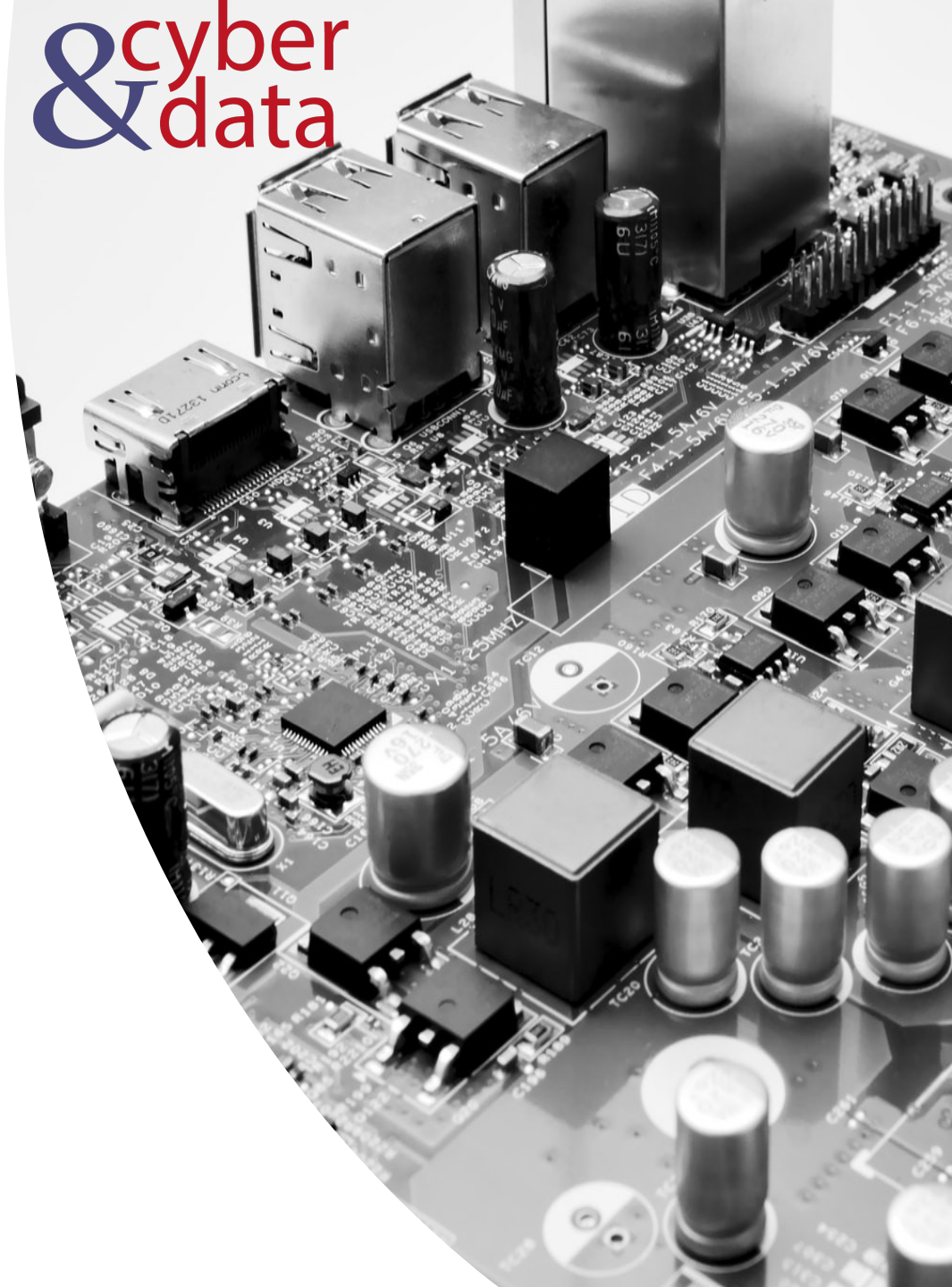
cyber & data

"From bits to information"

