013
TITAAN v021	1.804	6.763	5.212	0.073	0.026
TITAAN41 SYST	1.521	9.85	6.388	0.053	0.015
AFSIS 3.2 afd	1.573	6.412	5.925	0	0.024
AFSIS 3.2 afd man	1.734	10.489	5.991	0	0.025
AFSIS 3.2 bt	1.749	5.913	5.818	0	0.028
AFSIS 3.2 man mr	2.049	8.439	6.083	0	0.026
OSIRIS 3.0 A	1.775	7.44	5.645	0	0.044
OSIRIS 3.0 B	1.595	7.623	5.529	0	0.037
BMS 3.1 A	1.459	8.443	5.792	0.073	0.023
BMS 3.1 B	1.645	7.294	4.745	0.135	0.042

Buizer, 2010, p.63

Results of topology measurements (2)

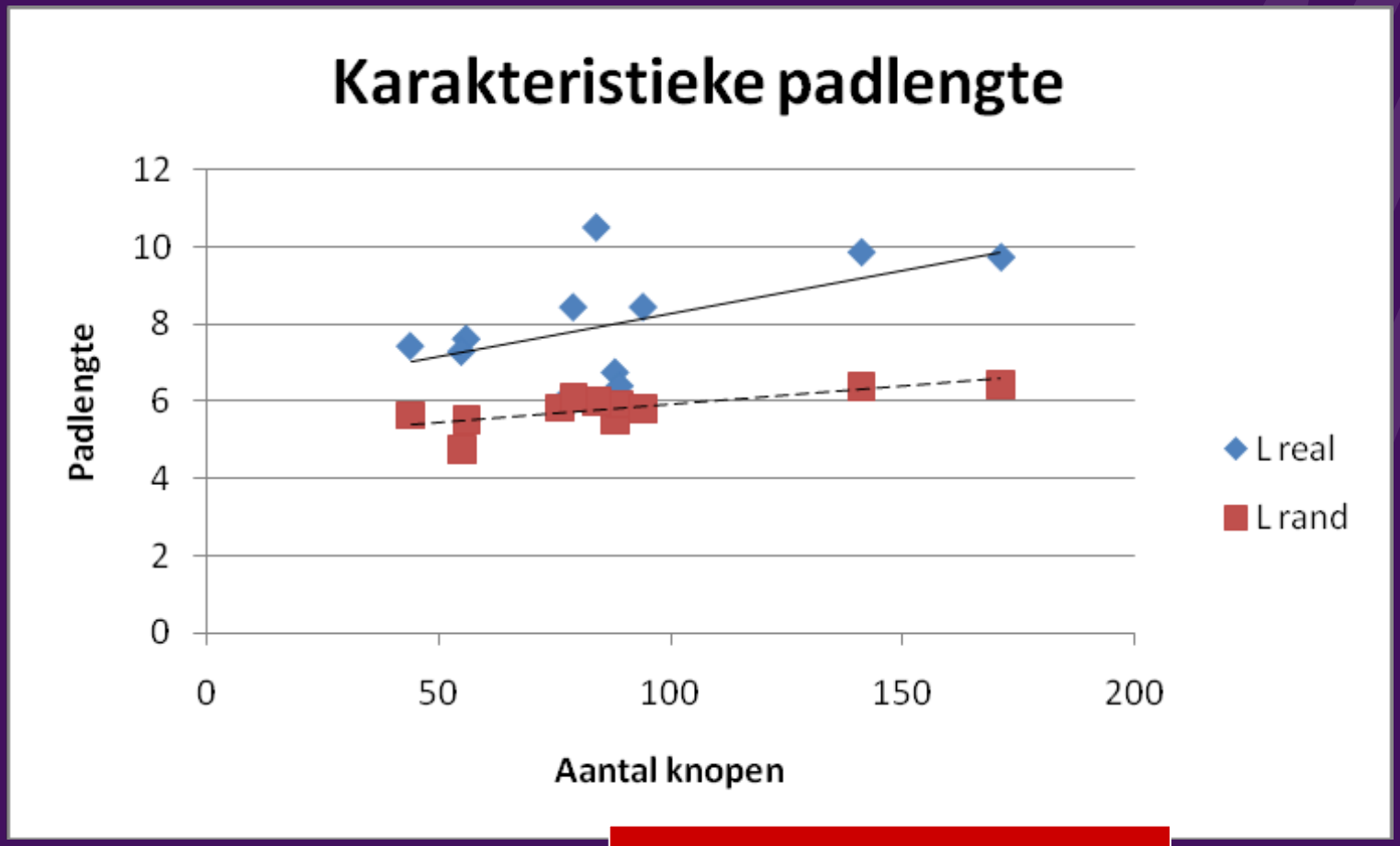
Degree distribution (log-log plots):



