

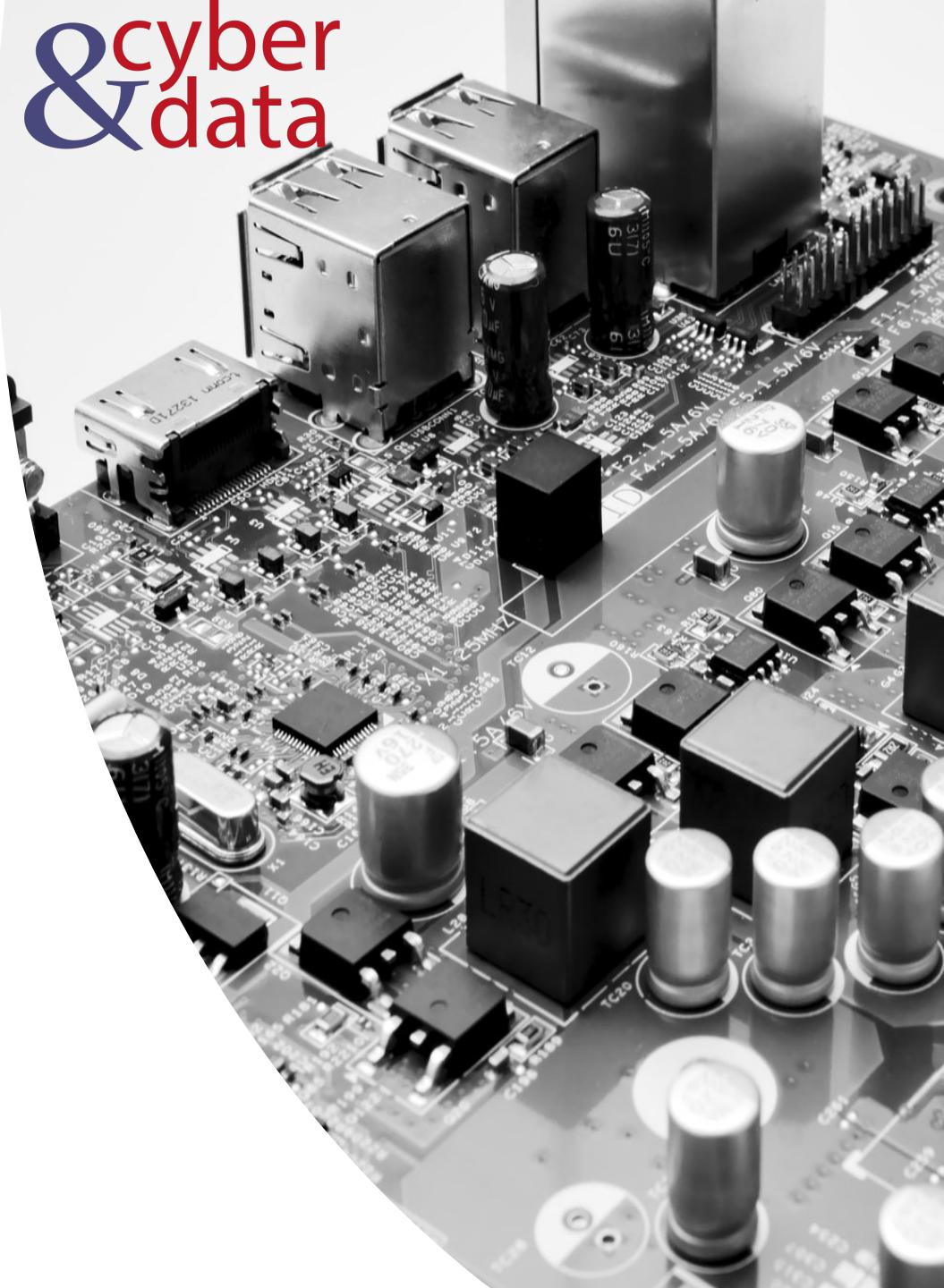
cyber & data

"From bits to information"

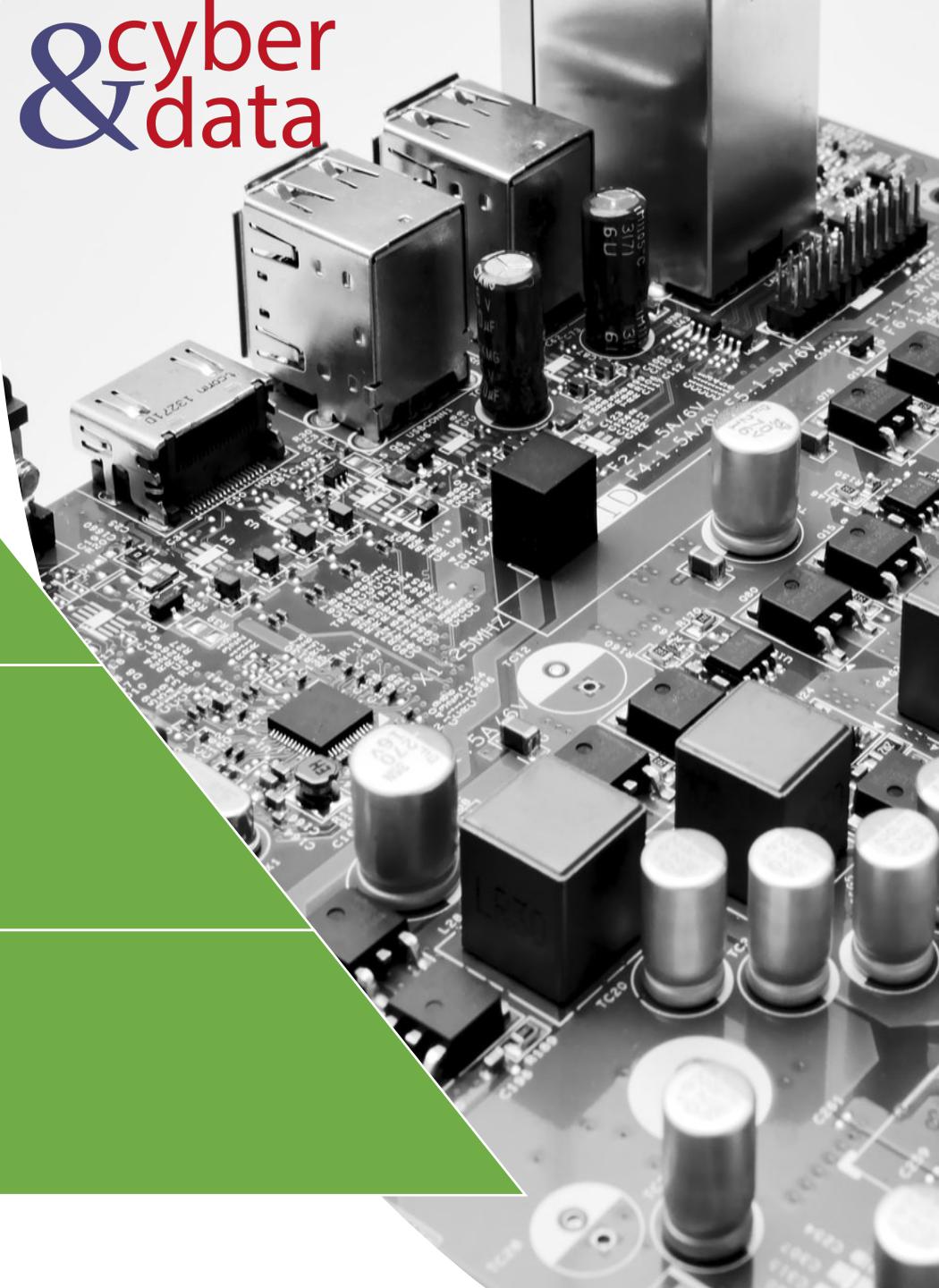
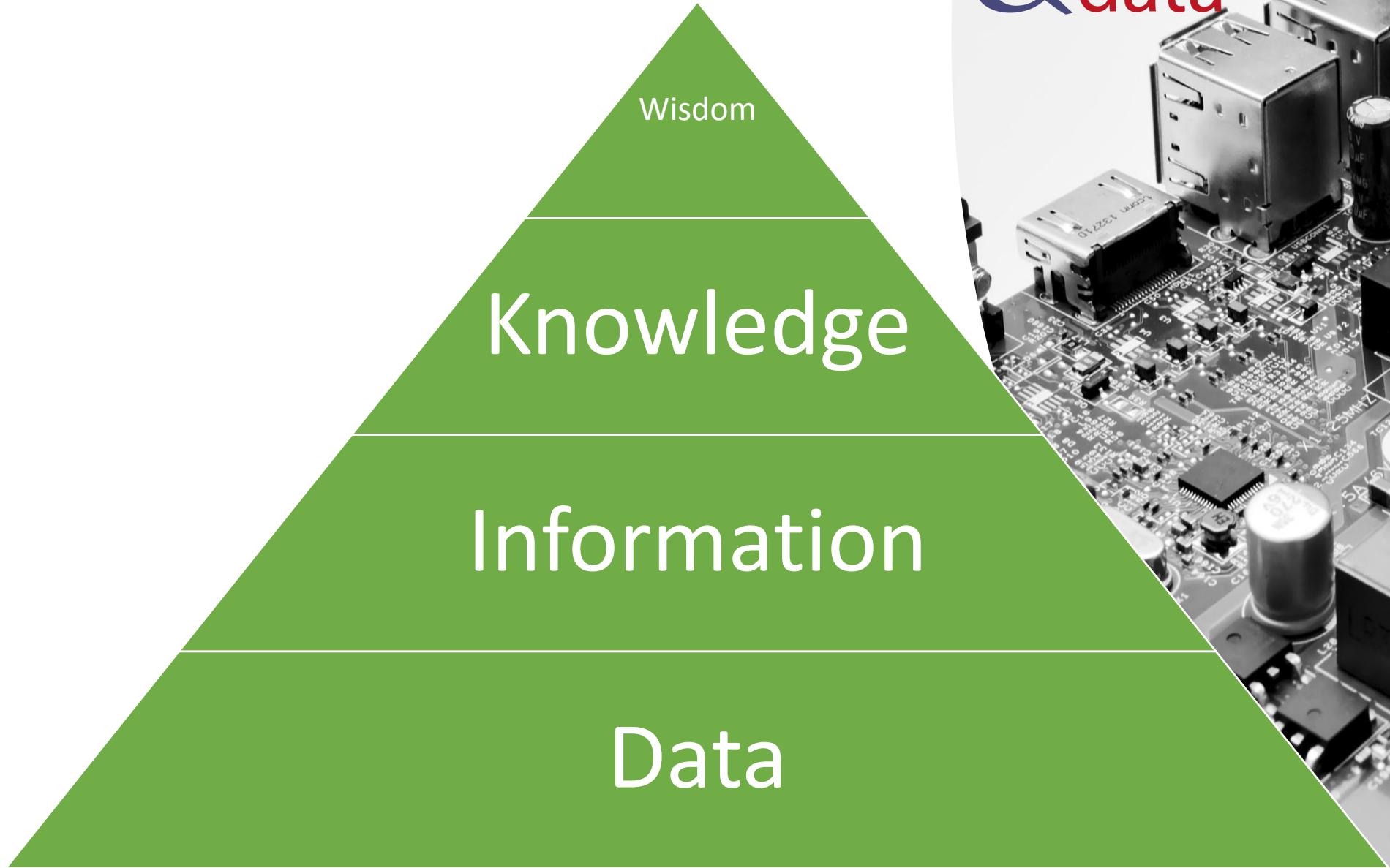
Defence Systems,
Policies and Risks

Outline

- Data, Information, Knowledge and Wisdom.
- Information Security and Forensic Computing.
- Impact and Harm.
- Risks, Costs and Benefits.
- Kill Chain Models.
- Defence Mechanisms.
- Defence-in-Depth.



Data to Wisdom

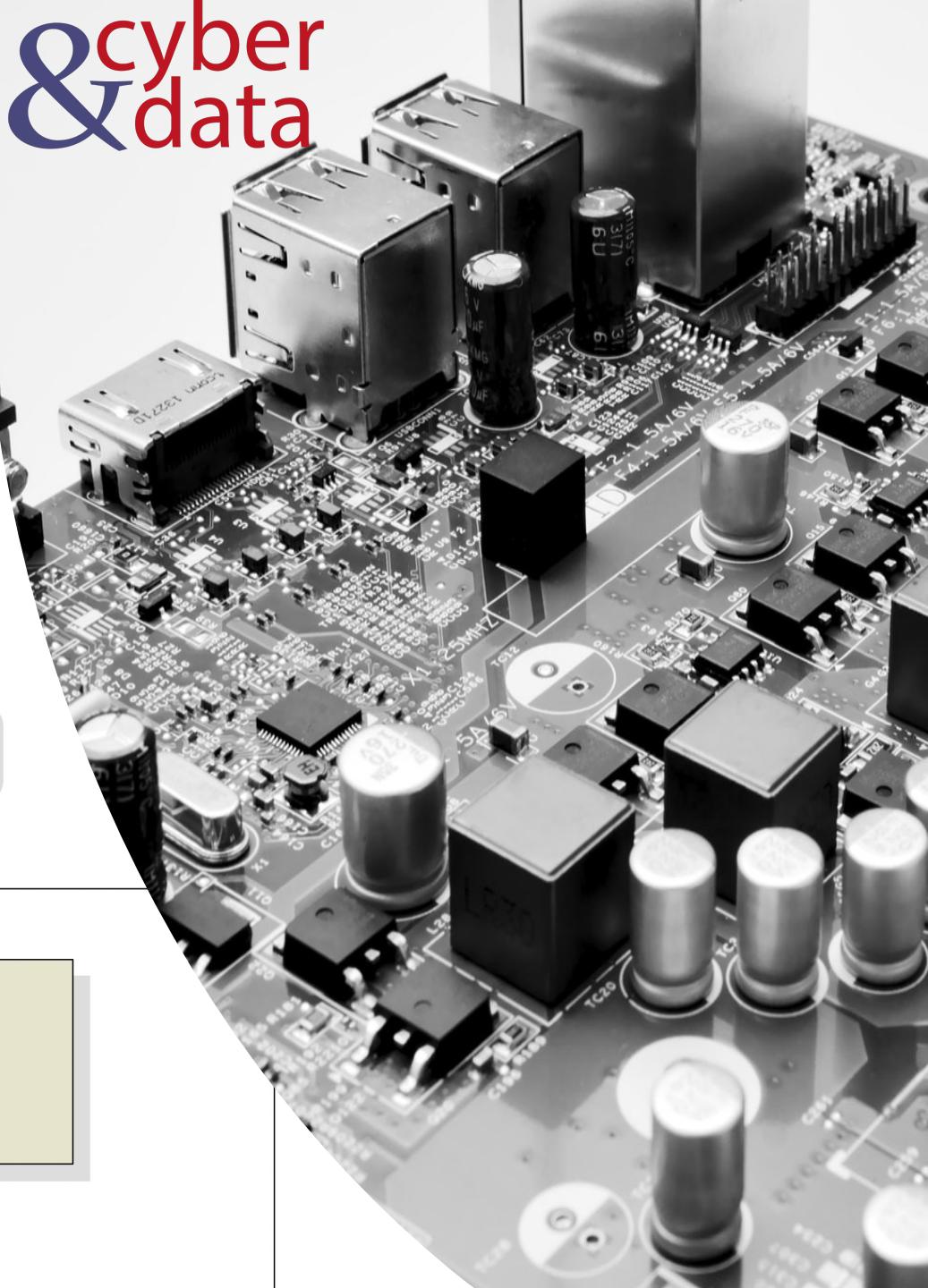
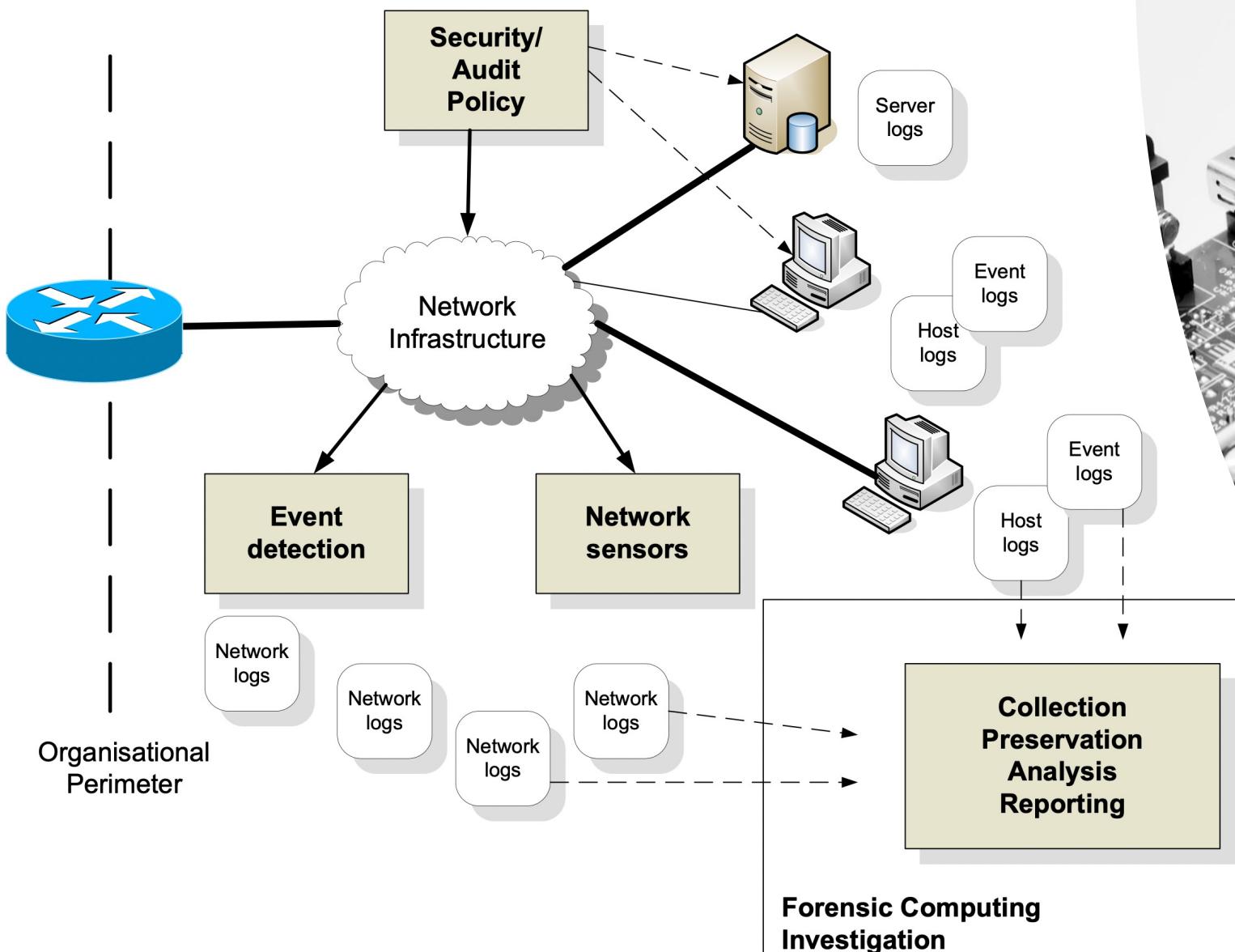


cyber & data

“From bits to information”

Security, Incident
Response and
Forensic
Computing

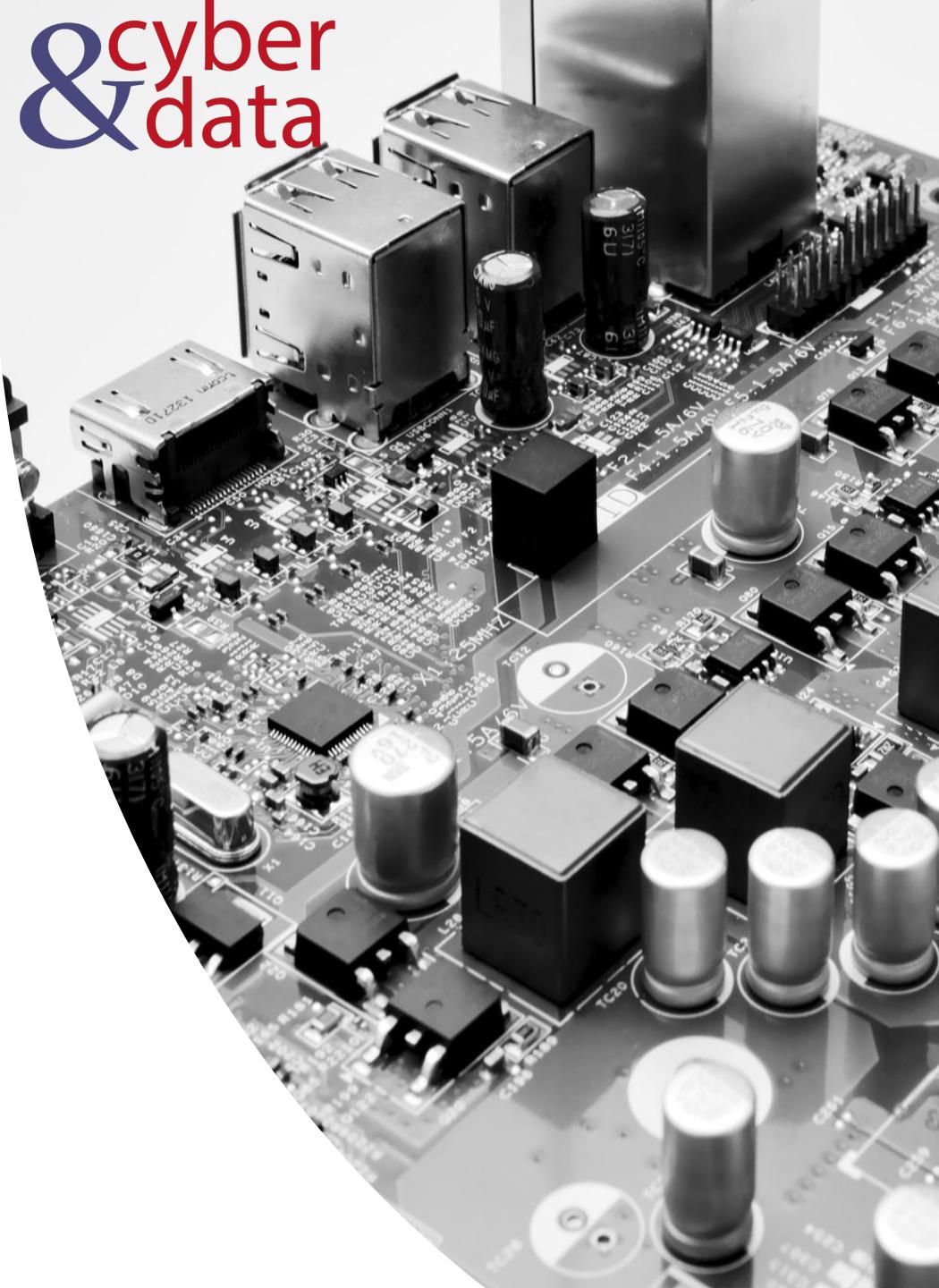
Information Security



cyber
&
data

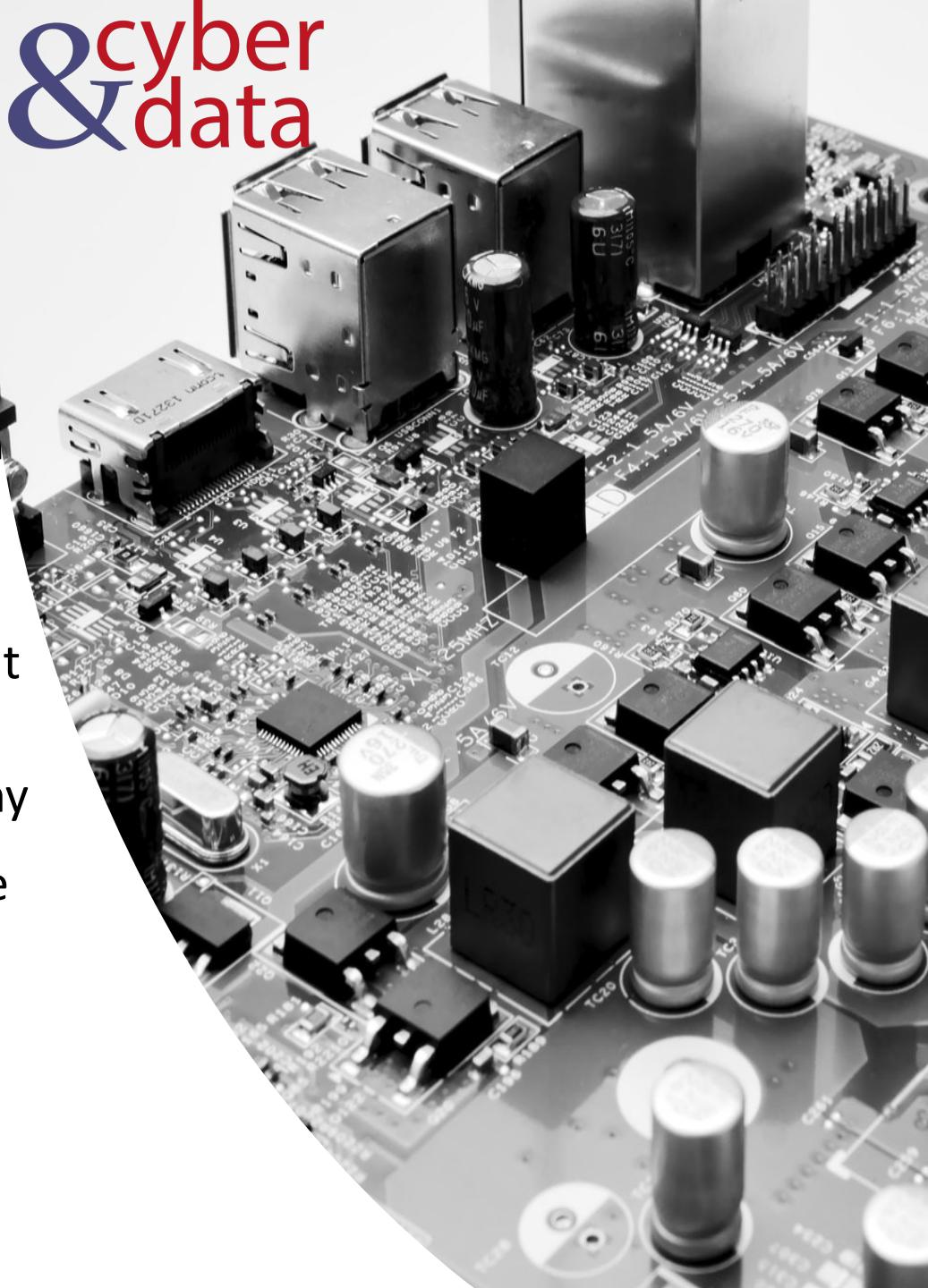
Investigation

- Investigating an intrusion on a system (incident response). This might lead to a criminal prosecution, but most of the time the intrusion is investigated in order to be able to detect it in the future, and to thwart the activities at an early stage.
- Investigation of a criminal activity (forensic computing). This might lead to a criminal prosecution, or to thwart the activities in the future.
- Investigation of a breach of security policy. This might lead to a disciplinary procedure within an organisation.



Due Care and Due Diligence

- With due care, the organisation must make sure that has taken the correct steps in the creation and implementation of its security policy and in its risk analysis.
- Then due diligence relates to the actual operation and maintenance of its security system, especially around vulnerability testing. Thus a company might take due care in analysing and designing their security policy, but not take due diligence in actually proving that it works. It can work the other way, in that a policy might be implemented with due diligence, but the originally creation of the policy has not been properly analysed/designed. It is thus important, in terms of any future liability, that security systems are designed, analysed, implemented and maintained with both due care and due diligence.

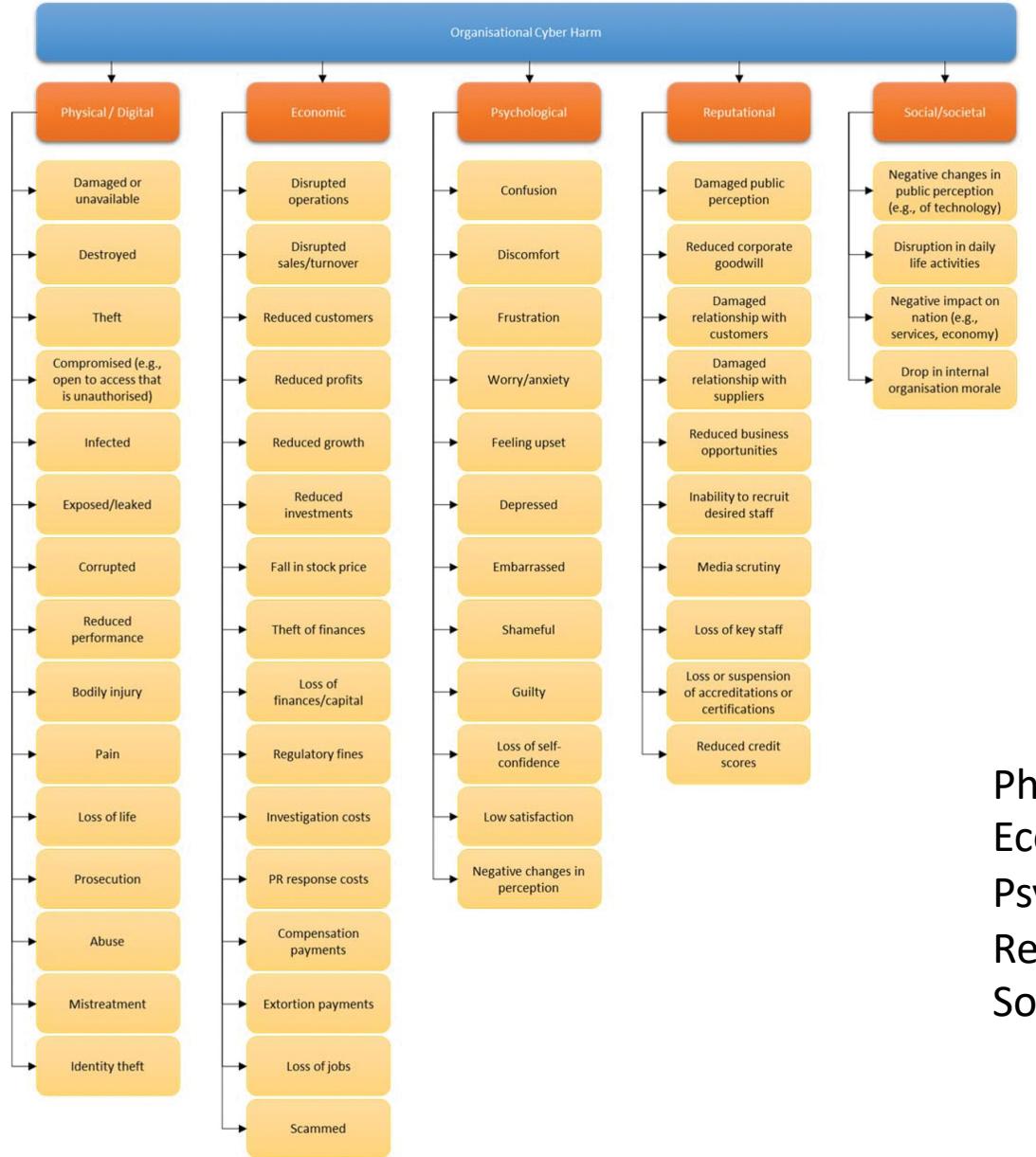


cyber & data

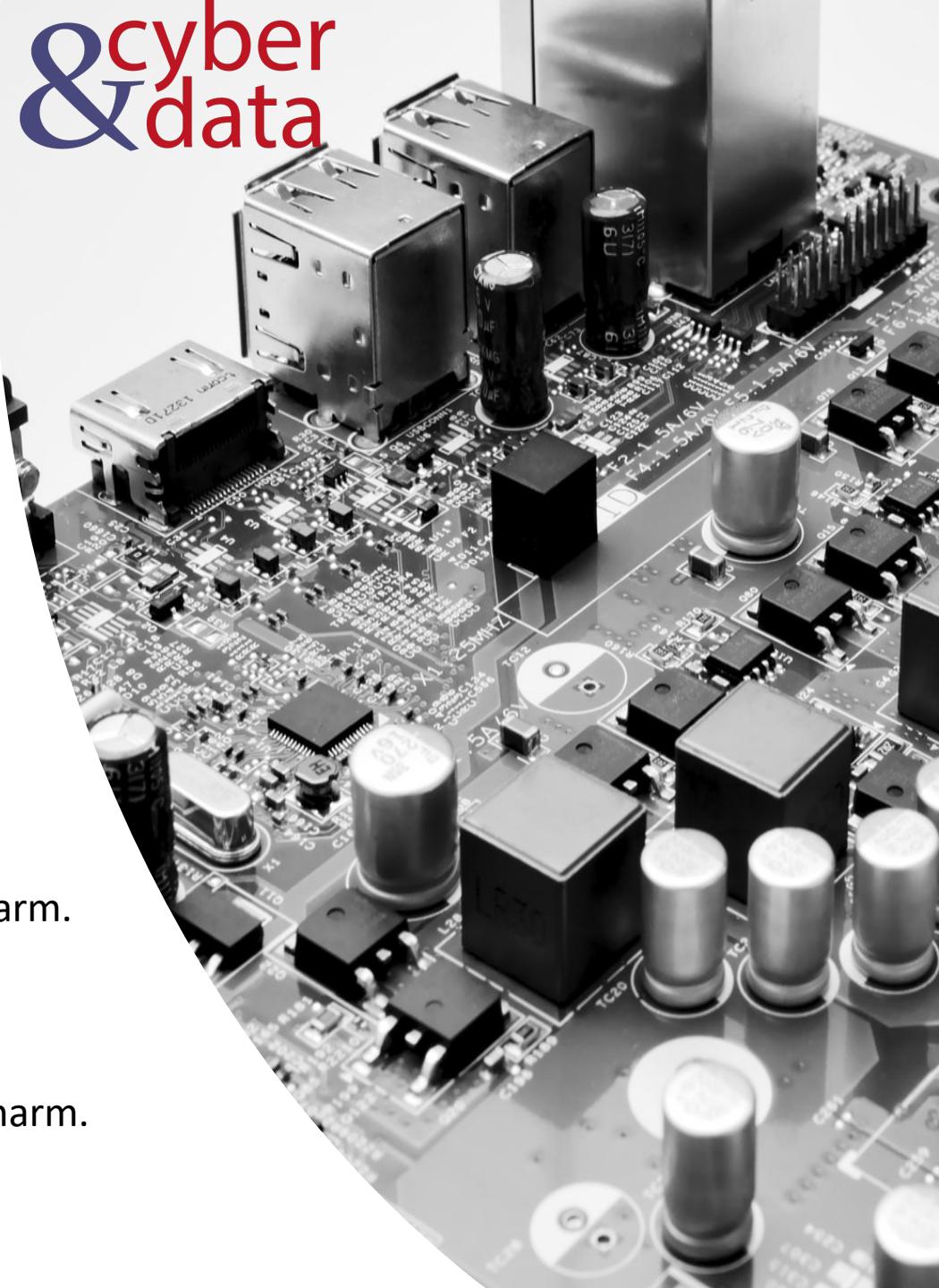
"From bits to information"

Impact and Harm

Impact and Harm



Physical or Digital harm.
Economic harm.
Psychological harm.
Reputational harm.
Social and Societal harm.



cyber & data

"From bits to information"

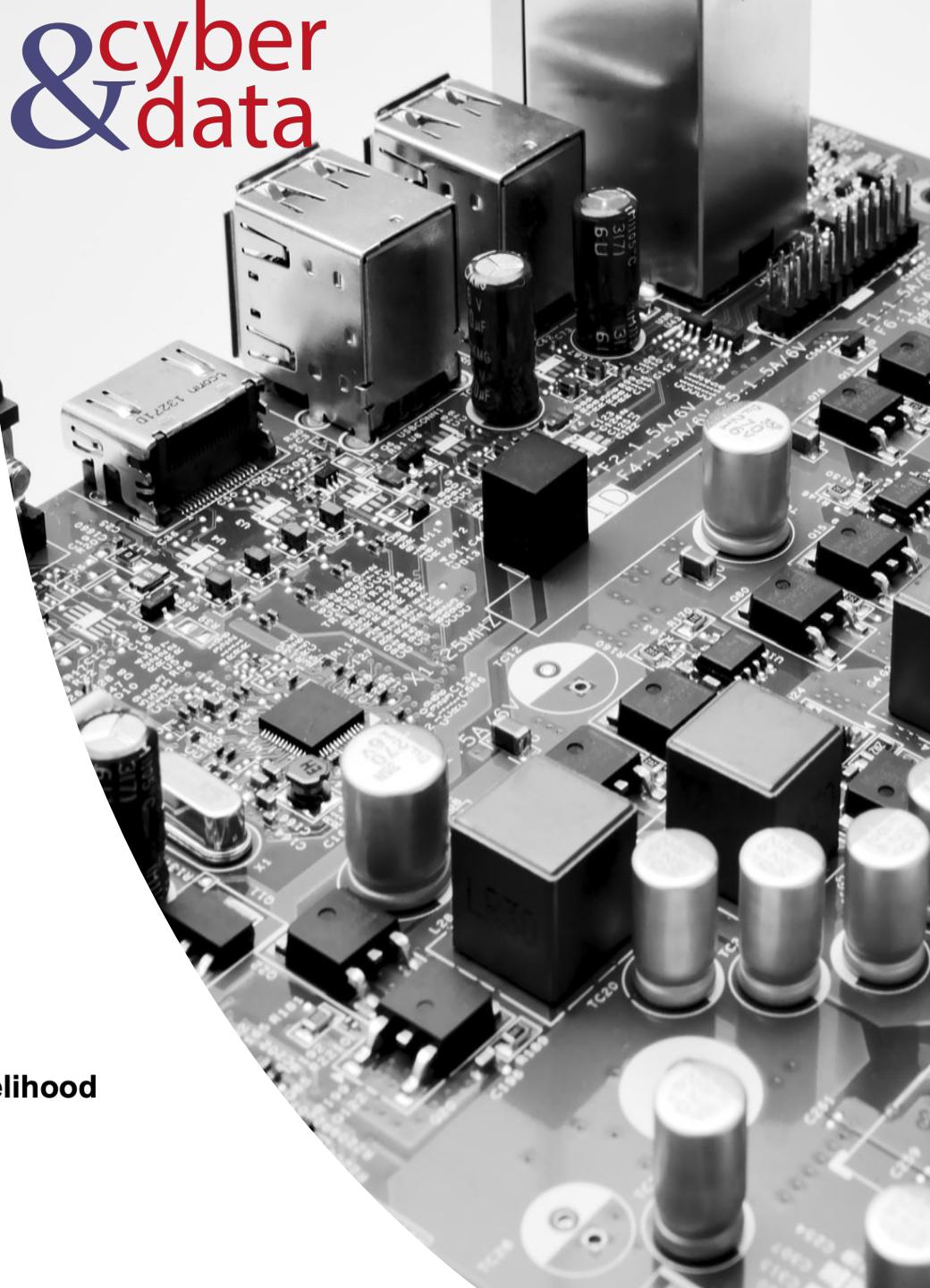
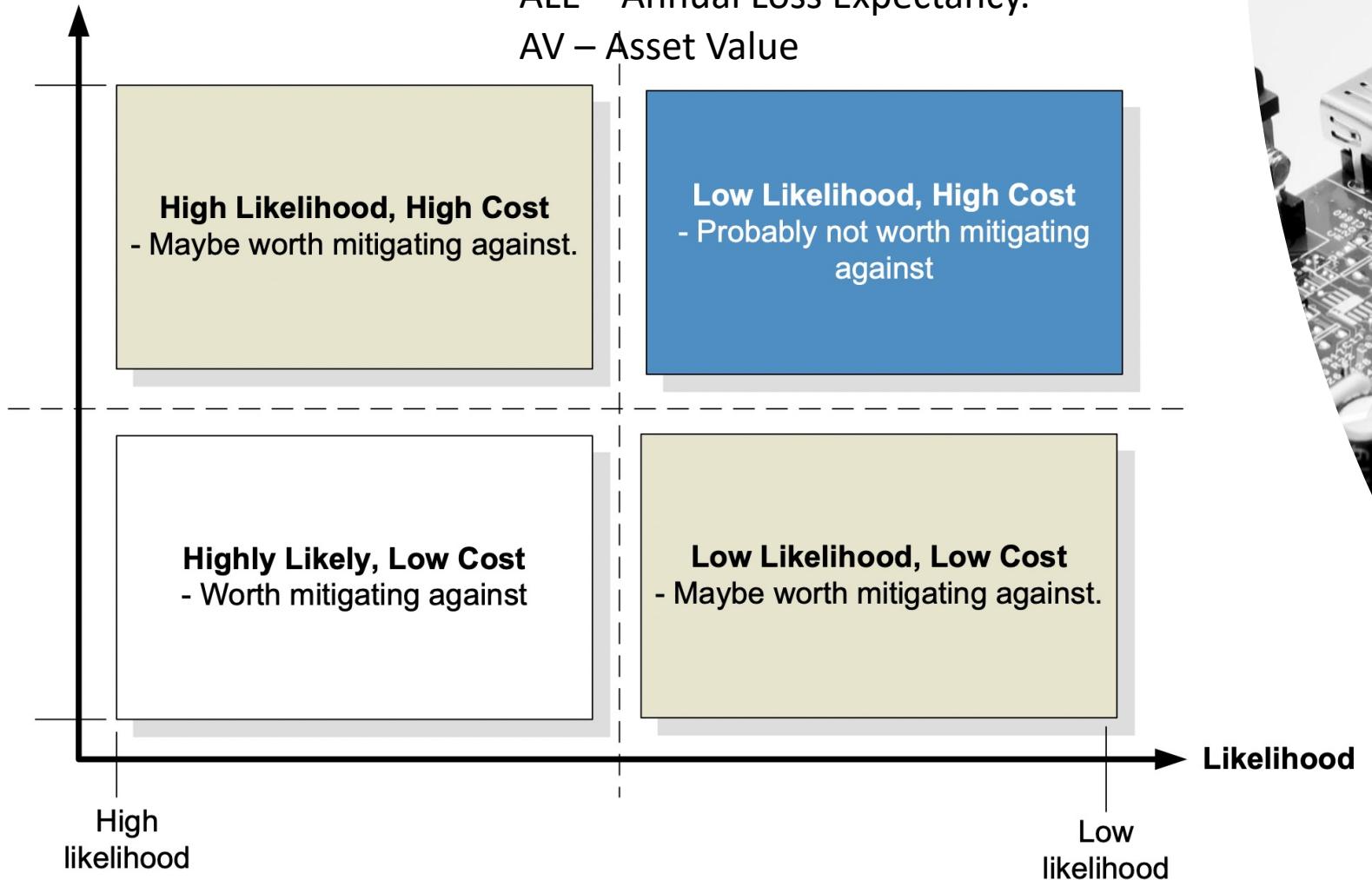
Risks, Costs and
Benefits

Risks, Costs and Benefits

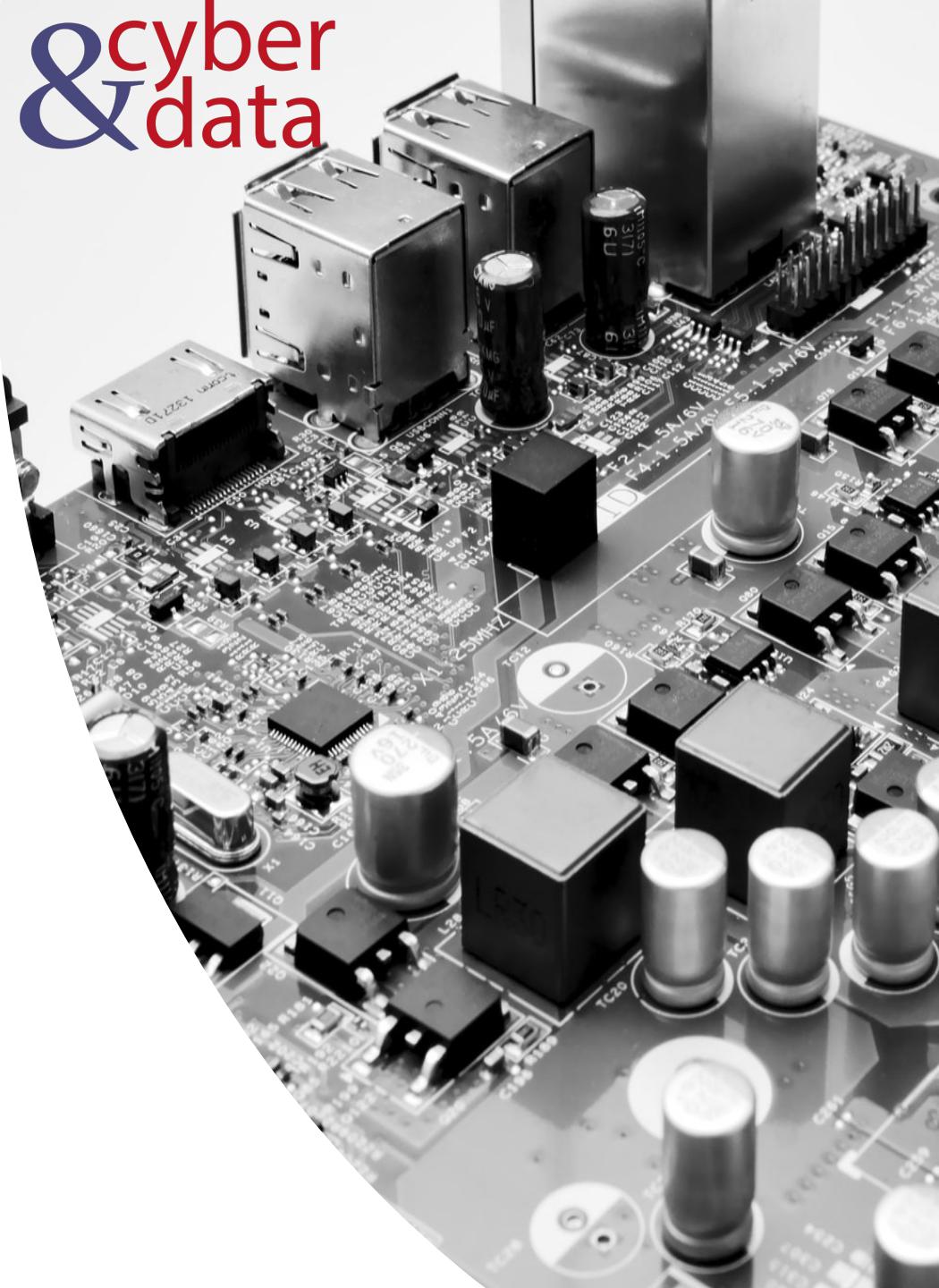
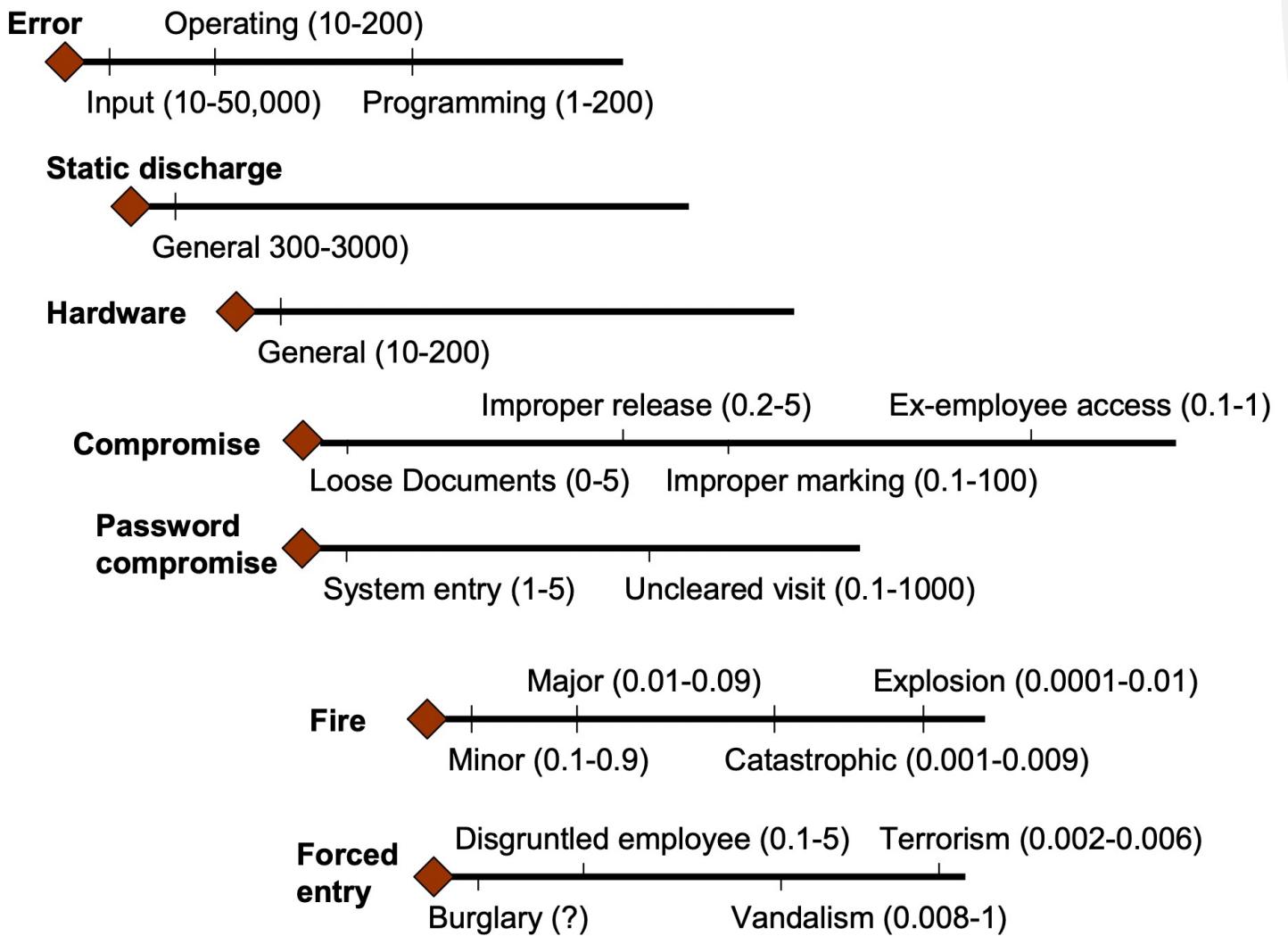
$$ALE = AV \times ARO$$

ALE – Annual Loss Expectancy.