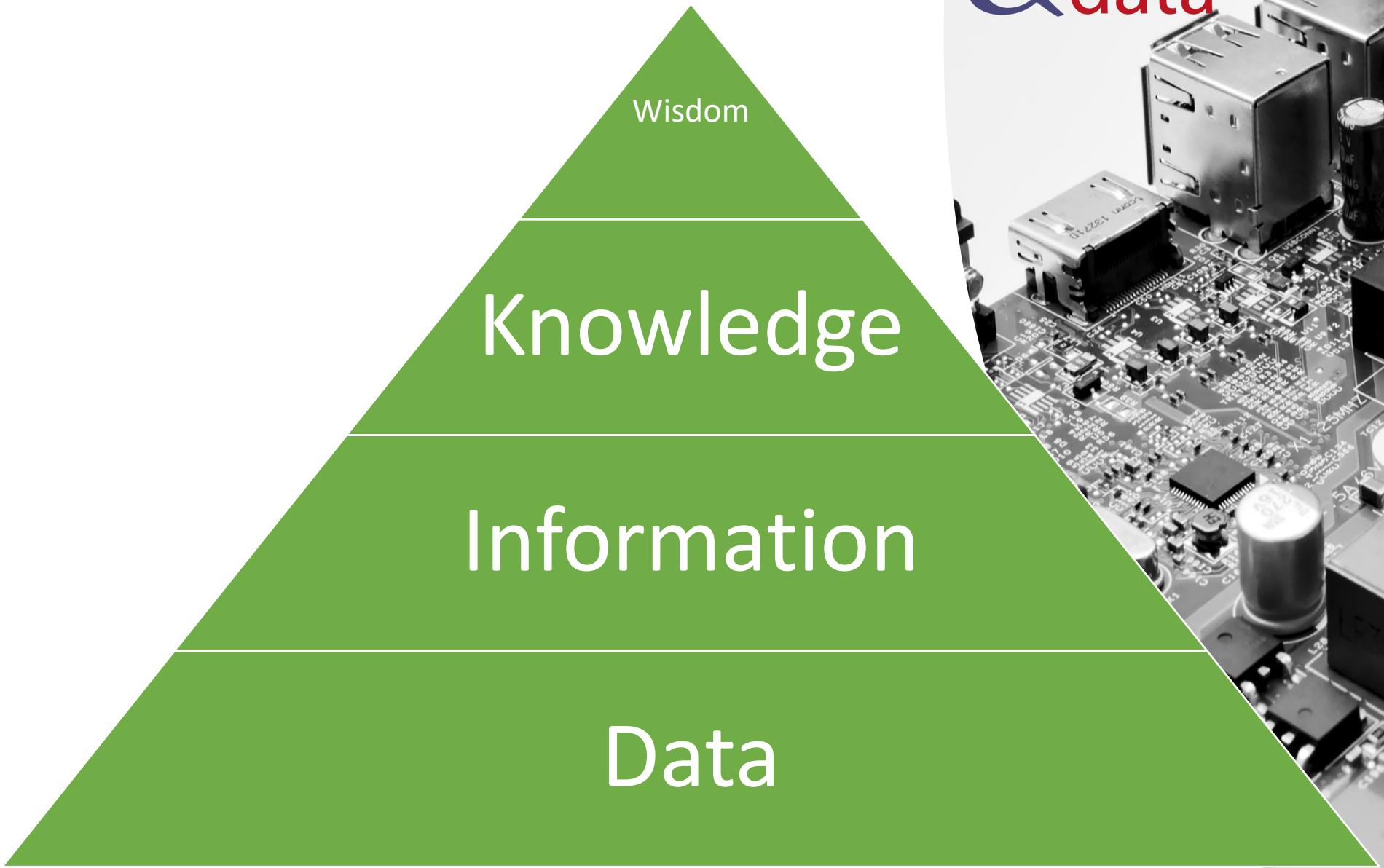
Defence Systems, Policies and Risks

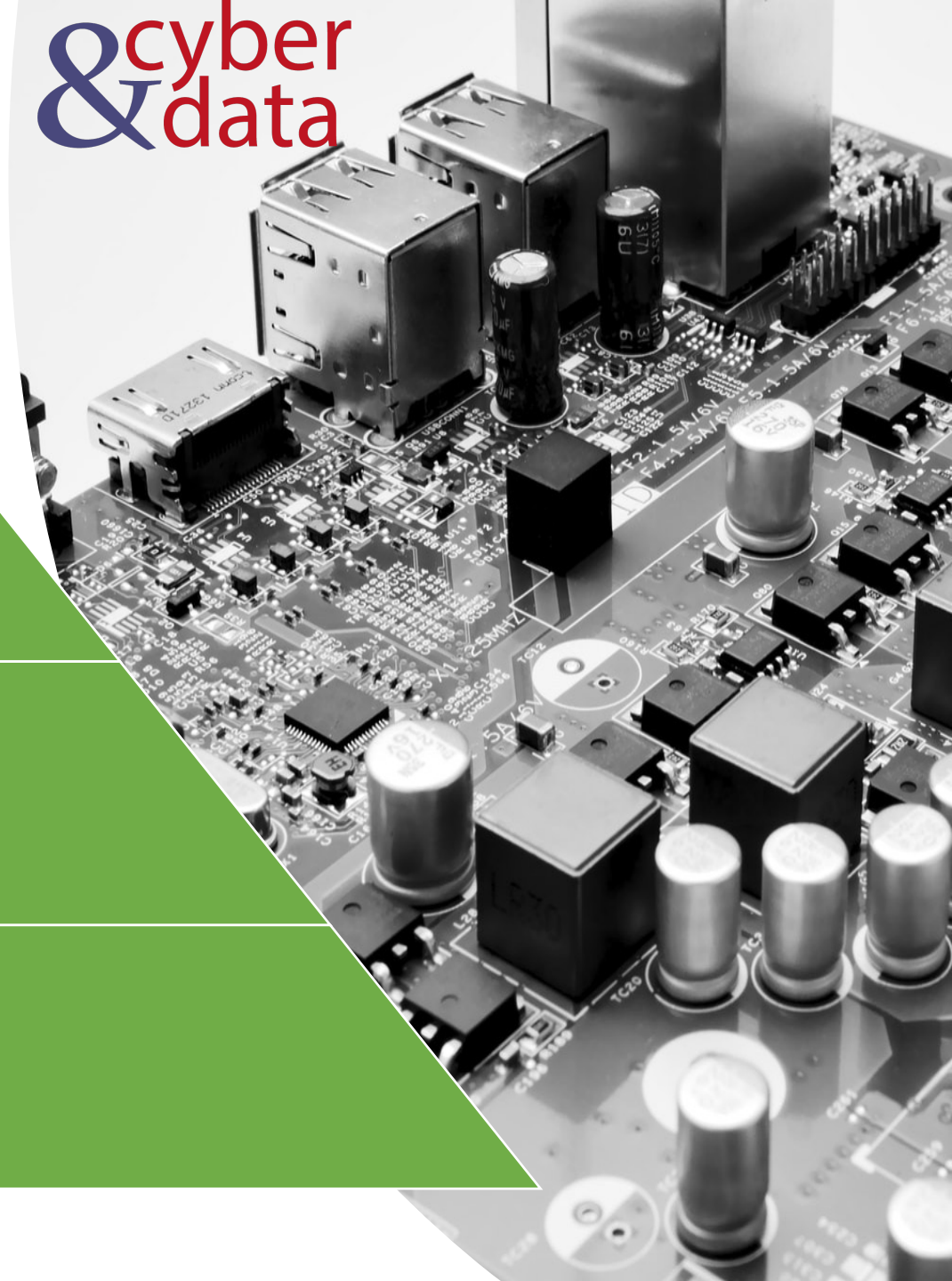
Outline

- 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



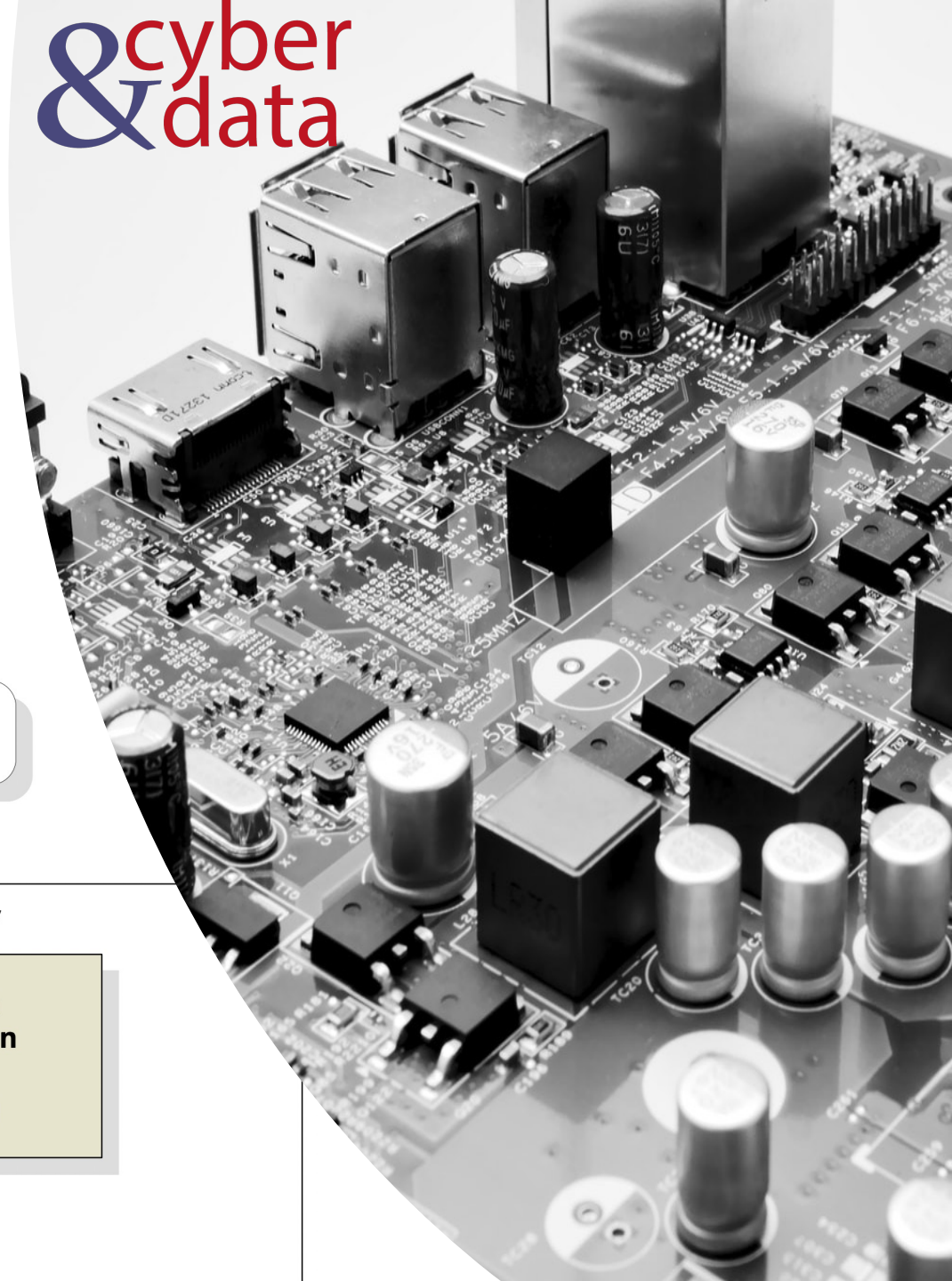


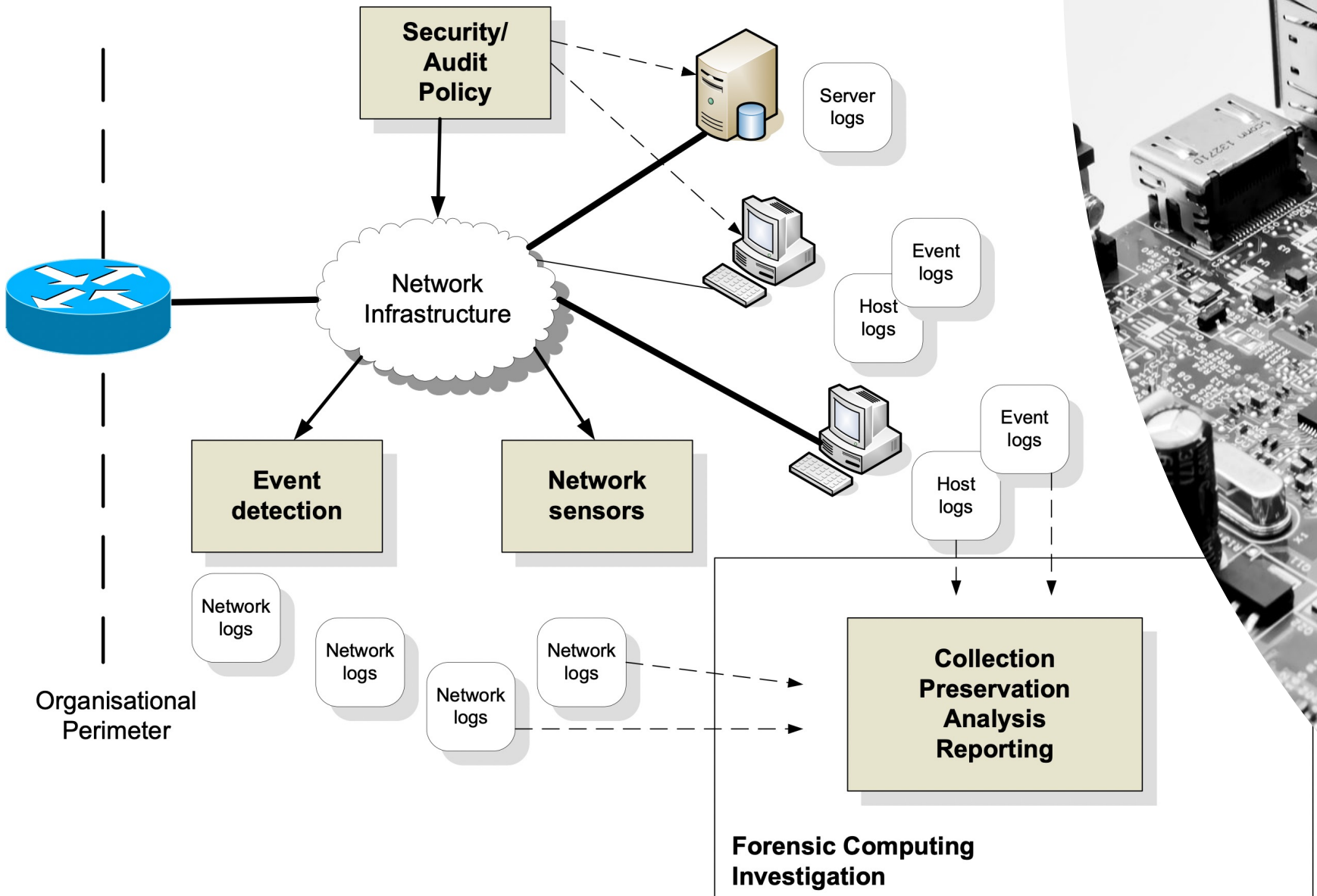
cyber & data

"From bits to information"