Buizer, 2010, Fig 5.1, p.33

Results of topology measurements (3)

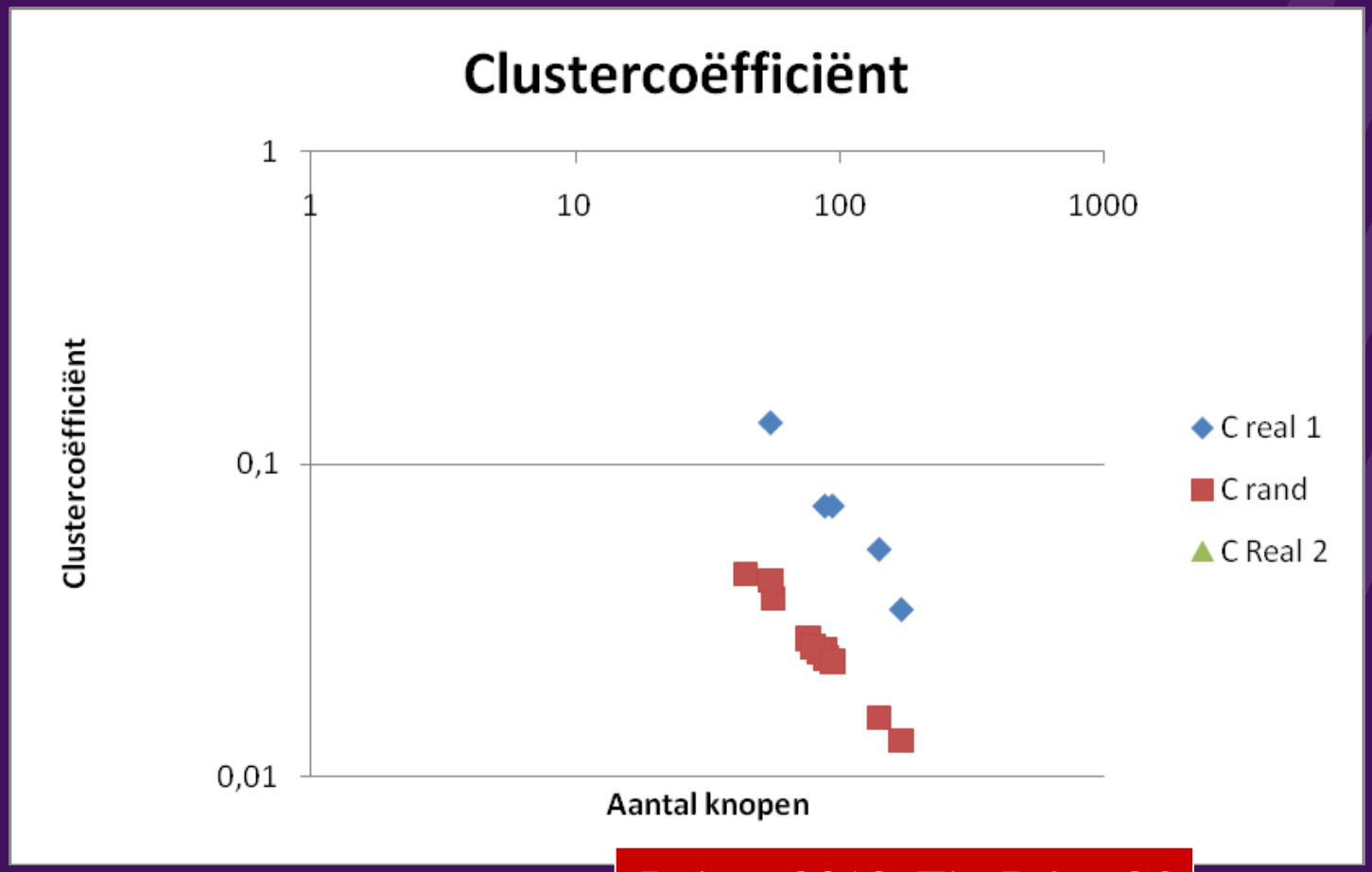
Characteristic path length:



Buizer, 2010, Fig 5.2, p.34

Results of topology measurements (4)

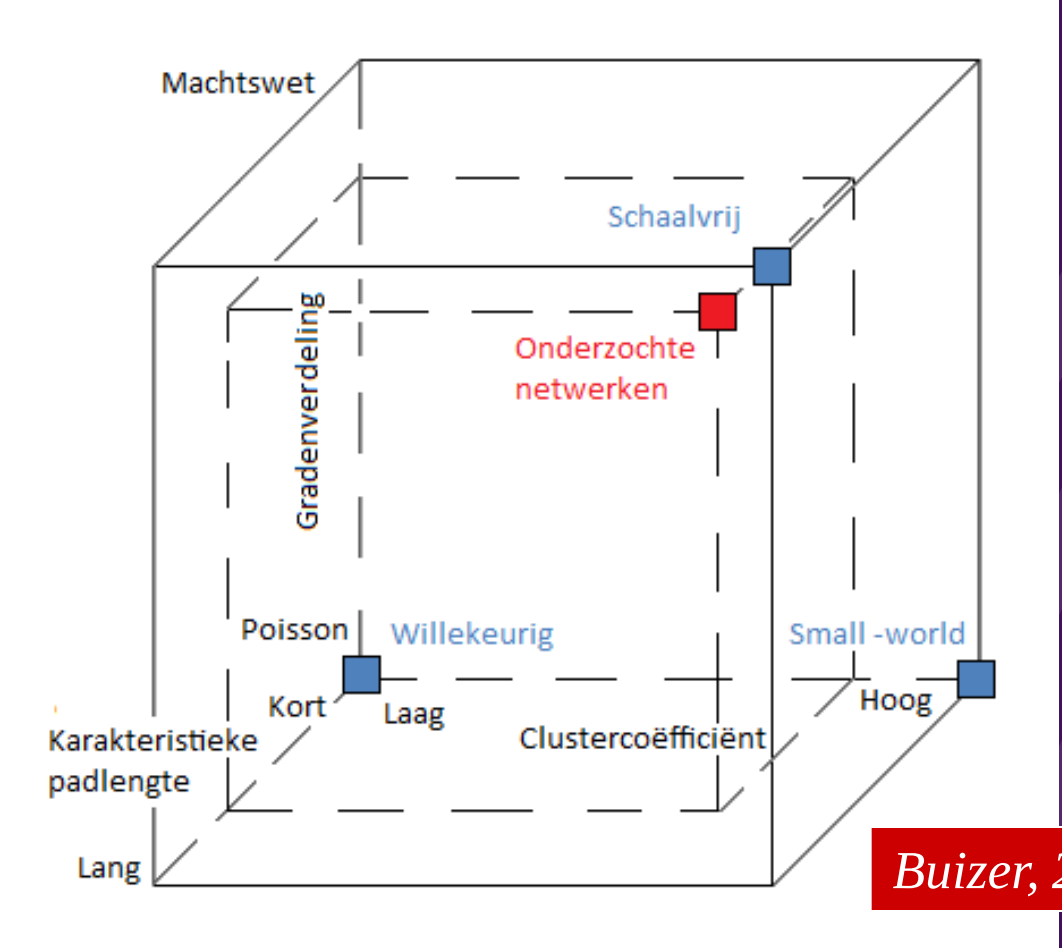
Cluster coefficient:



Buizer, 2010, Fig 5.4, p.36

Results of topology measurements (5)

Researched networks closest to scale-free:



Buizer, 2010, Fig 5.5, p.37

Conclusions & recommendations

Conclusion:

- C2 systems we studied closest to scale-free:
  - Like Internet and WWW
  - Confirms speculation in Grant et al, 2007 (12th ICCRTS)
- May reflect hierarchical command structure

Consequence:

- C2 systems likely to be vulnerable to targeted attack

Recommendations:

- Study other services' & nations' C2 systems
- Doctrine for C2 system design should consider network topology & its implication for vulnerability

Any questions?