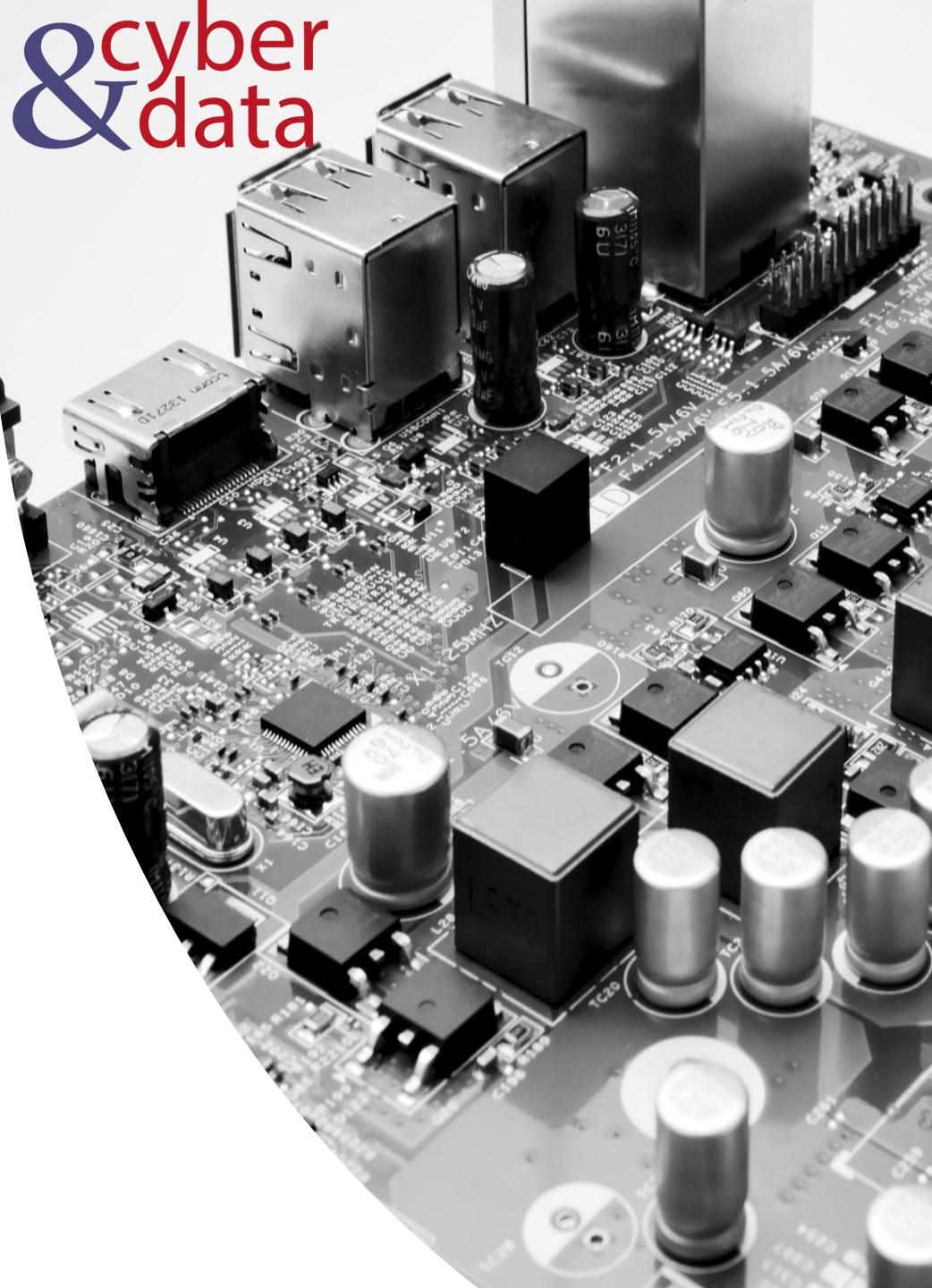
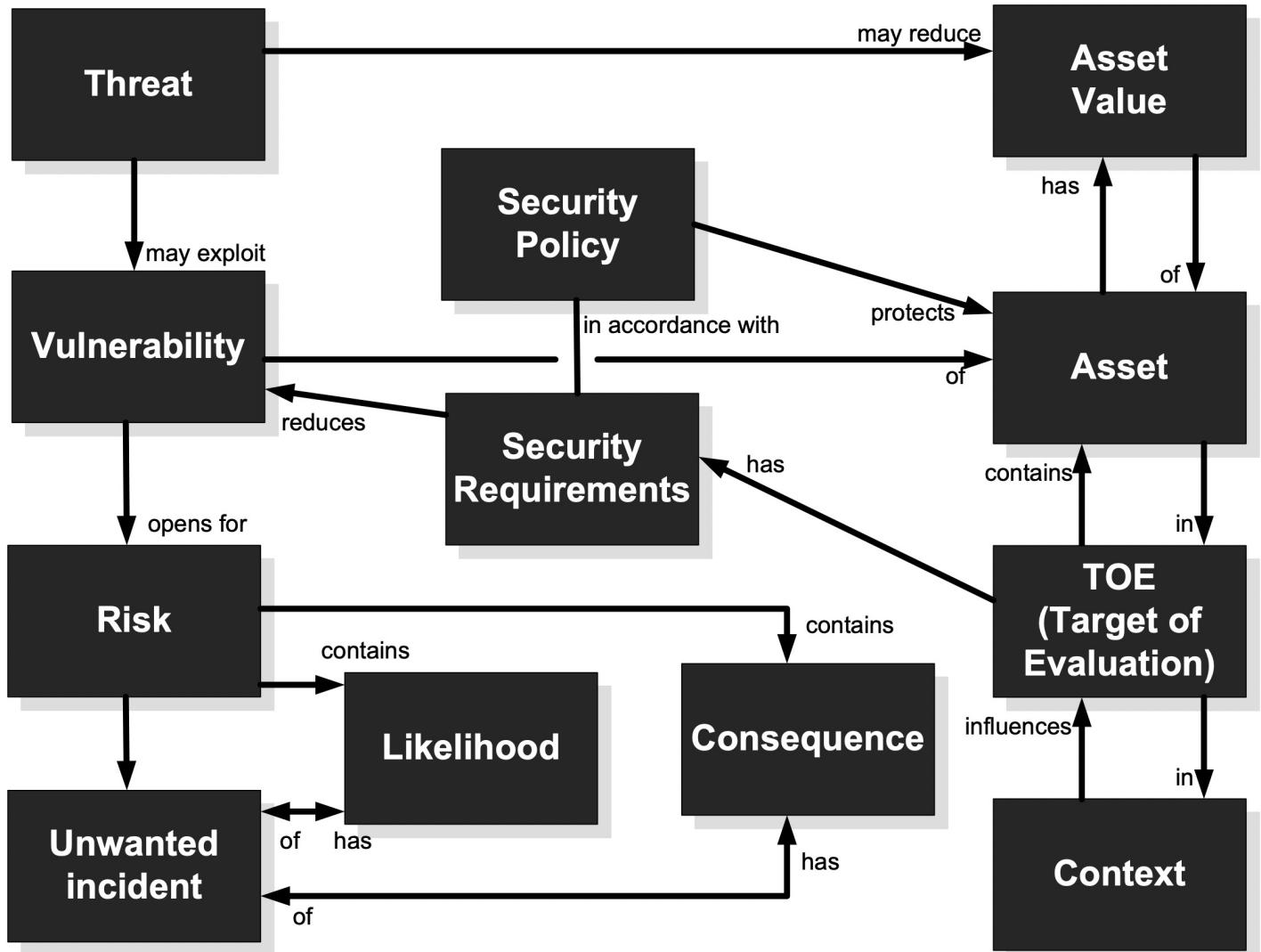
AV – Asset Value



Risks, Costs and Benefits

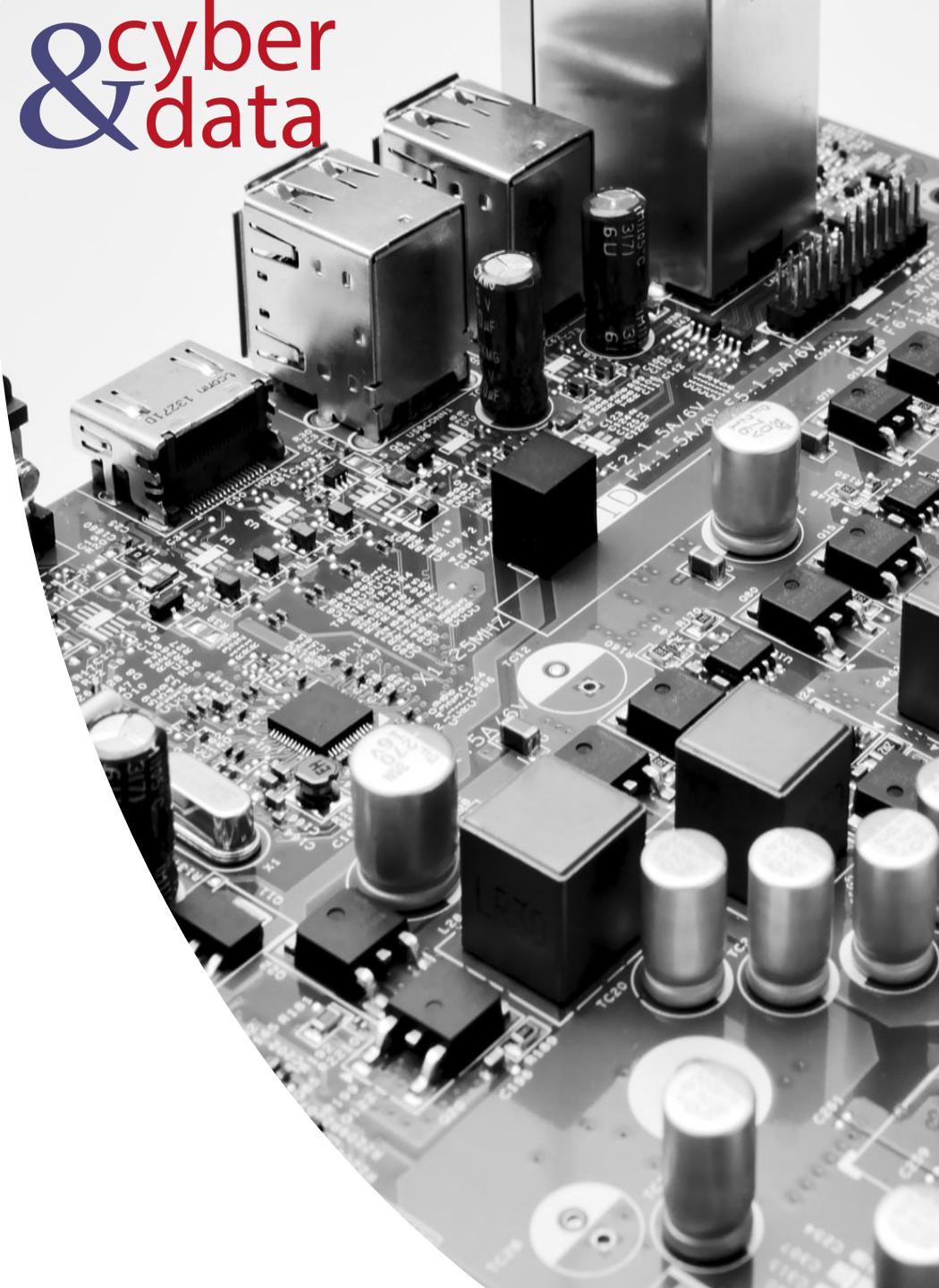
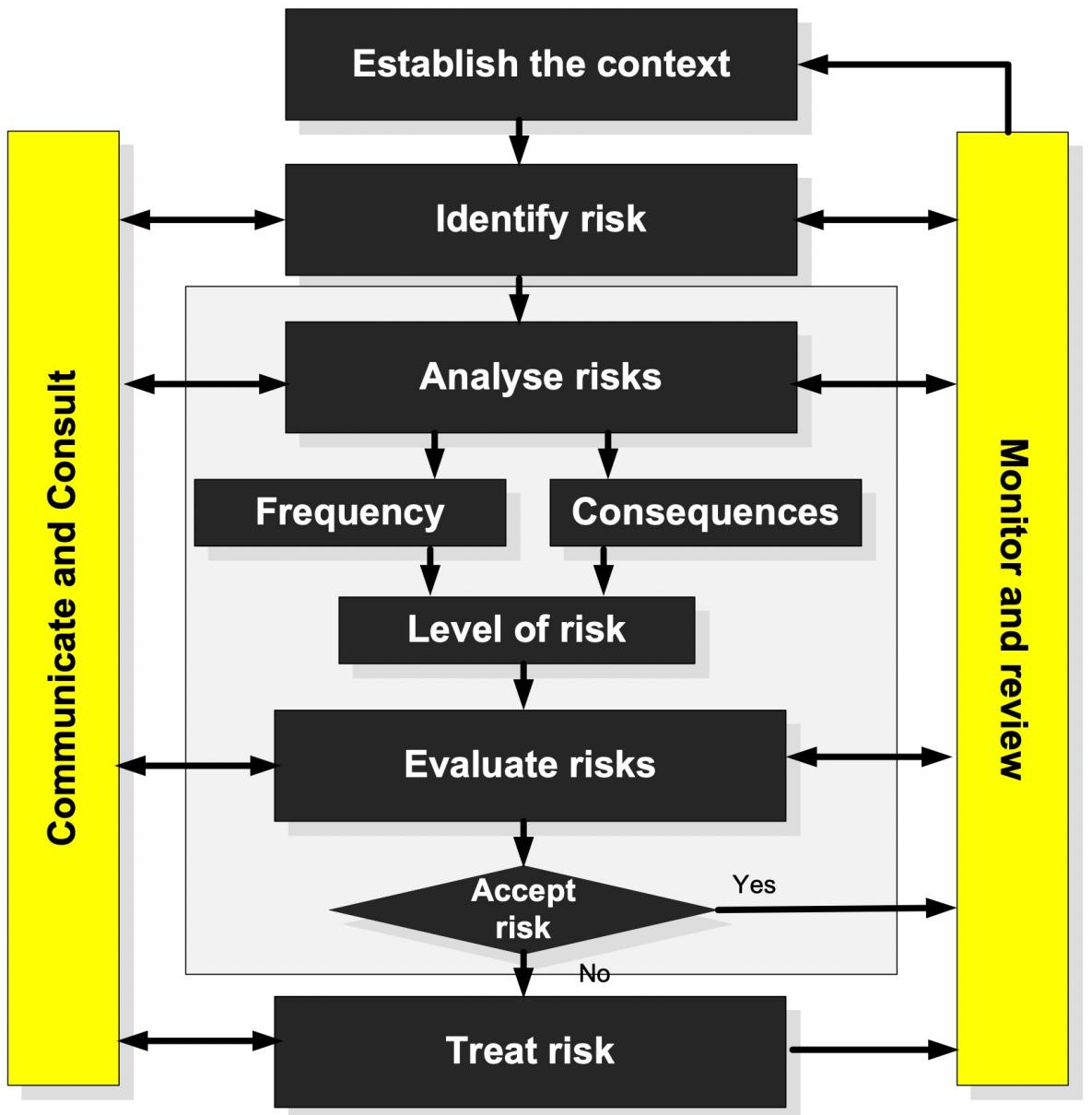


CORAS Ontology



cyber
&
data

CORAS Risk Management



cyber
&
data

cyber & data

“From bits to information”

Kill Chain Model

Incident Taxonomy

A Threat:

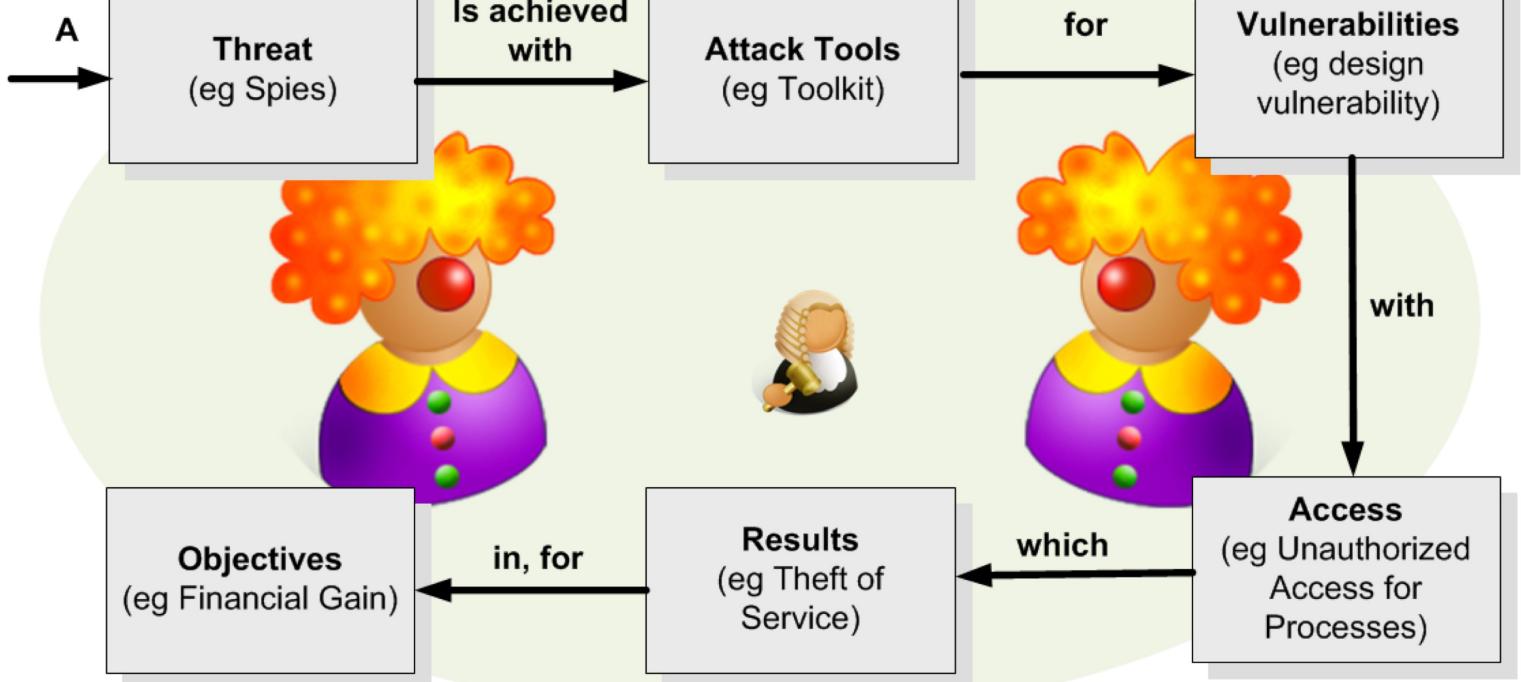
- Hacker.
- Spies
- Terrorists.
- Corporate Raiders.
- Professional Criminals.
- Vandals.
- Military Forces.

is achieved with Attack Tools:

- User command.
- Script or program.
- Autonomous Agent.
- Toolkit
- Distributed Tool.
- Data Tap.

for Vulnerabilities:

- Implementation vulnerability.
- Design vulnerability.
- Configuration vulnerability.



for Objectives:

- Challenge/Status.
- Political Gain.
- Financial Gain.
- Damage.
- Destruction of an Enemy.

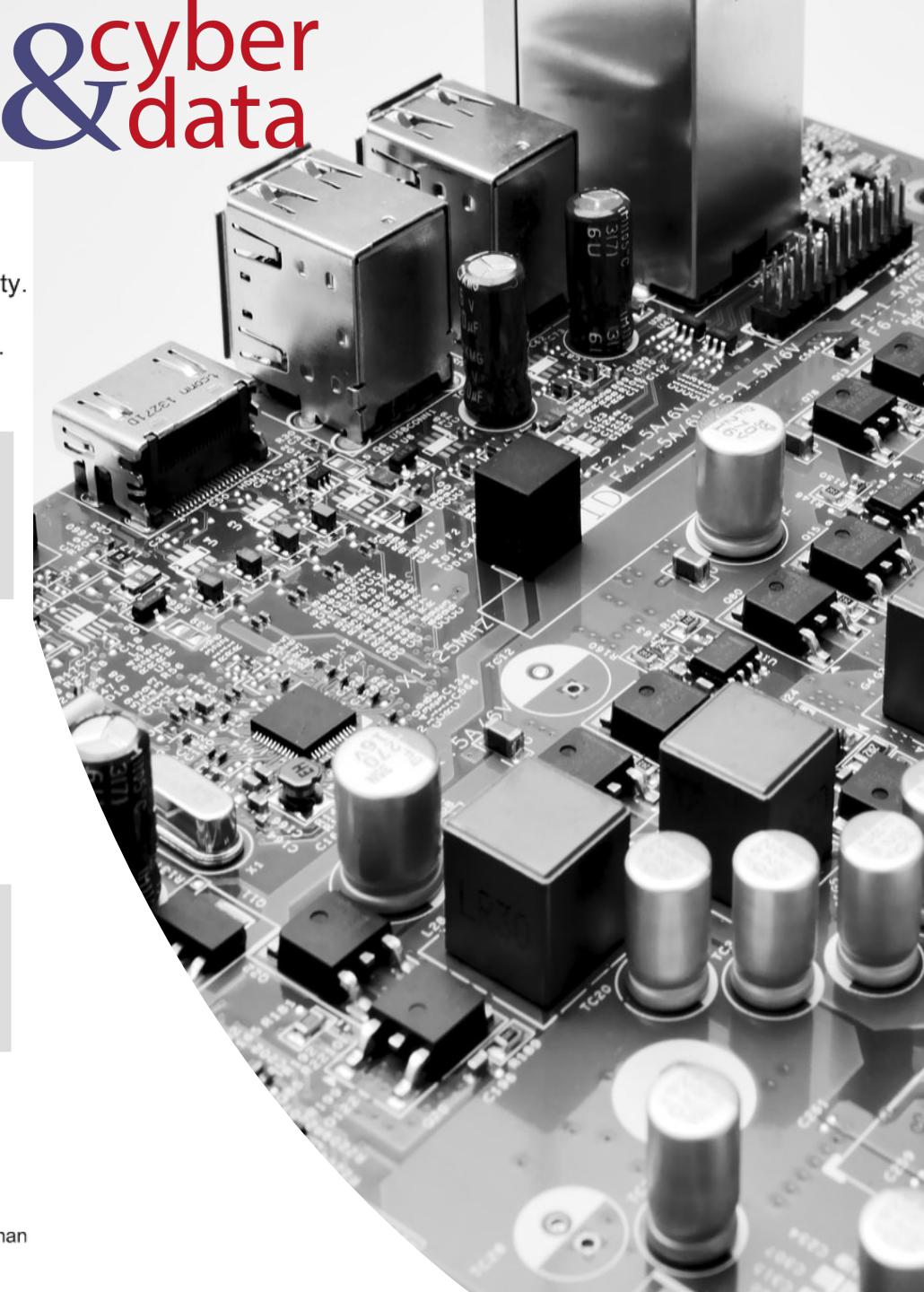
which Results in:

- Corruption of Information.
- Disclosure of Information.
- Theft of Service.
- Denial-of-Service.

with Access for:

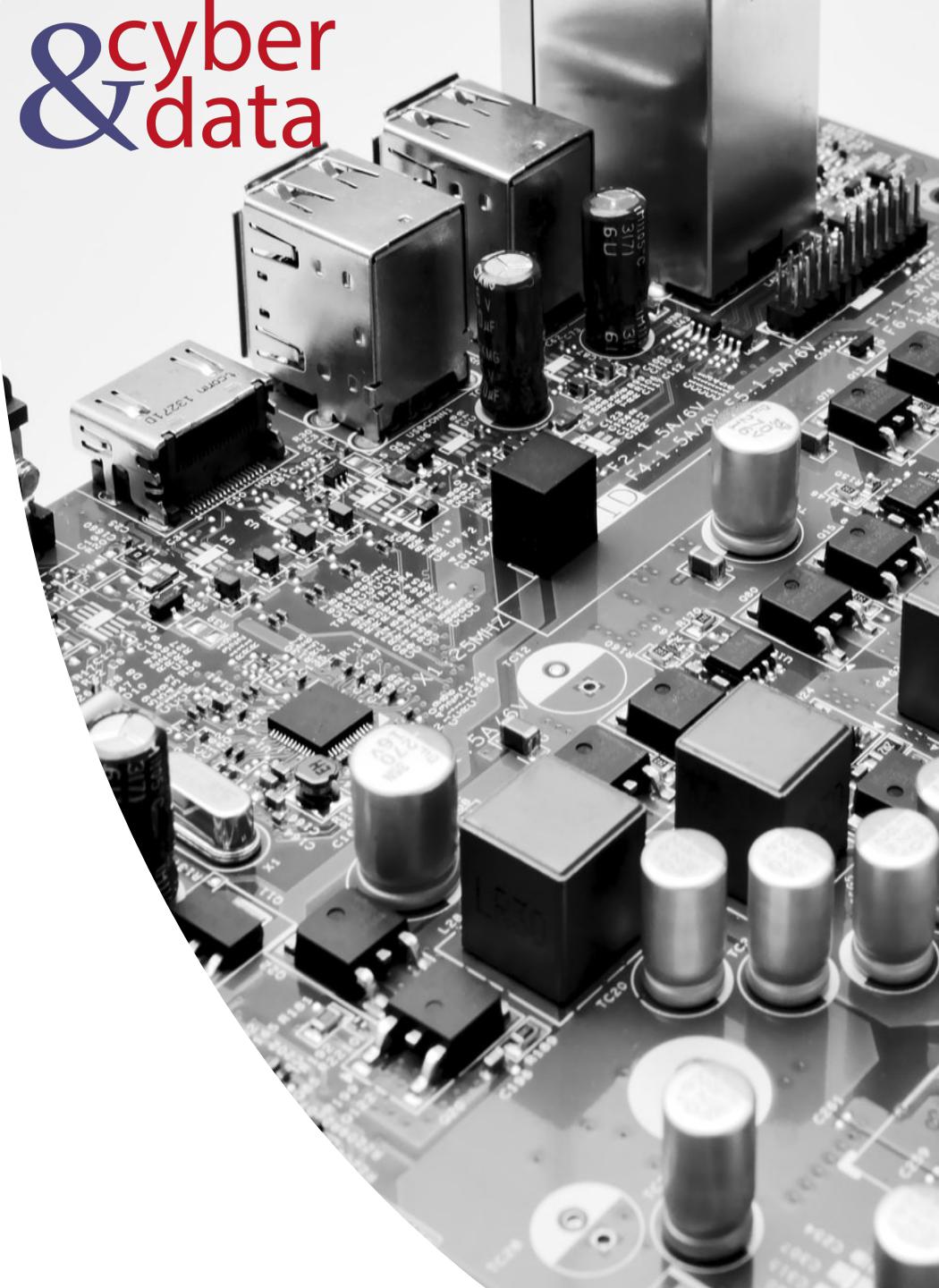
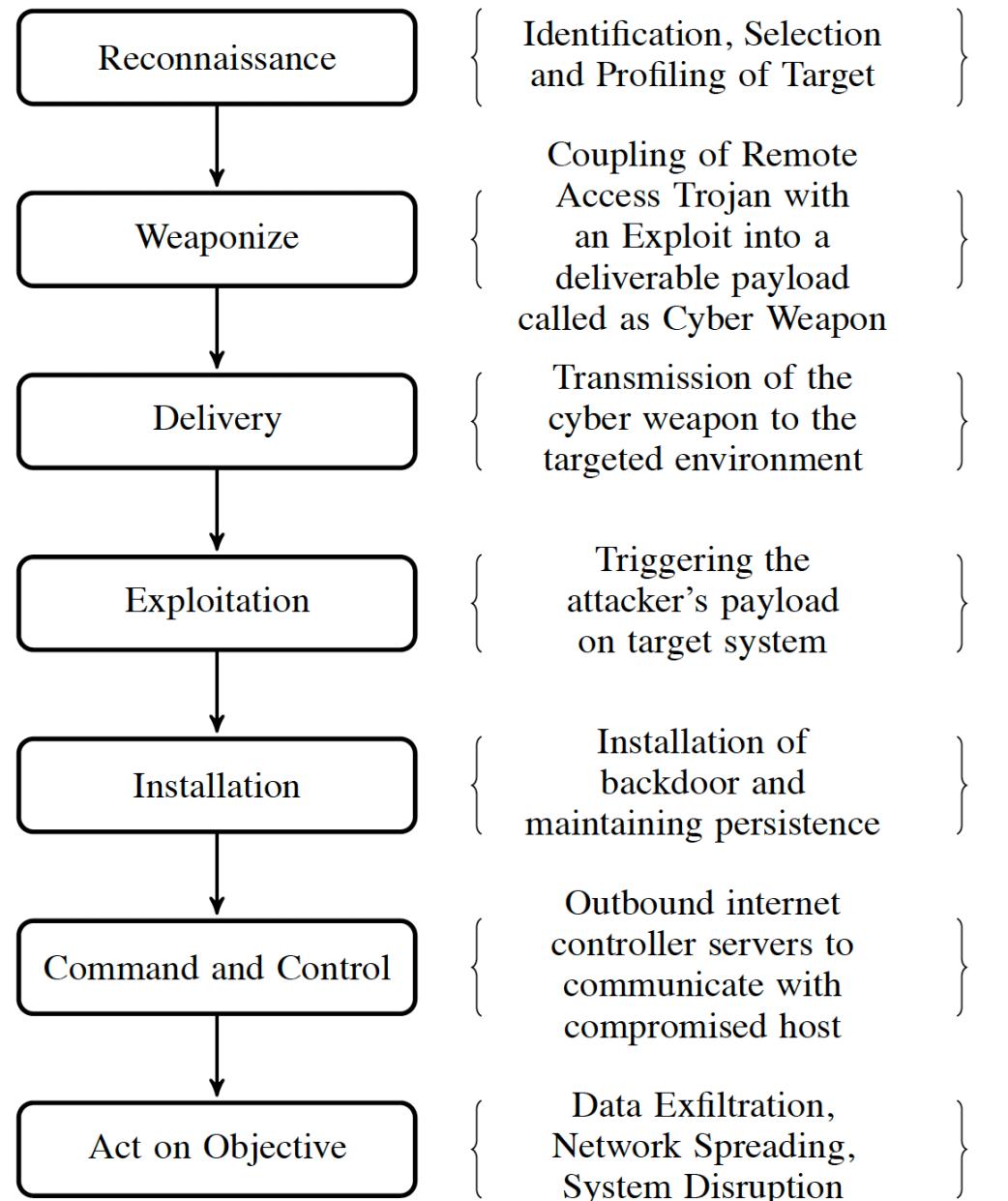
- Files.
- Data in transit.
- Objects in Transit.
- Invocations in Transit.

Author: Prof Bill Buchanan



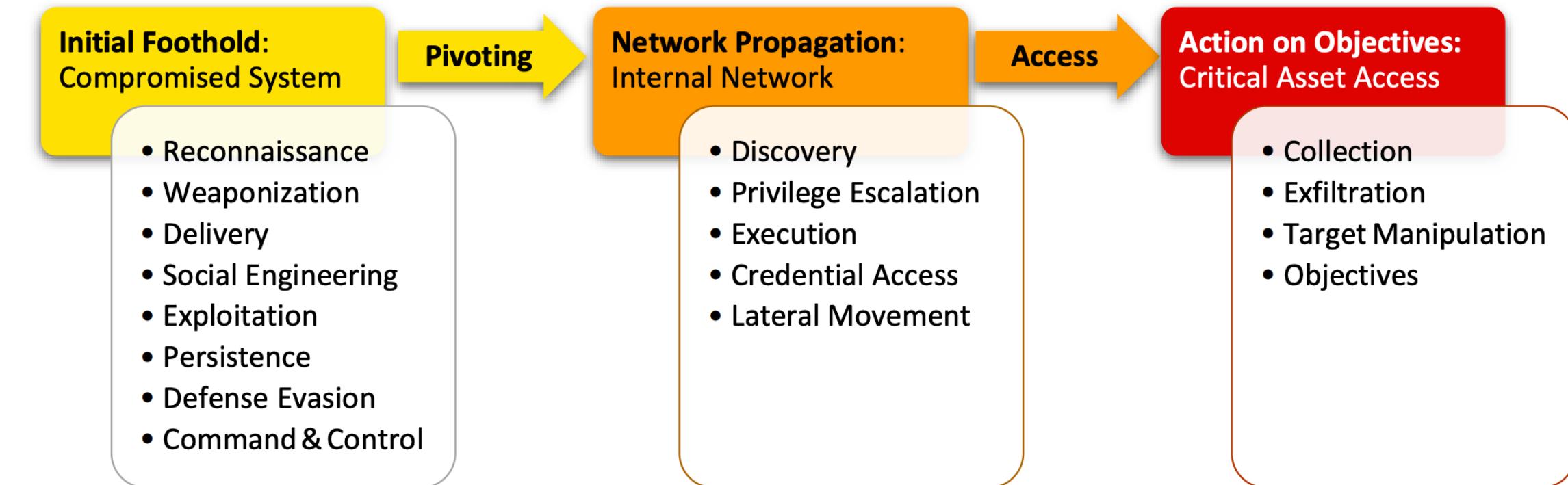
cyber
&
data

Kill Chain Model



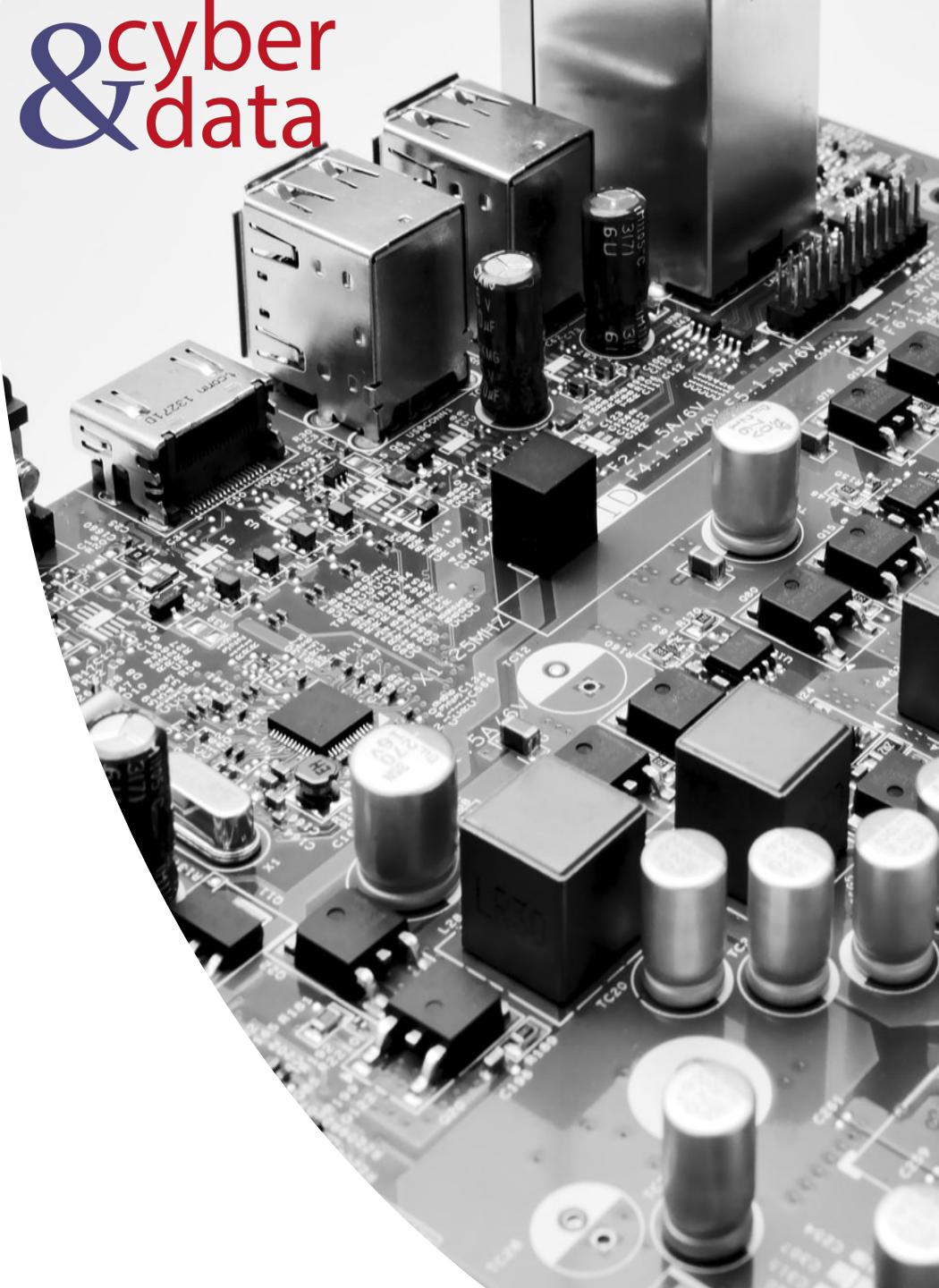
Unified Kill Chain Phases

cyber
& data



Unified Kill Chain Model

#	<i>Unified Kill Chain</i>	<i>Cyber Kill Chain® (CKC)</i>					<i>UKC after literature study</i>					<i>UKC after Red Team C1</i>					<i>UKC after Red Team C2</i>					<i>UKC after Red Team C3</i>					<i>UKC after Red Team KC</i>				
		<i>Laliberte</i>	<i>Nachreiner</i>	<i>Bryant</i>	<i>Malone</i>	<i>MITRE ATT&CK™</i>	<i>UKC after literature study</i>	<i>UKC after Red Team C1</i>	<i>UKC after Red Team C2</i>	<i>UKC after Red Team C3</i>	<i>UKC after Red Team KC</i>	<i>UKC after APT28 C4 & KC</i>																			
1	<i>Reconnaissance</i>	1	1	1	1	1	1	1	1	1	1	1																			
2	<i>Weaponization</i>	2	3	3	3	2	2	2	2	2	2	2																			
3	<i>Delivery</i>	3	5	5	6	3	7	7	3	3	3	3																			
4	<i>Social Engineering</i>	5	6	6	11	5	3	3	4	4	4	4																			
5	<i>Exploitation</i>	6	8	8	14	6	5	4	5	5	5	5																			
6	<i>Persistence</i>	8	14	9	18	8	6	6	5	6	6	6																			
7	<i>Defense Evasion</i>	18	18	14	16	10	11	8	6	7	7	7																			
8	<i>Command & Control</i>		18			5	7	9	8	8	8	8																			
9	<i>Pivoting</i>					11	13	11	9	9	9	9																			
10	<i>Discovery</i>					14	10	10	11	11	11	10																			
11	<i>Privilege Escalation</i>					17	14	14	10	10	10	11																			
12	<i>Execution</i>					18	12	12	14	14	14	12																			
13	<i>Credential Access</i>						15	13	12	12	12	13																			
14	<i>Lateral Movement</i>						16	17	13	13	13	14																			
15	<i>Collection</i>						8	15	17	17	17	15																			
16	<i>Exfiltration</i>							16	15	15	15	15																			
17	<i>Target Manipulation</i>								16	16	16	16																			
18	<i>Objectives</i>											18																			



cyber
&
data

cyber & data

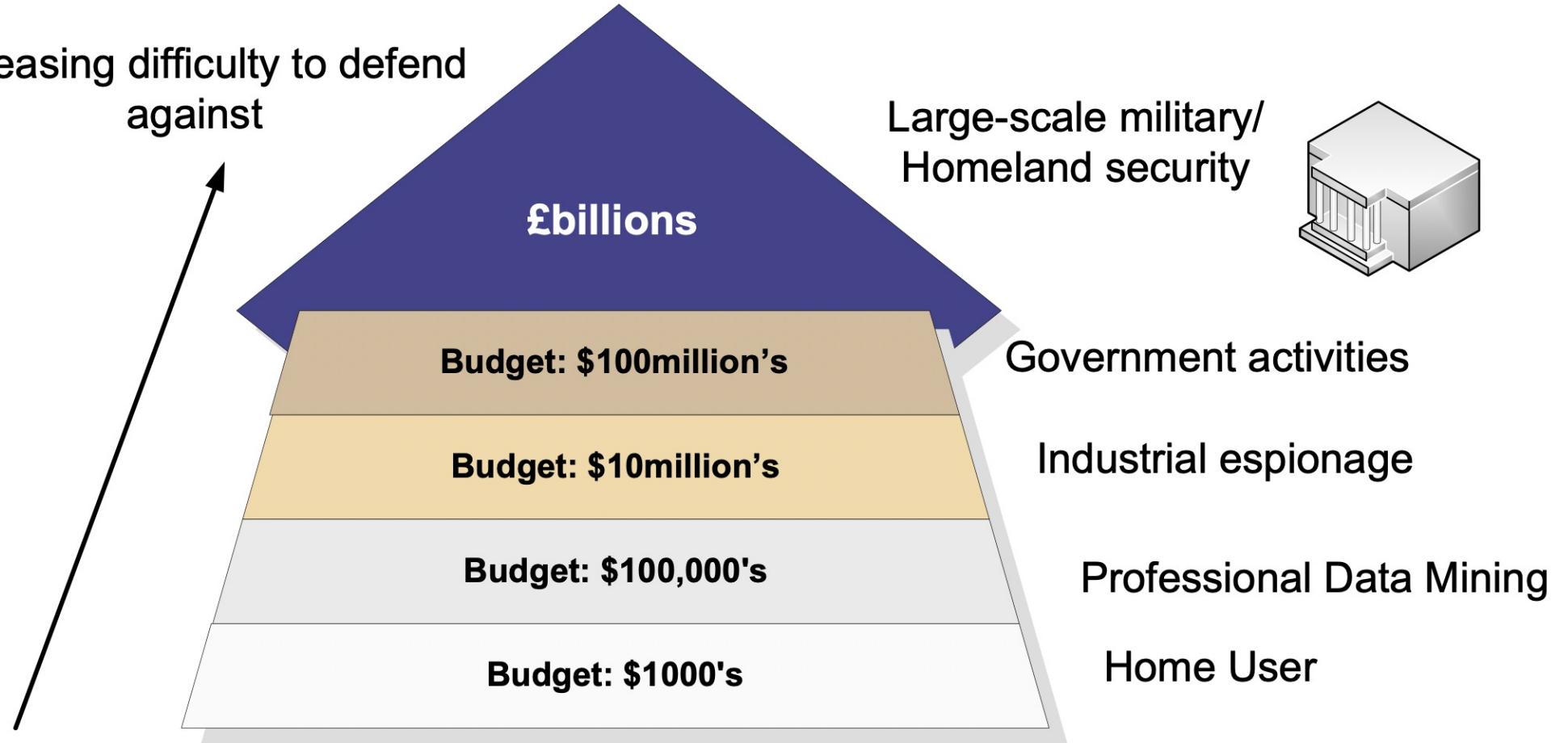
“From bits to information”

Defence
Mechanisms

Types of intelligence

Aims/objectives

- ## Increasing difficulty to defend against



often causes the most problems

cyber & data

"From bits to information"