Security, Incident Response and Forensic Computing

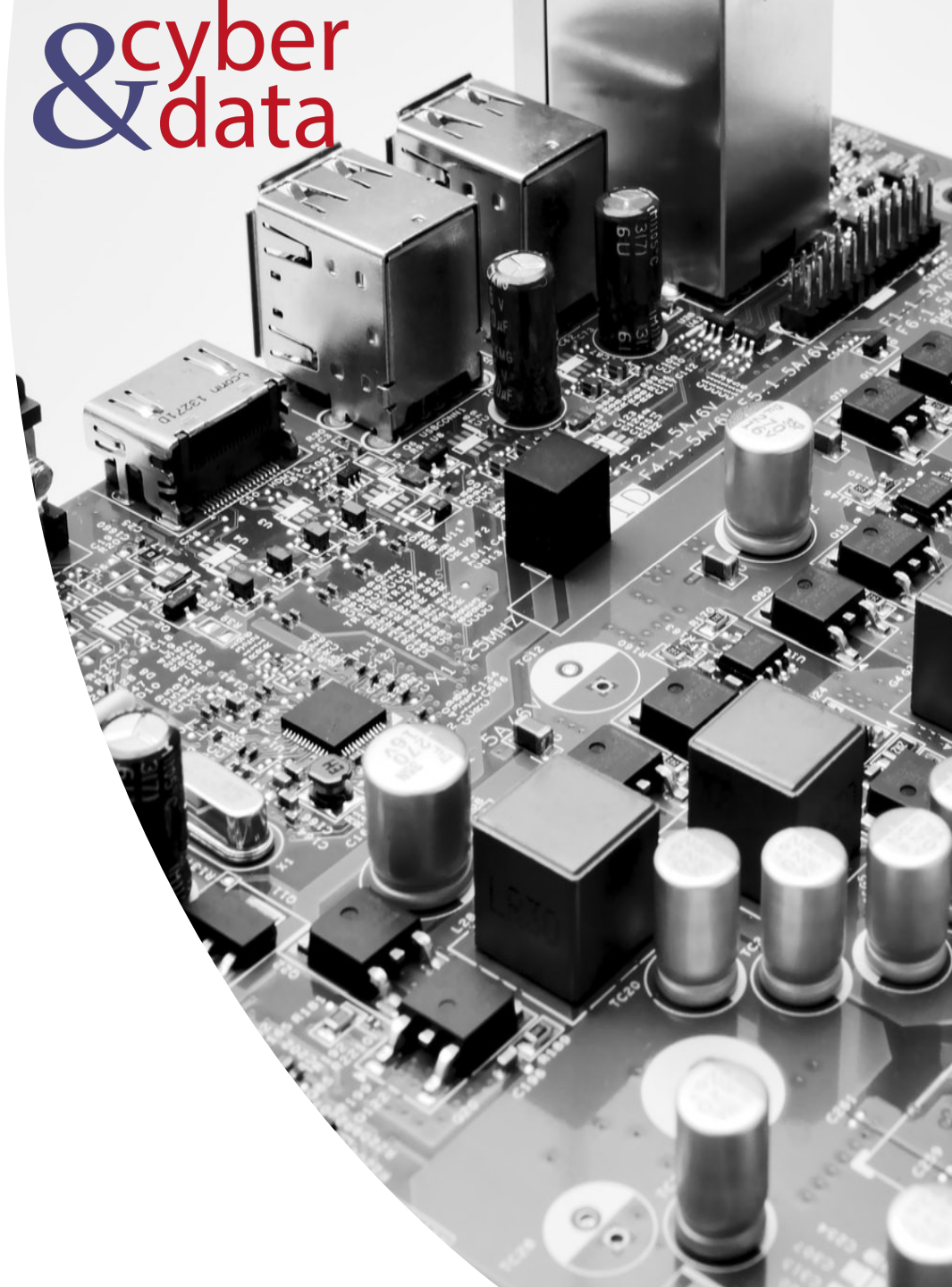
Information Security





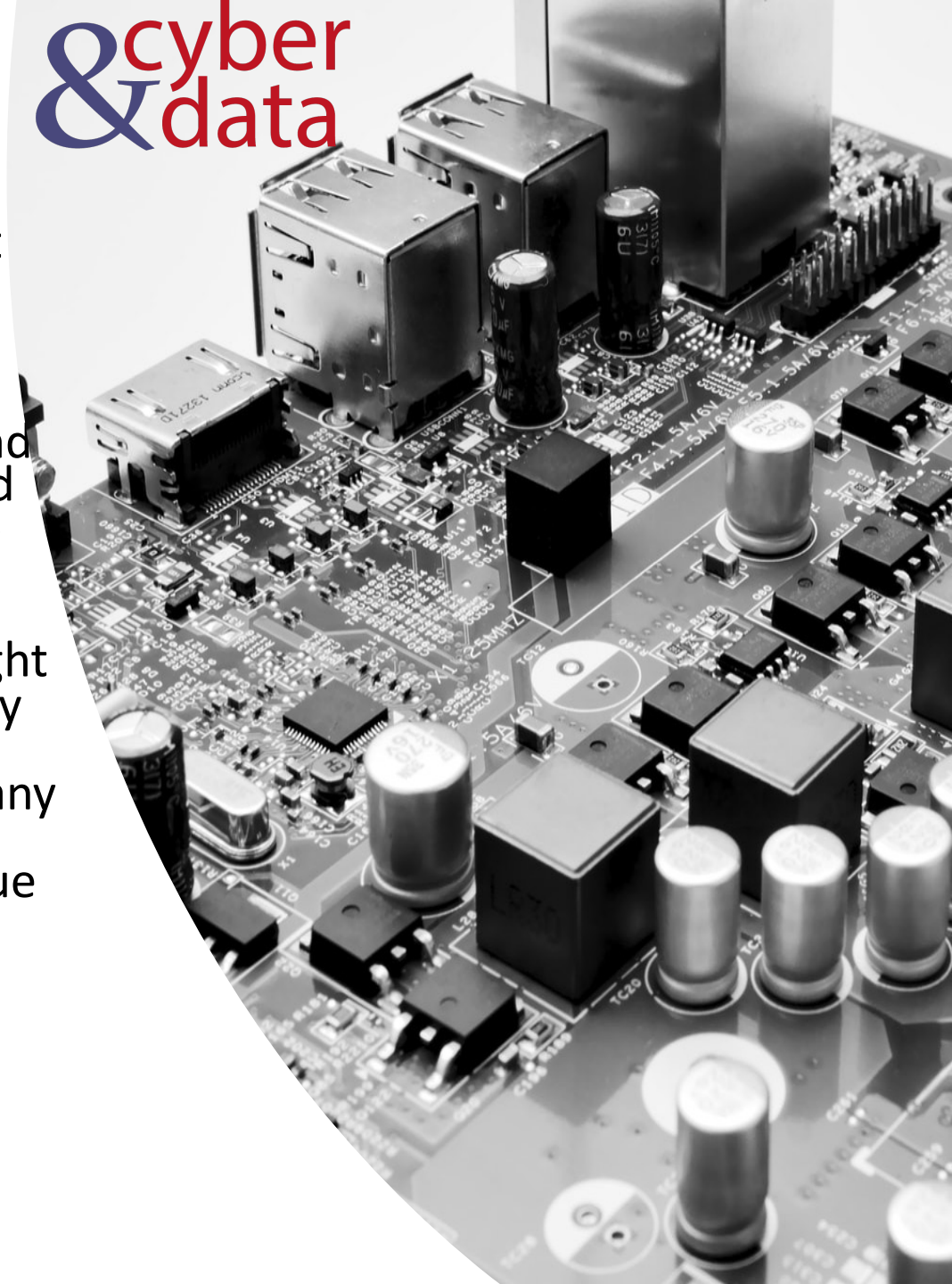
Investigation

- 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

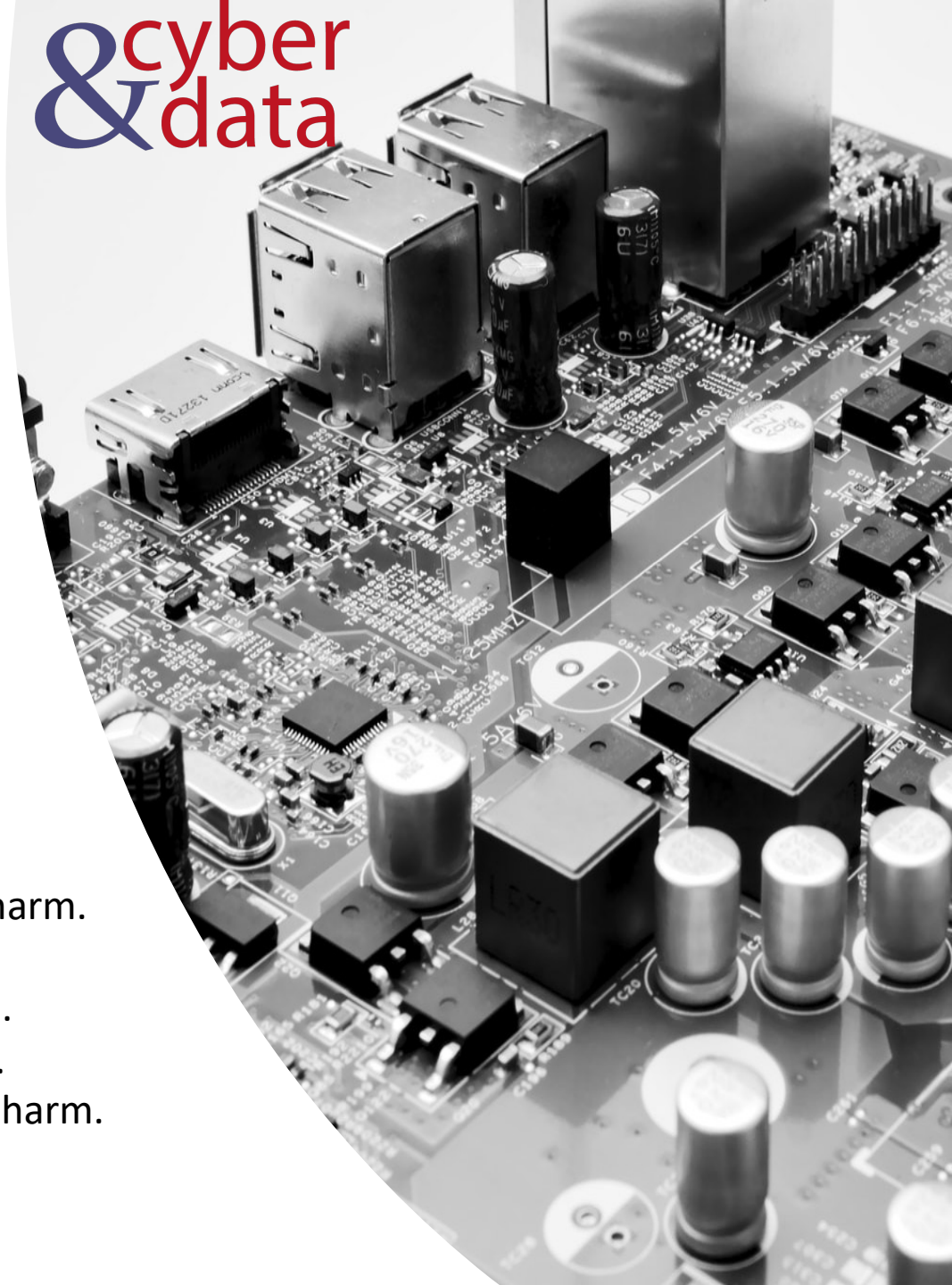
- With due care, the organisation must make sure that has taken the correct steps in the creation and