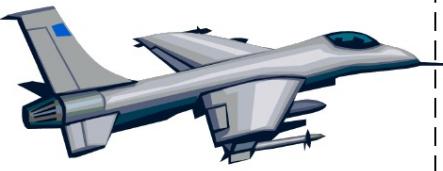
Defence in Depth

Defence in depth

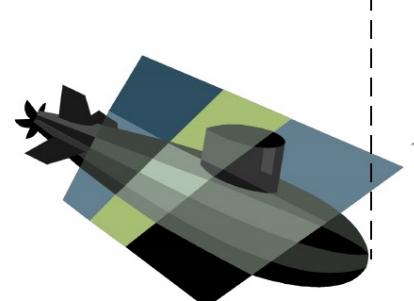
cyber
&
data



Defence



Defence



Forth-level
defence



Defence



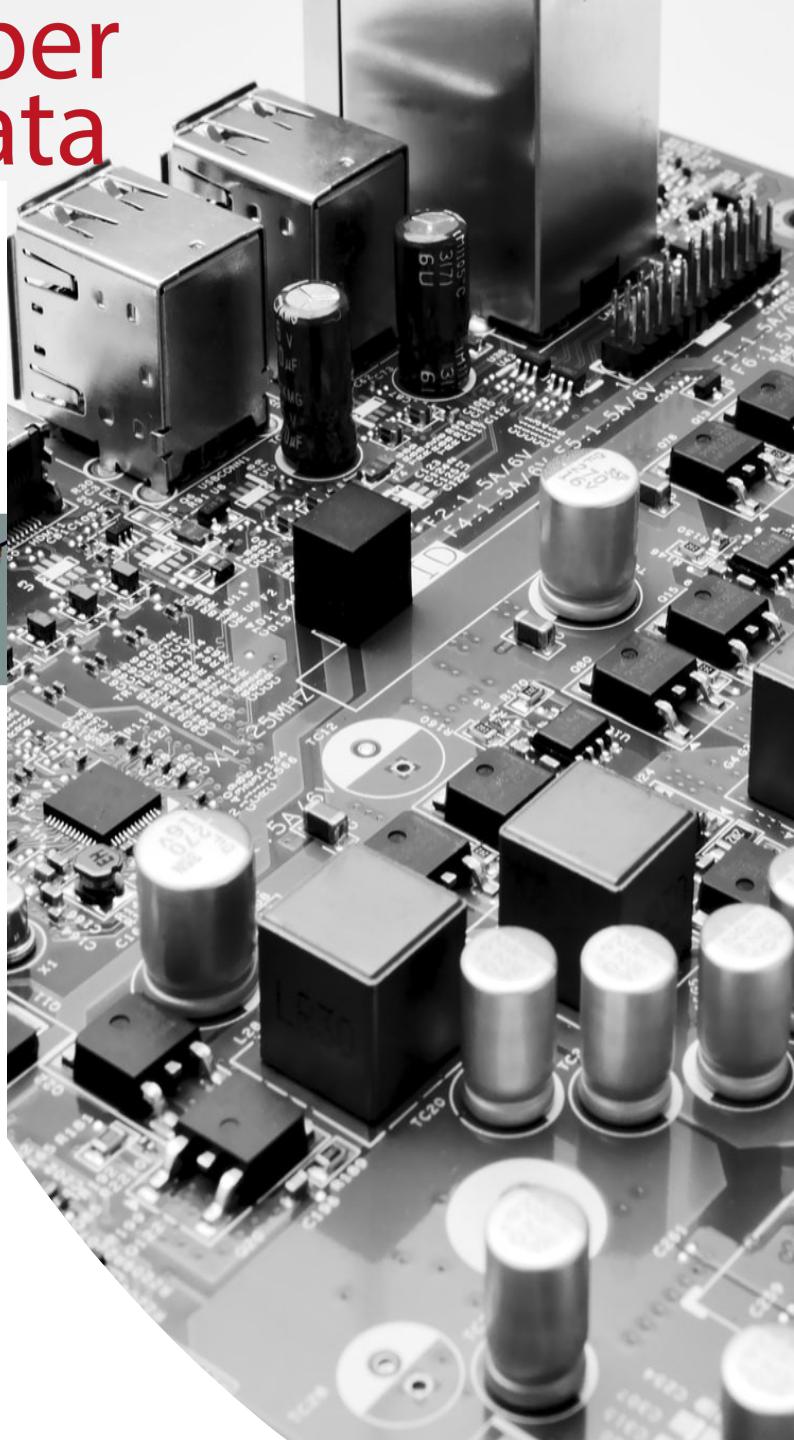
Second-level
defence



Defence

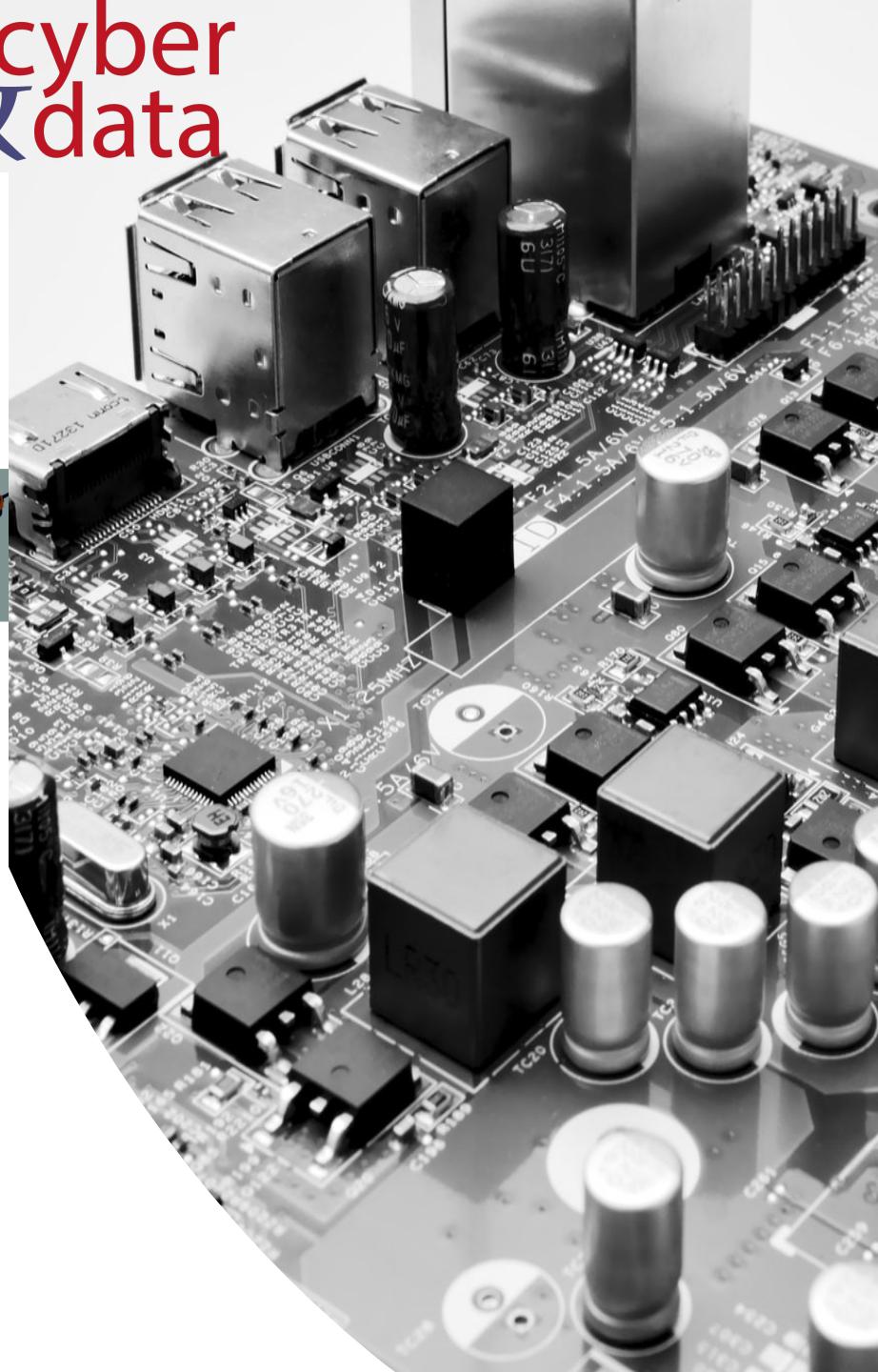
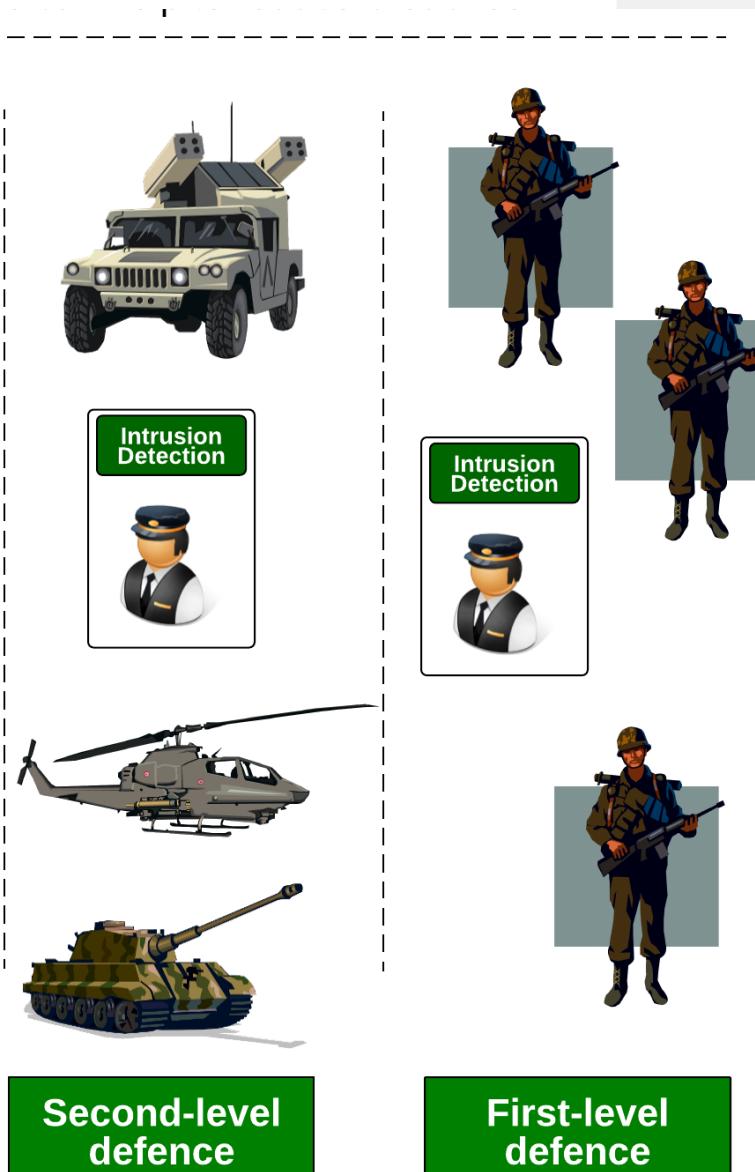
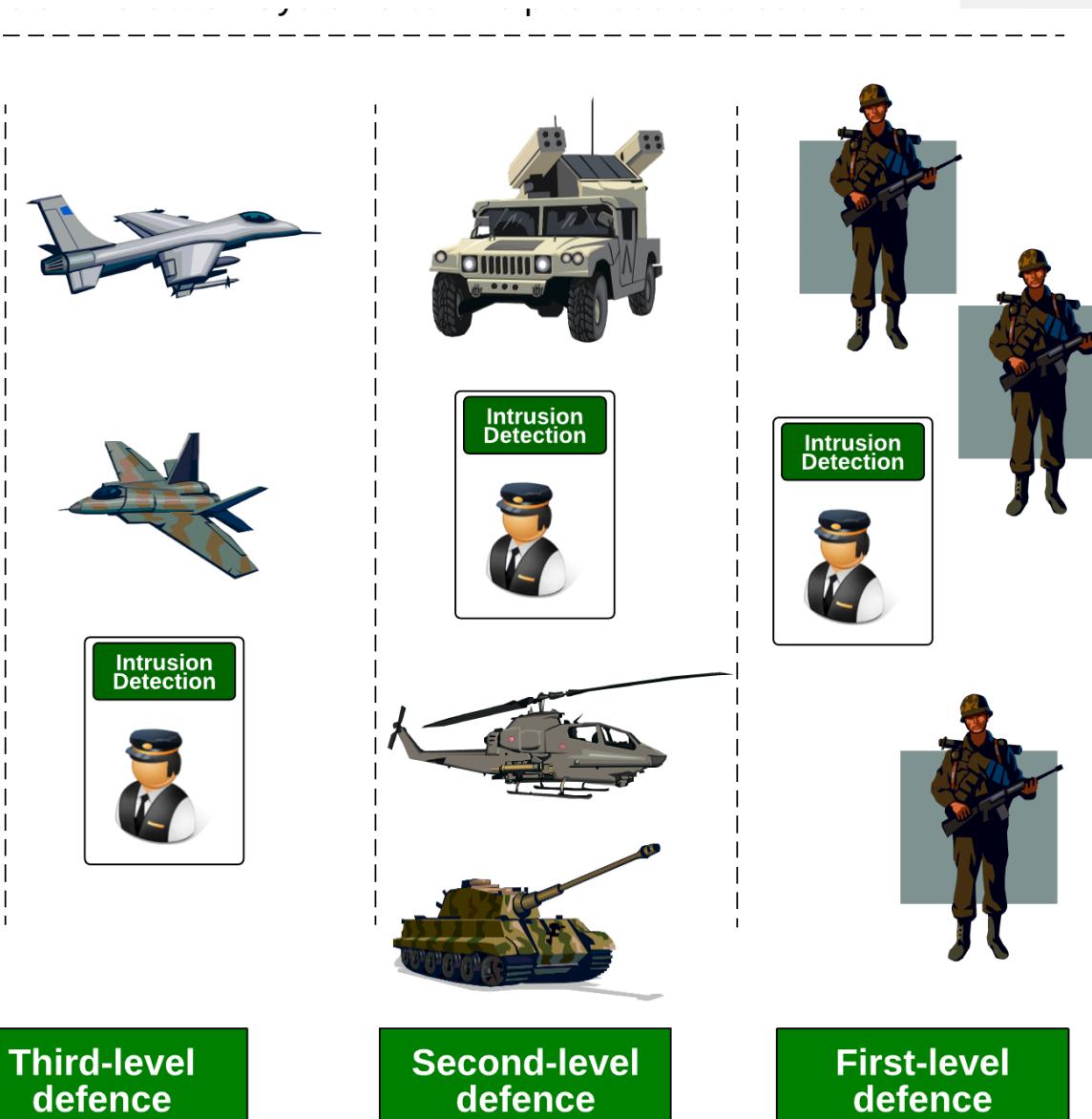
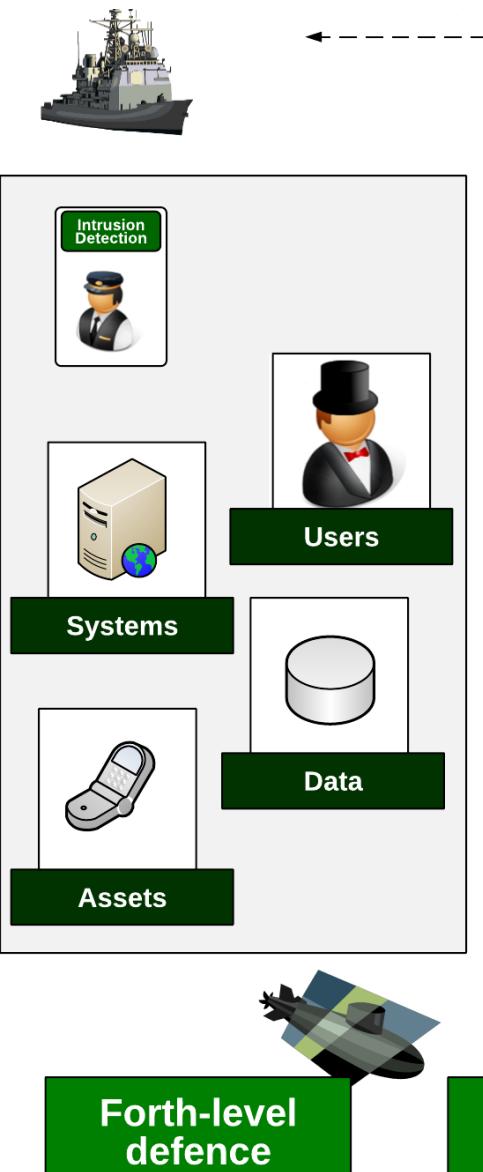


First-level
defence



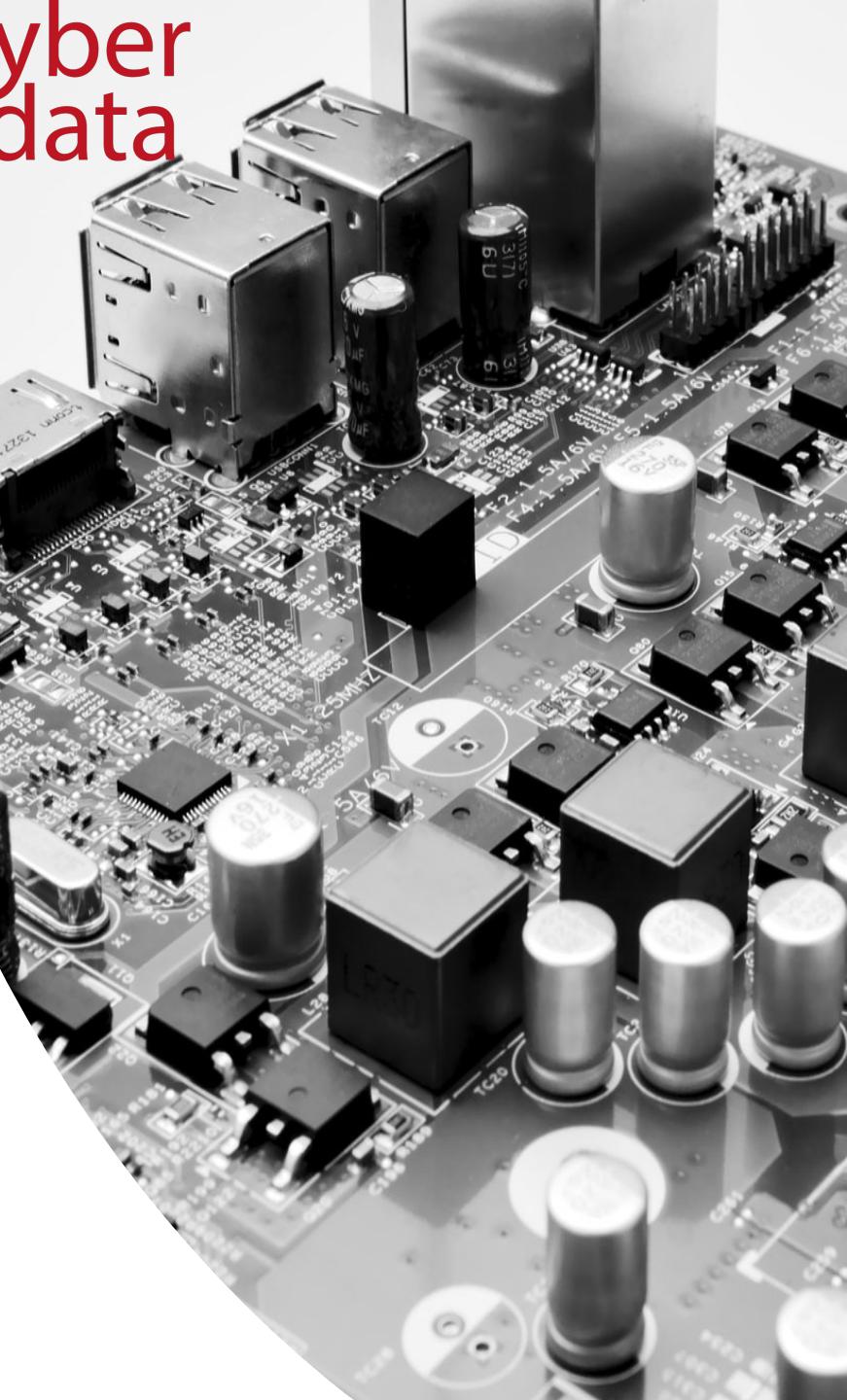
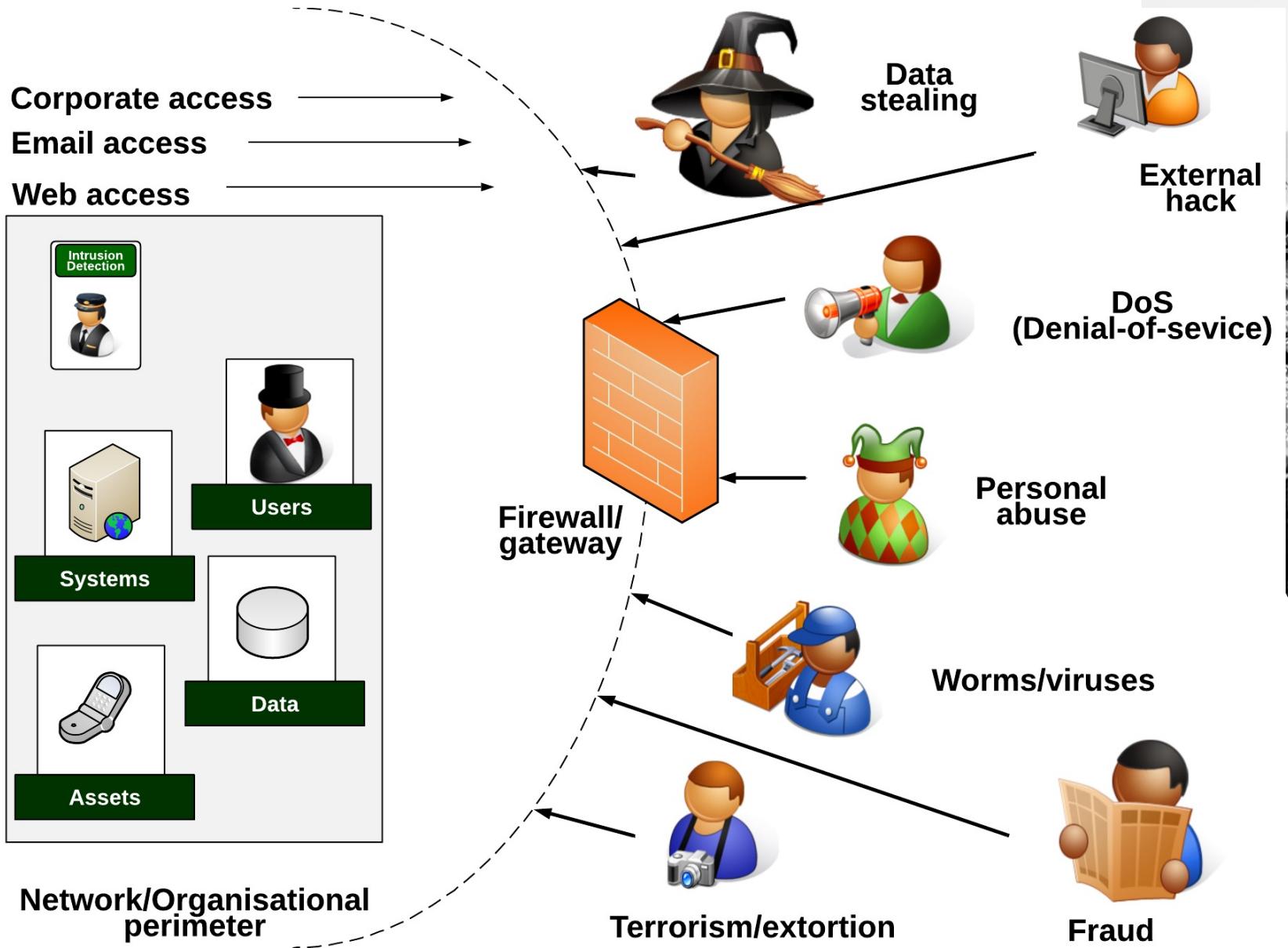
Defence in depth

cyber
& data



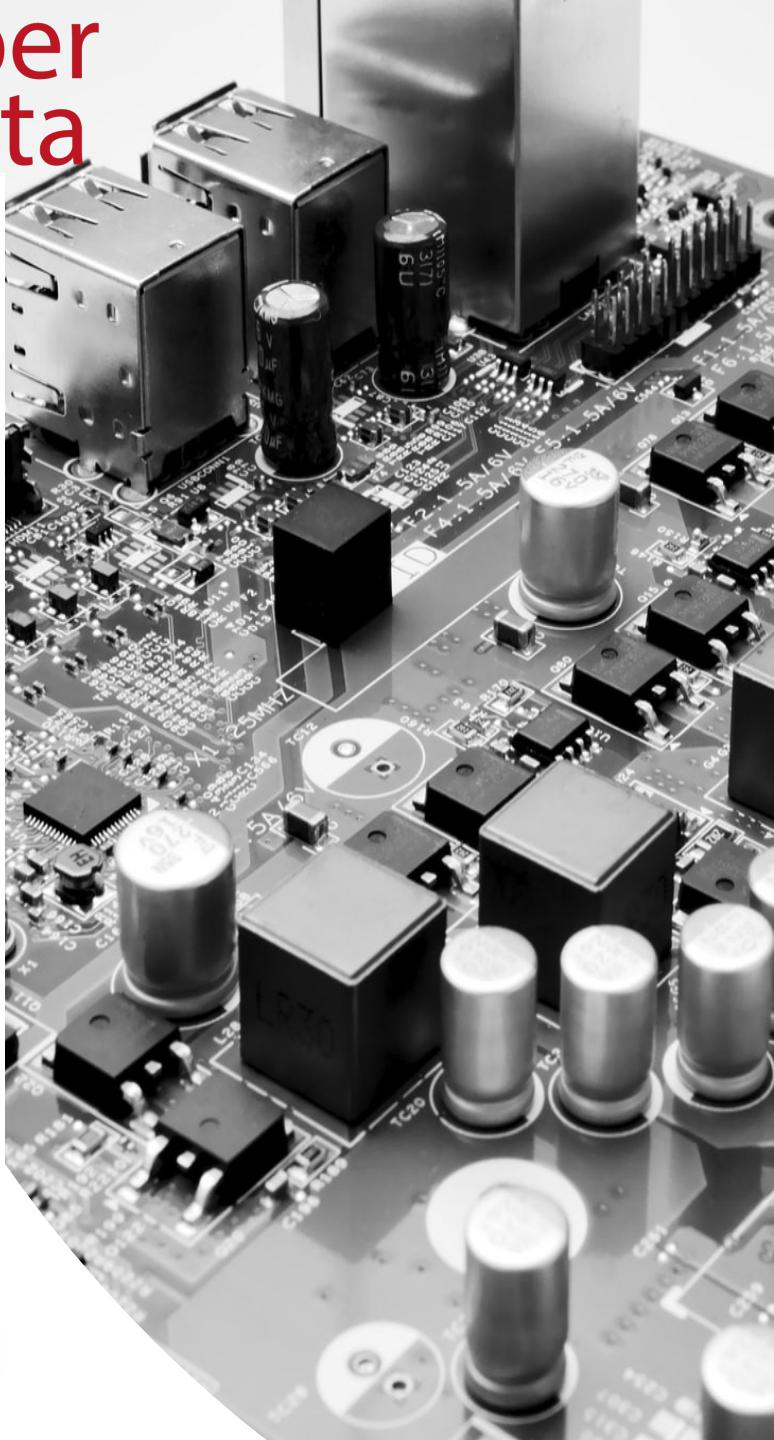
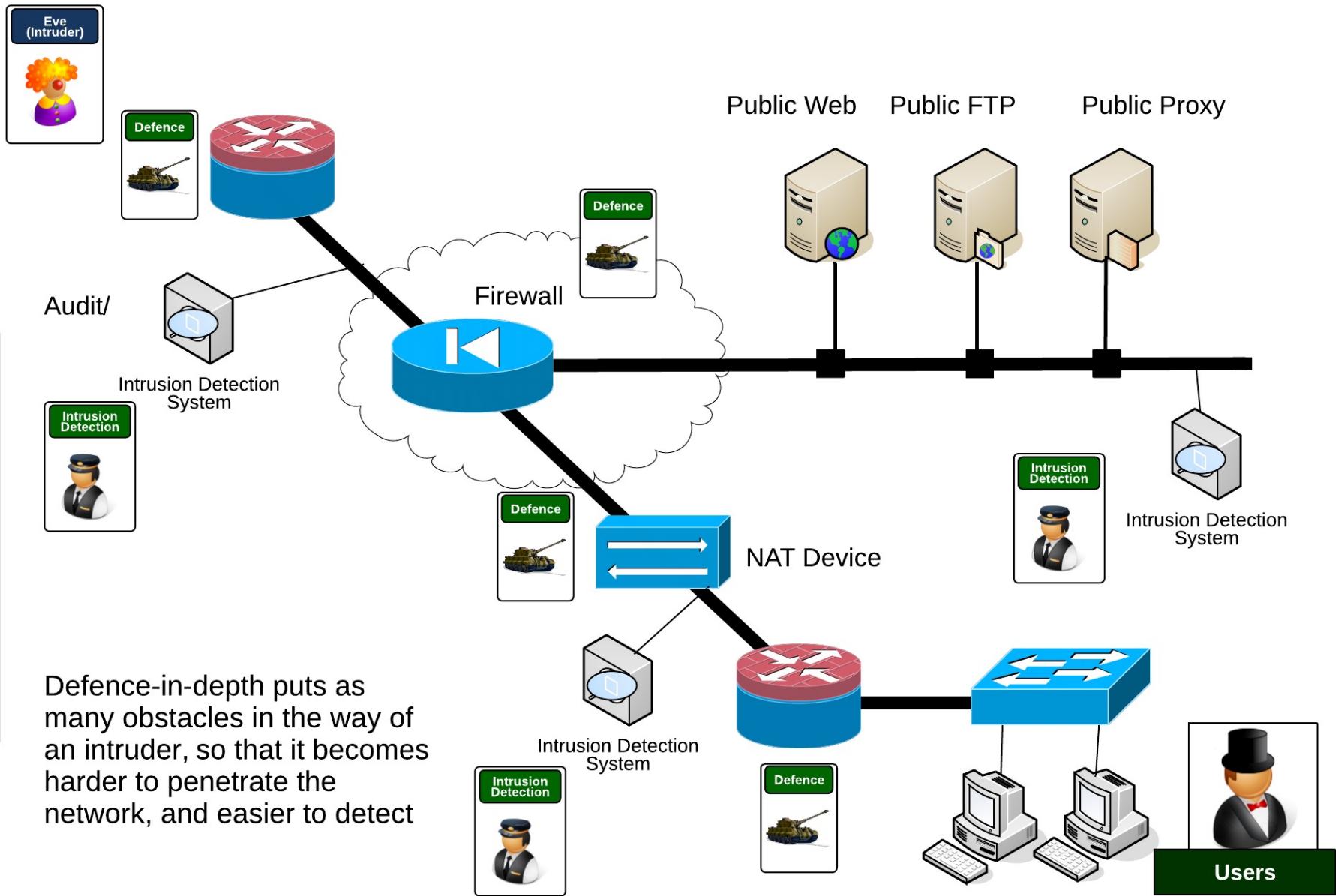
Threats

cyber
& data



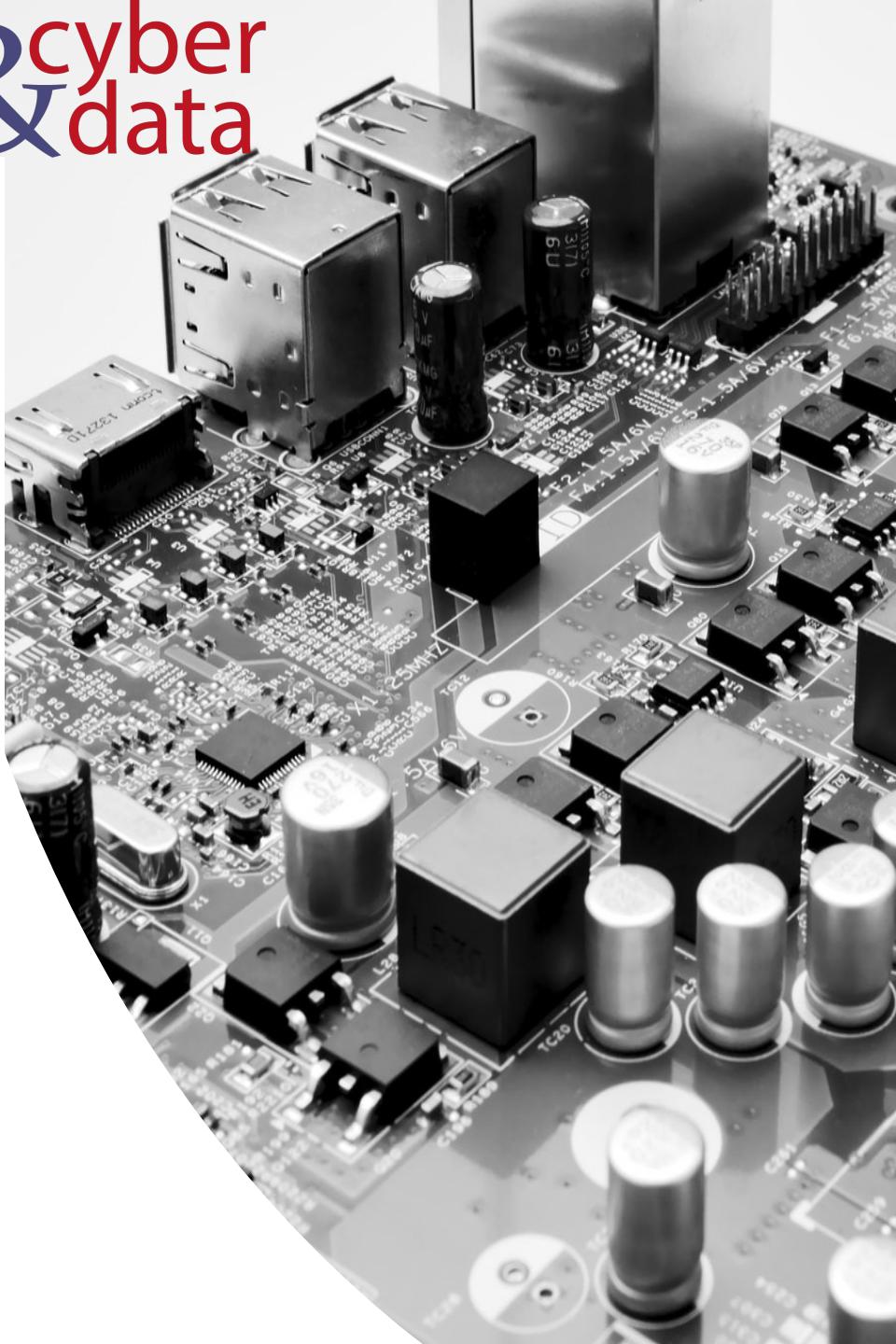
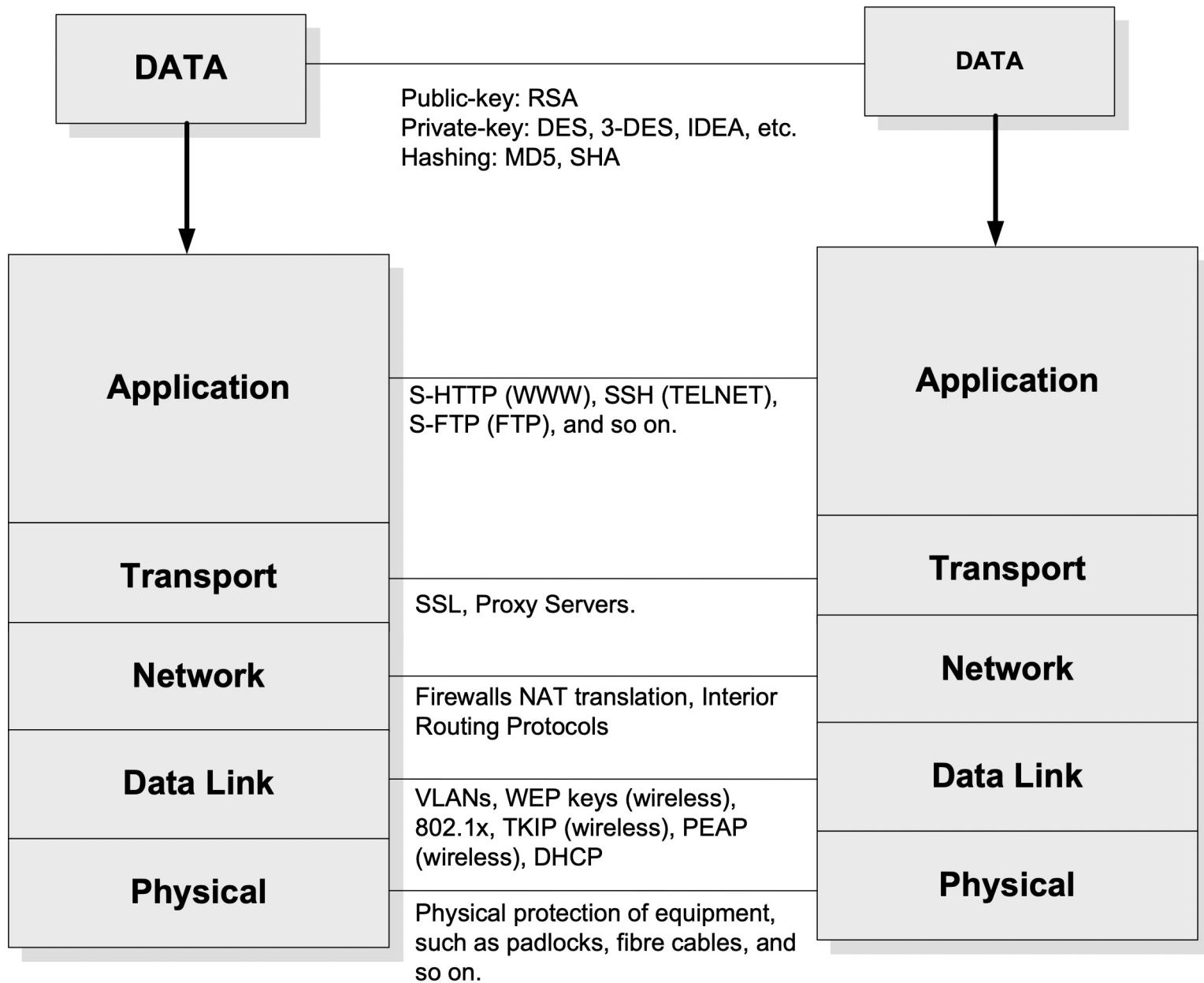
Defence in depth

cyber
& data



Layered Model

cyber
&
data



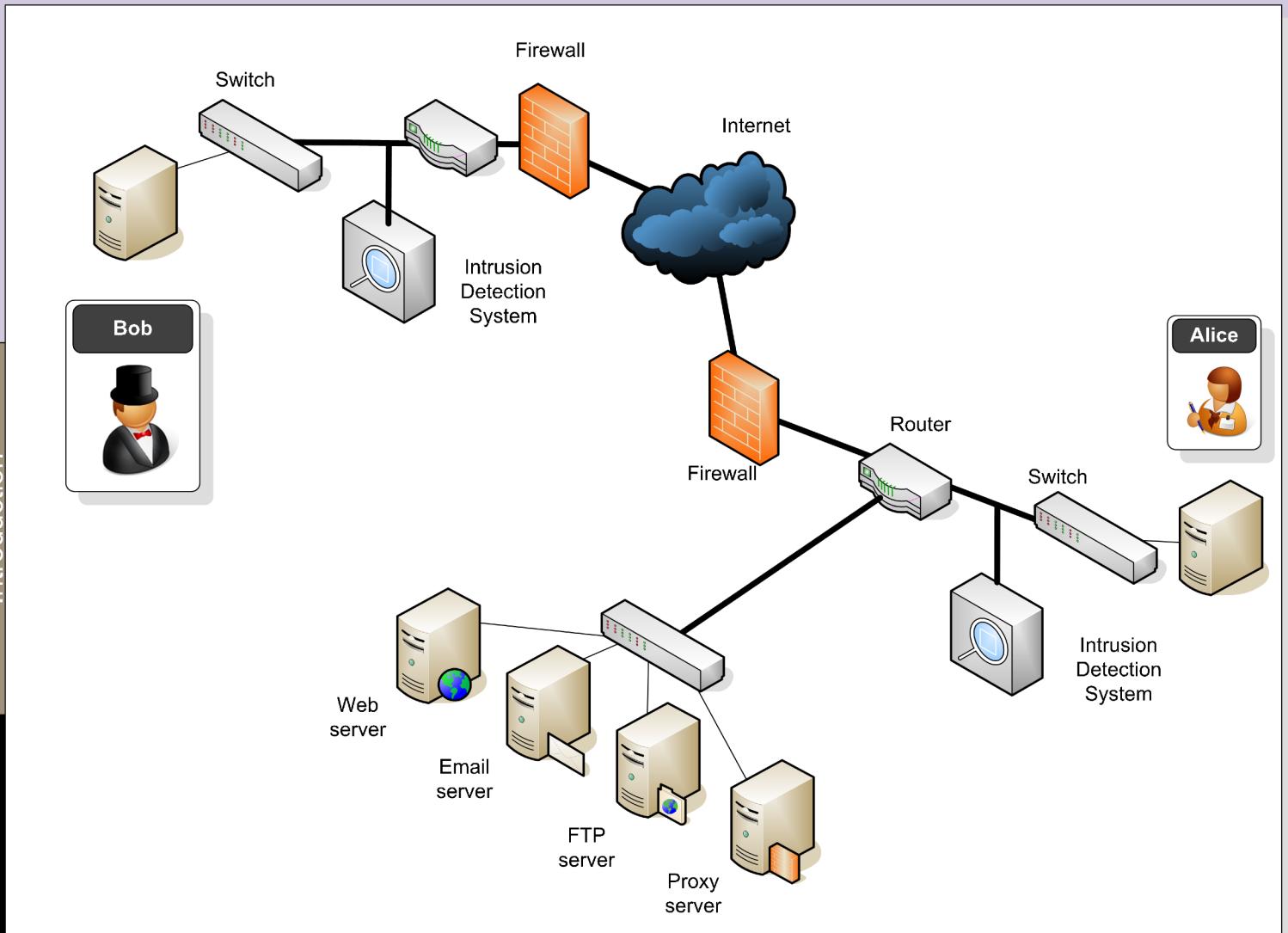
cyber & data

“From bits to information”