implementation of its security policy and in its risk analysis.
- Then due diligence relates to the actual operation and maintenance of its security system, especially around vulnerability testing. Thus 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.



"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

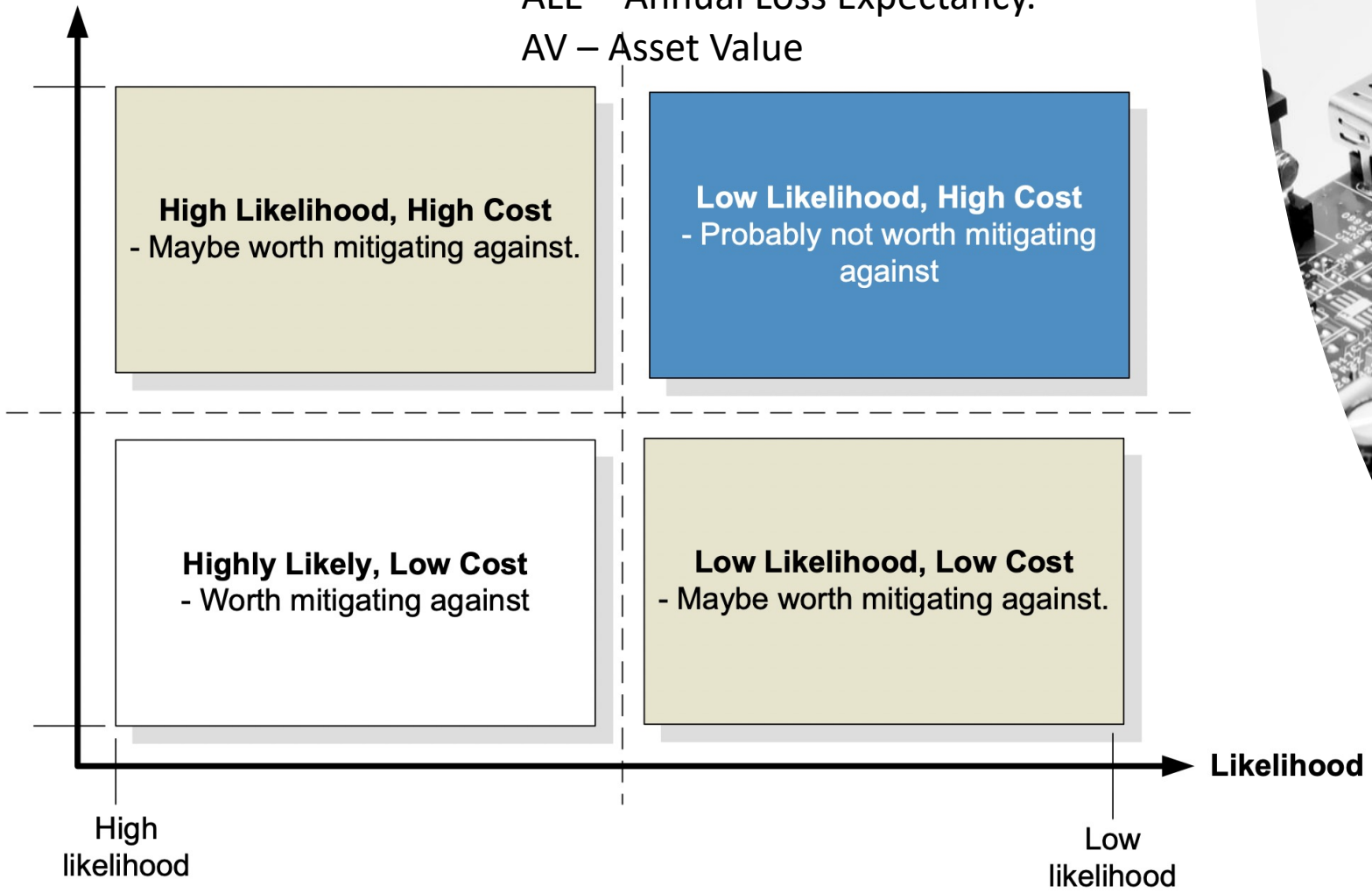
"From bits to information"