Network Security

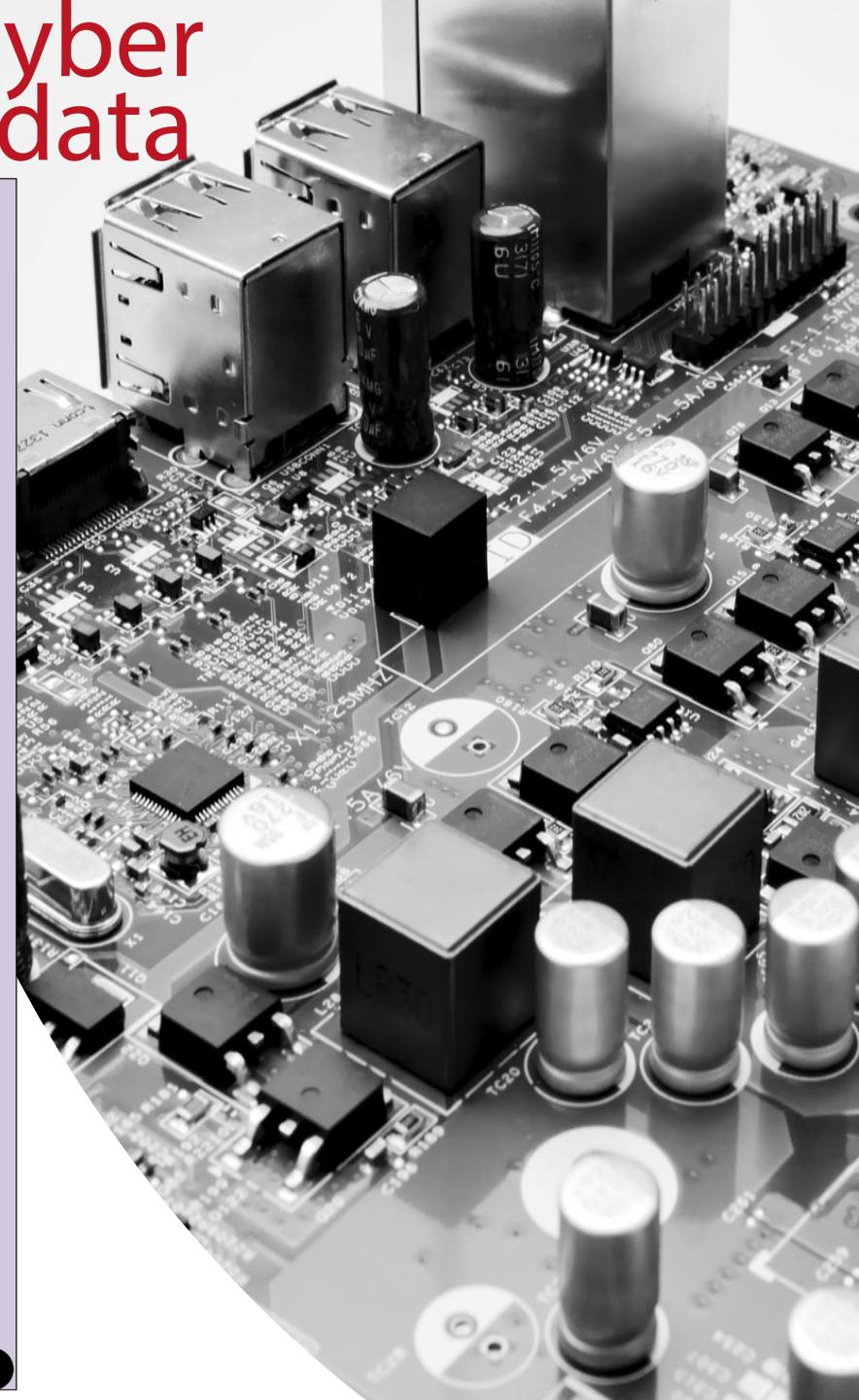
Layered Model

cyber
&
data



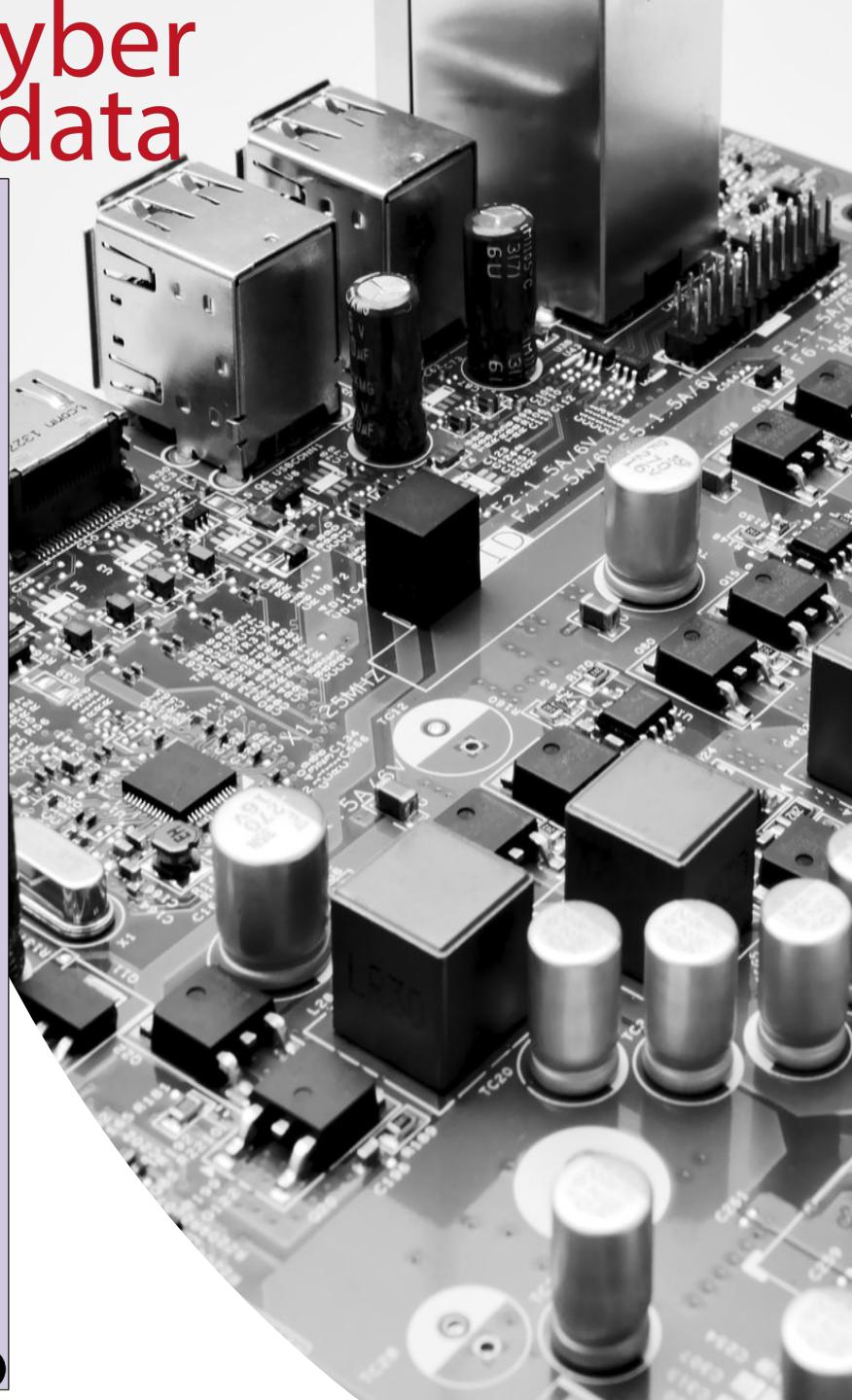
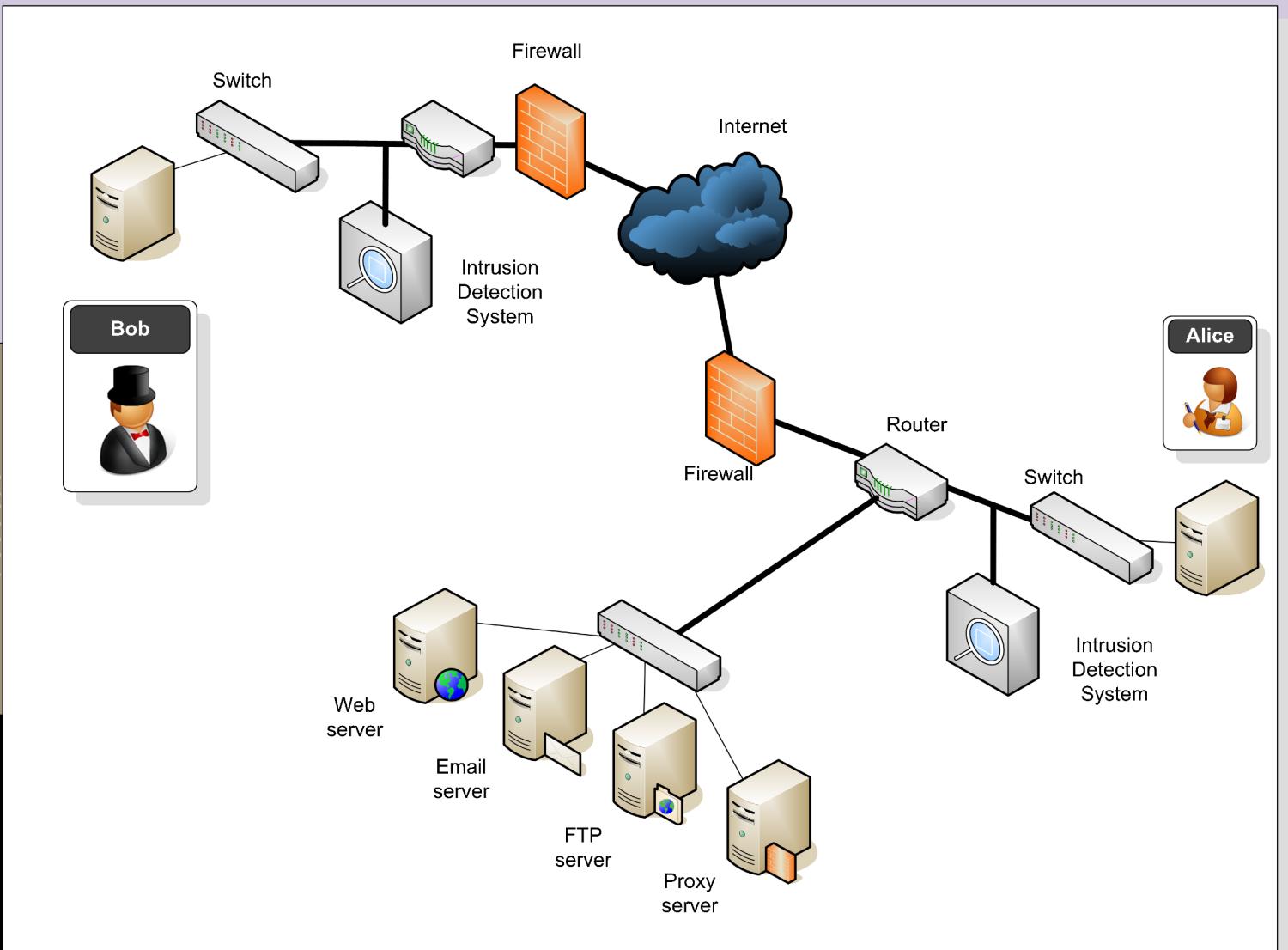
Author: Prof Bill Buchanan

Example Infrastructure



Layered Model

cyber
&
data

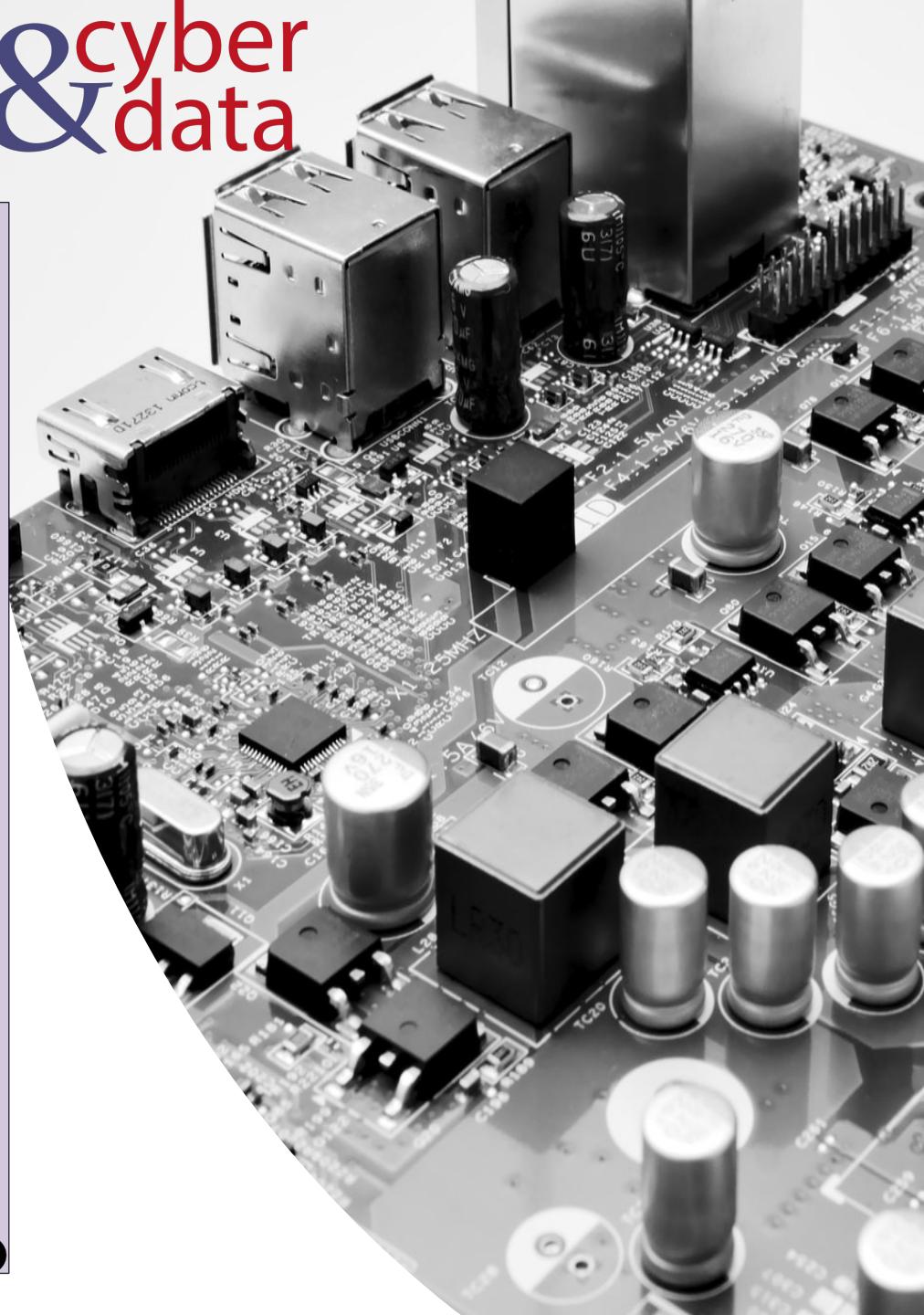
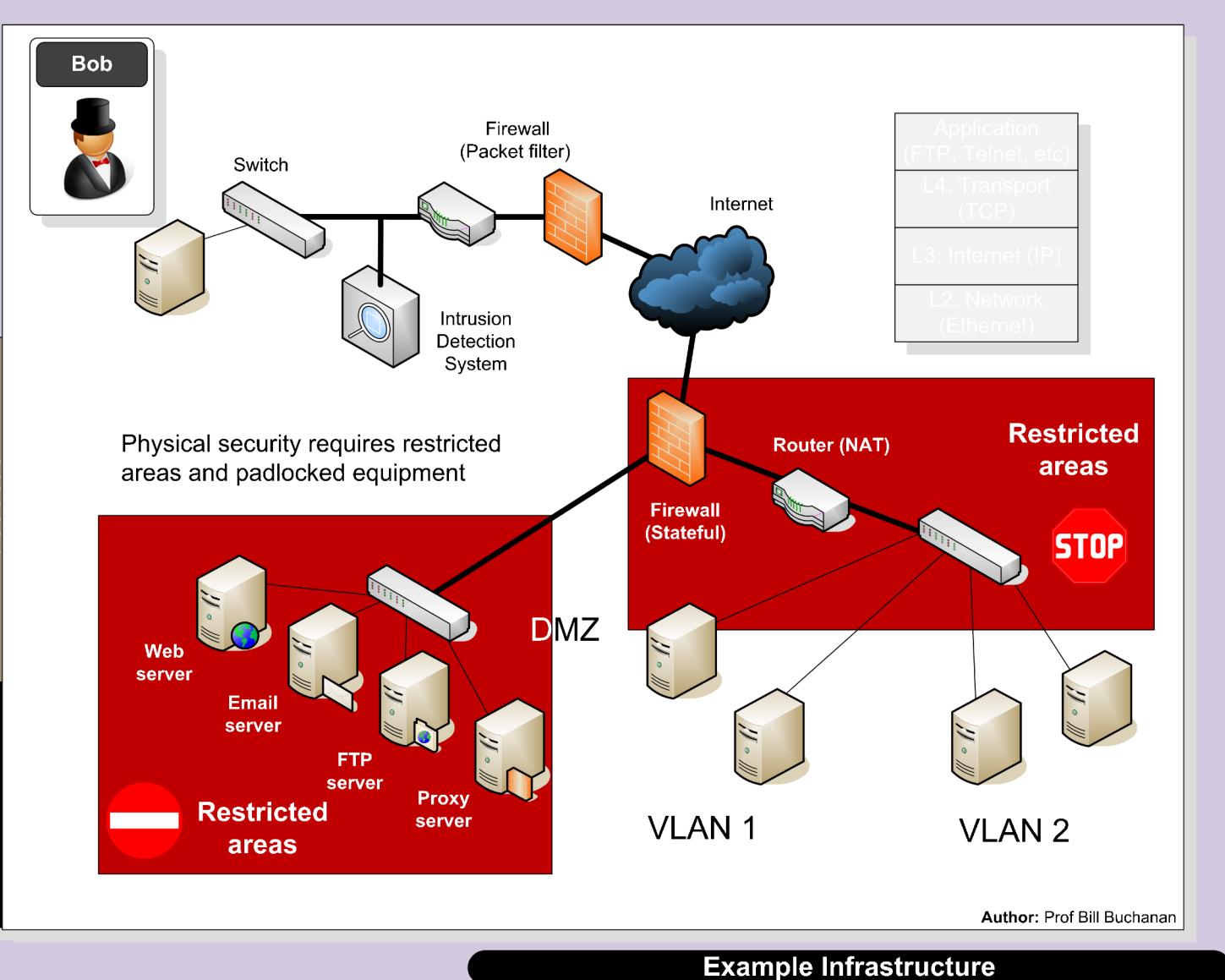


Layered Model

cyber
&
data

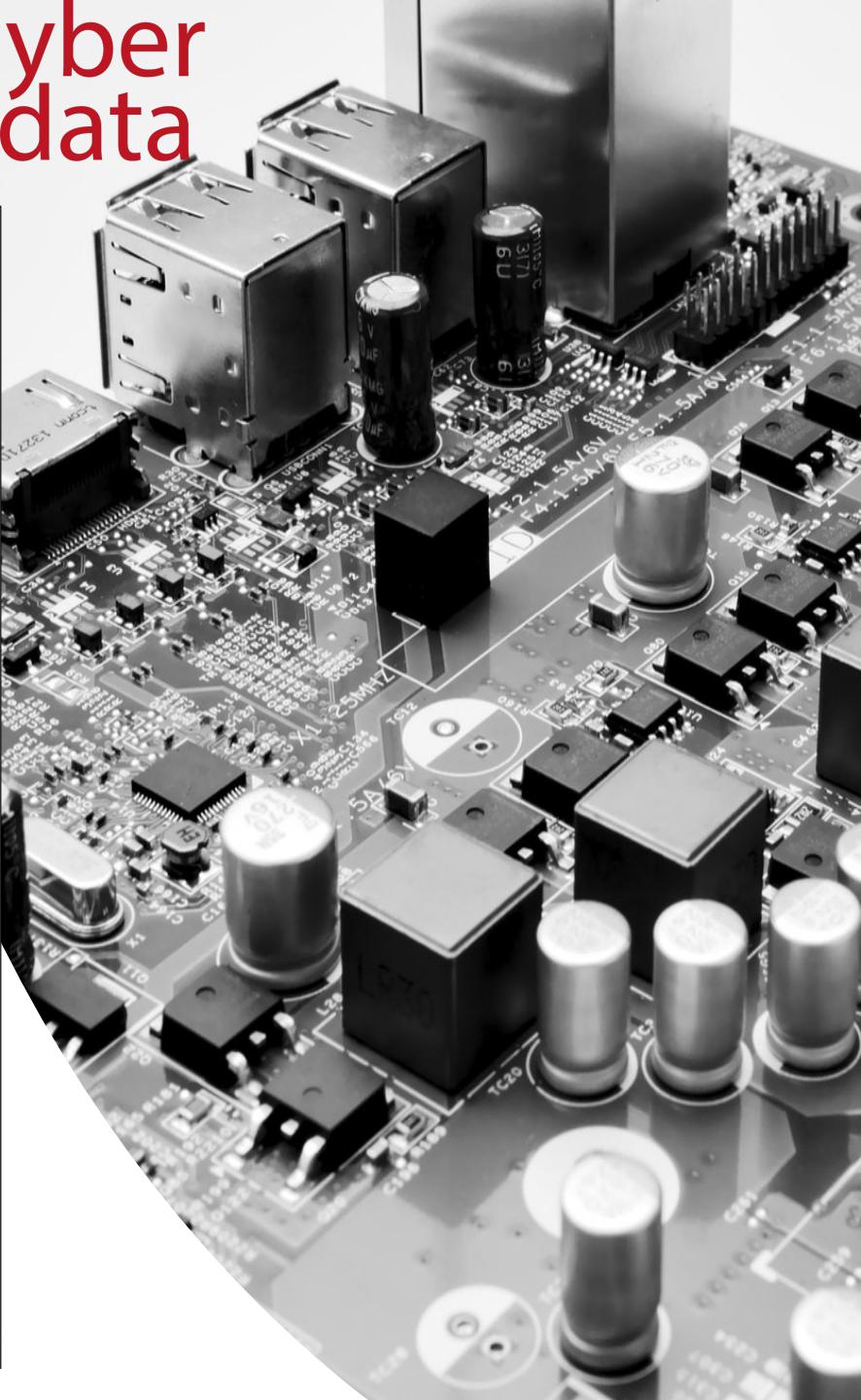
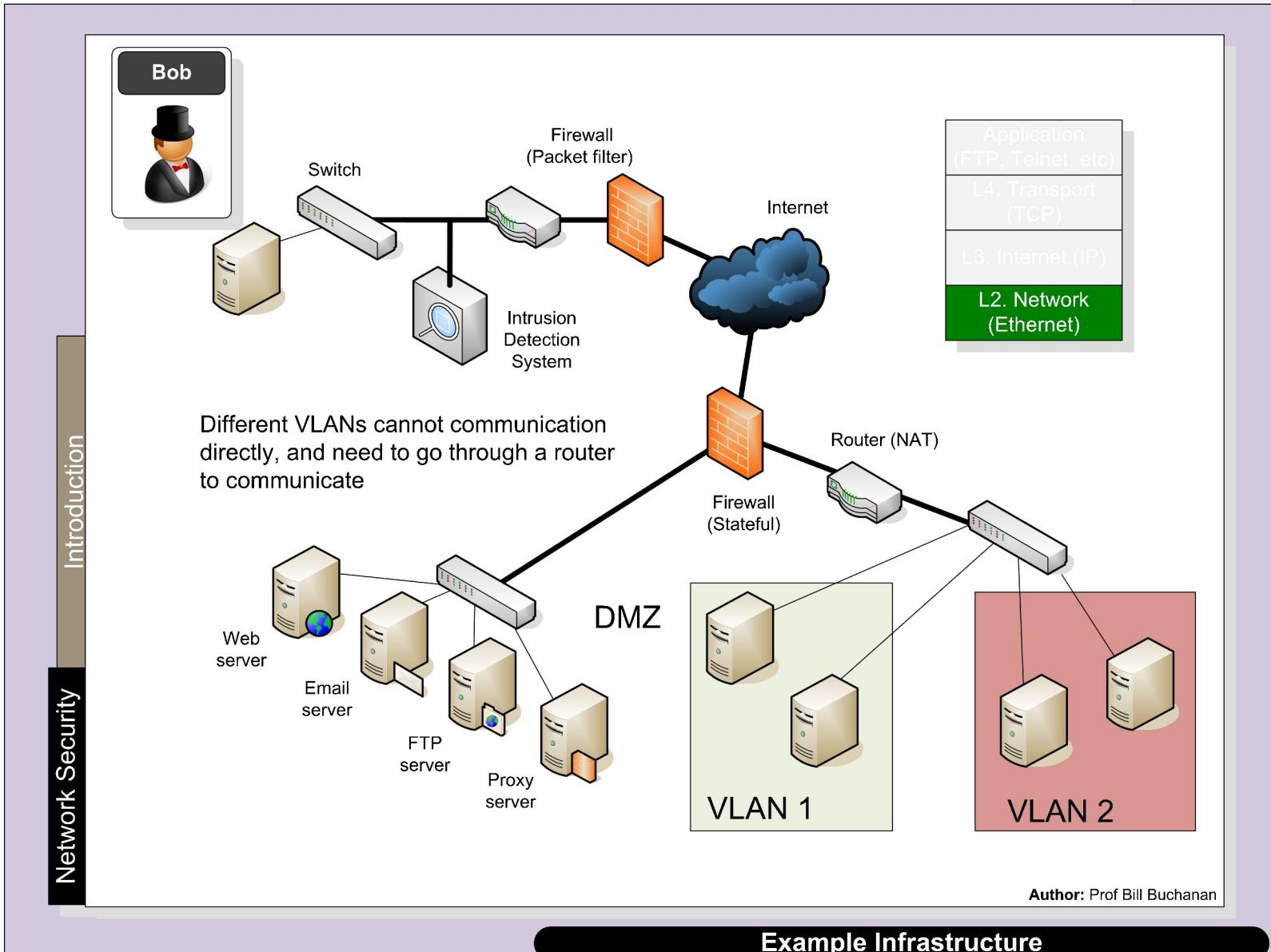
Introduction

Network Security



Layered Model

cyber
&
data

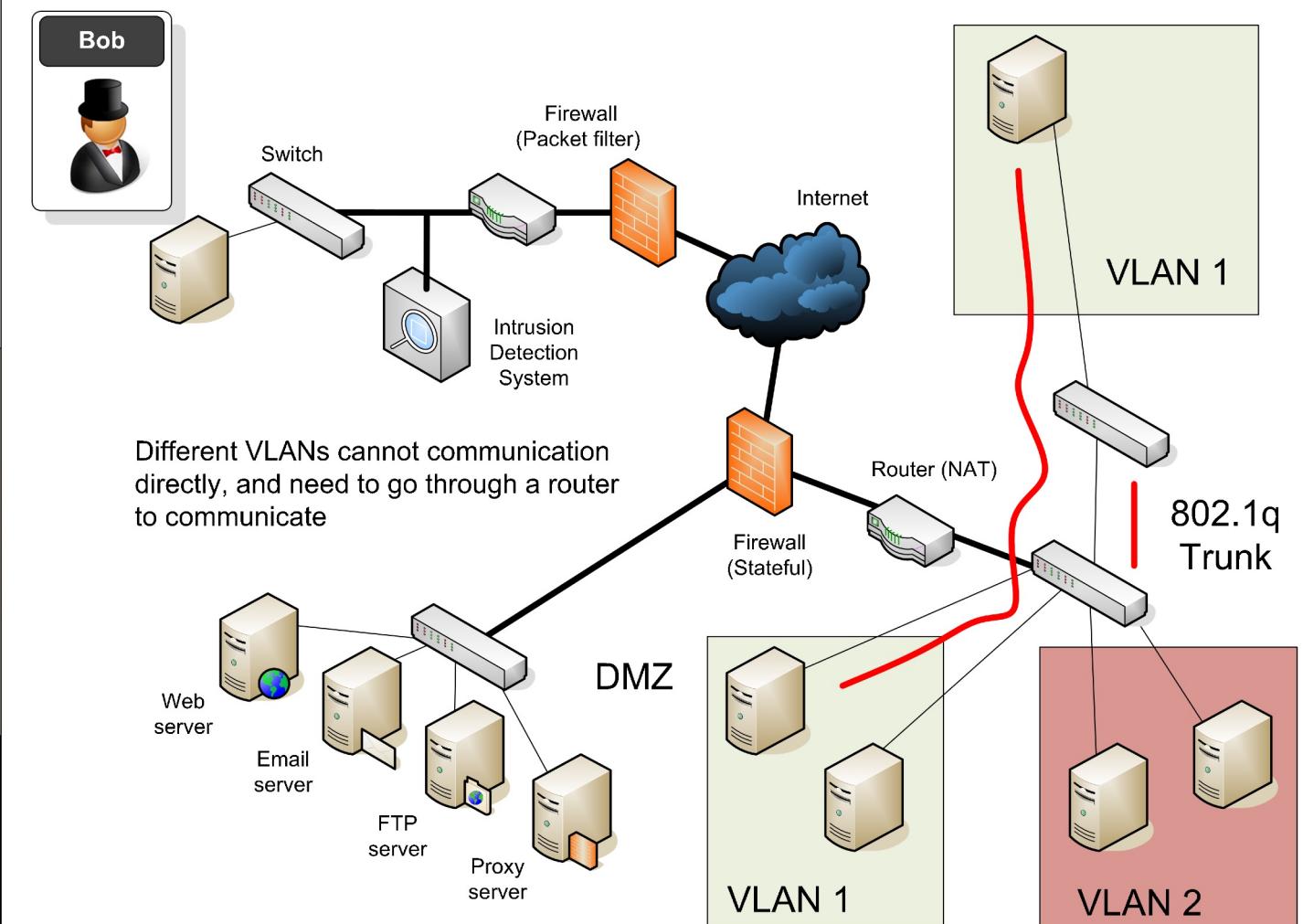


Layered Model

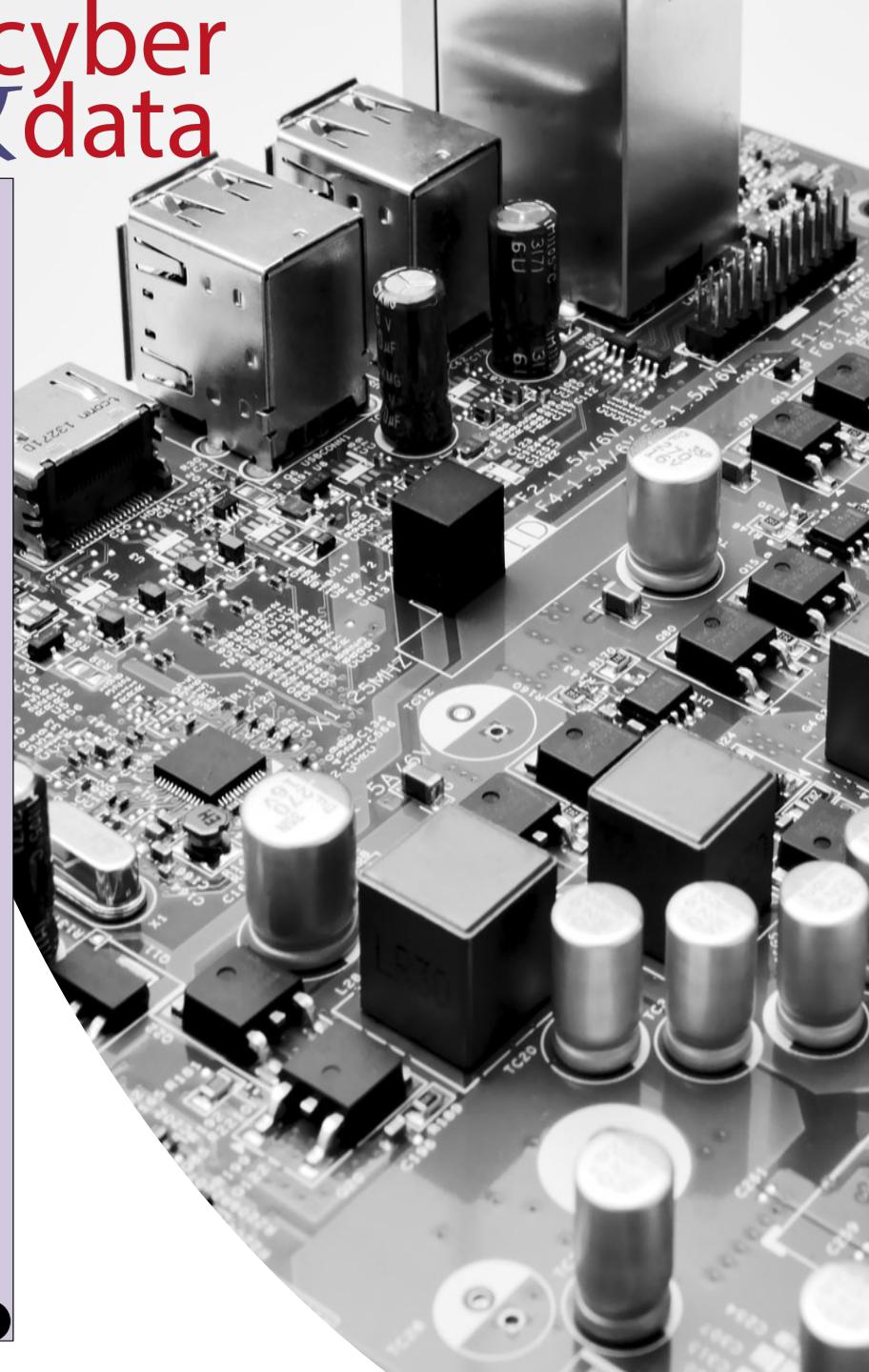
cyber
&
data

Introduction

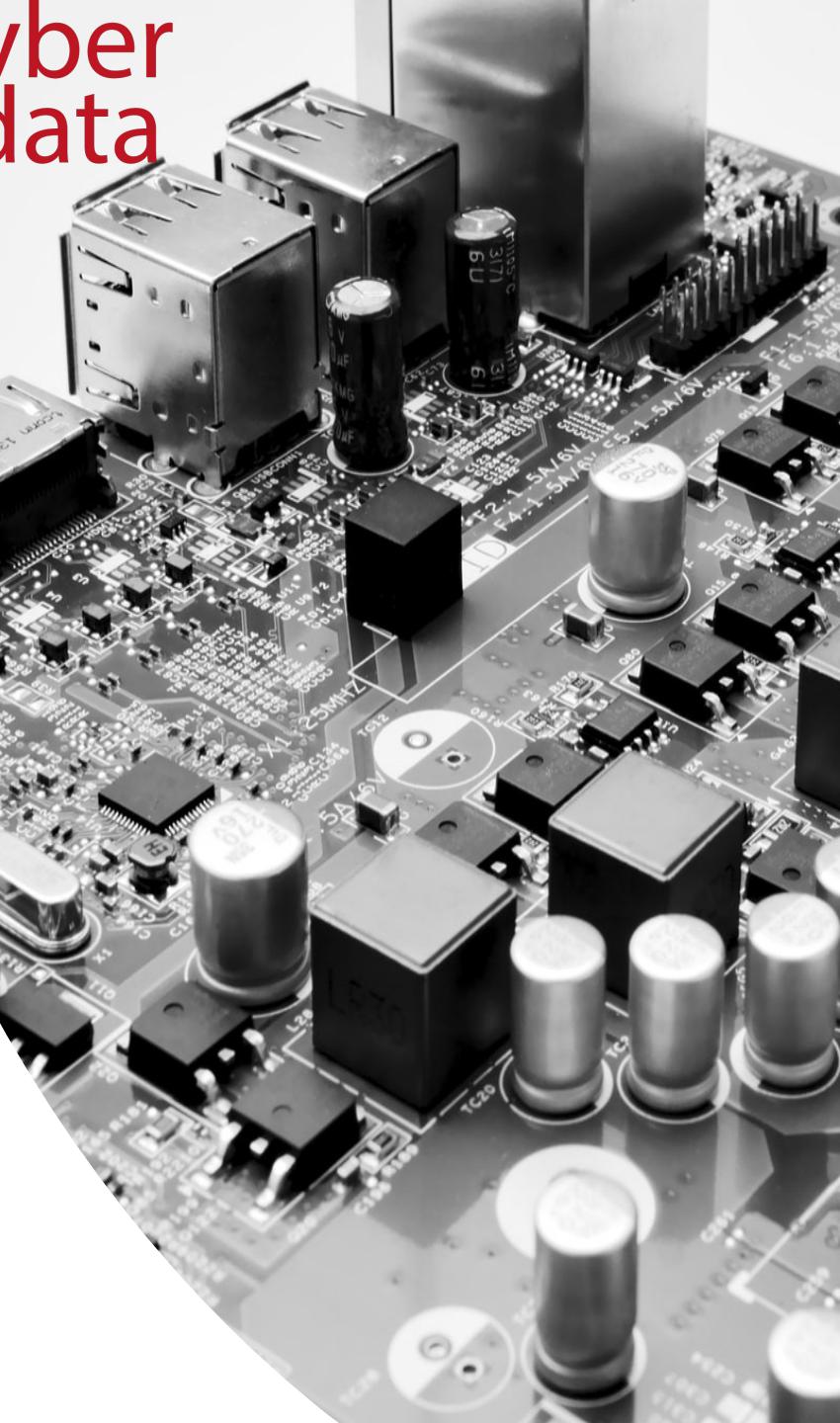
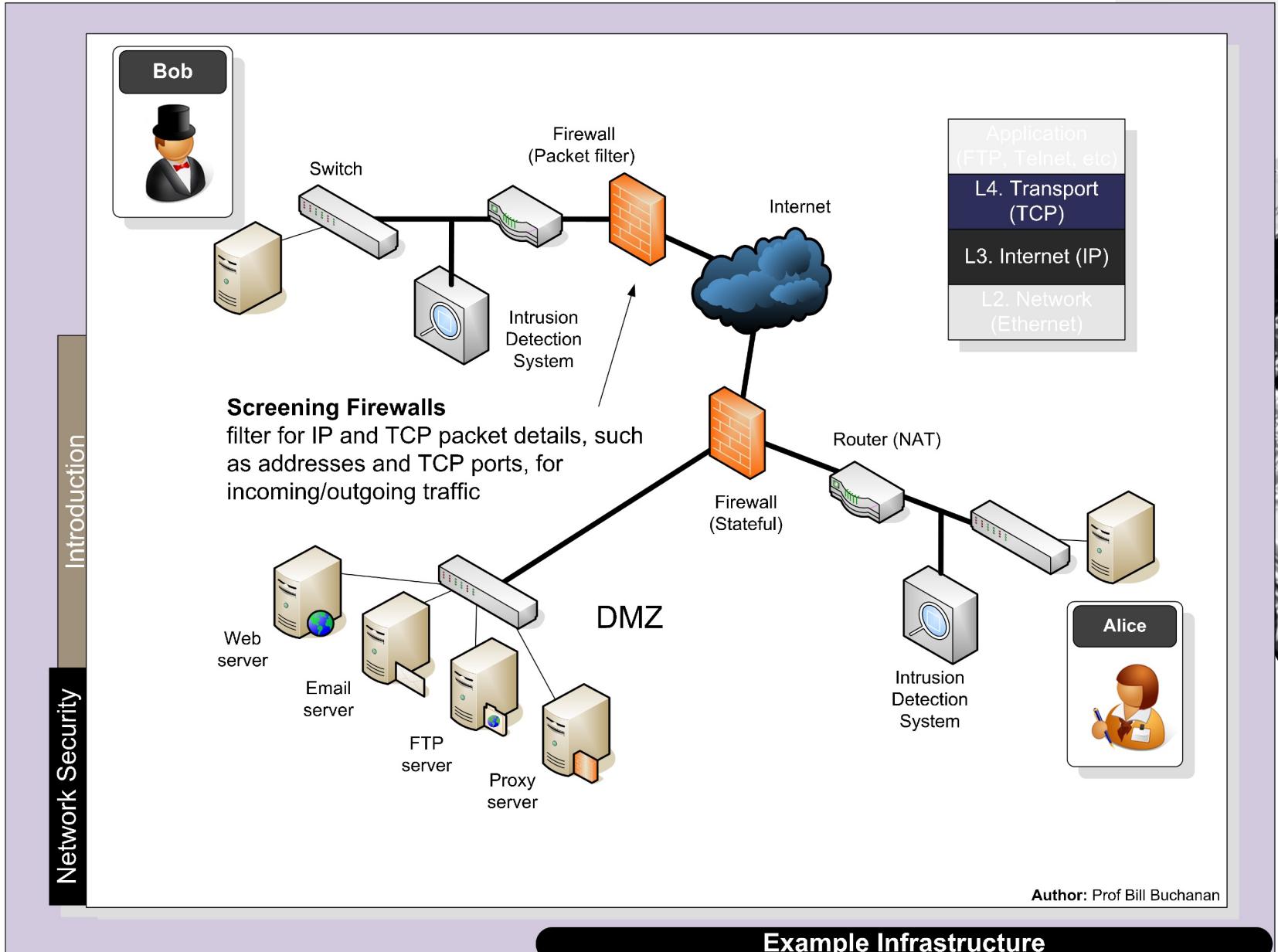
Network Security



Example Infrastructure

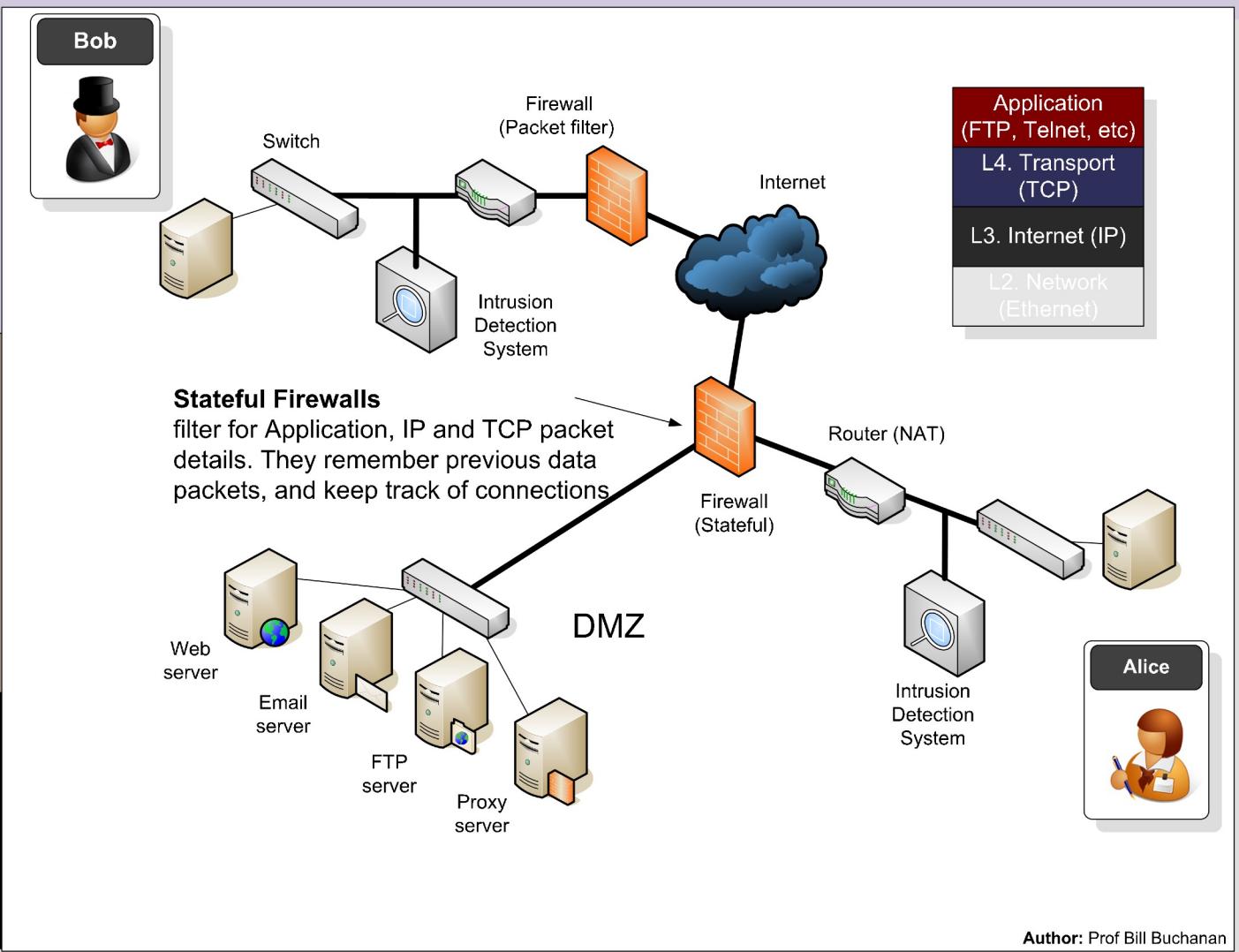


Layered Model

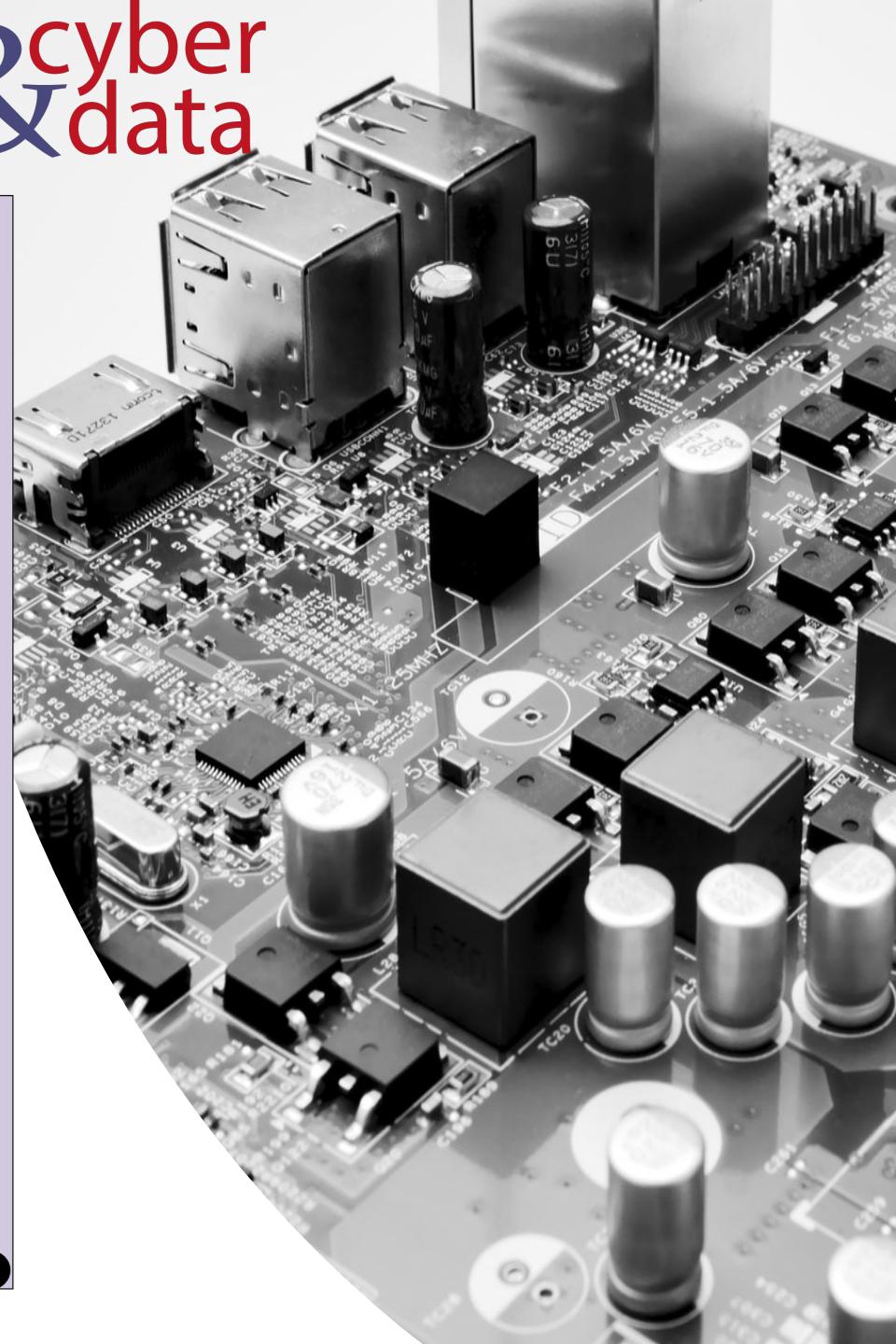


Layered Model

cyber
&
data



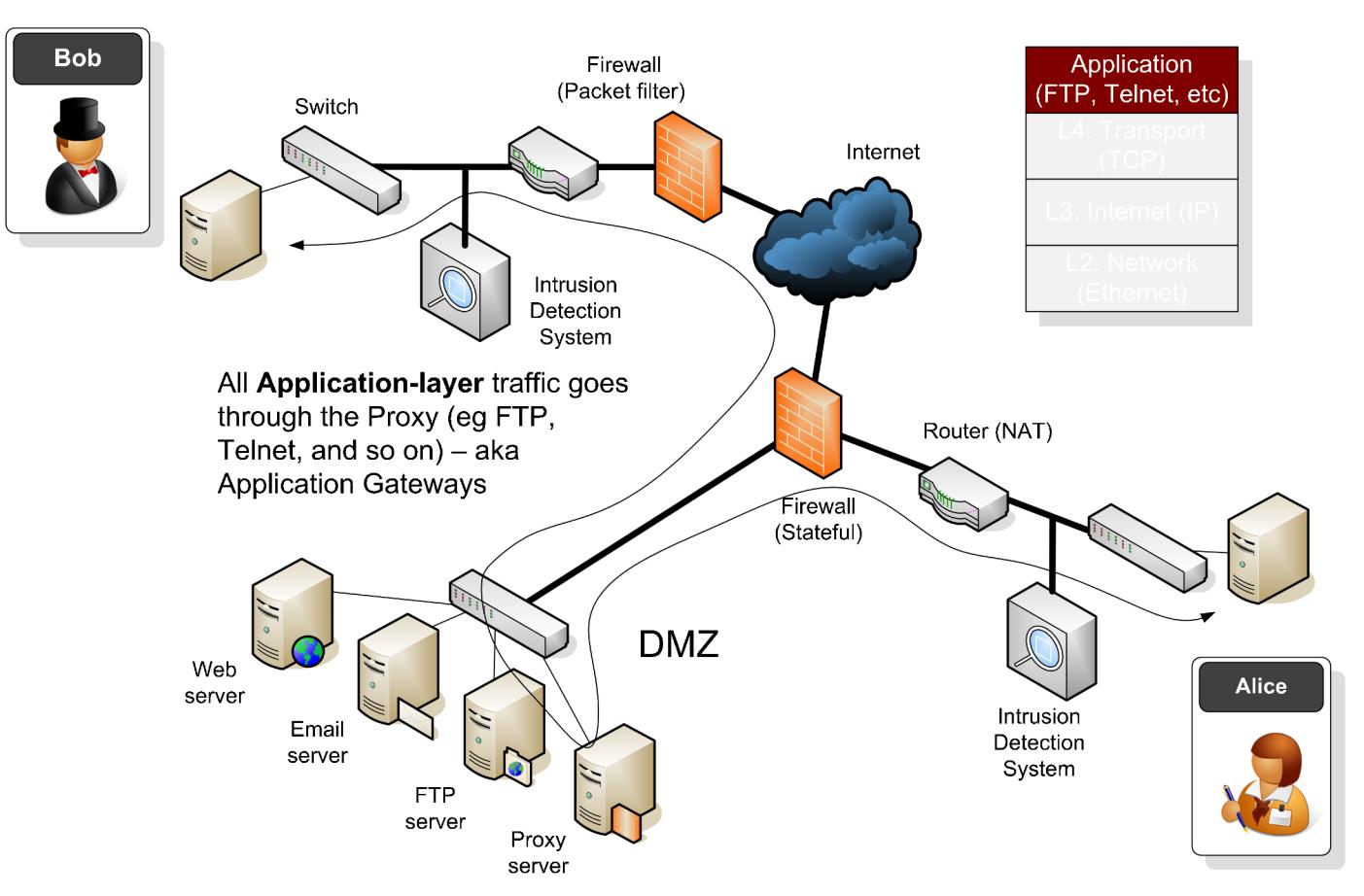
Example Infrastructure



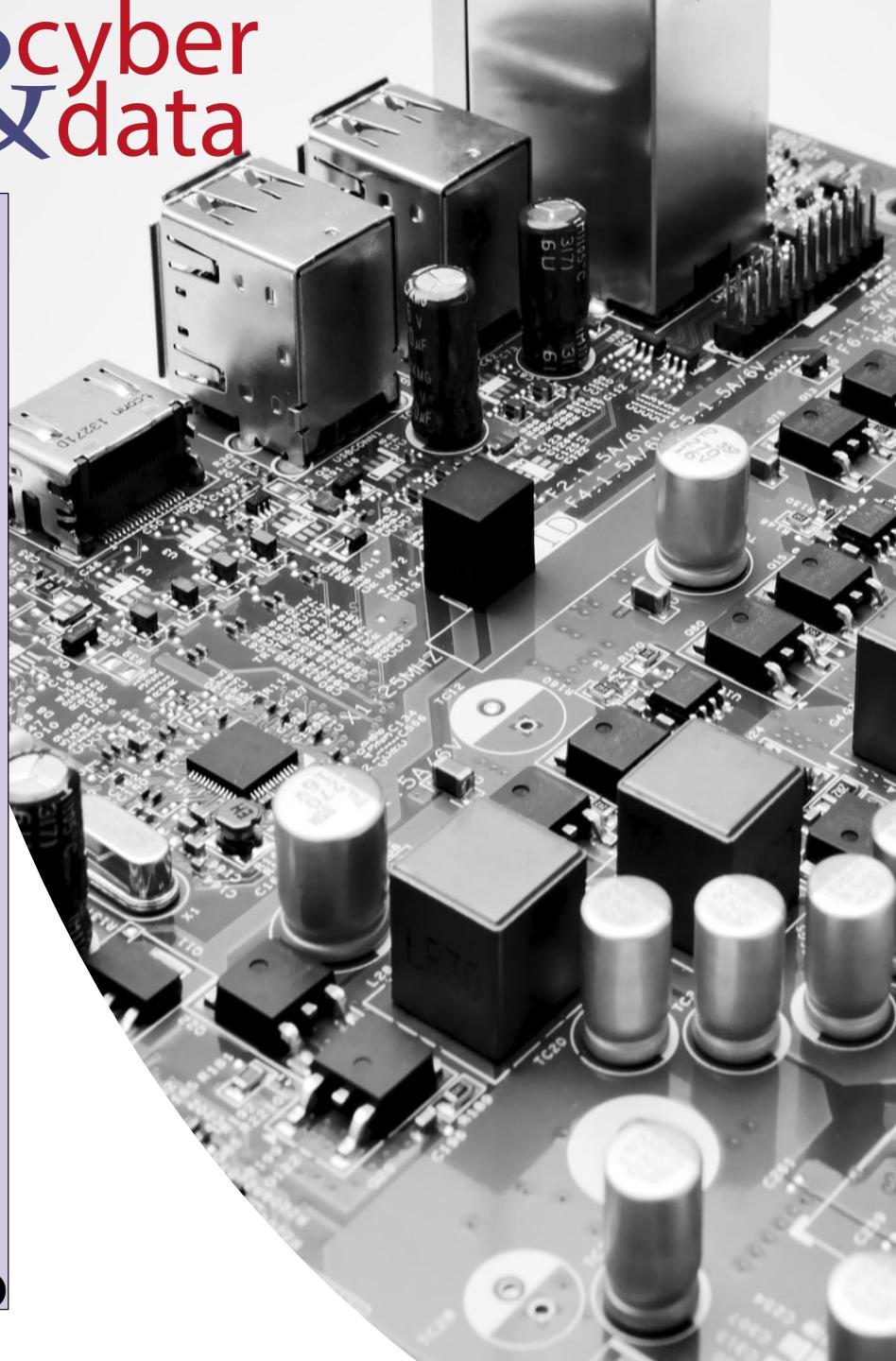
Layered Model

cyber
&
data

Network Security Introduction



Example Infrastructure

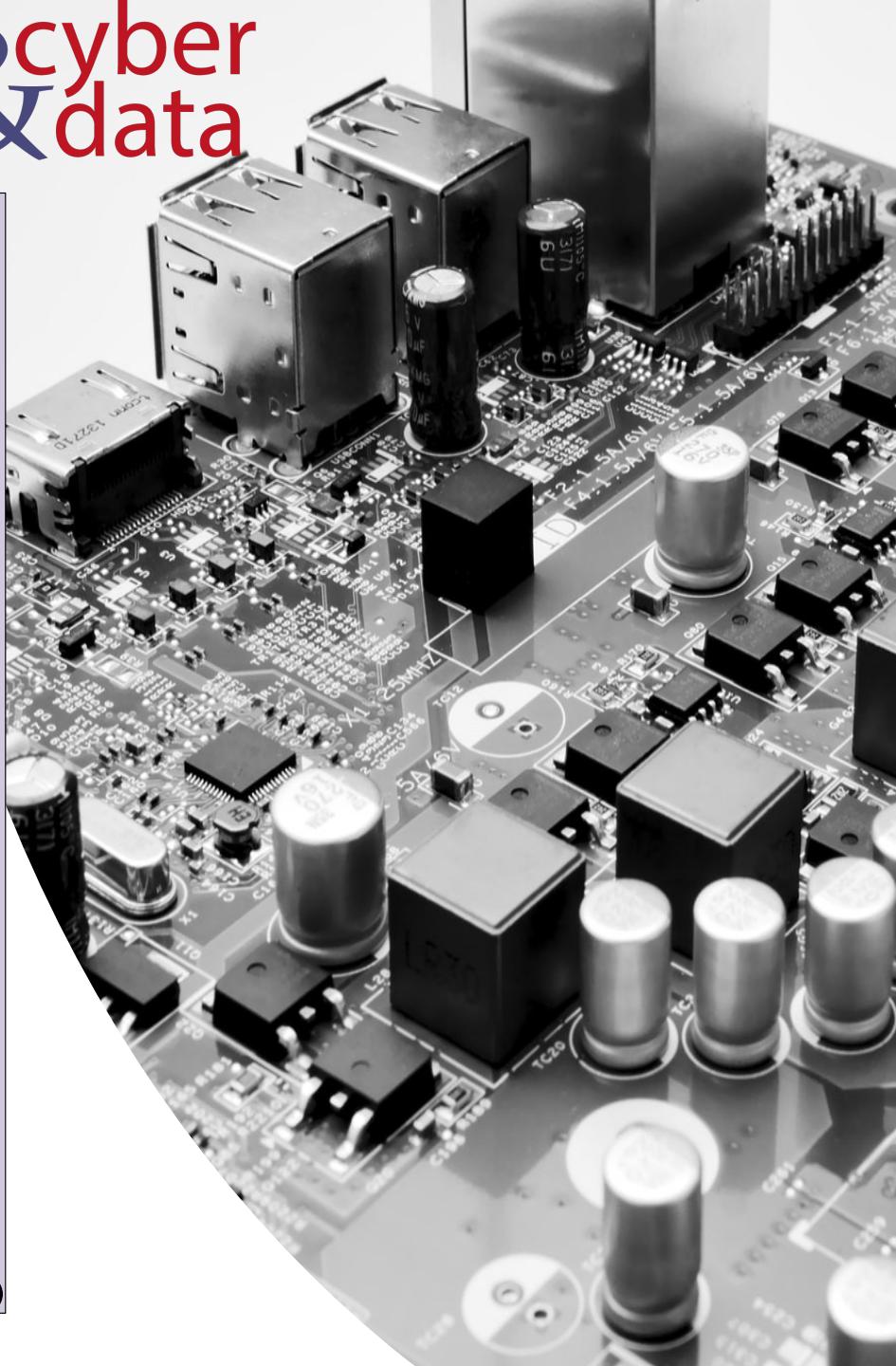
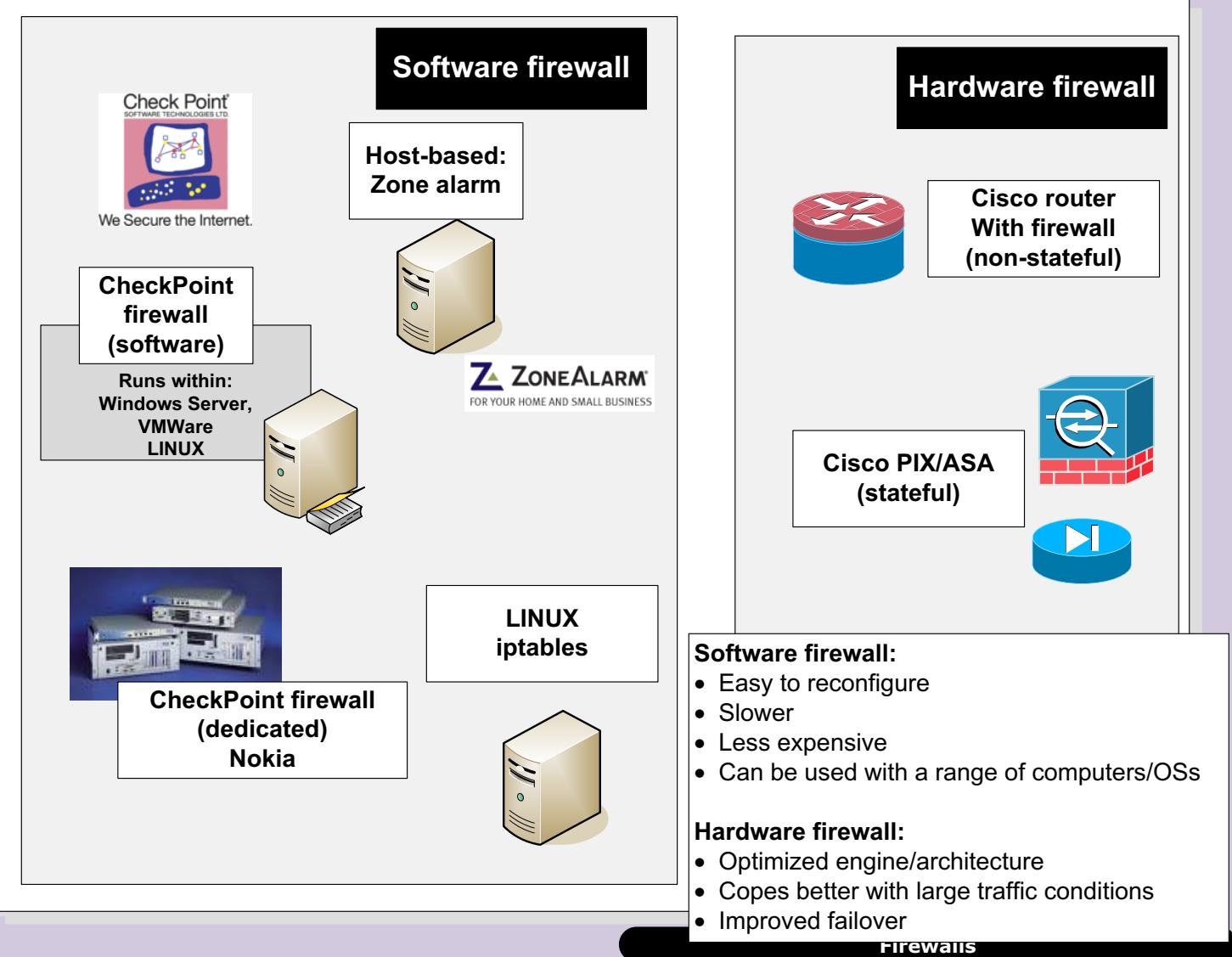


Layered Model

cyber
&
data

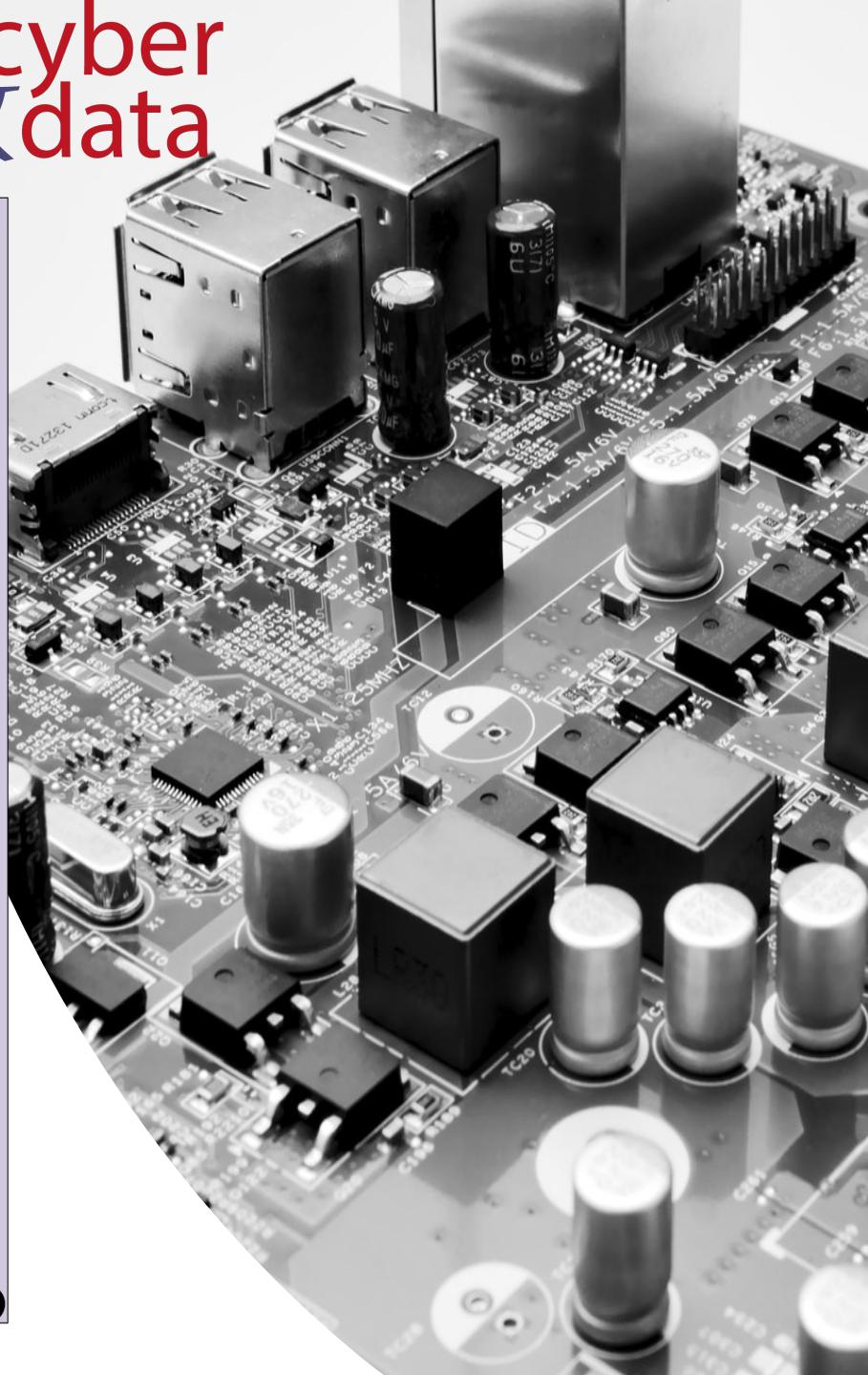
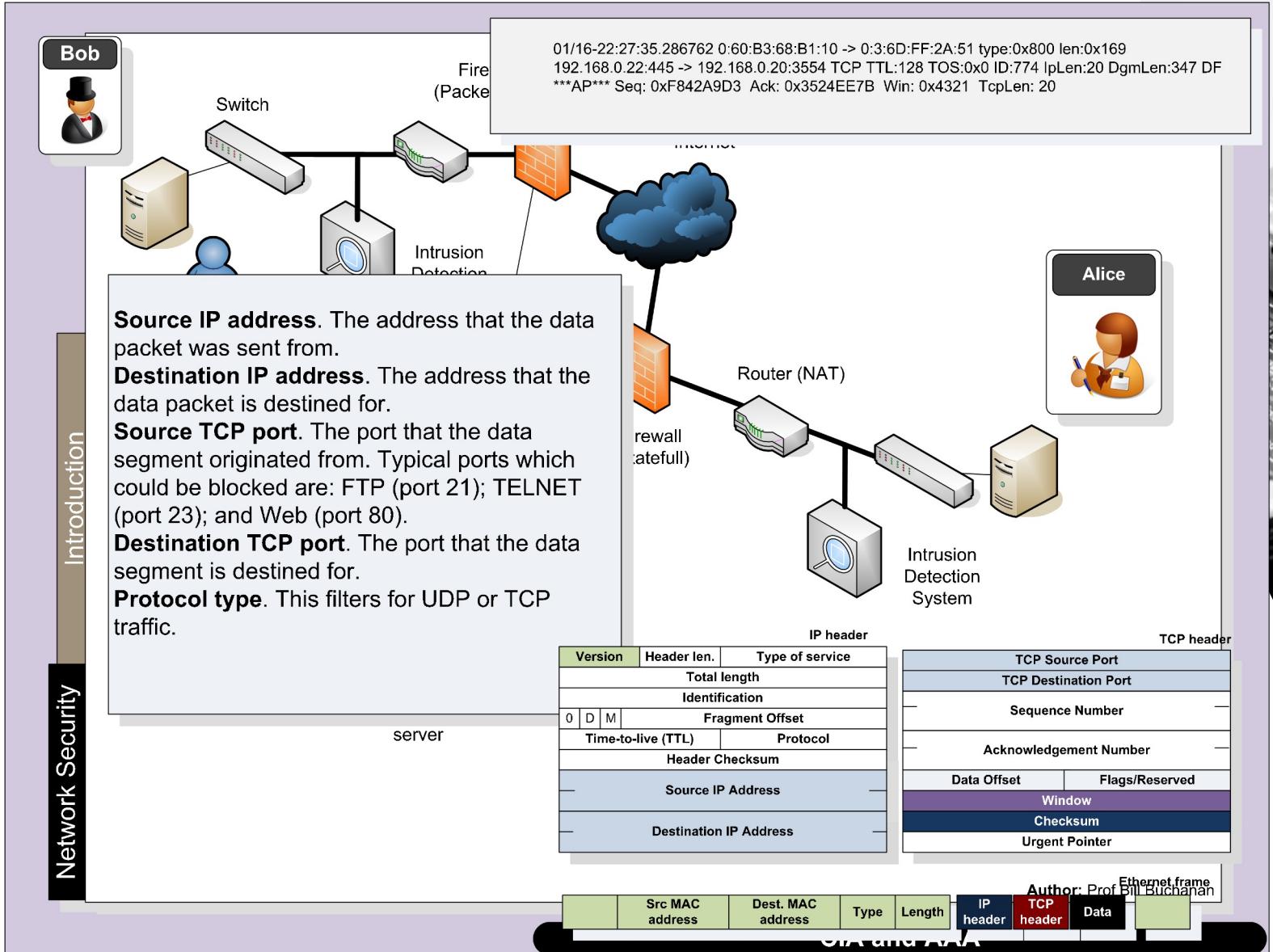
Introduction

Network Security



Layered Model

cyber
&
data



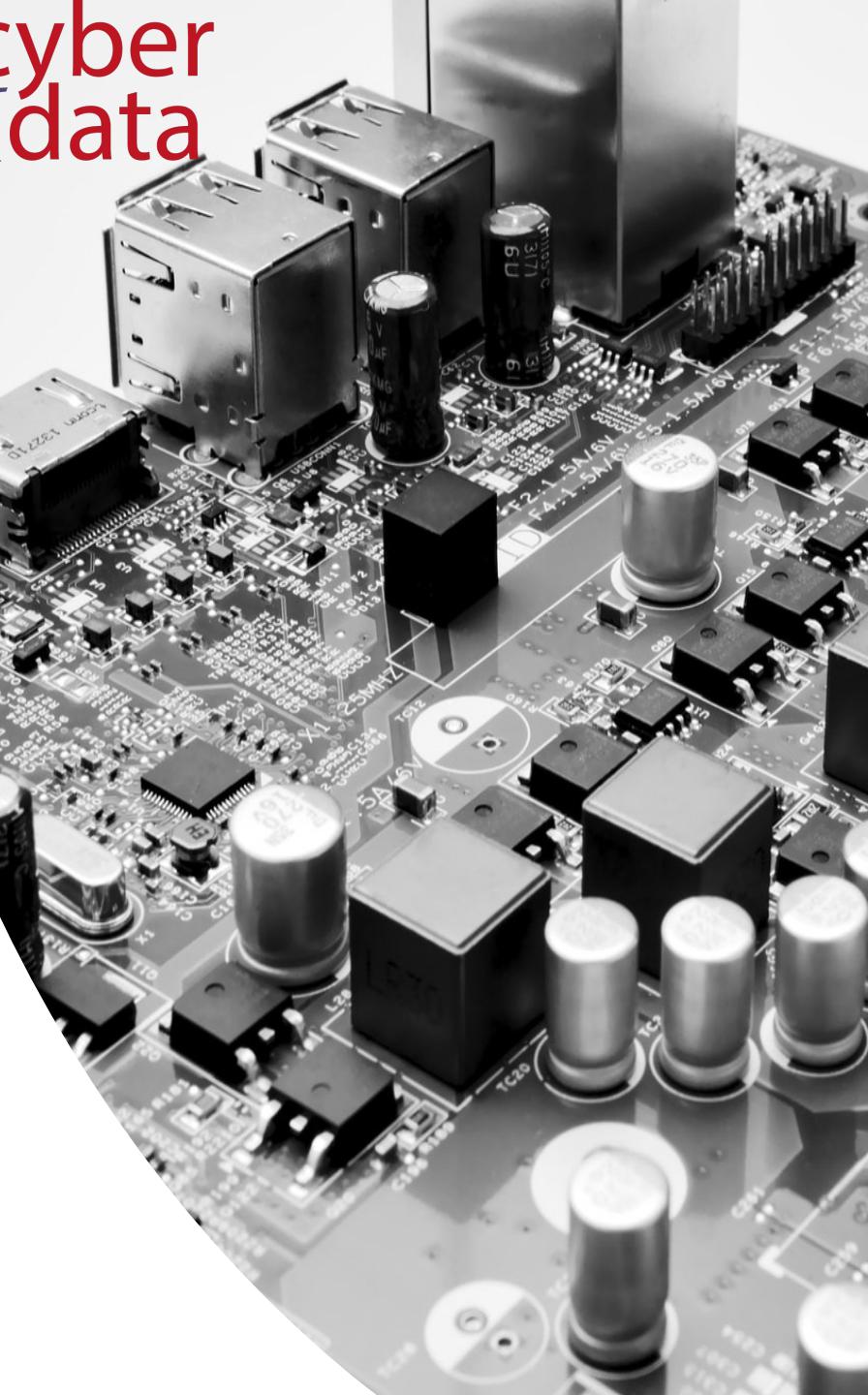
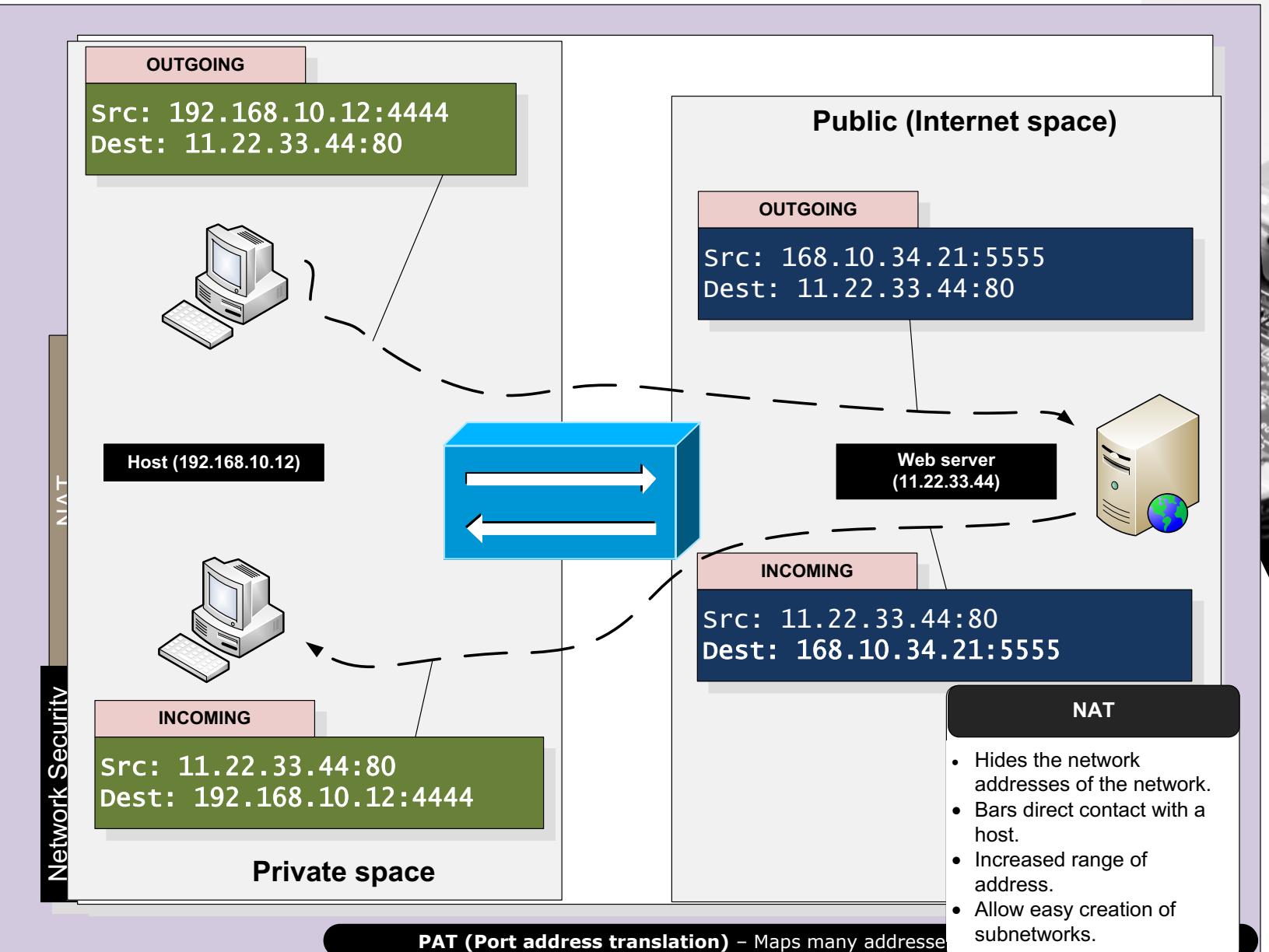
cyber & data

“From bits to information”

NAT

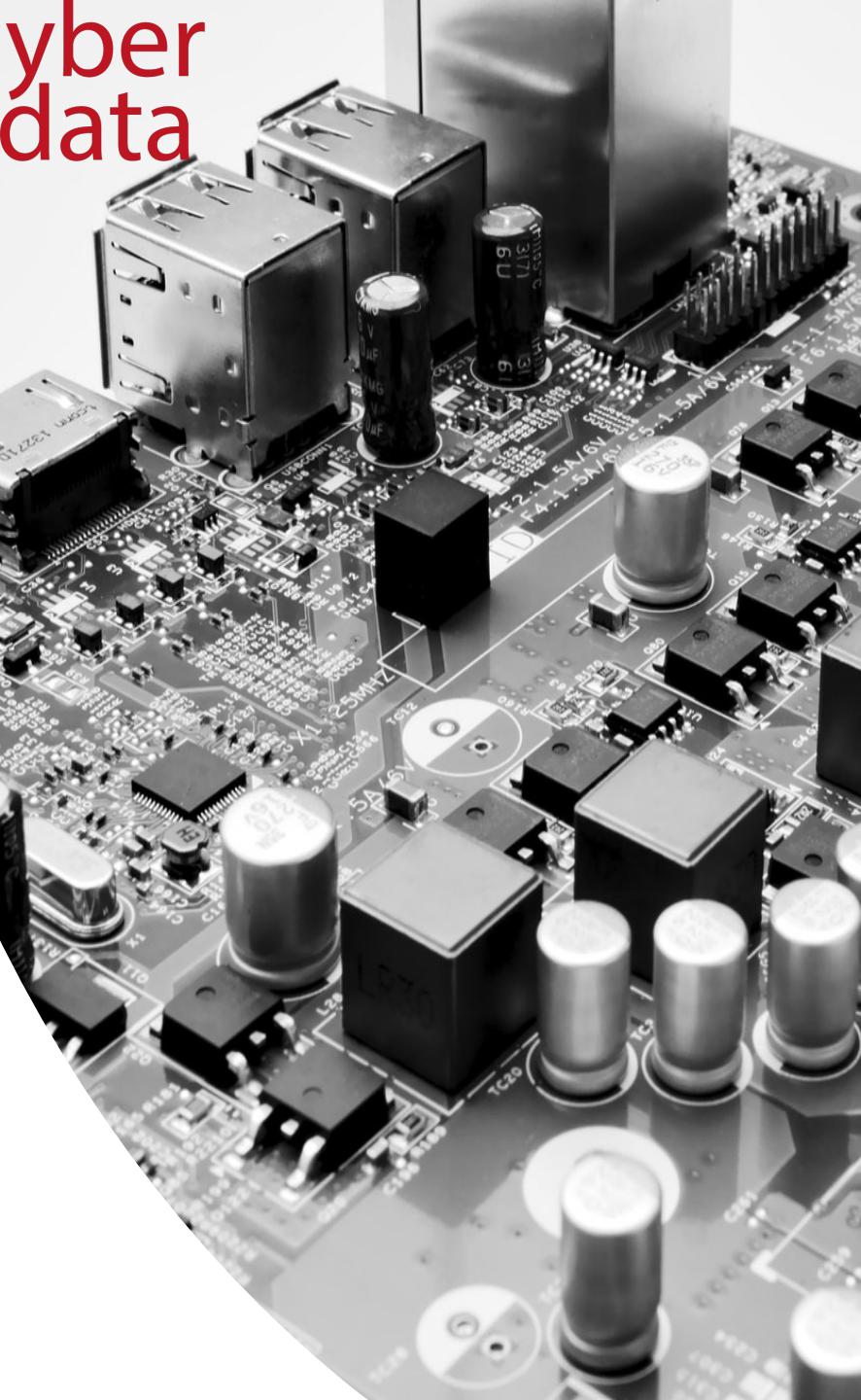
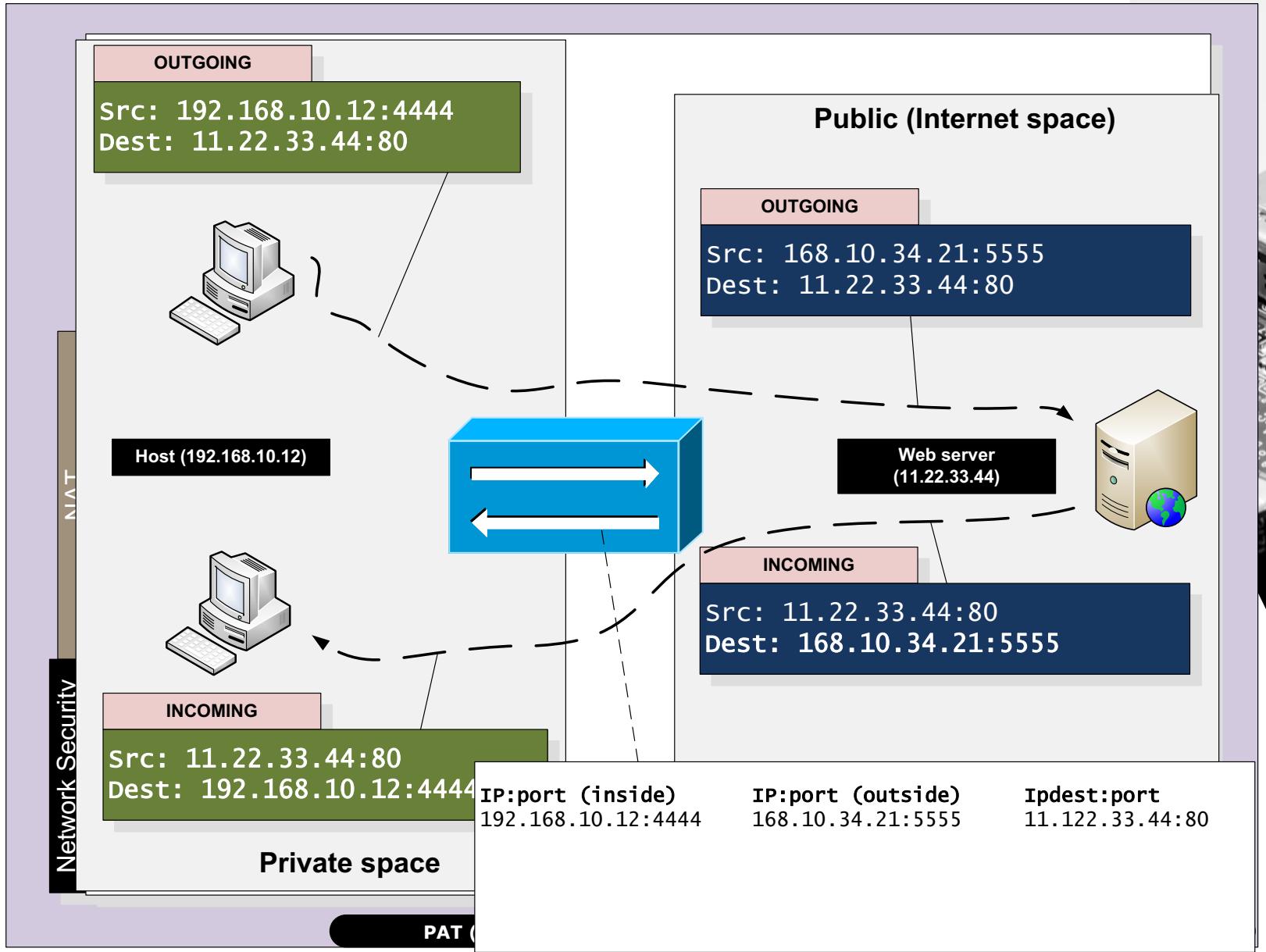
Layered Model

cyber
&
data



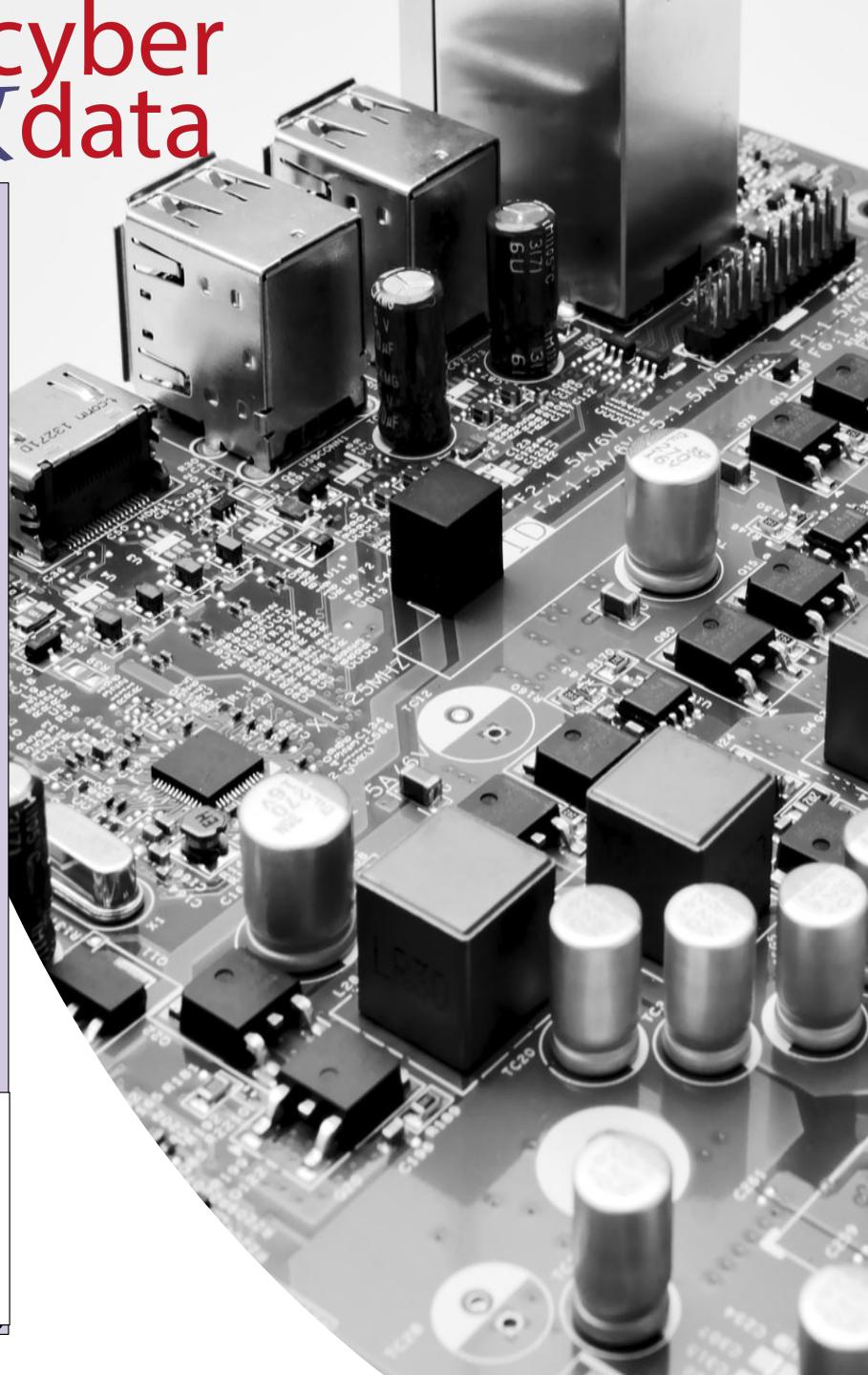
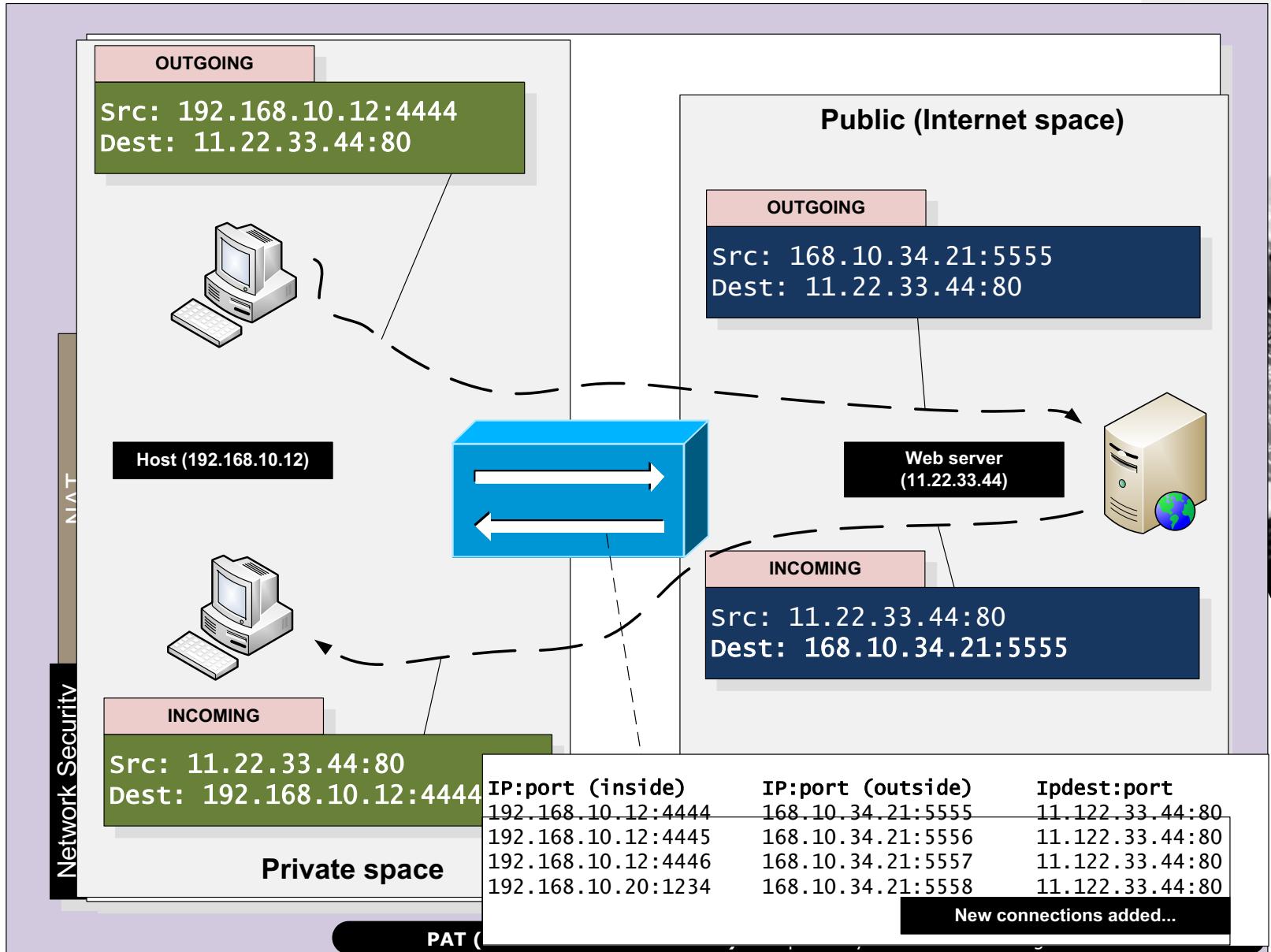
Layered Model

cyber
& data



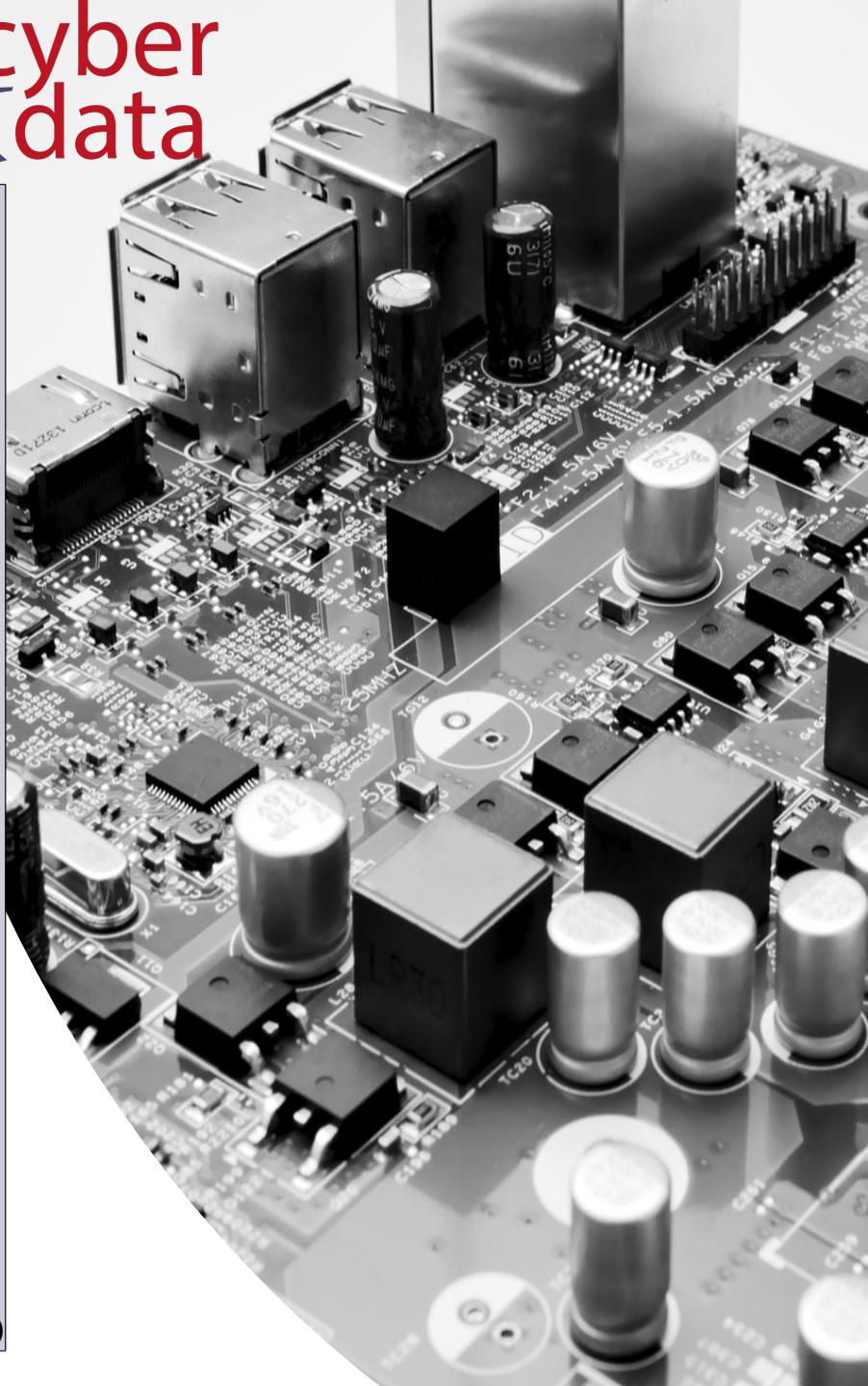
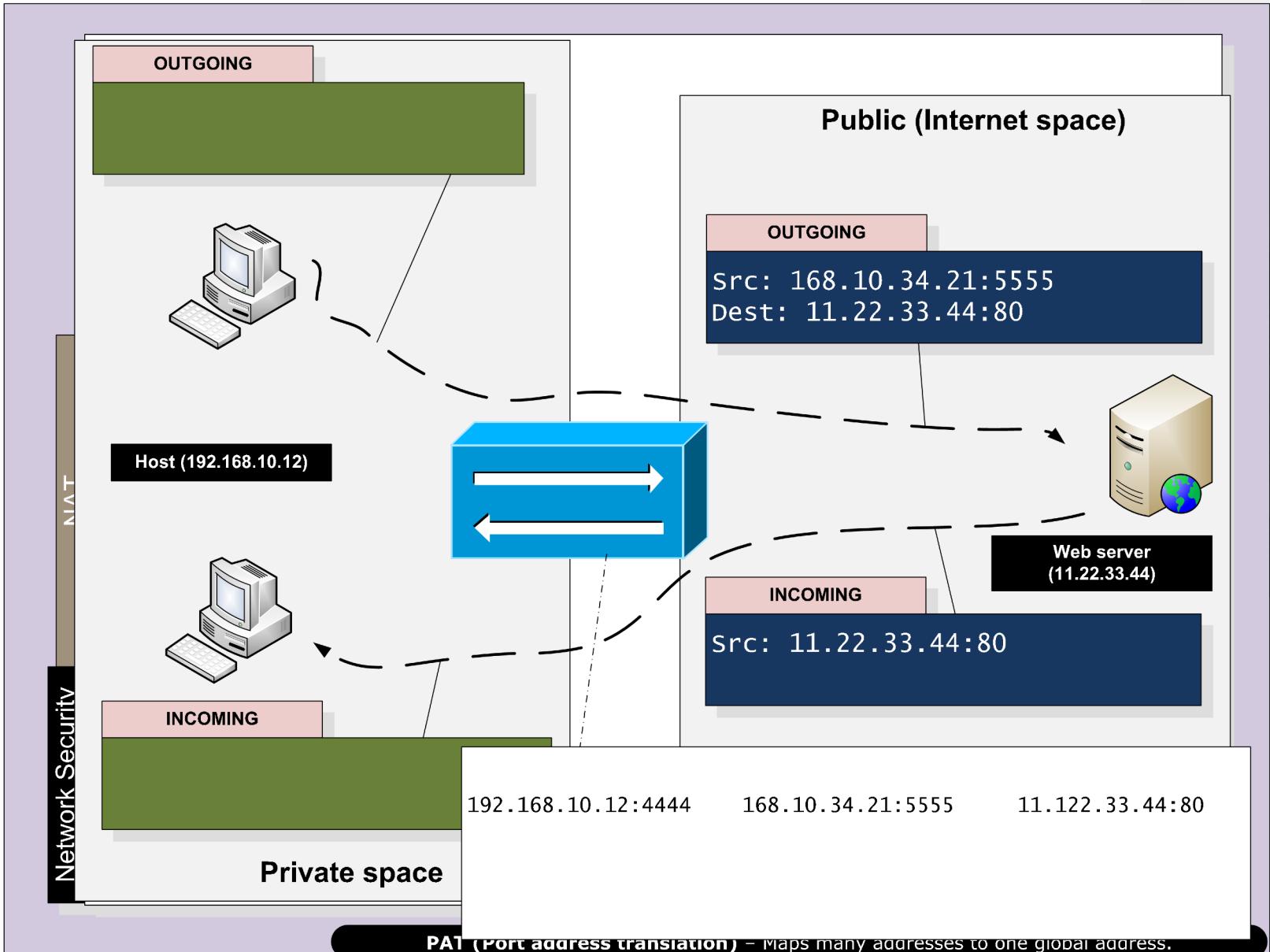
Layered Model