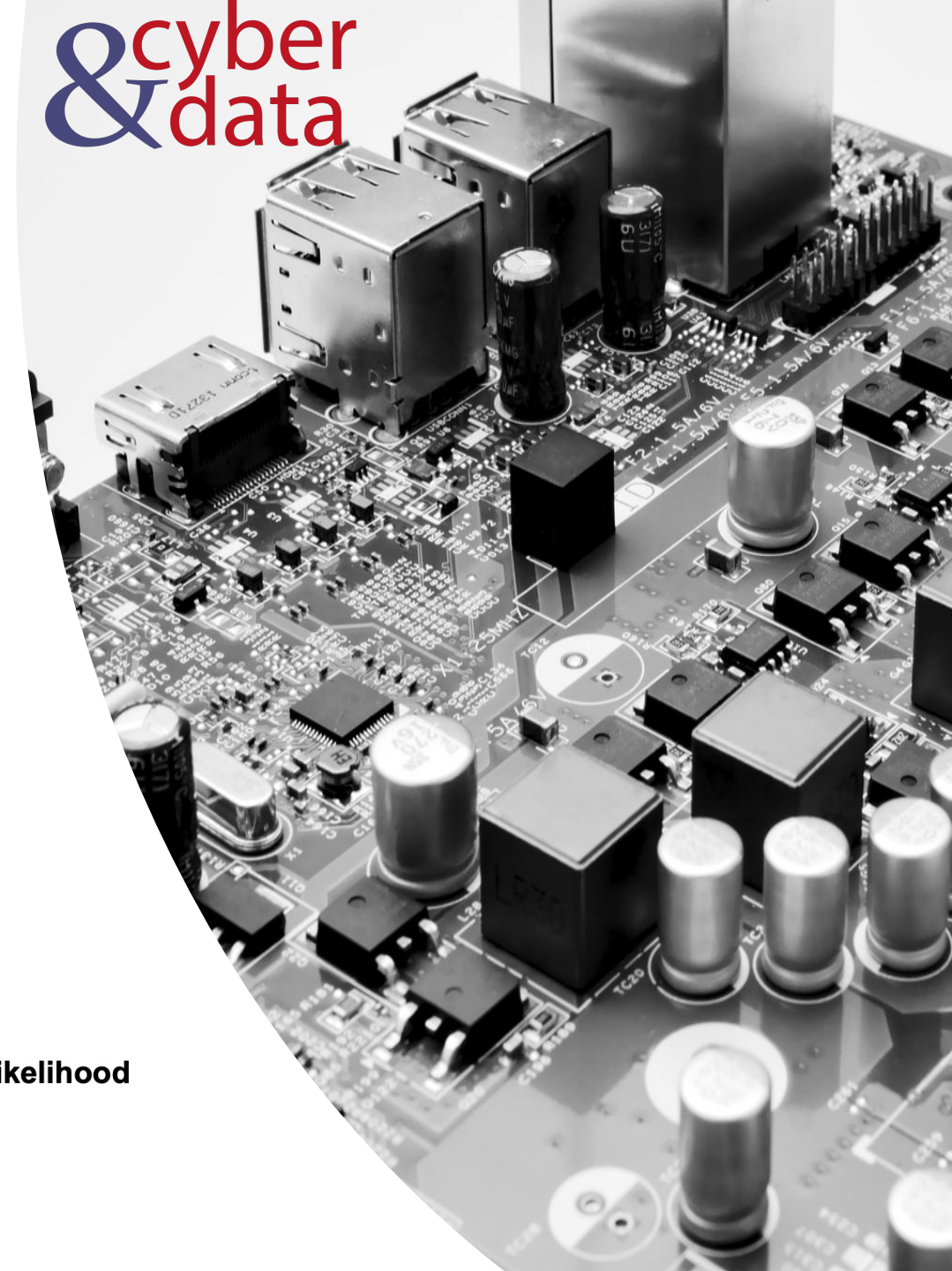
Risks, Costs and Benefits

Risks, Costs and Benefits

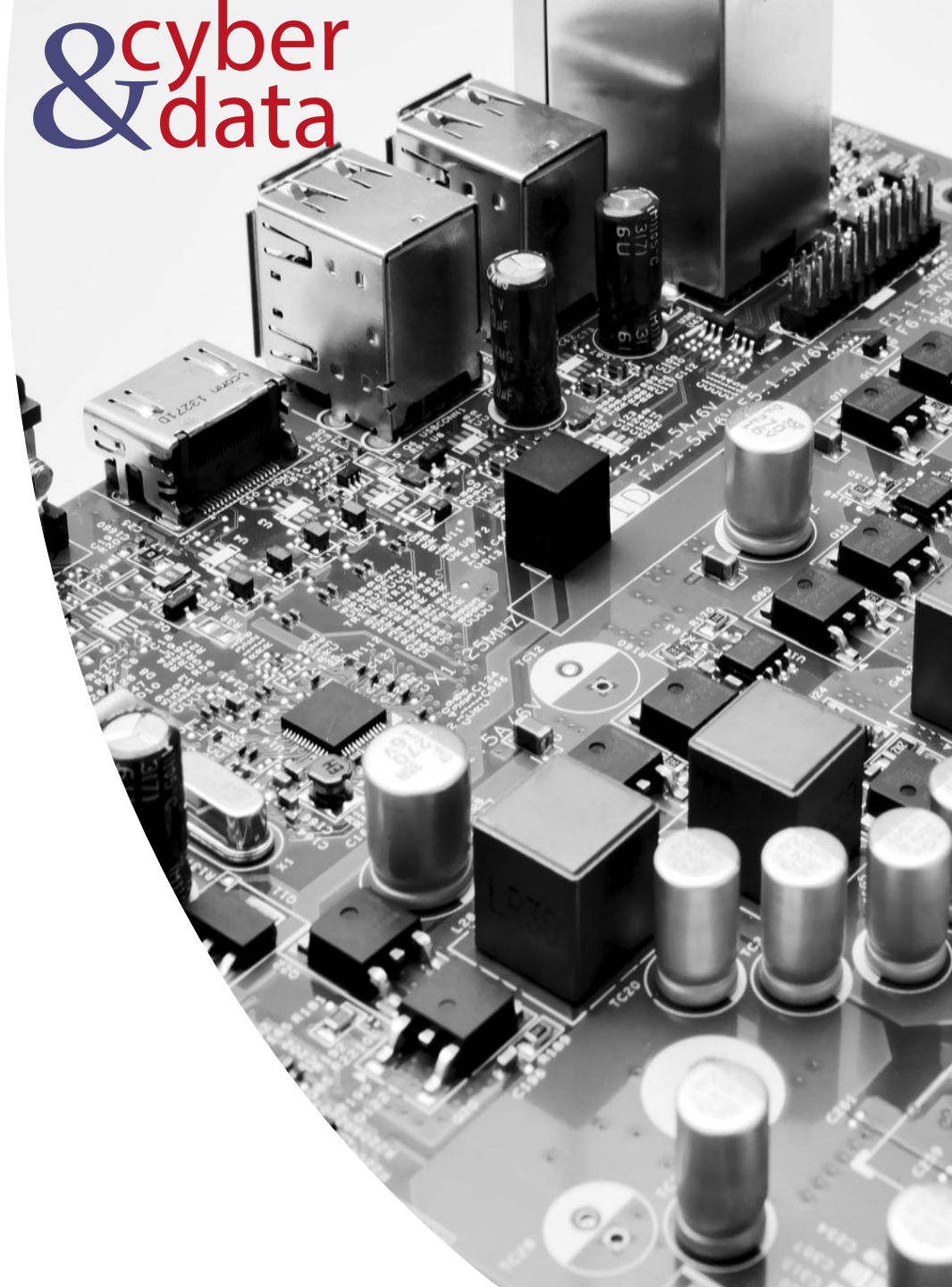
ALE = AV x ARO

ALE – Annual Loss Expectancy.
AV – Asset Value





Risks, Costs and Benefits



Error Operating (10-200)
Input (10-50,000) Programming (1-200)