cyber
& data



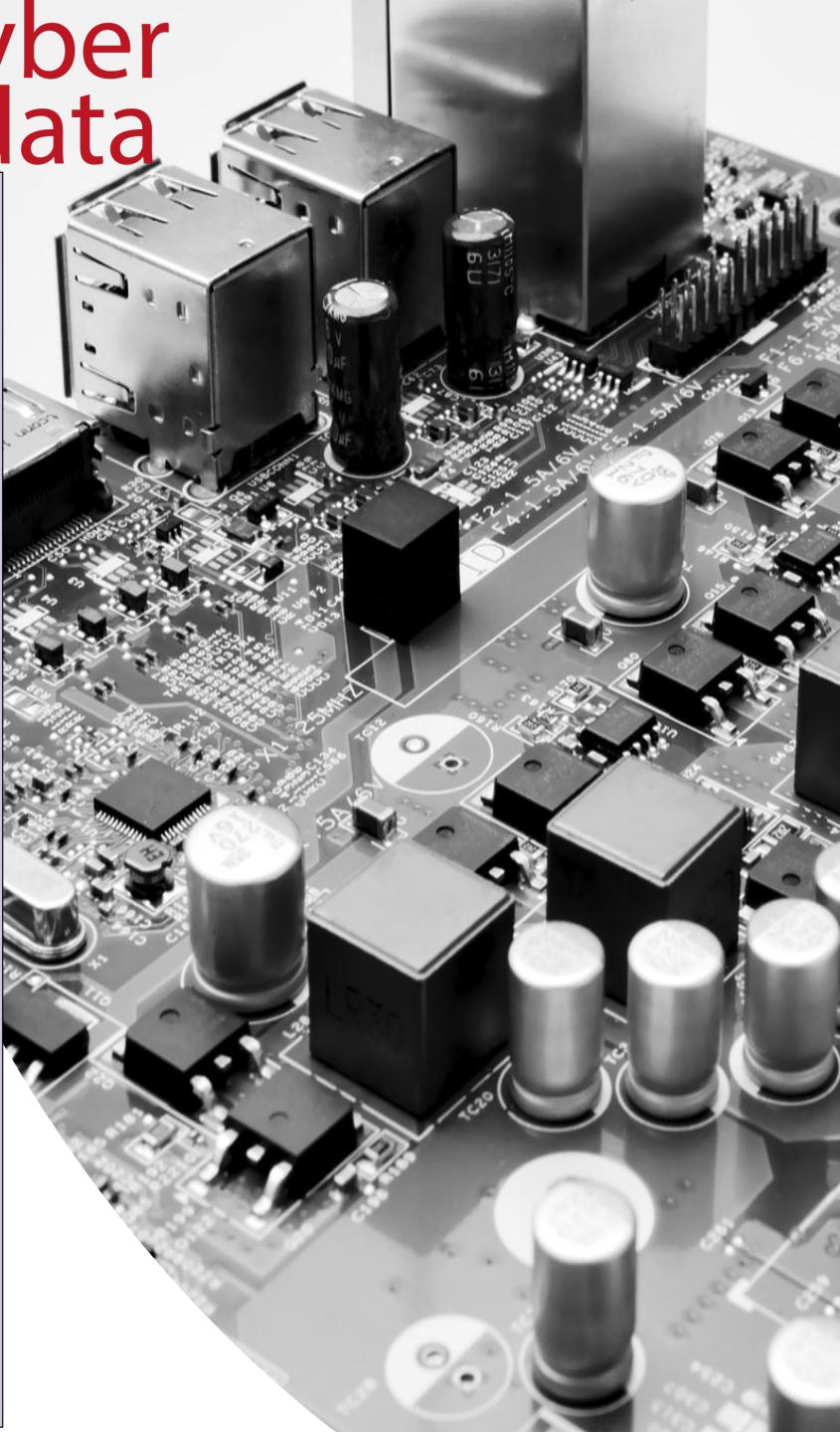
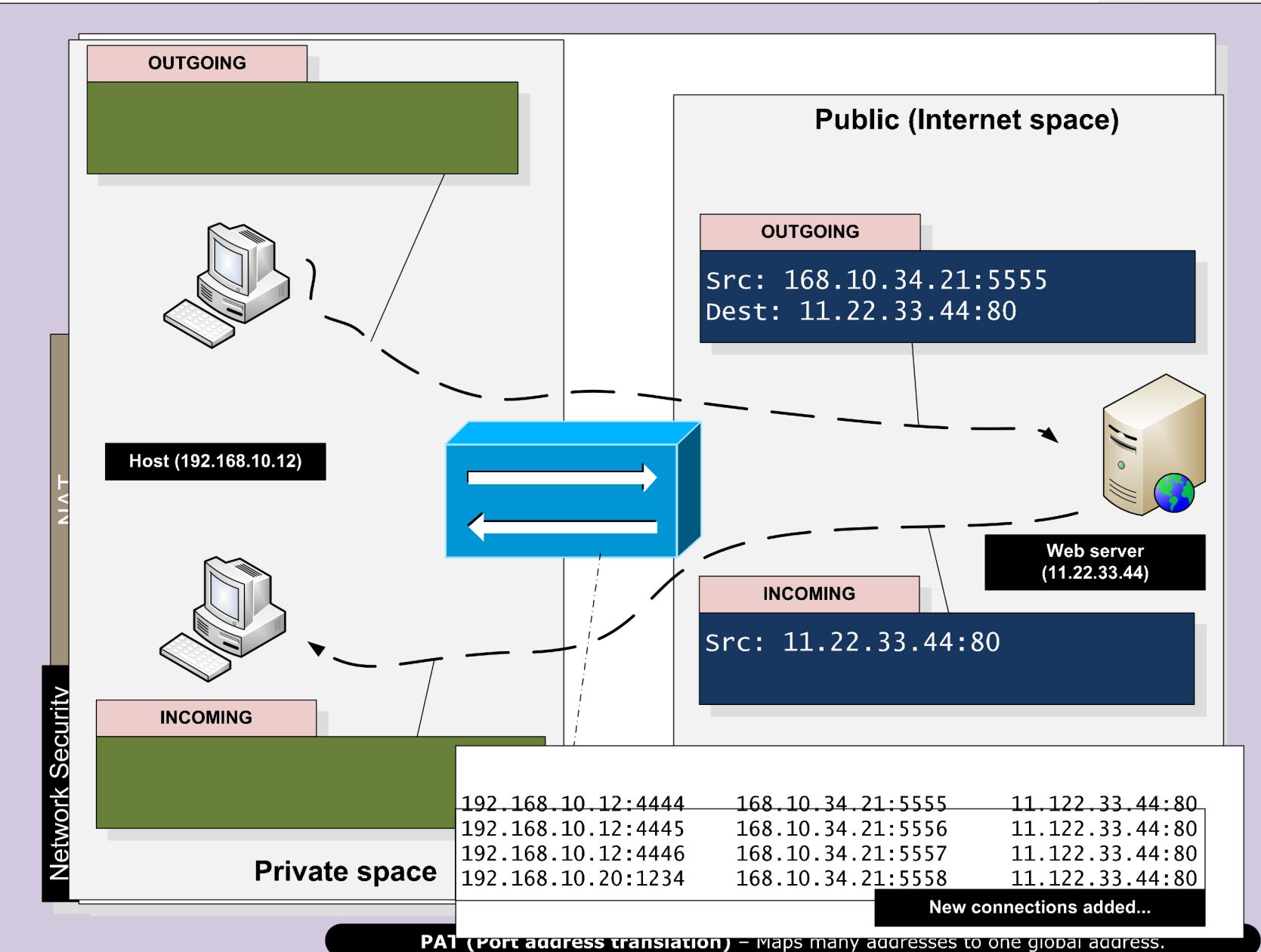
Layered Model

cyber
&
data

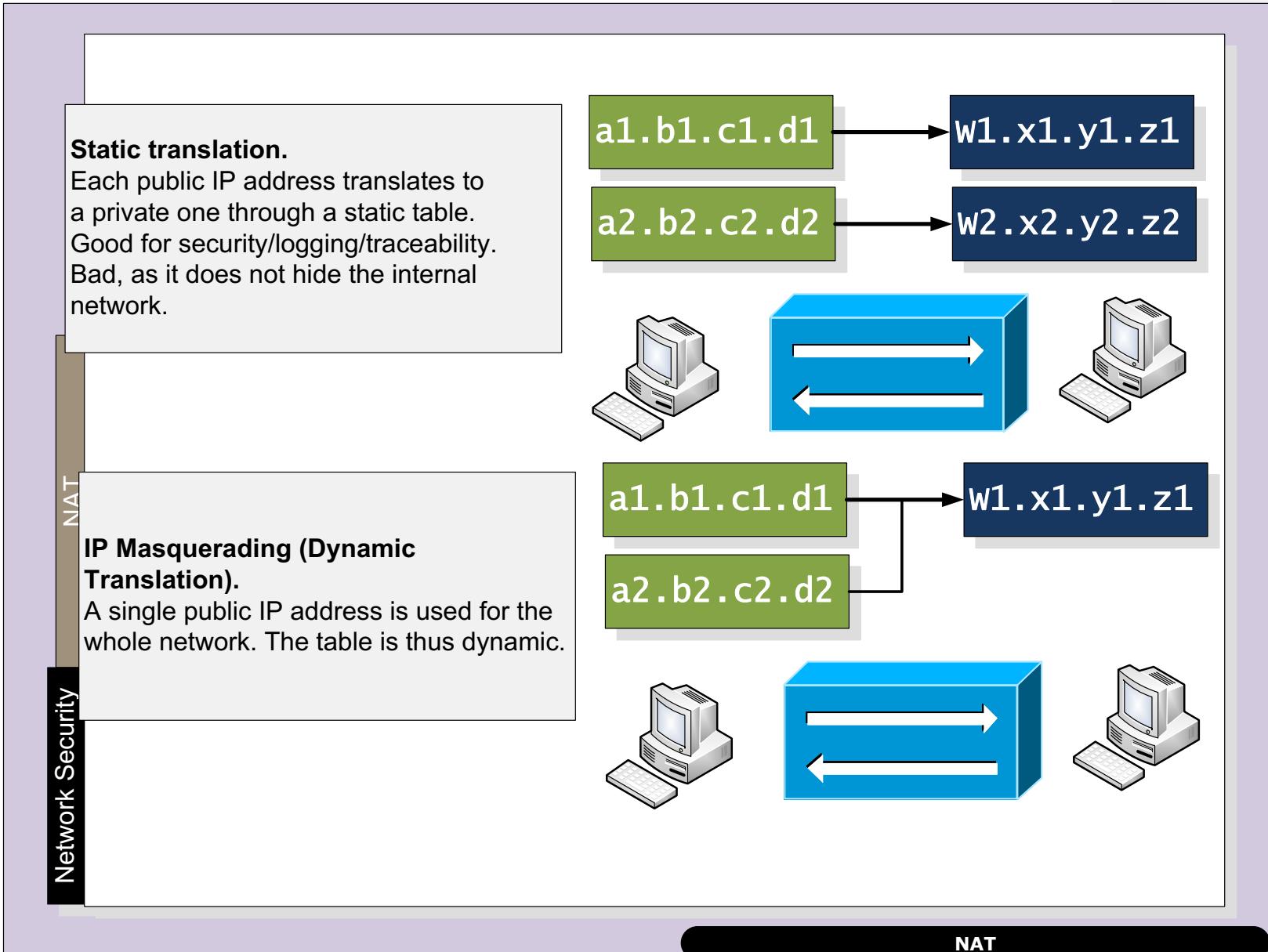


Layered Model

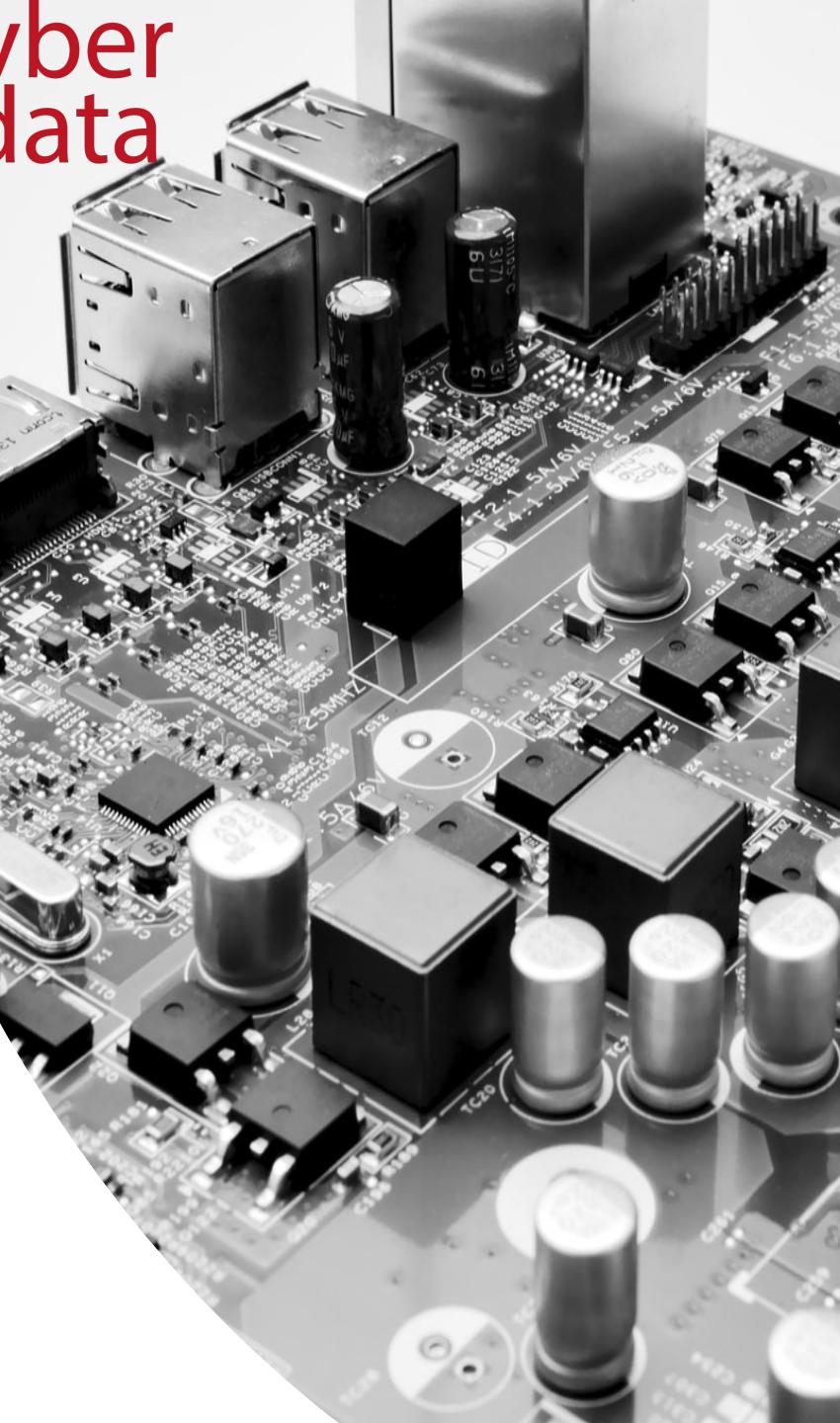
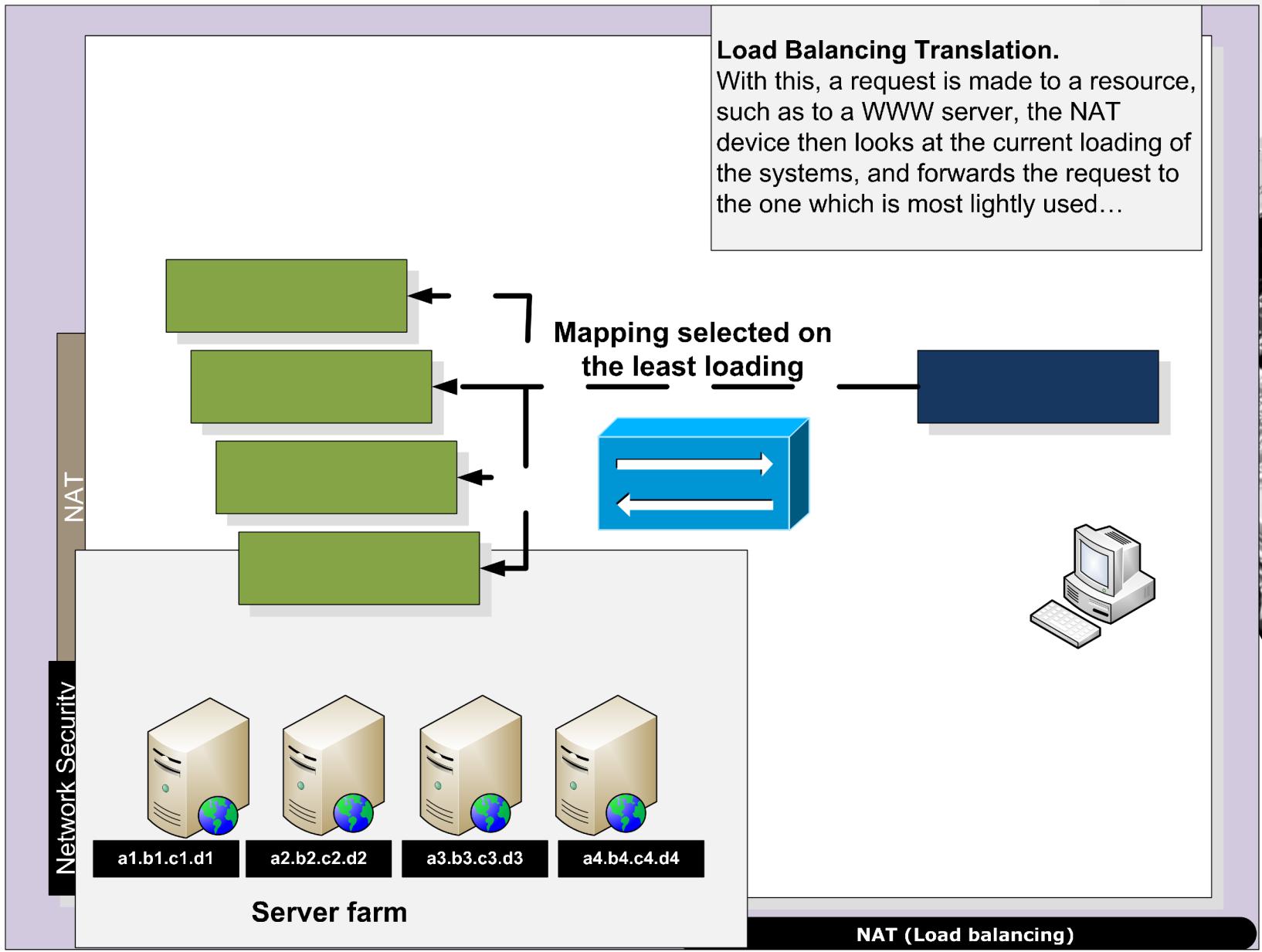
cyber
&
data



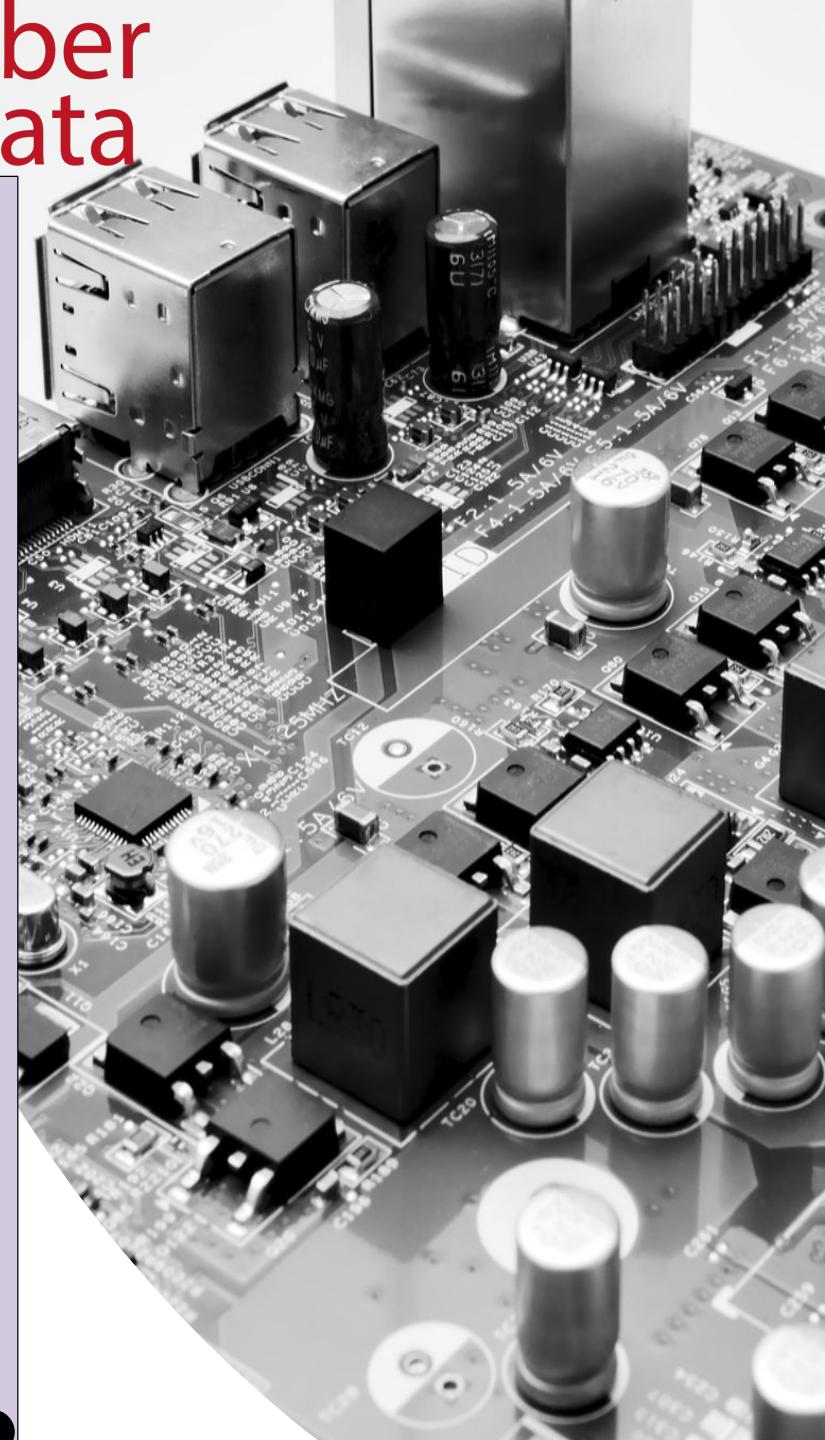
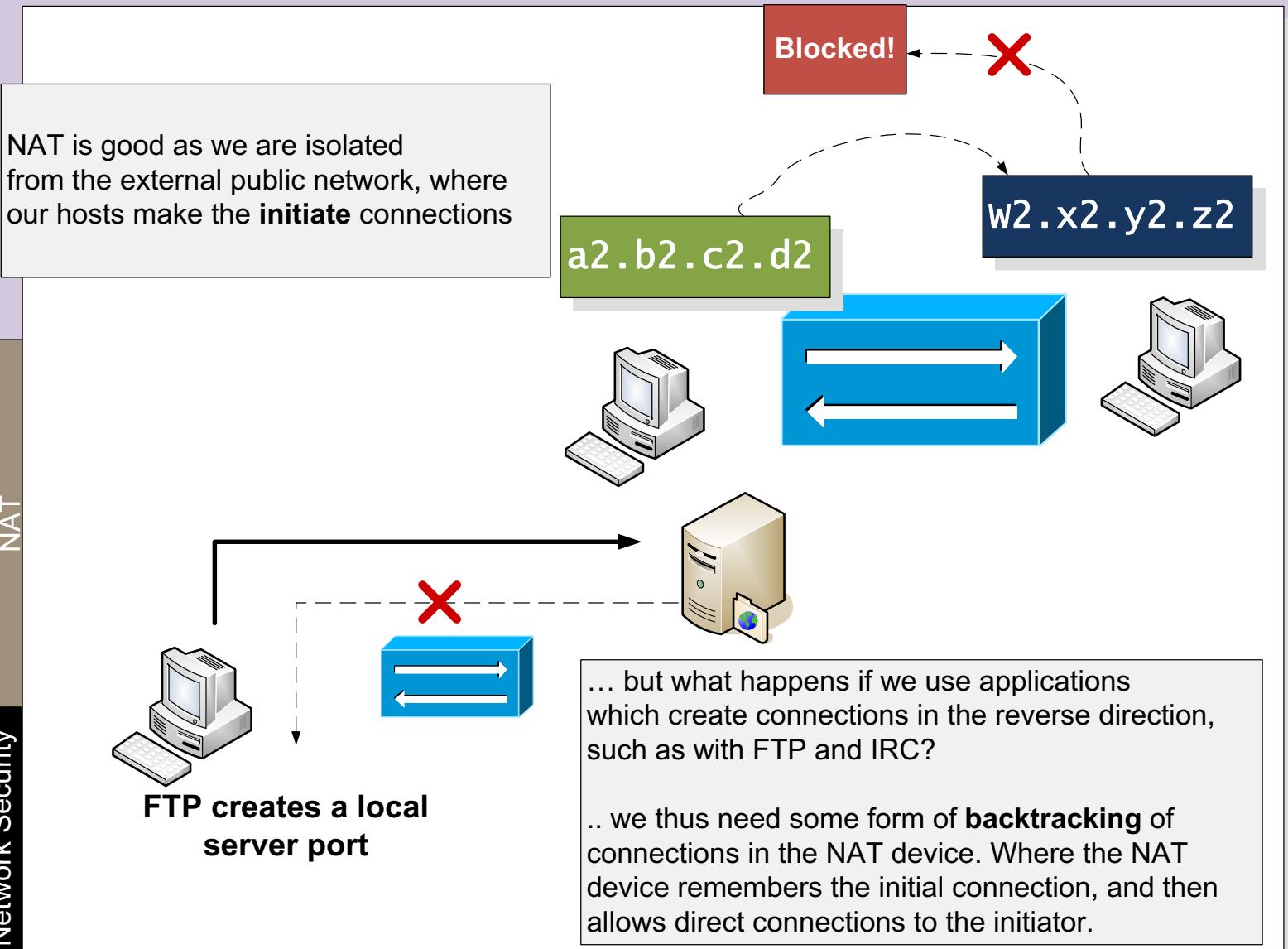
Layered Model



Layered Model



Layered Model

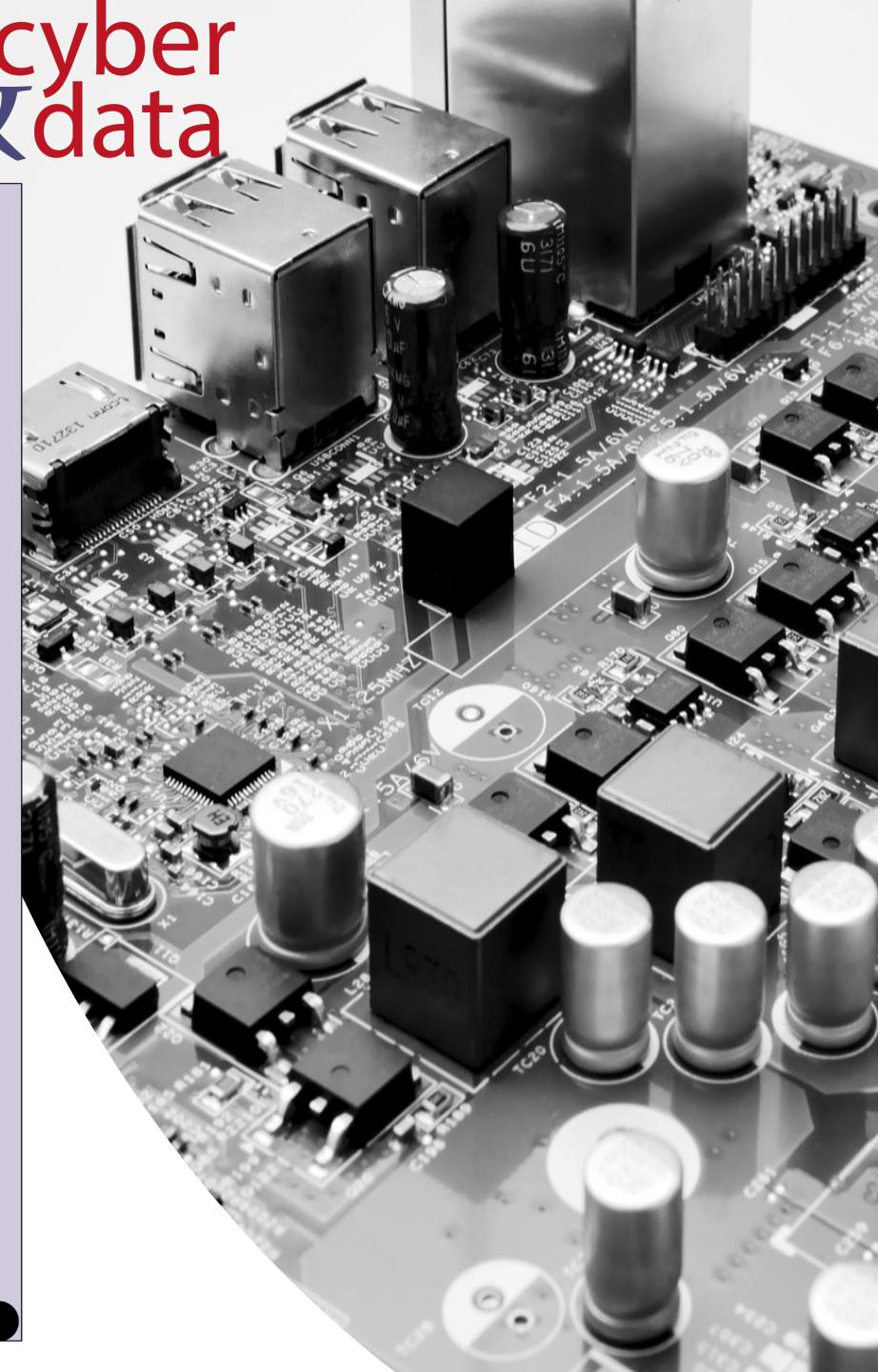
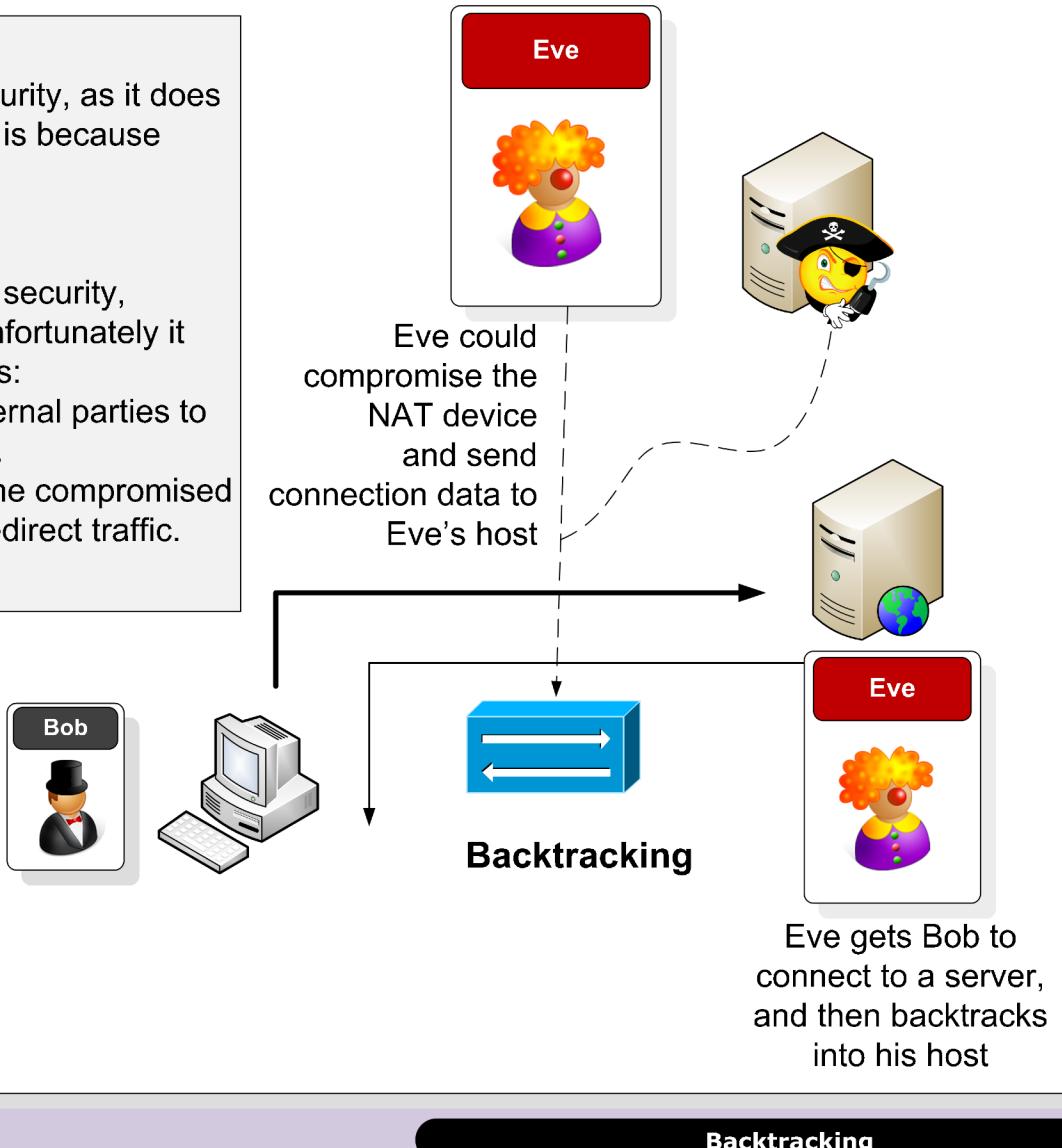


Layered Model

Static NAT is poor for security, as it does not hide the network. This is because there is a one-to-one mapping.

Dynamic NAT is good for security, as it hides the network. Unfortunately it has two major weaknesses:

- *Backtracking* allows external parties to trace back a connection.
- If the NAT device become compromised the external party can redirect traffic.



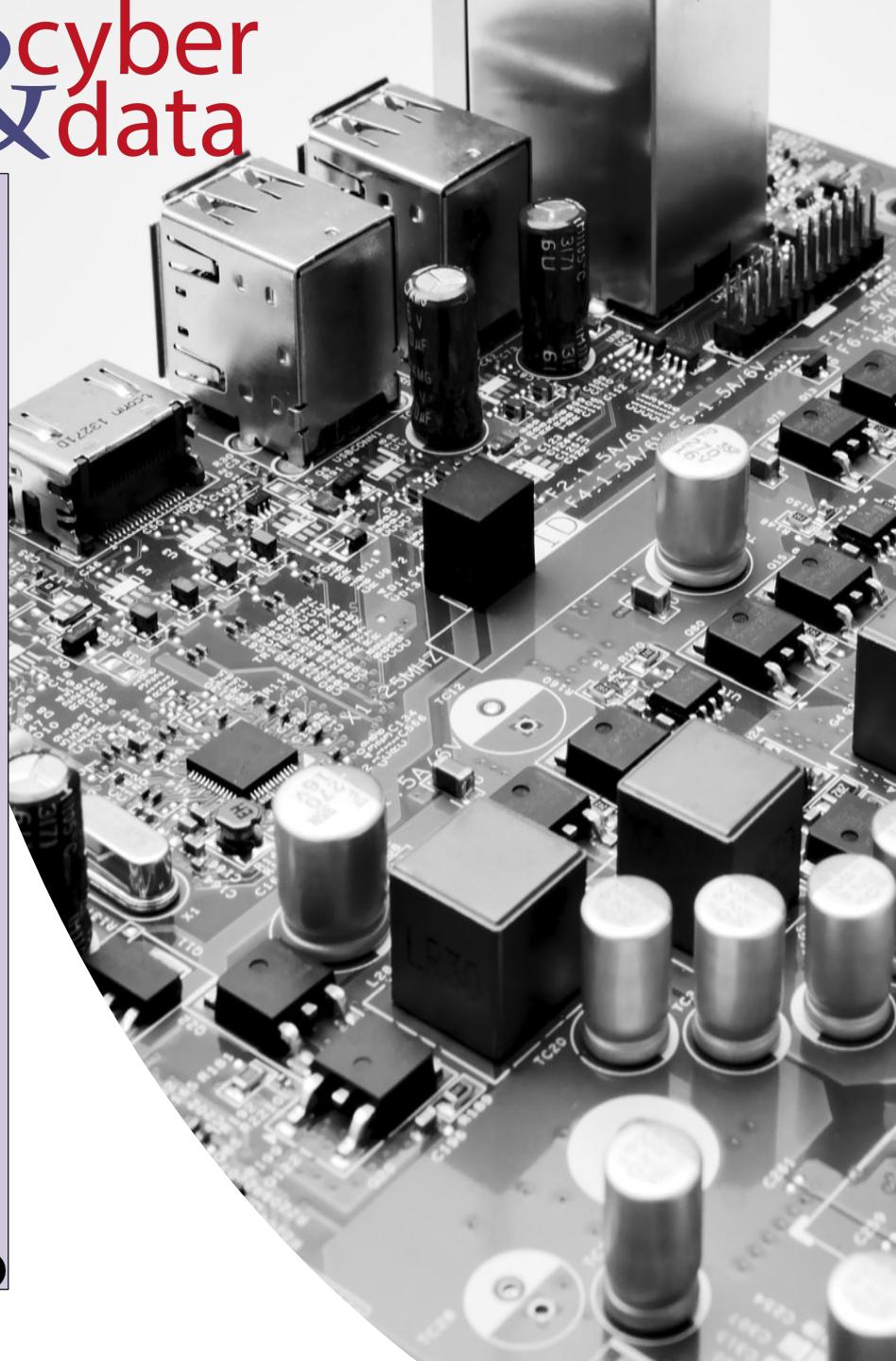
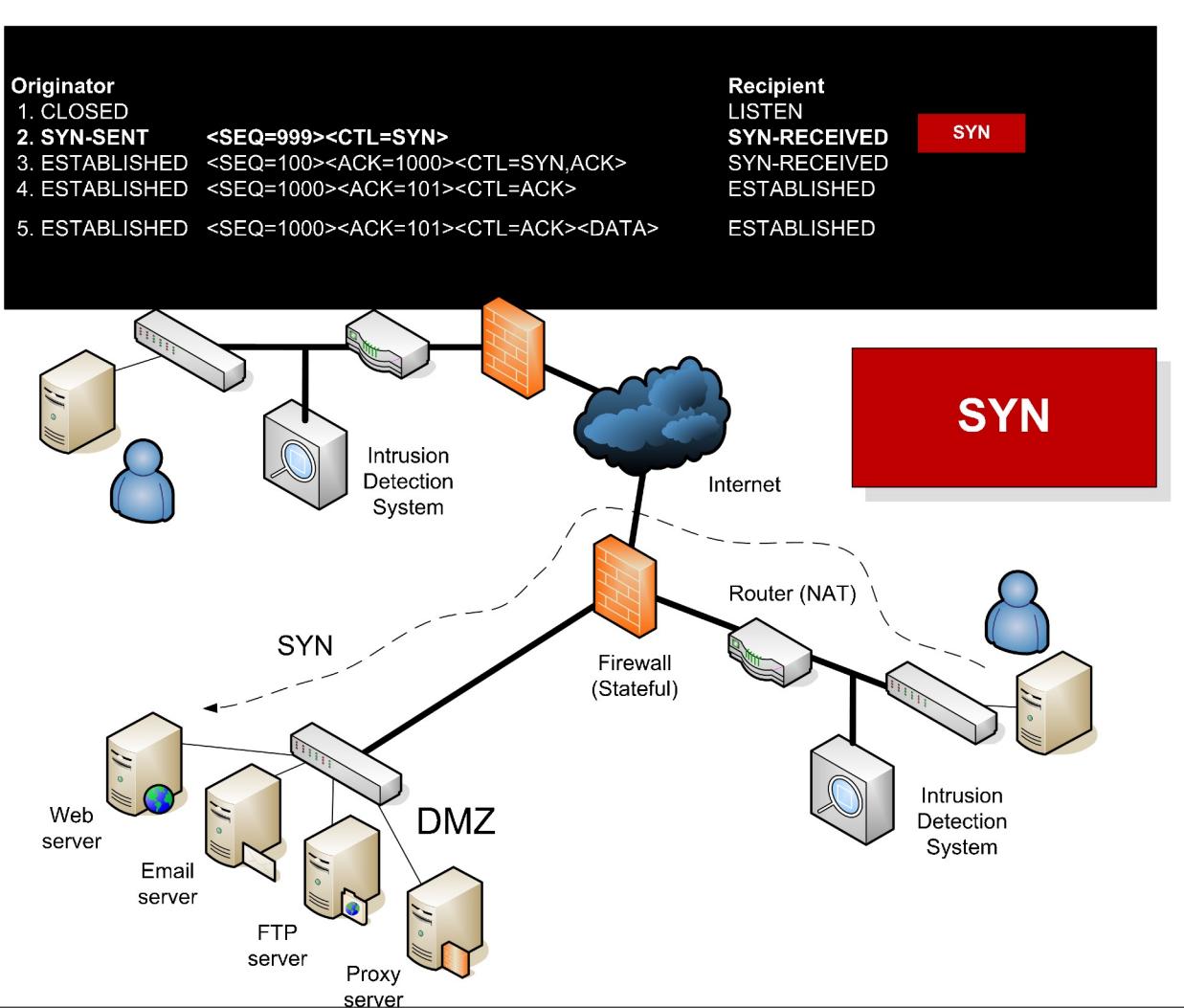
cyber & data

“From bits to information”

Stateful Firewalls

Layered Model

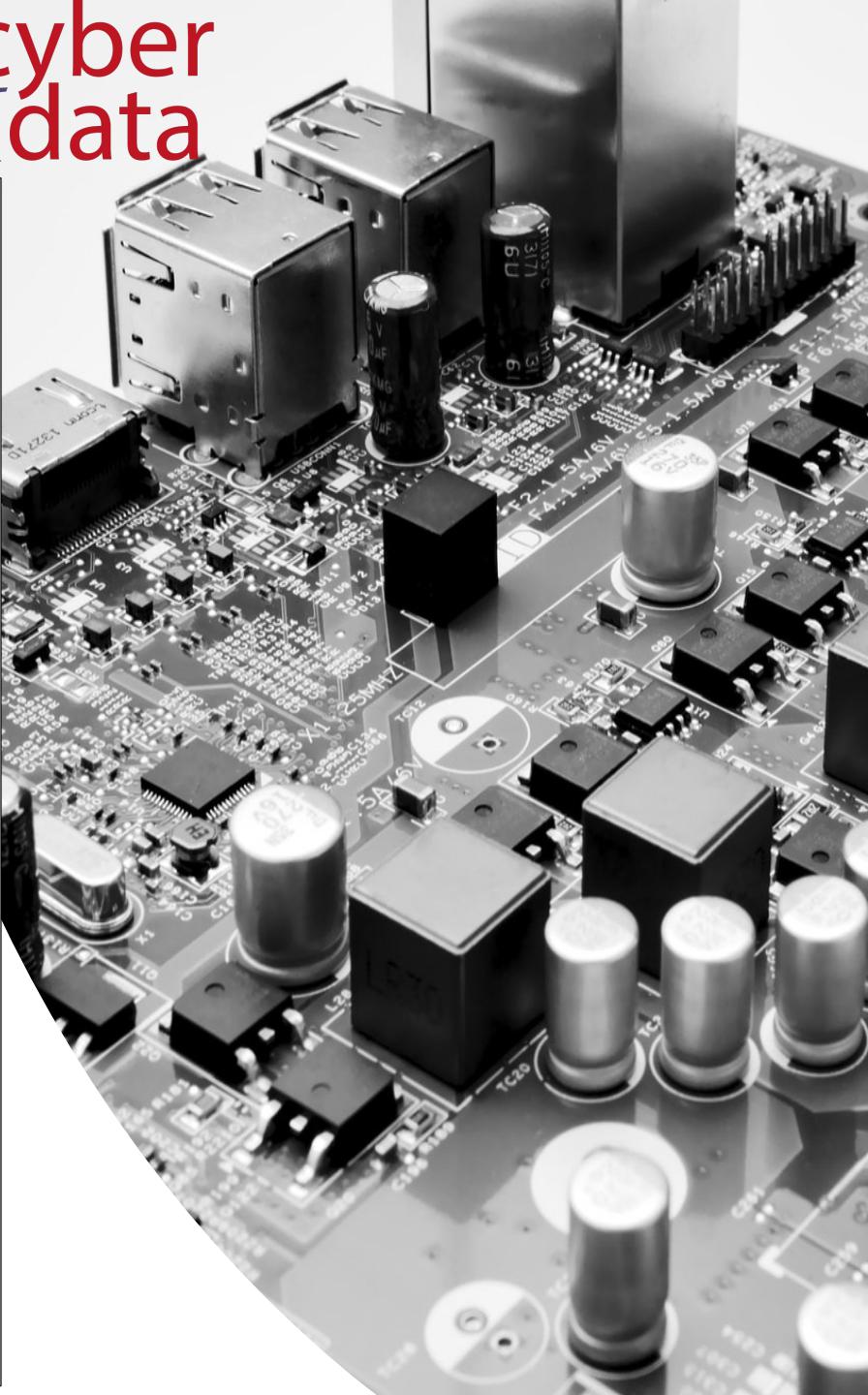
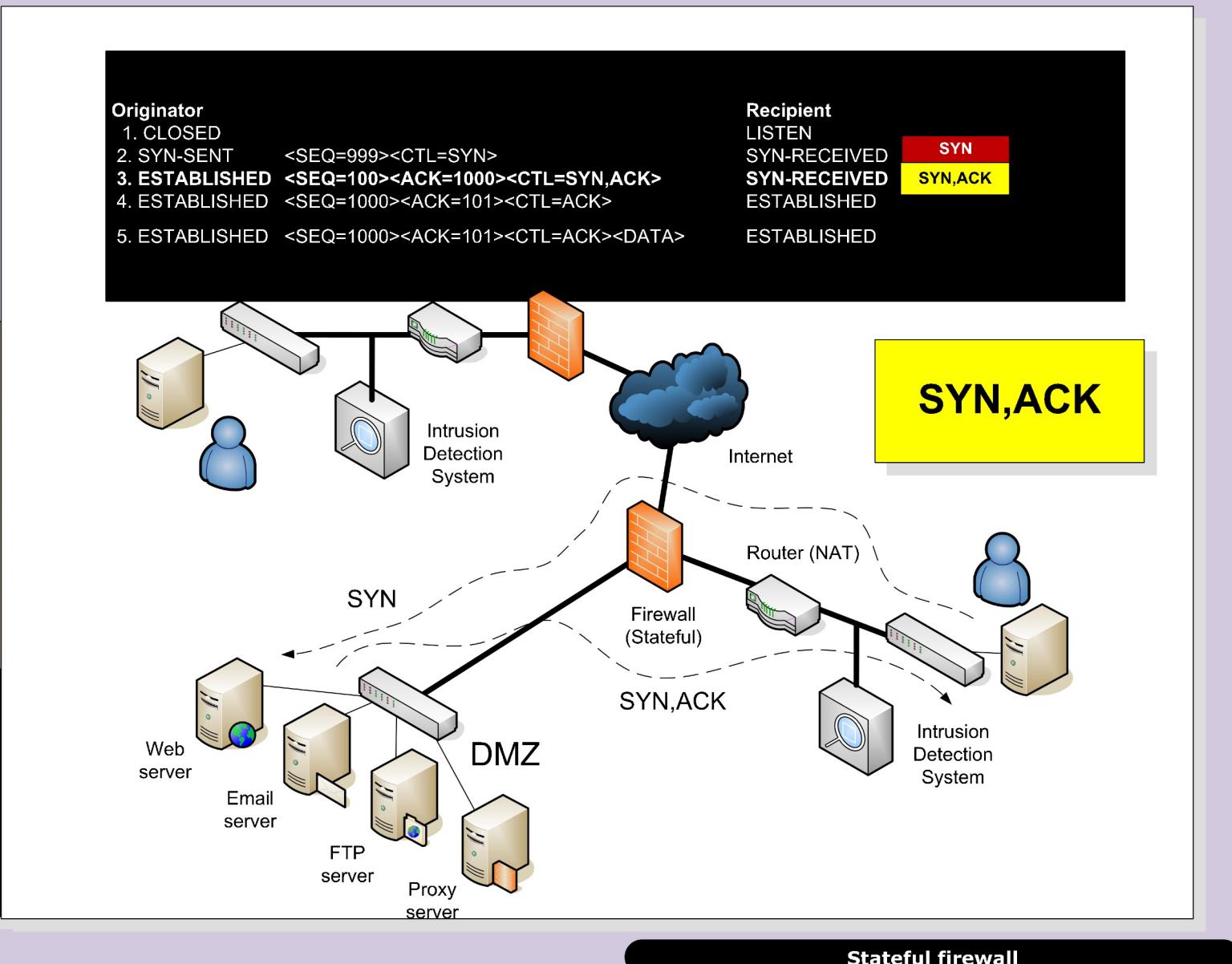
cyber
&
data



Layered Model

cyber
&
data

Network Security Stateful firewall



Layered Model

cyber
&
data

Originator

1. CLOSED LISTEN
2. SYN-SENT <SEQ=999><CTL=SYN>
3. ESTABLISHED <SEQ=100><ACK=1000><CTL=SYN,ACK>
- 4. ESTABLISHED** <SEQ=1000><ACK=101><CTL=ACK>
5. ESTABLISHED <SEQ=1000><ACK=101><CTL=ACK><DATA>

Recipient

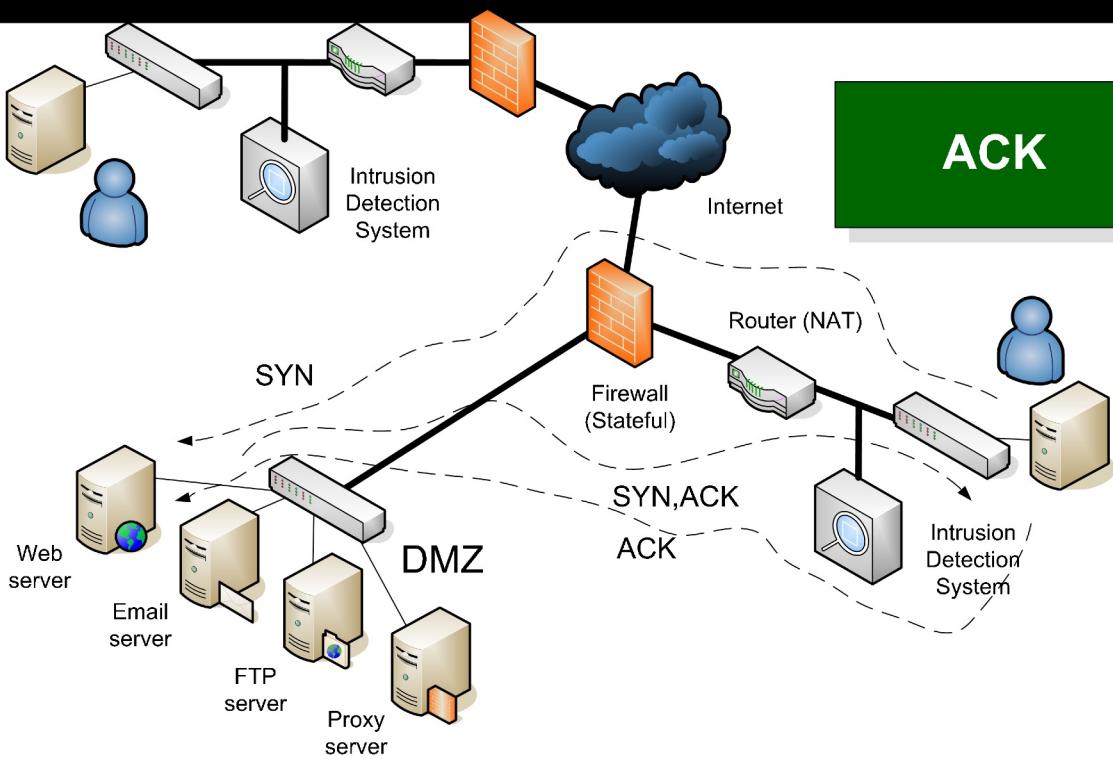
SYN-RECEIVED
SYN-RECEIVED
ESTABLISHED
ESTABLISHED

SYN
SYN,ACK
ACK

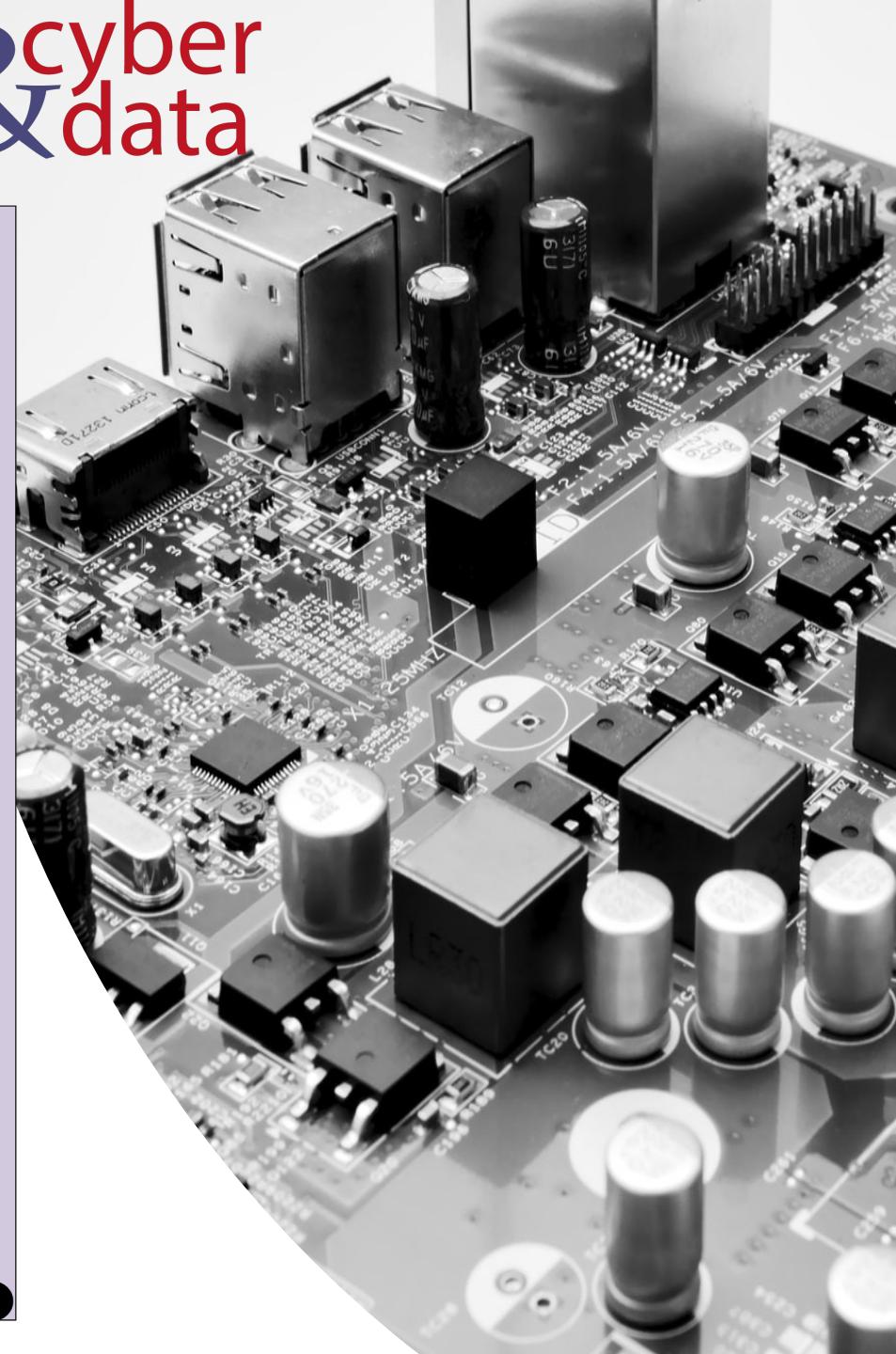
ACK

Stateful firewall

Network Security



Stateful firewall



Layered Model

cyber
&
data

Stateful firewalls

Network Security

www.napier.ac.uk?

DNS server

192.168.1.101

TCP port=4213

SYN
Src Port=4213, Dest Port=80

TCP port=80

146.176.1.188

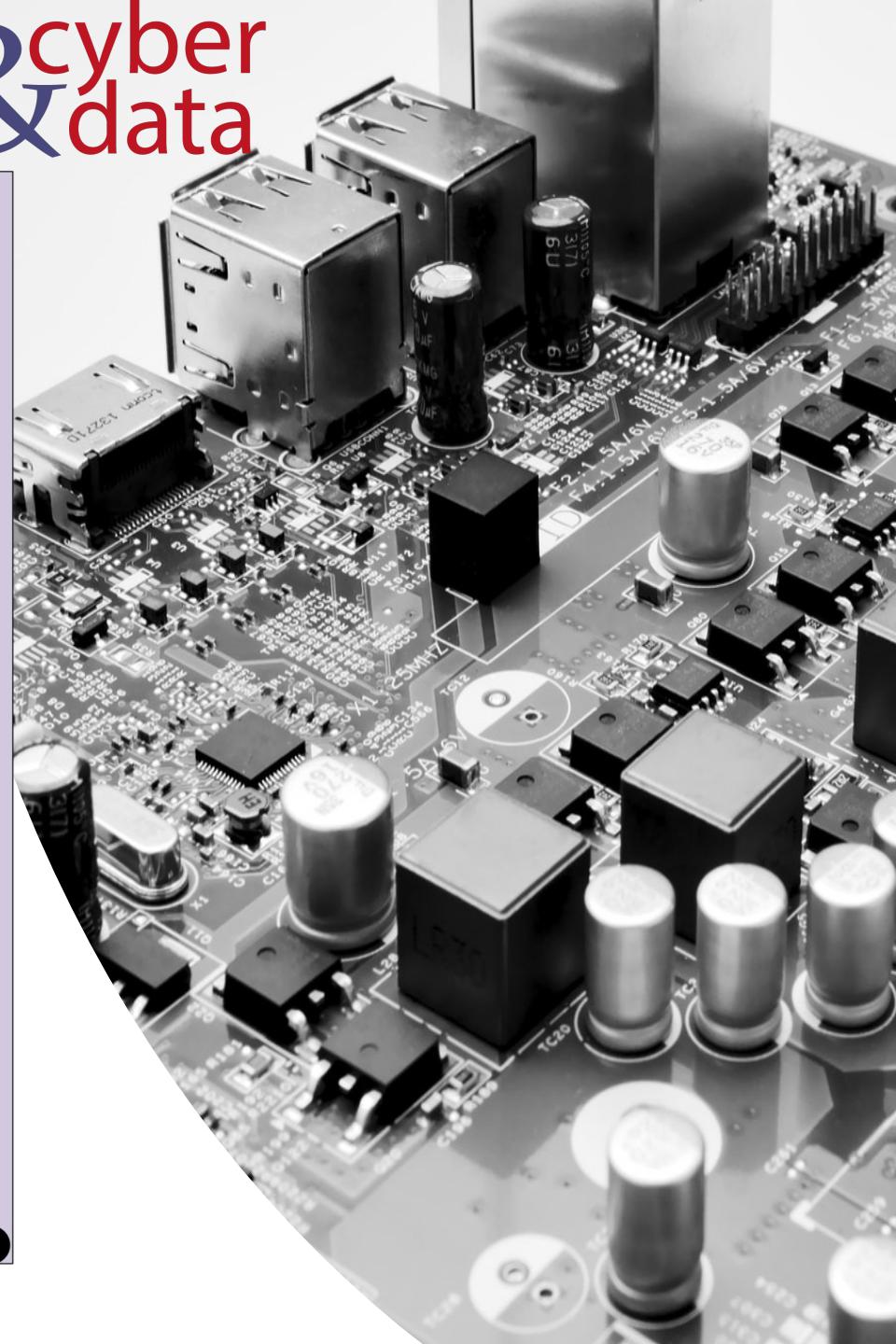
146.176.1.188

Client-server (SYN)

SYN

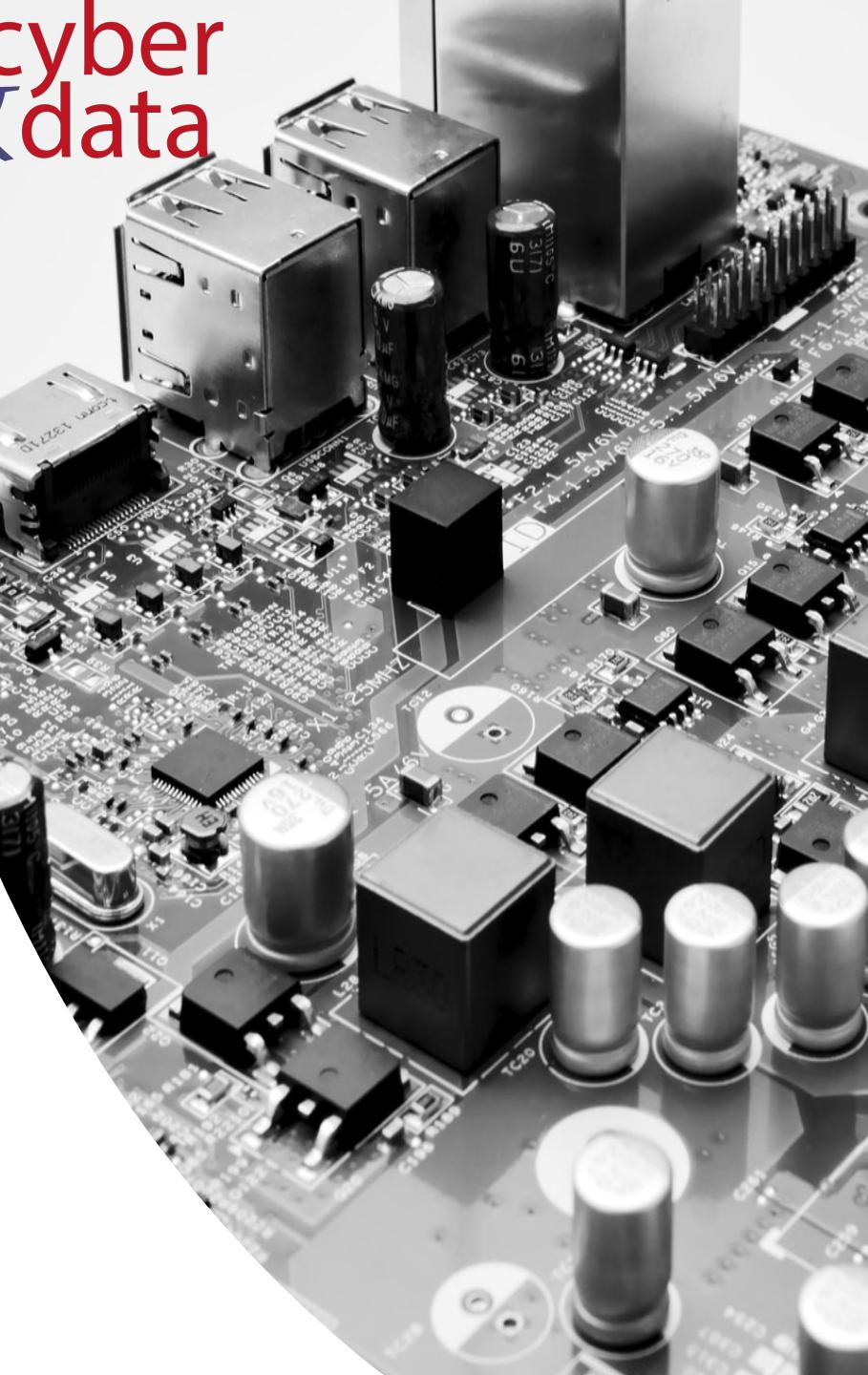
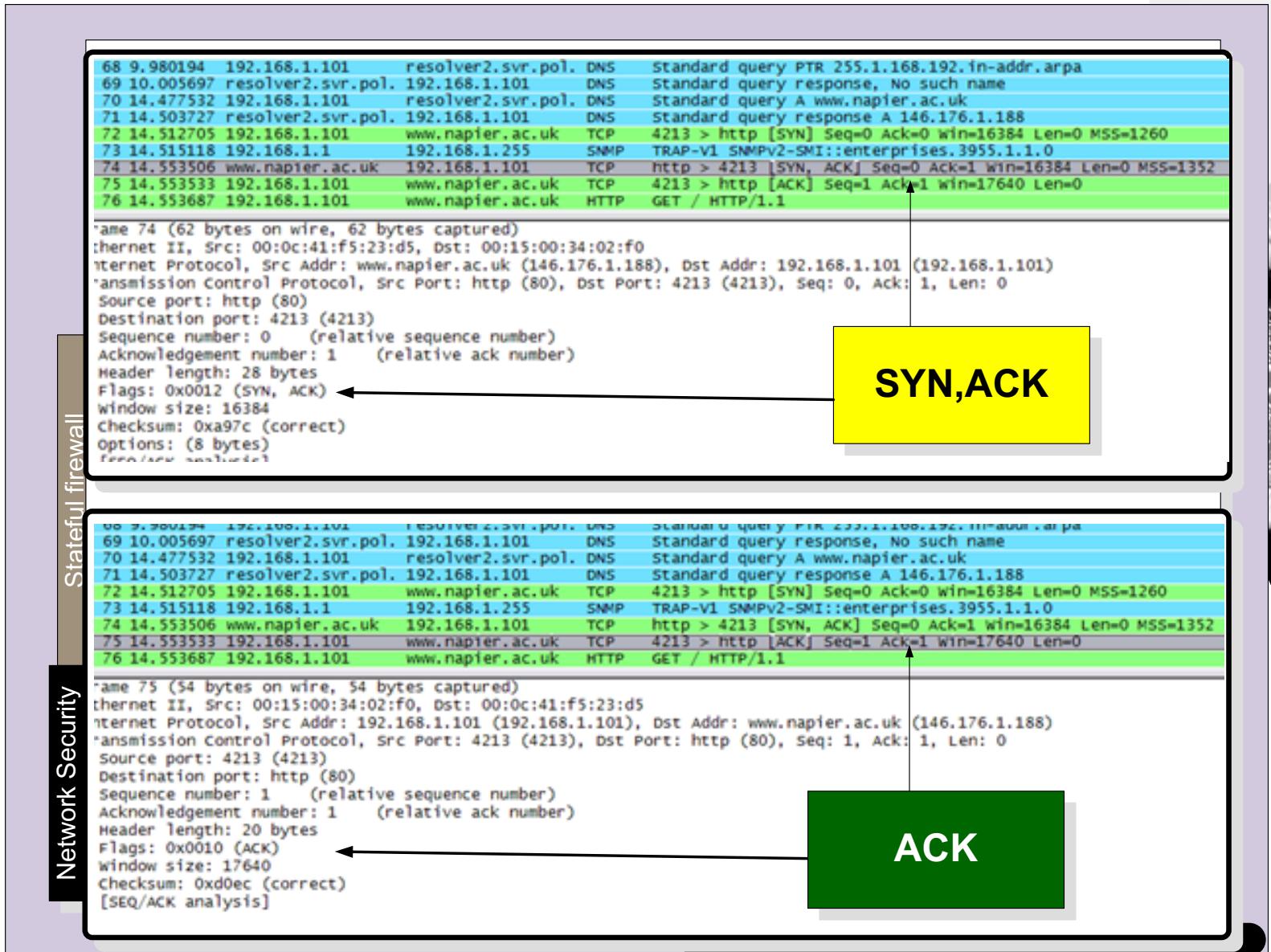
```
68 9.980194 192.168.1.101 resolver2.srv.pol. DNS Standard query PTR 255.1.168.192.in-addr.arpa
69 10.005697 resolver2.srv.pol. 192.168.1.101 DNS Standard query response, No such name
70 14.477532 192.168.1.101 resolver2.srv.pol. DNS Standard query A www.napier.ac.uk
71 14.503727 resolver2.srv.pol. 192.168.1.101 DNS Standard query response A 146.176.1.188
72 14.512705 192.168.1.101 www.napier.ac.uk TCP 4213 > http [SYN] Seq=0 Ack=0 Win=16384 Len=0 MSS=1260
73 14.515118 192.168.1.1 192.168.1.255 SNMP TRAP-V1 SNMPv2-SMI::enterprises.3955.1.1.0
74 14.553506 www.napier.ac.uk 192.168.1.101 TCP http > 4213 [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0 MSS=1352
75 14.553533 192.168.1.101 www.napier.ac.uk TCP 4213 > http [ACK] Seq=1 Ack=1 Win=17640 Len=0
76 14.553687 192.168.1.101 www.napier.ac.uk HTTP GET / HTTP/1.1

ame 72 (62 bytes on wire, 62 bytes captured)
Ethernet II, Src: 00:15:00:34:02:f0, Dst: 00:0c:41:f5:23:d5
Internet Protocol, Src Addr: 192.168.1.101 (192.168.1.101), Dst Addr: www.napier.ac.uk (146.176.1.188)
Transmission Control Protocol, Src Port: 4213 (4213), Dst Port: http (80), seq: 0, Ack: 0, Len: 0
Source port: 4213 (4213)
Destination port: http (80)
Sequence number: 0 (relative sequence number)
Header length: 28 bytes
Flags: 0x0002 (SYN)
Window size: 16384
Checksum: 0x3c0c (correct)
Options: (8 bytes)
```



Layered Model

cyber
&
data



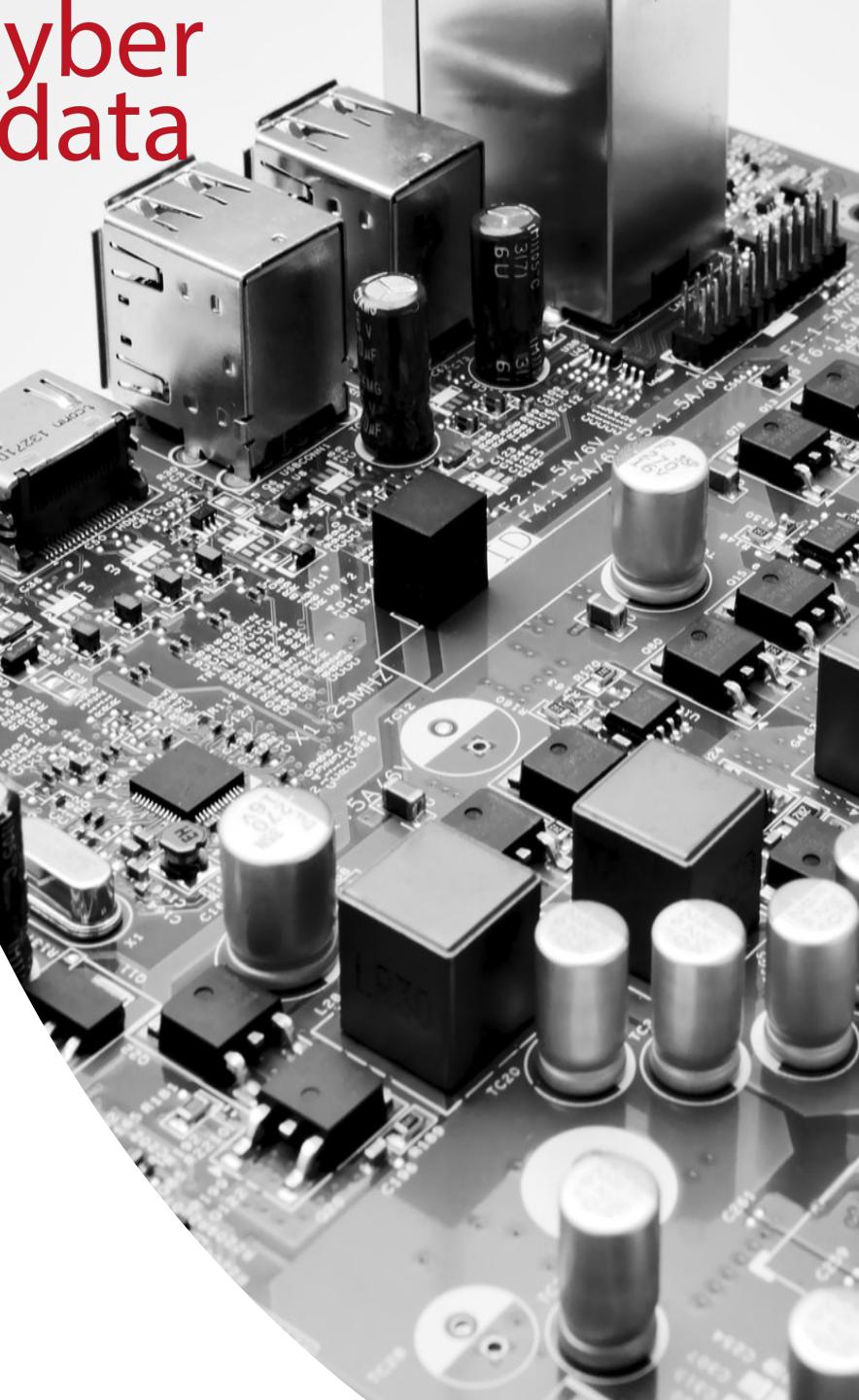
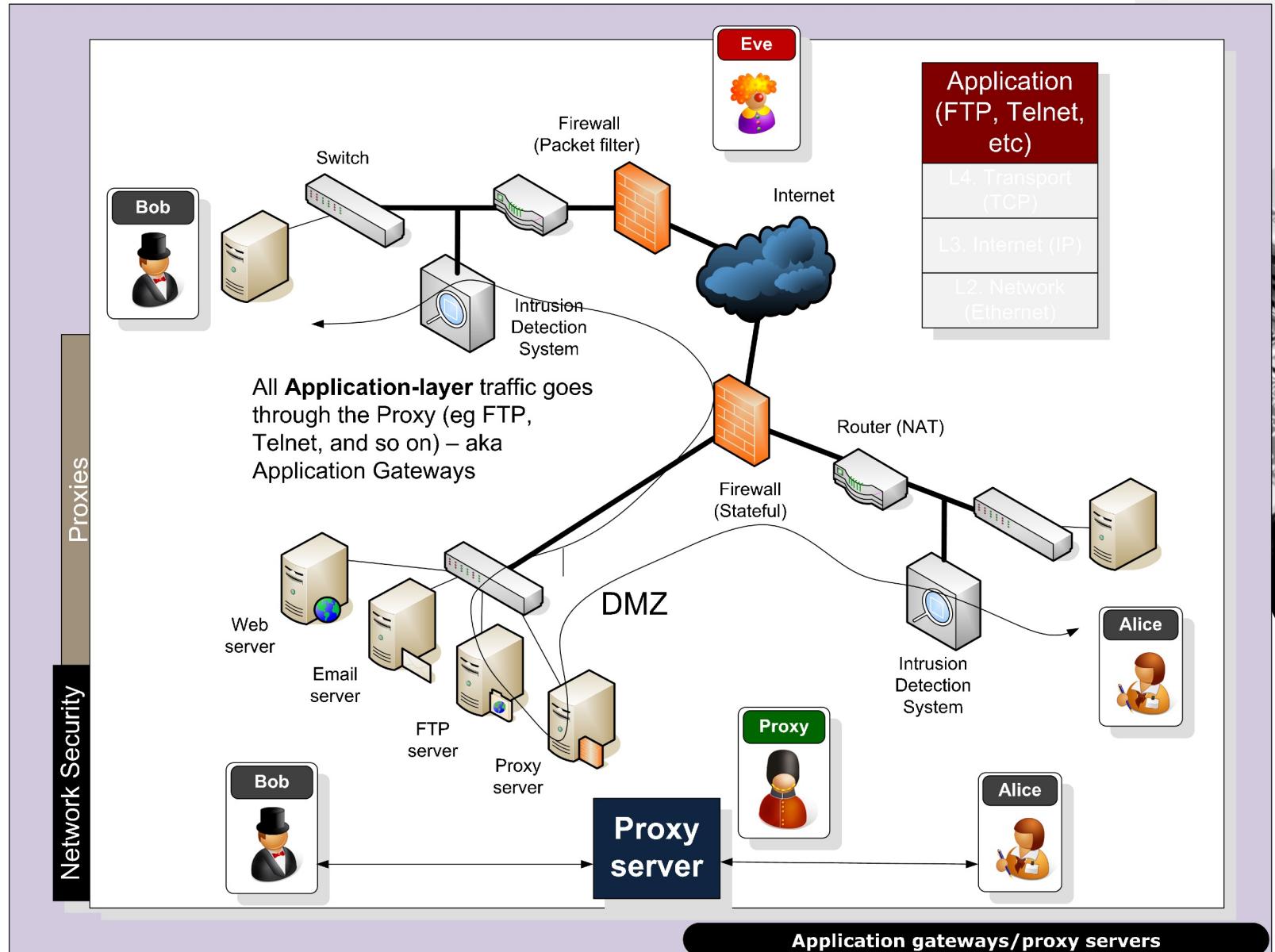
cyber & data

“From bits to information”

Proxies

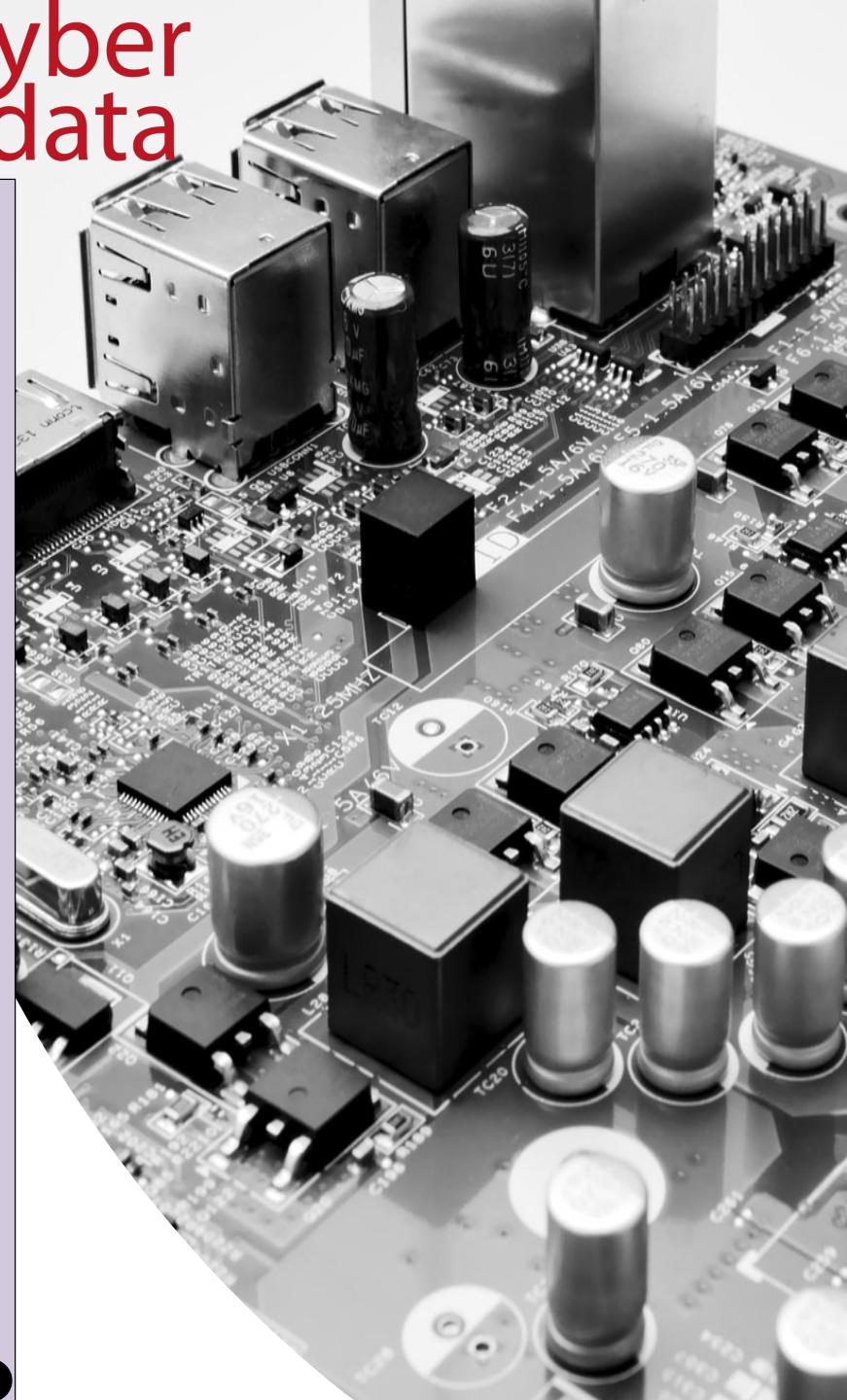
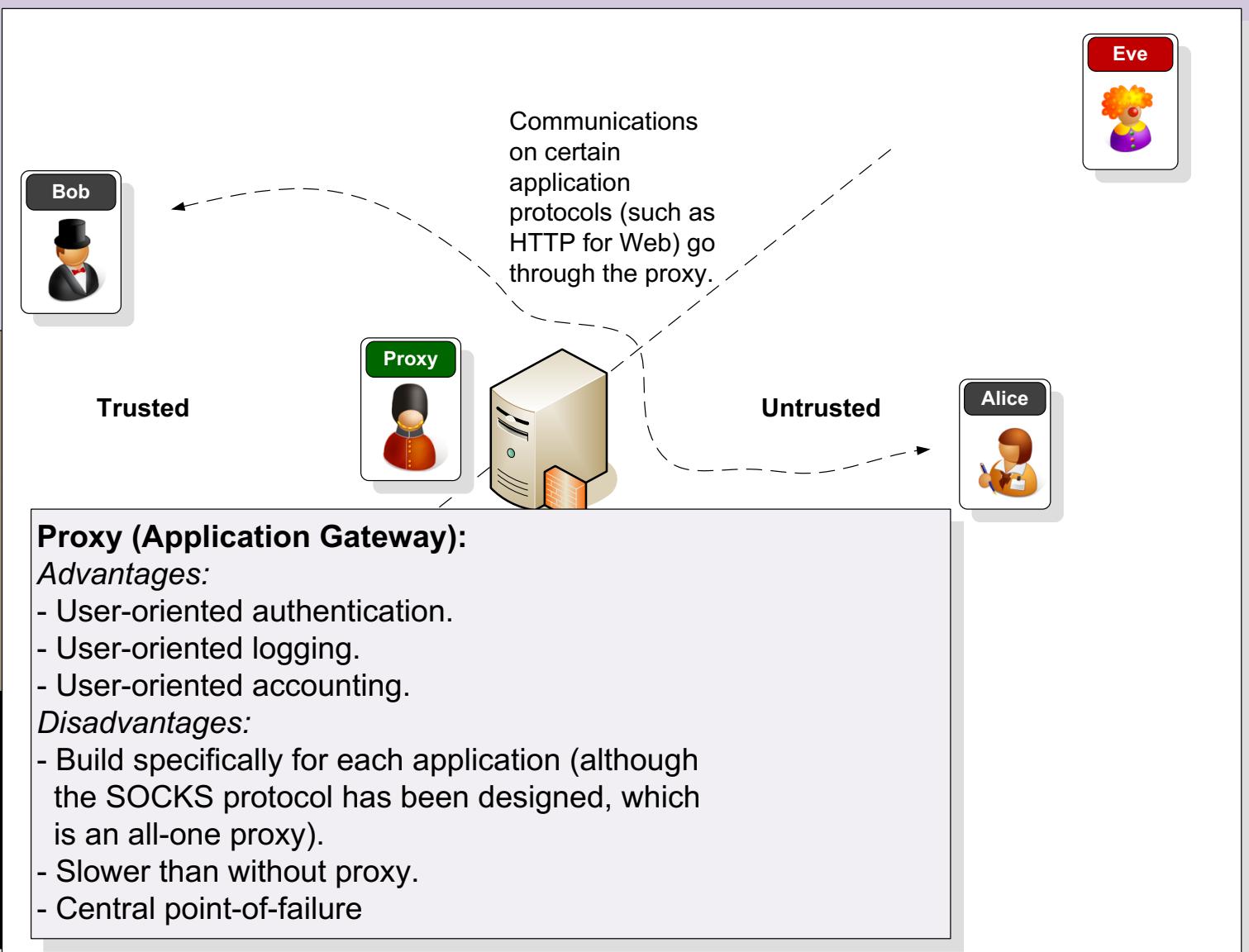
Layered Model

cyber
&
data



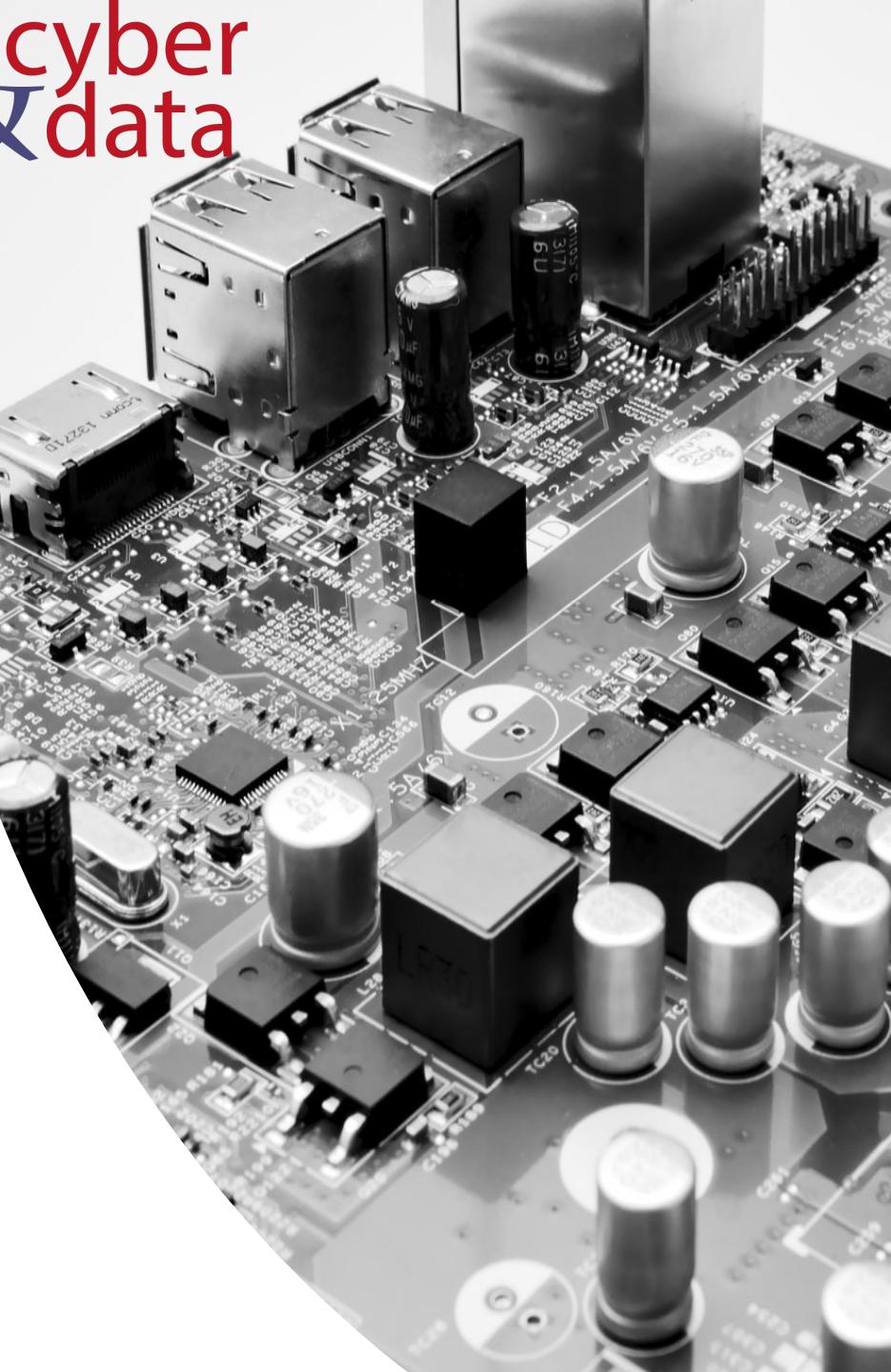
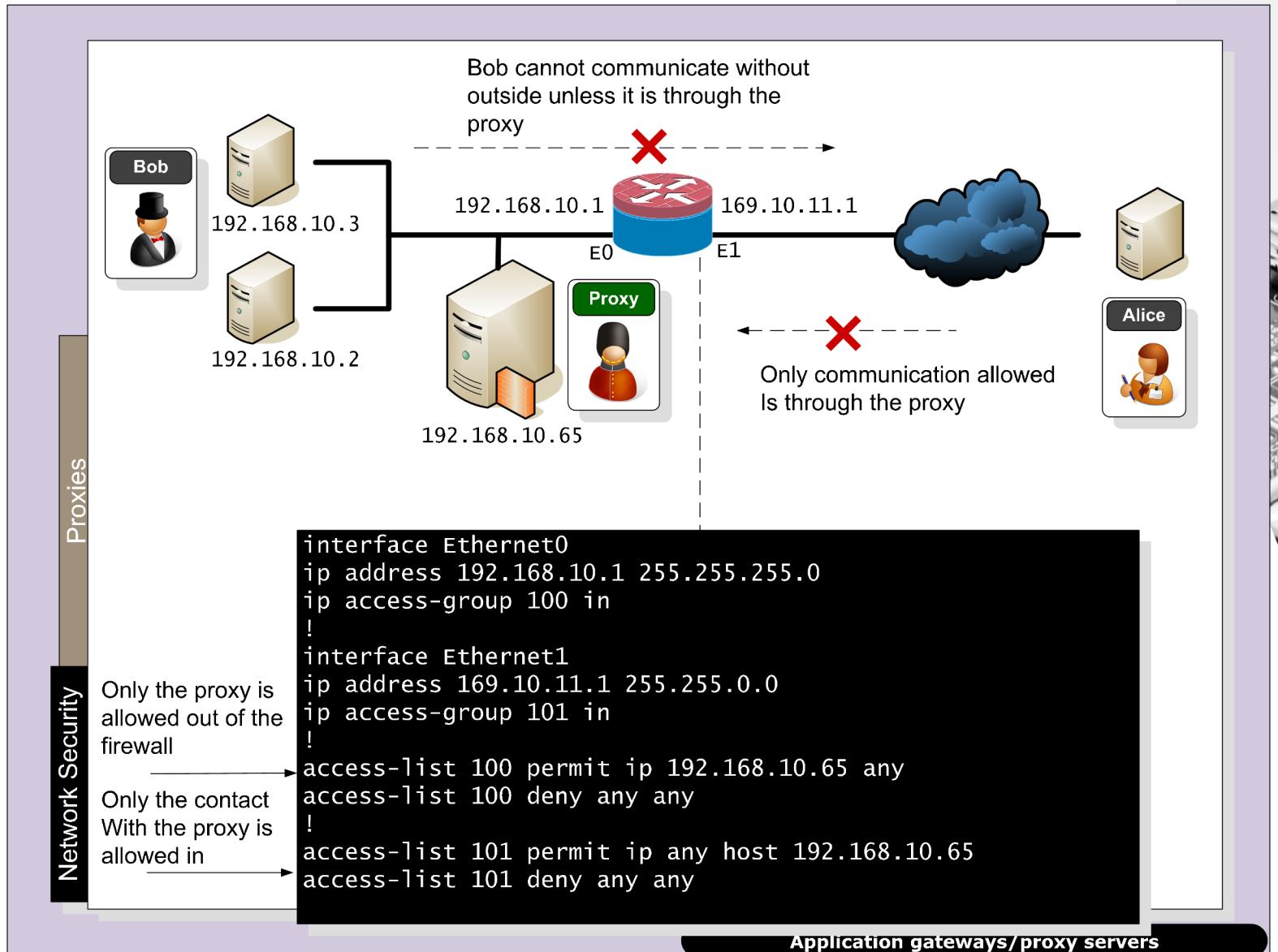
Layered Model