Static discharge
General 300-3000)

Hardware
General (10-200)

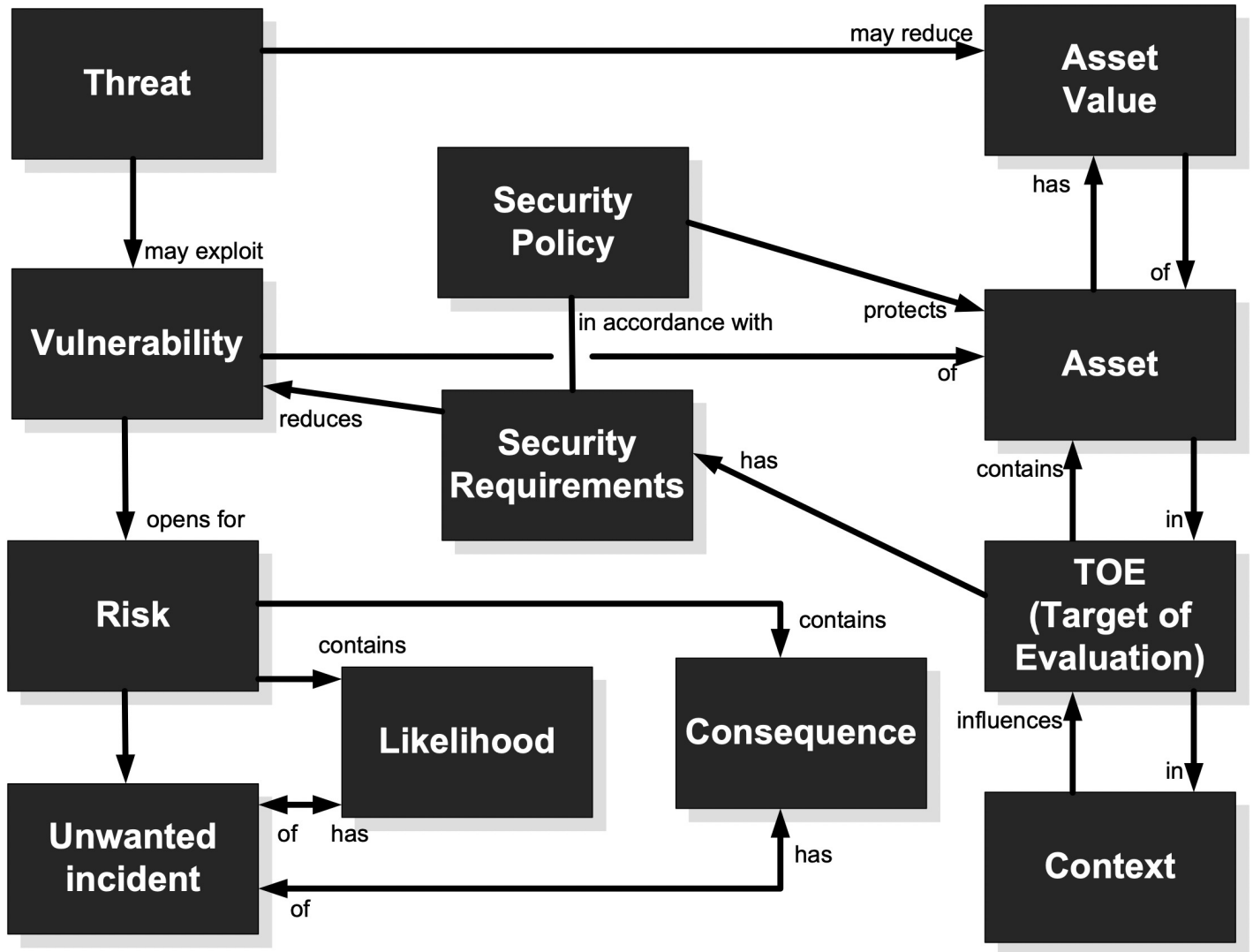
Improper release (0.2-5) Ex-employee access (0.1-1)
Compromise
Loose Documents (0-5) Improper marking (0.1-100)

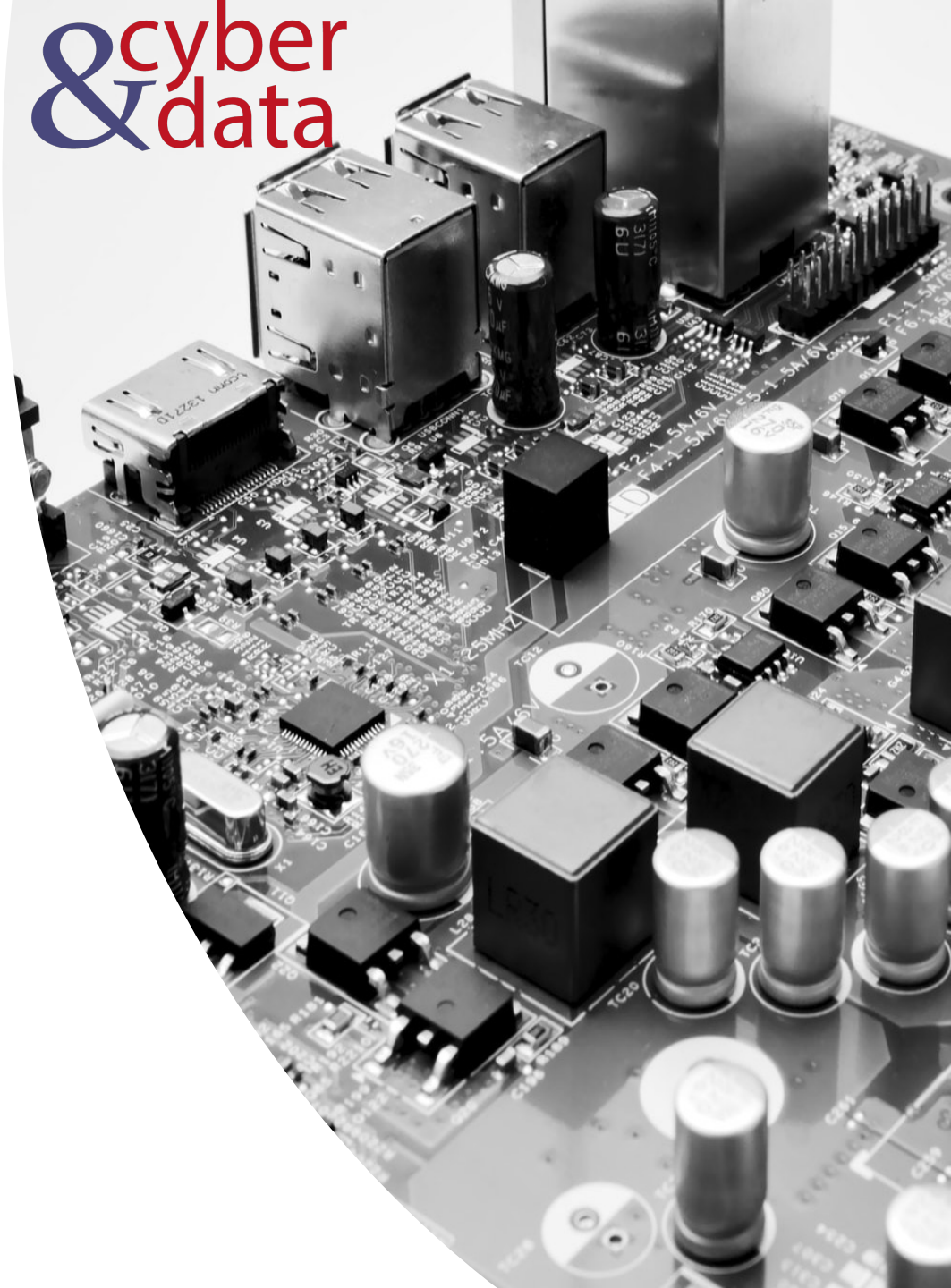
Password compromise
System entry (1-5) Uncleared visit (0.1-1000)

Major (0.01-0.09) Explosion (0.0001-0.01)
Fire
Minor (0.1-0.9) Catastrophic (0.001-0.009)

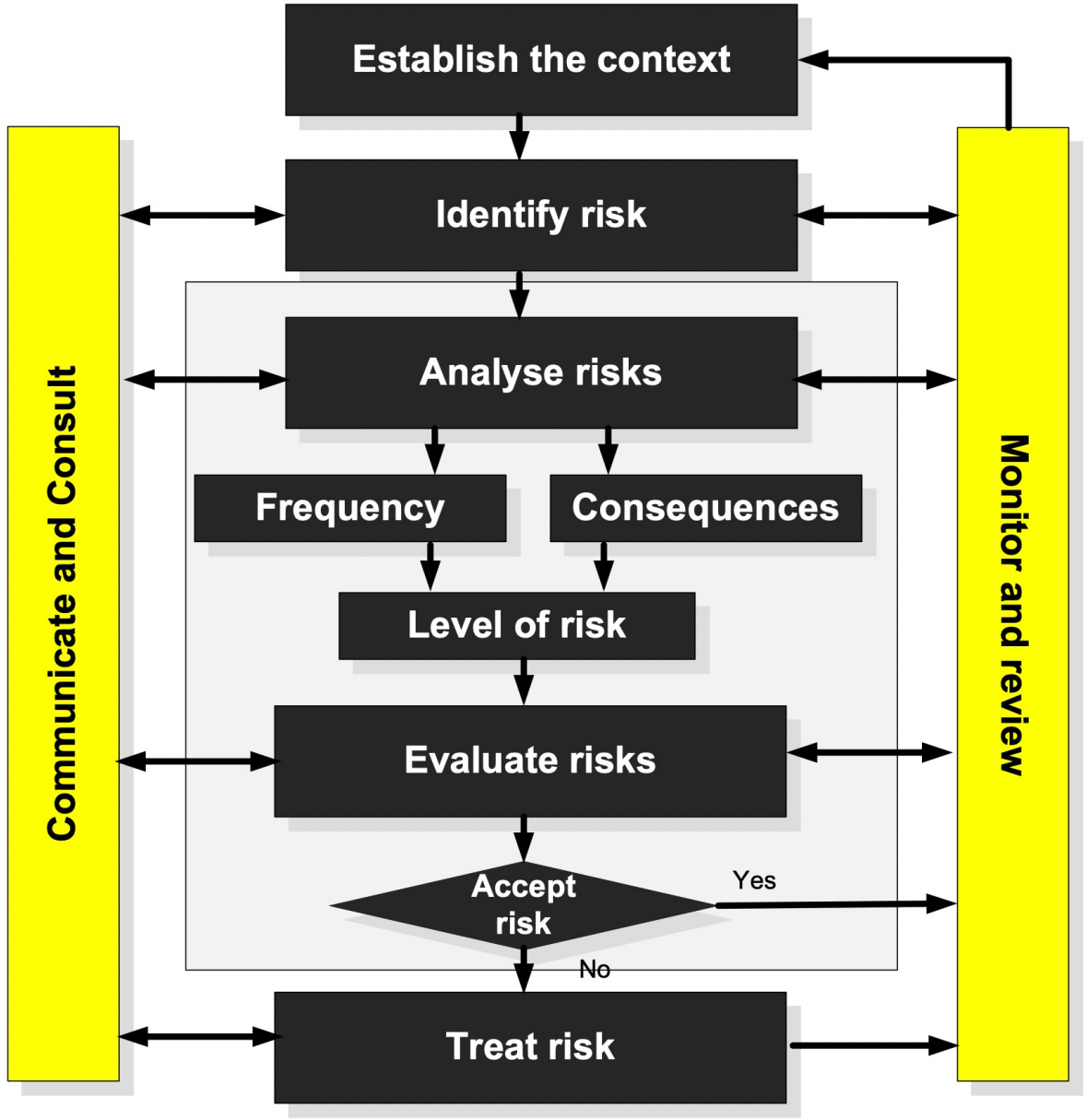
Disgruntled employee (0.1-5) Terrorism (0.002-0.006)
Forced entry
Burglary (?) Vandalism (0.008-1)