cyber
&
data



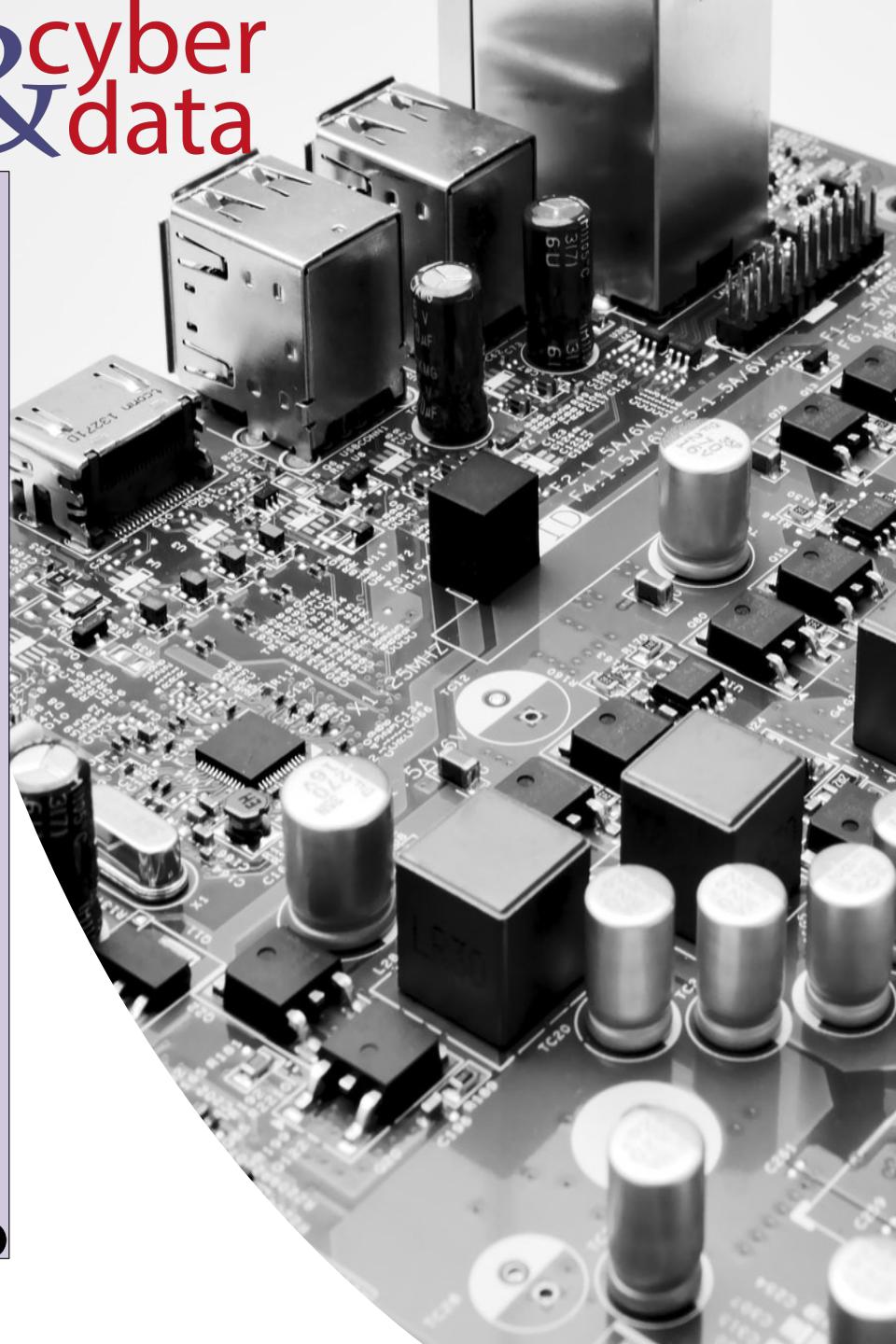
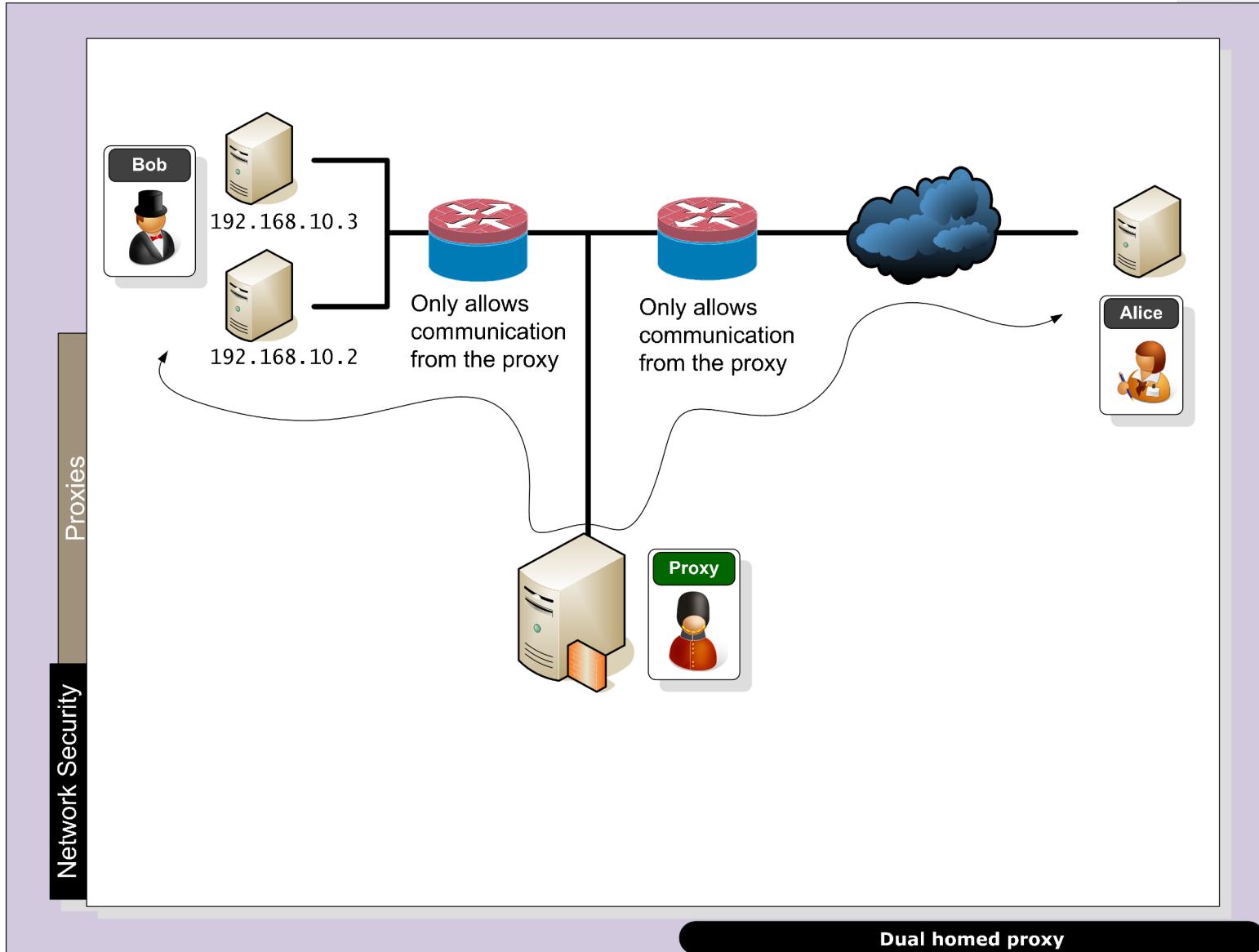
Layered Model

cyber
&
data



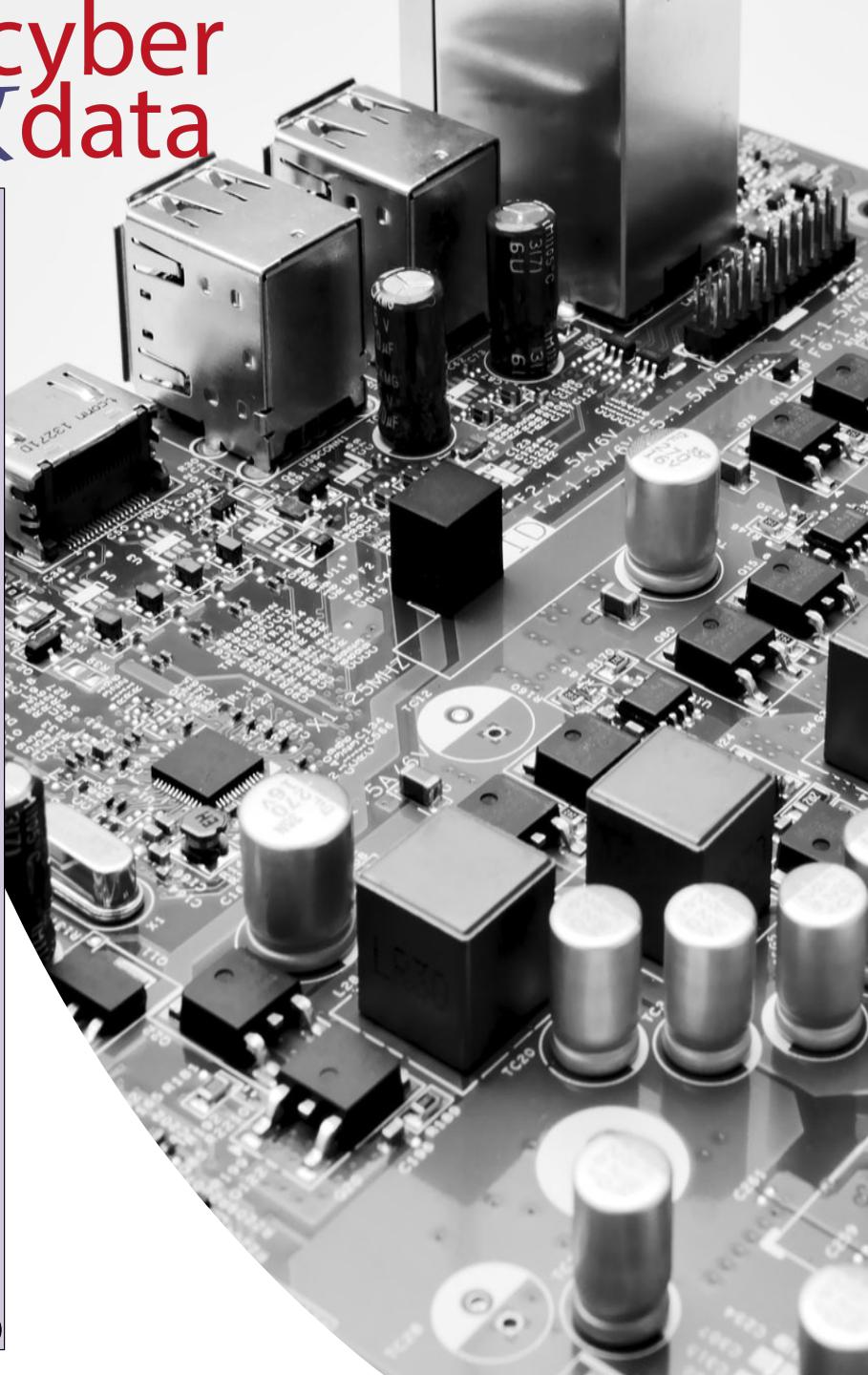
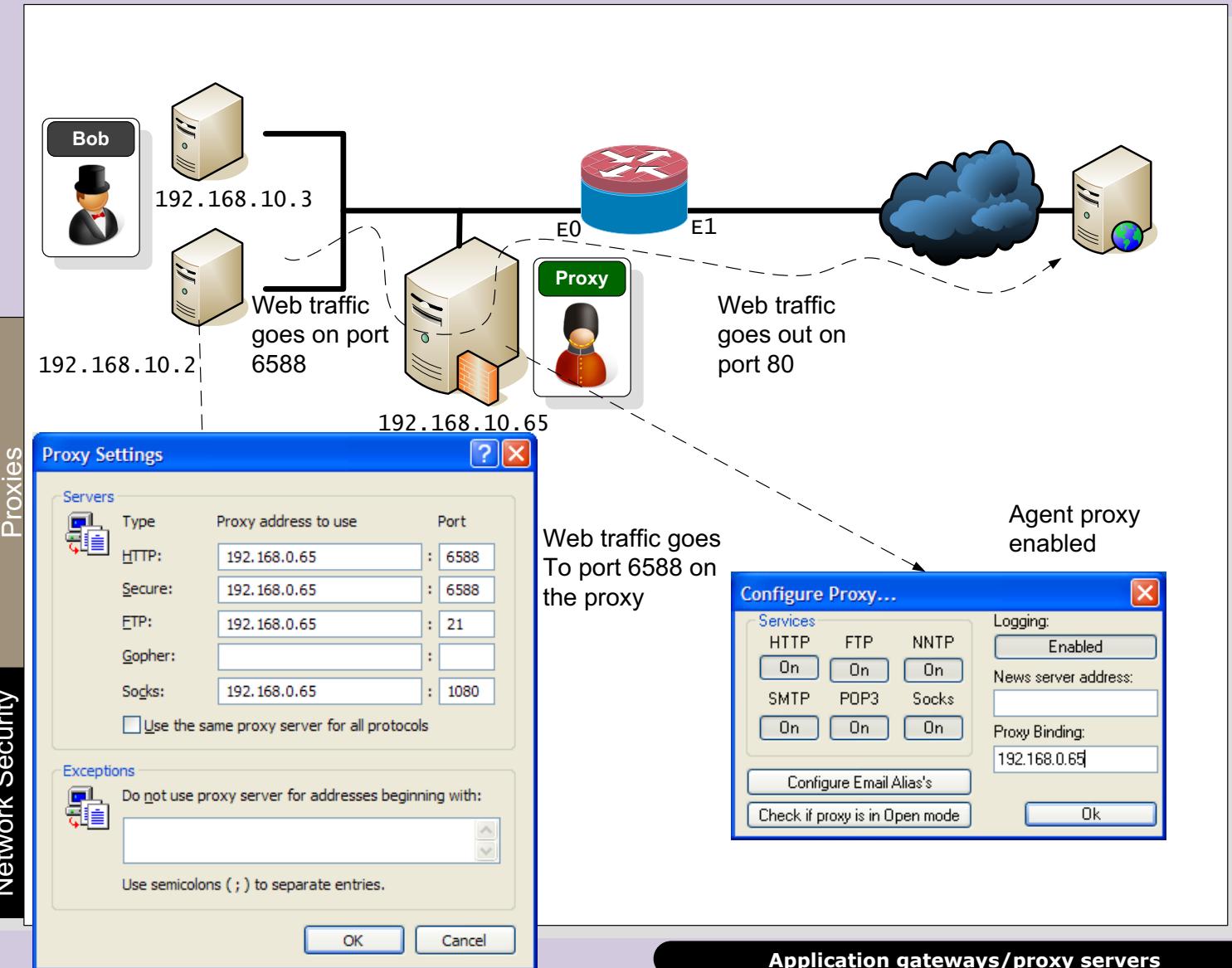
Layered Model

cyber
&
data



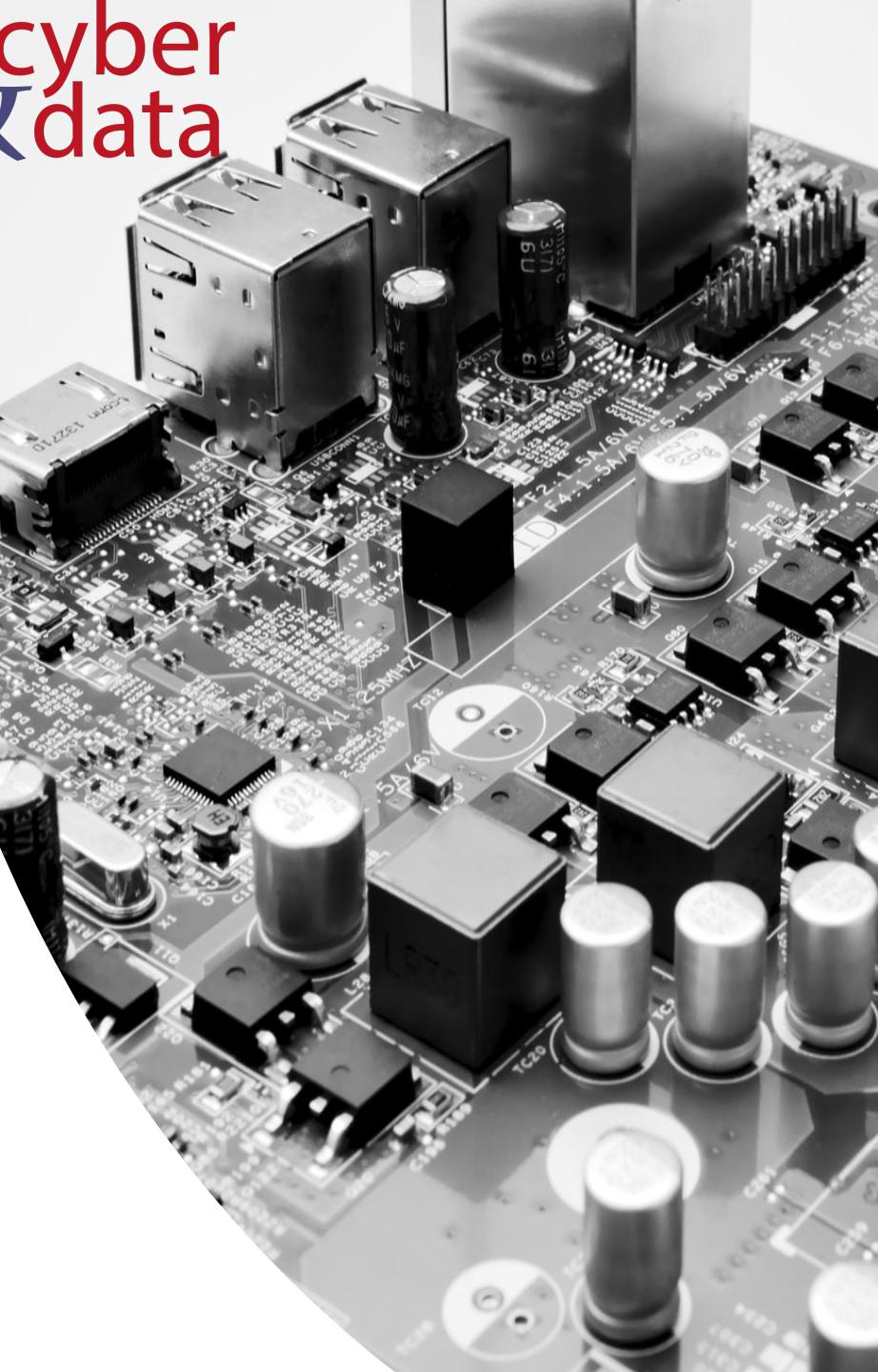
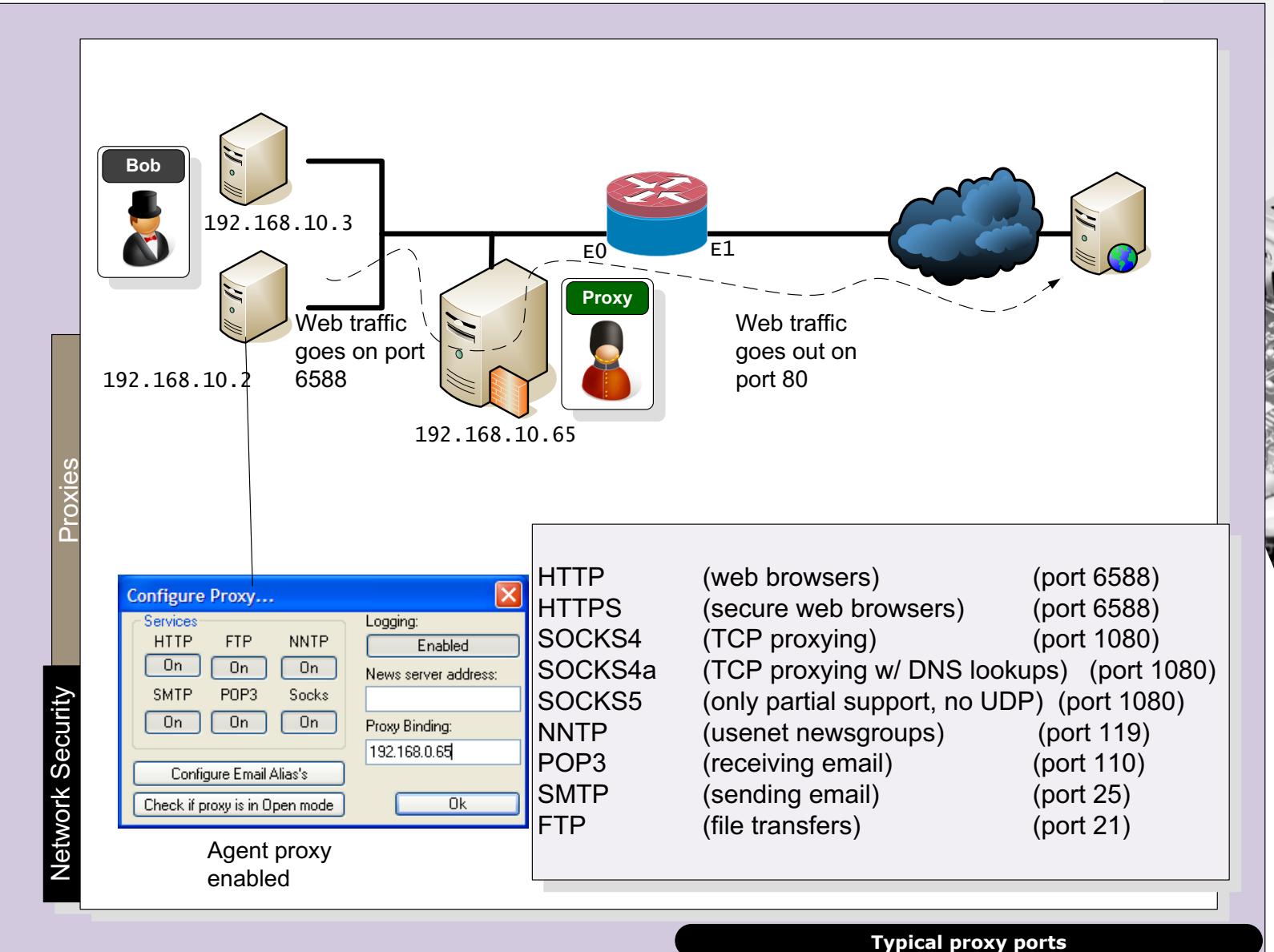
Layered Model

cyber
&
data



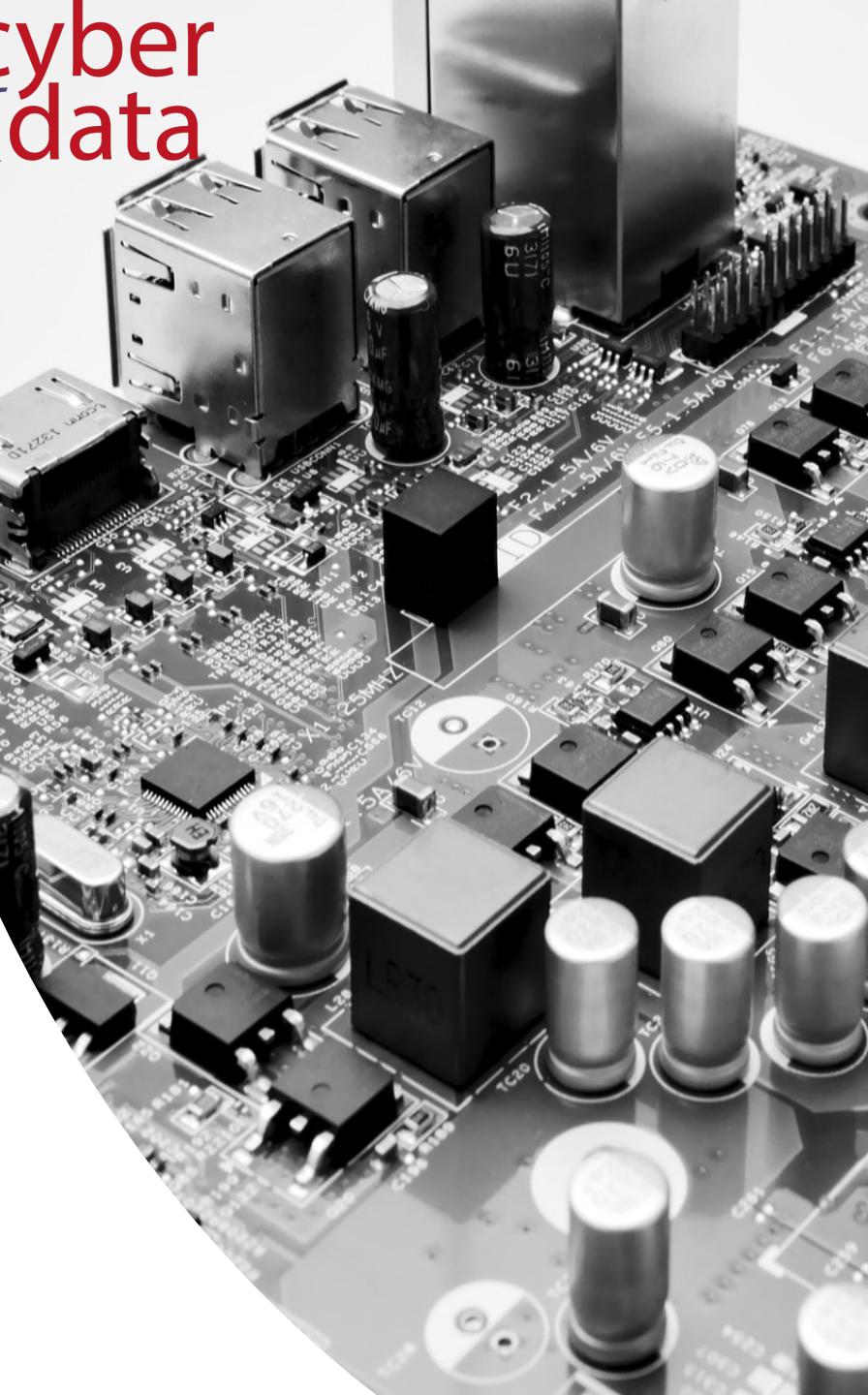
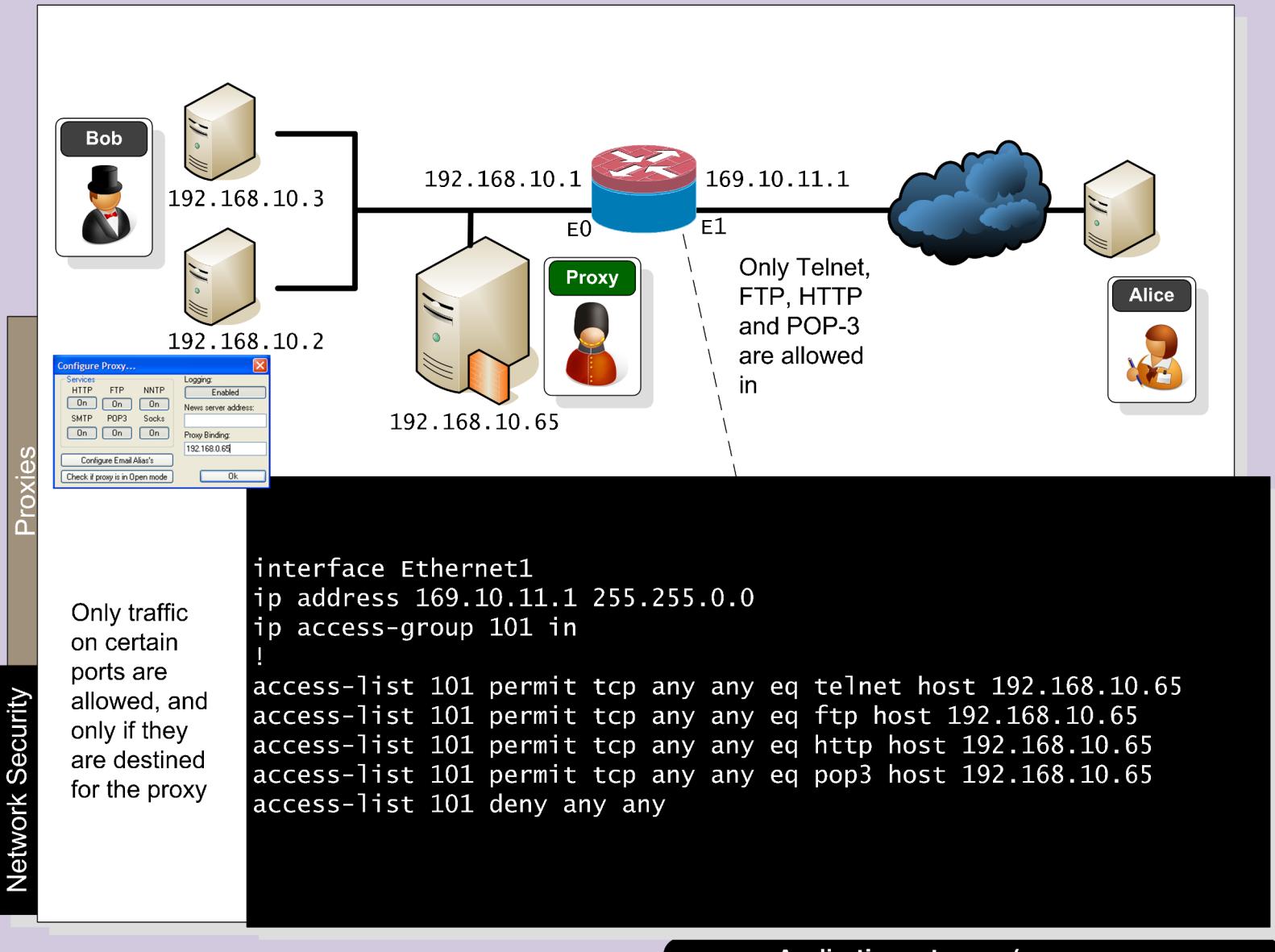
Layered Model

cyber
&
data



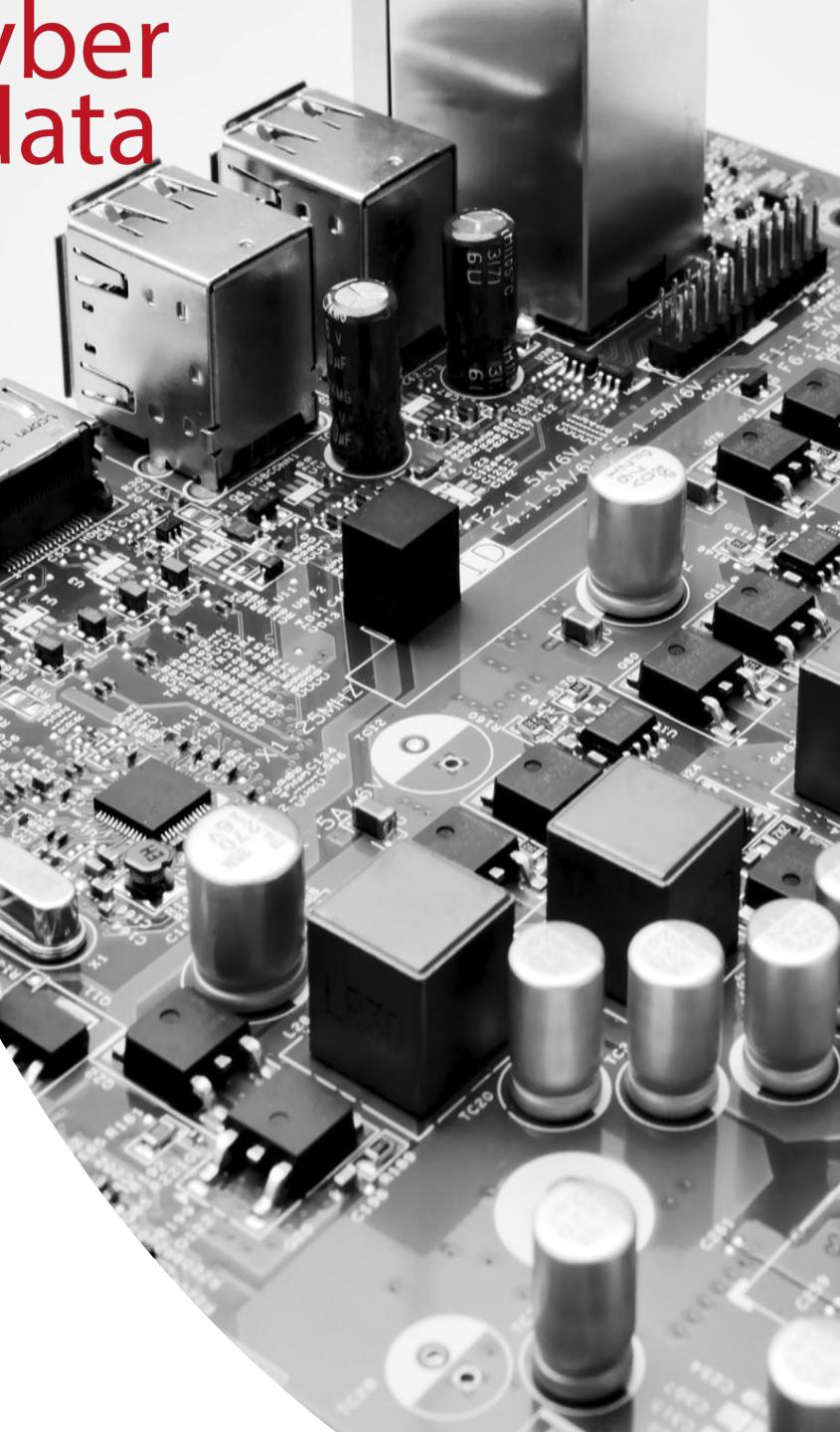
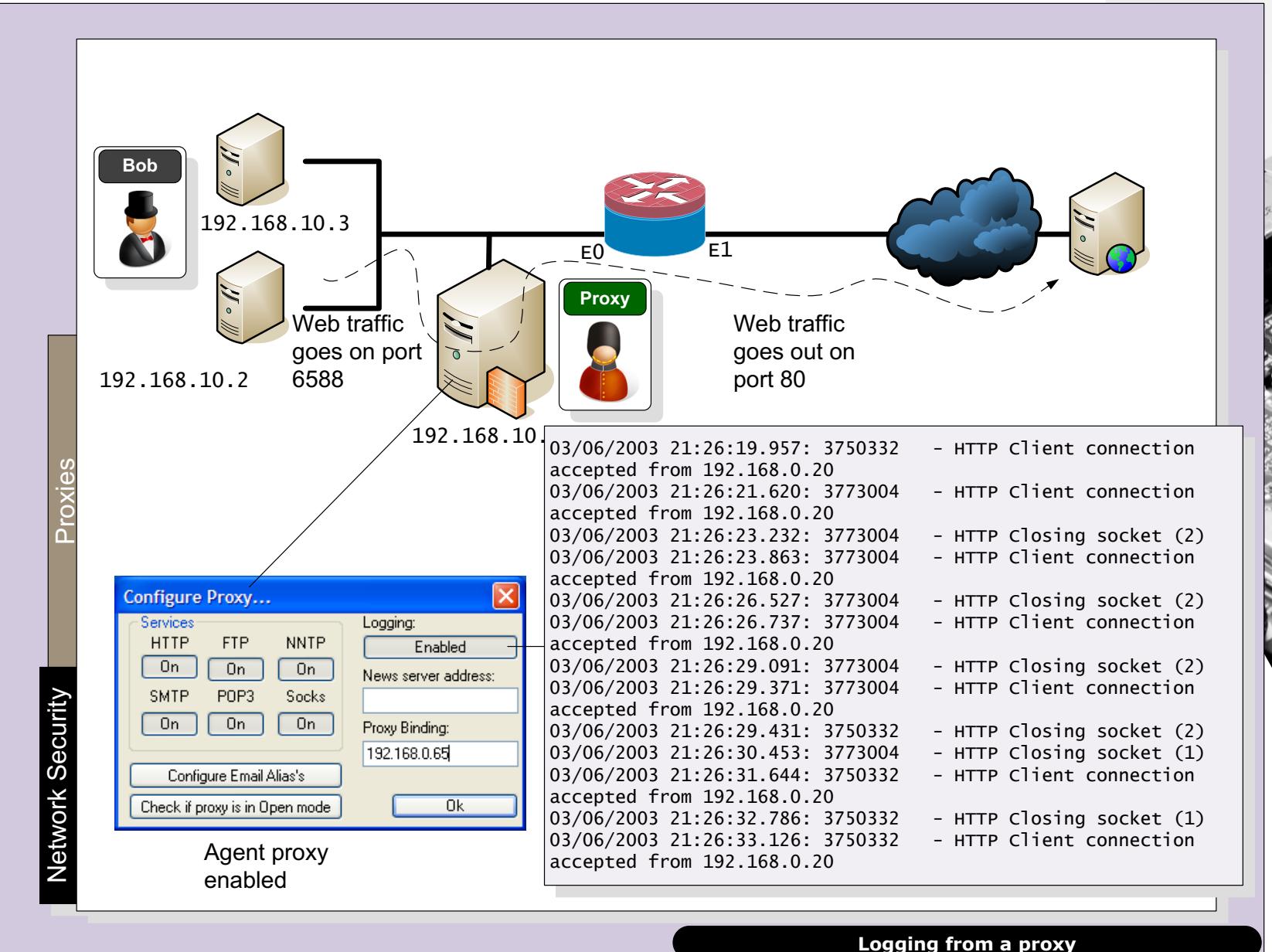
Layered Model

cyber
&
data



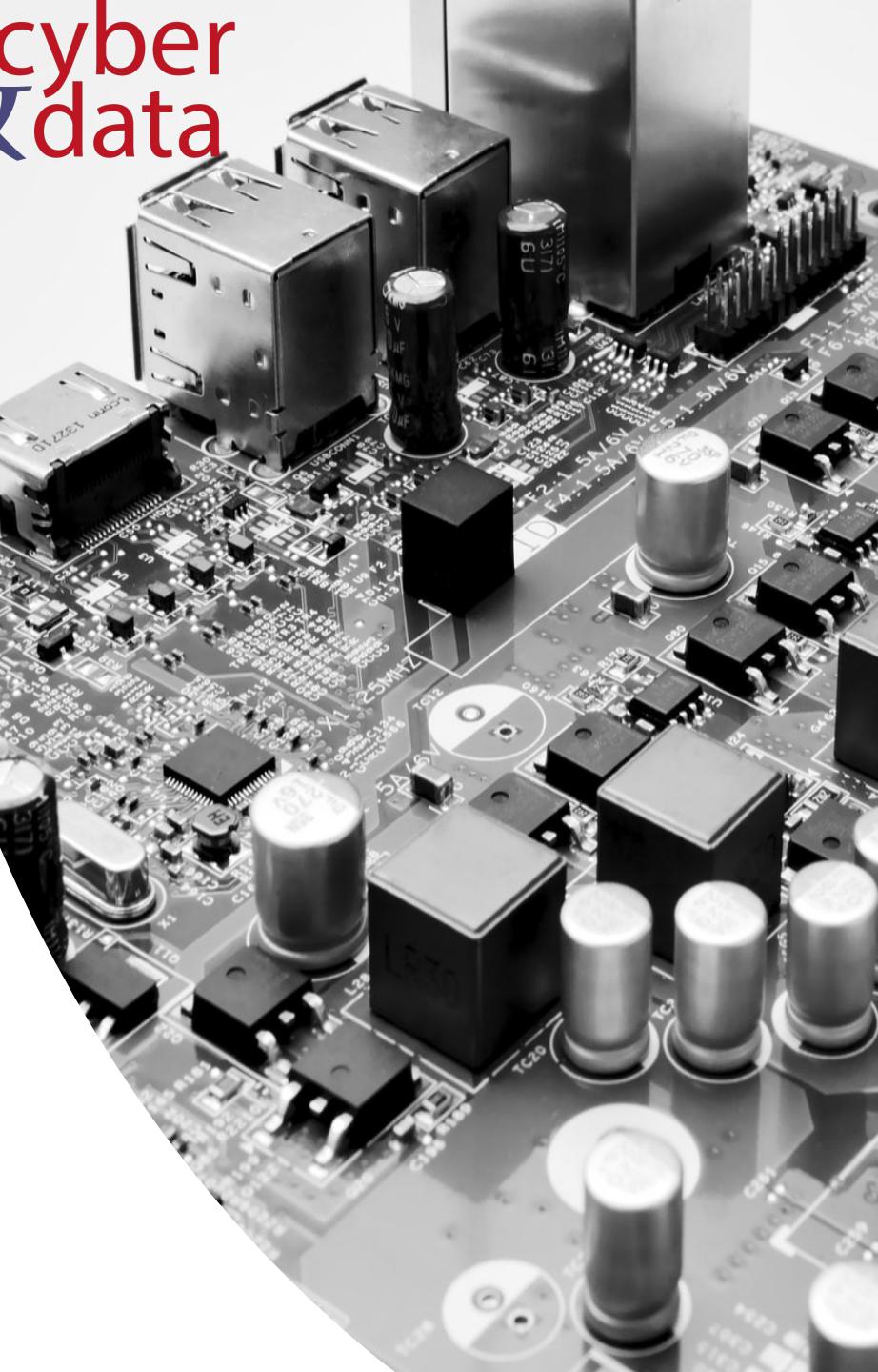
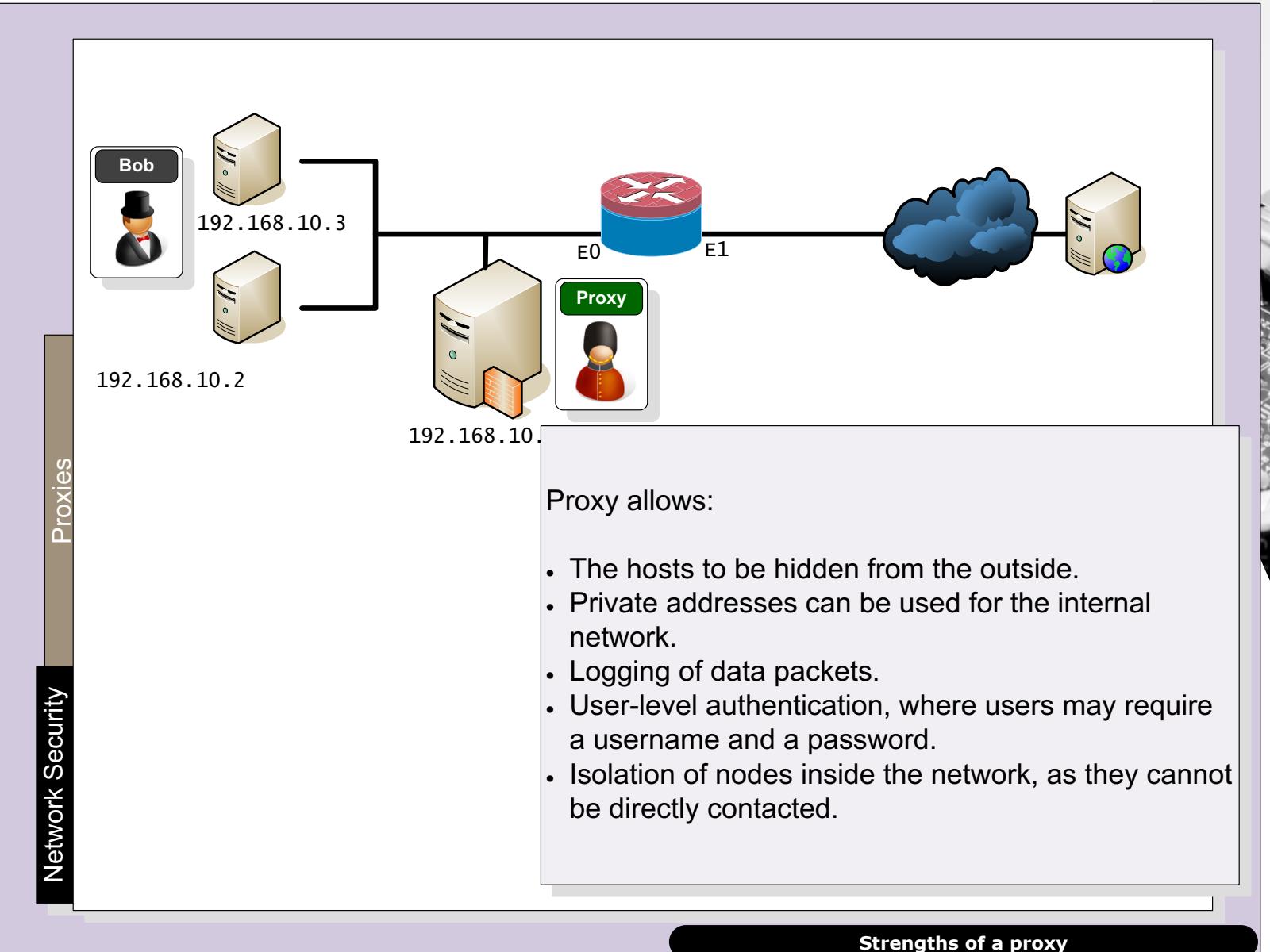
Layered Model

cyber
&
data



Layered Model

cyber
&
data



cyber & data

"From bits to information"

Defence Systems,
Policies and Risks