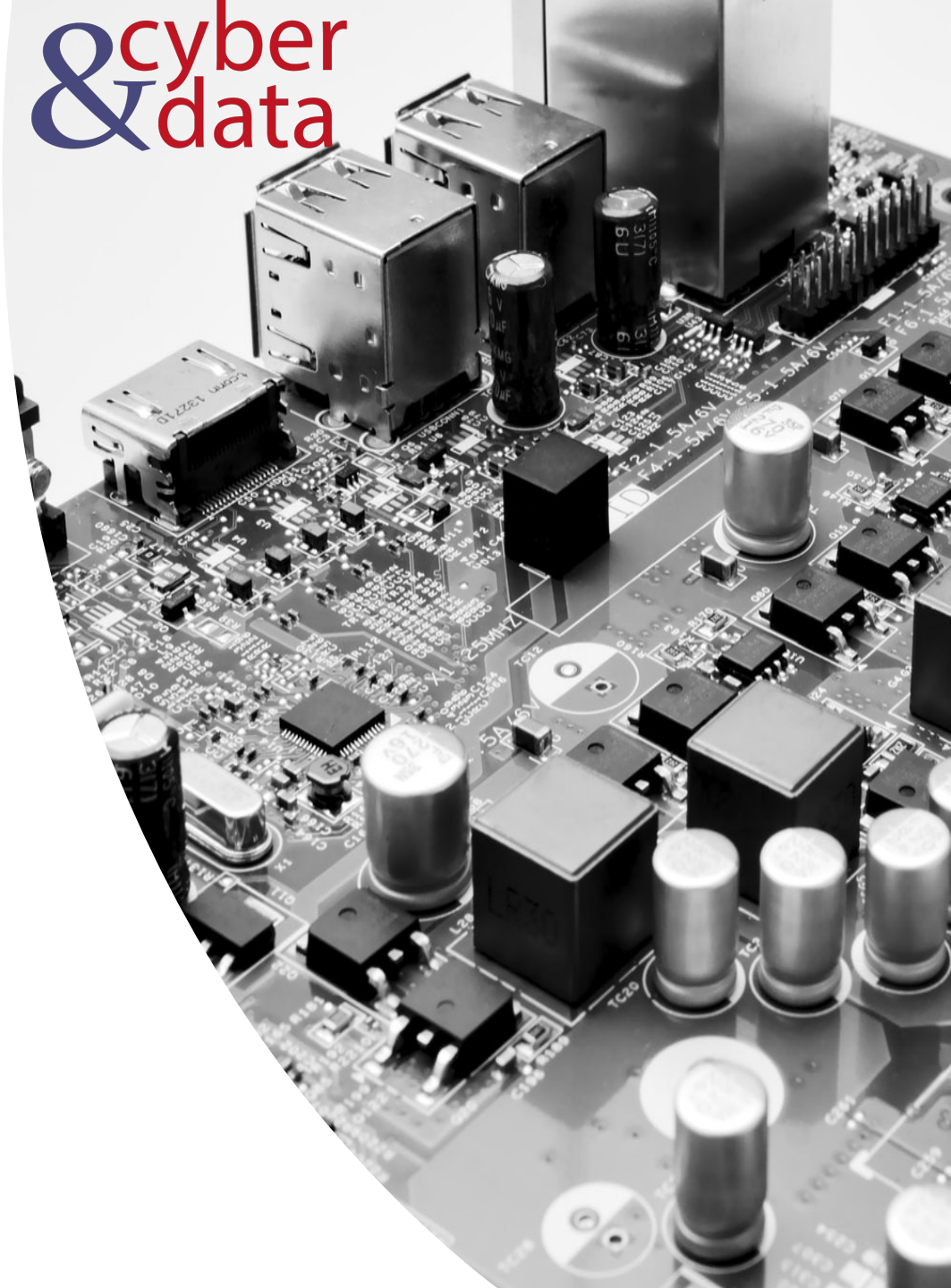
CORAS Ontology





CORAS Risk Management



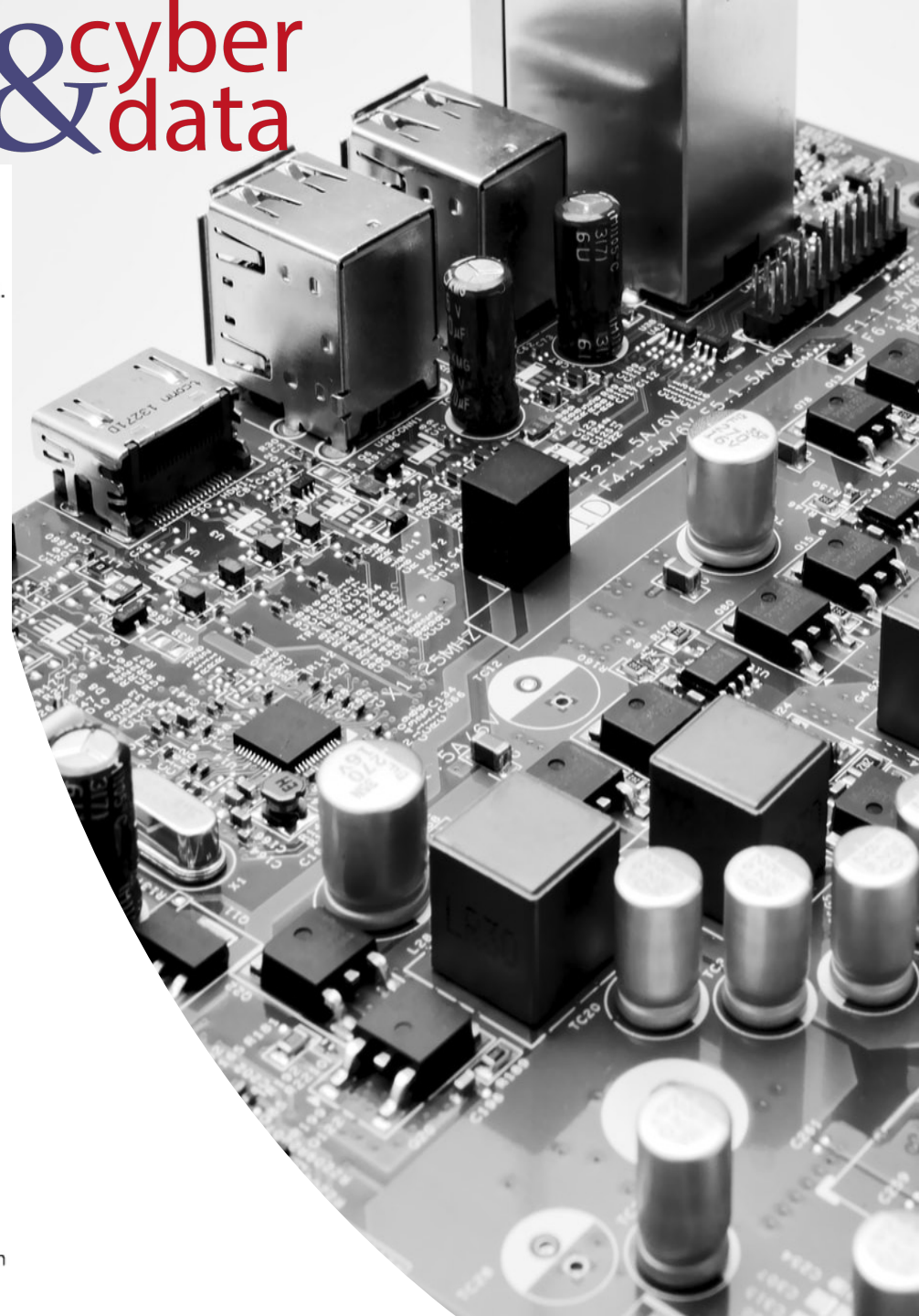


cyber & data

"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.

A **Threat** (eg Spies) **Is achieved with** **Attack Tools** (eg Toolkit) **for** **Vulnerabilities** (eg design vulnerability) **with** **Access** (eg Unauthorized Access for Processes) **which** **Results** (eg Theft of Service) **in, for** **Objectives** (eg Financial Gain)

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

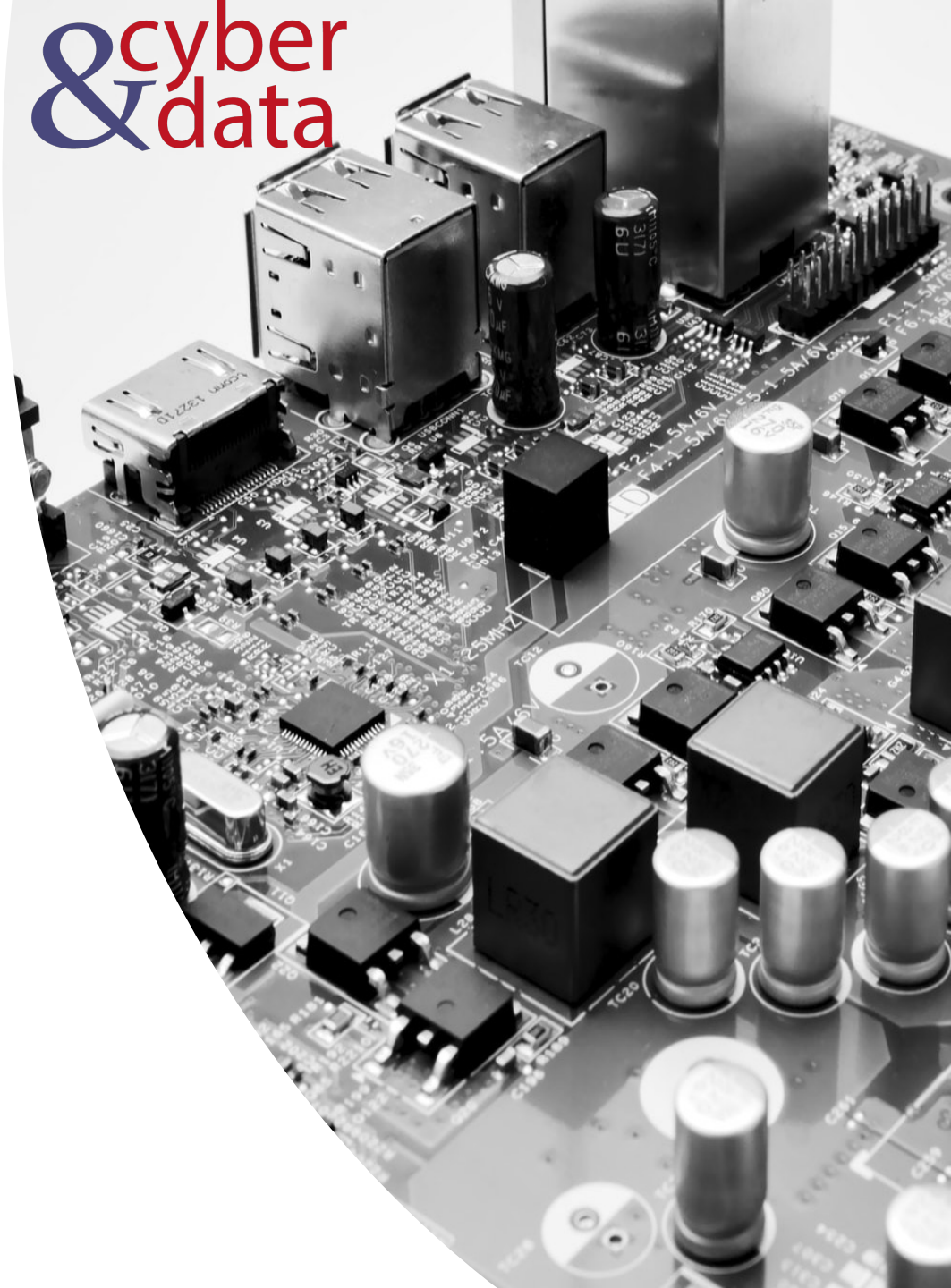
which Results in:
- Corruption of Information.
- Disclosure of Information.
- Theft of Service.
- Denial-of-Service.

with Access for:
- Files.
- Data in transit.
- Objects in Transit.
- Invocations in Transit.

Author: Prof Bill Buchanan

Kill Chain Model

Reconnaissance	Identification, Selection and Profiling of Target
Weaponize	Coupling of Remote Access Trojan with an Exploit into a deliverable payload called as Cyber Weapon
Delivery	Transmission of the cyber weapon to the targeted environment
Exploitation	Triggering the attacker's payload on target system
Installation	Installation of backdoor and maintaining persistence
Command and Control	Outbound internet controller servers to communicate with compromised host
Act on Objective	Data Exfiltration, Network Spreading, System Disruption



Unified Kill Chain Phases

Initial Foothold: Compromised System

- Reconnaissance
- Weaponization
- Delivery
- Social Engineering
- Exploitation
- Persistence
- Defense Evasion
- Command & Control

Pivoting

Network Propagation: Internal Network

- Discovery
- Privilege Escalation
- Execution
- Credential Access
- Lateral Movement

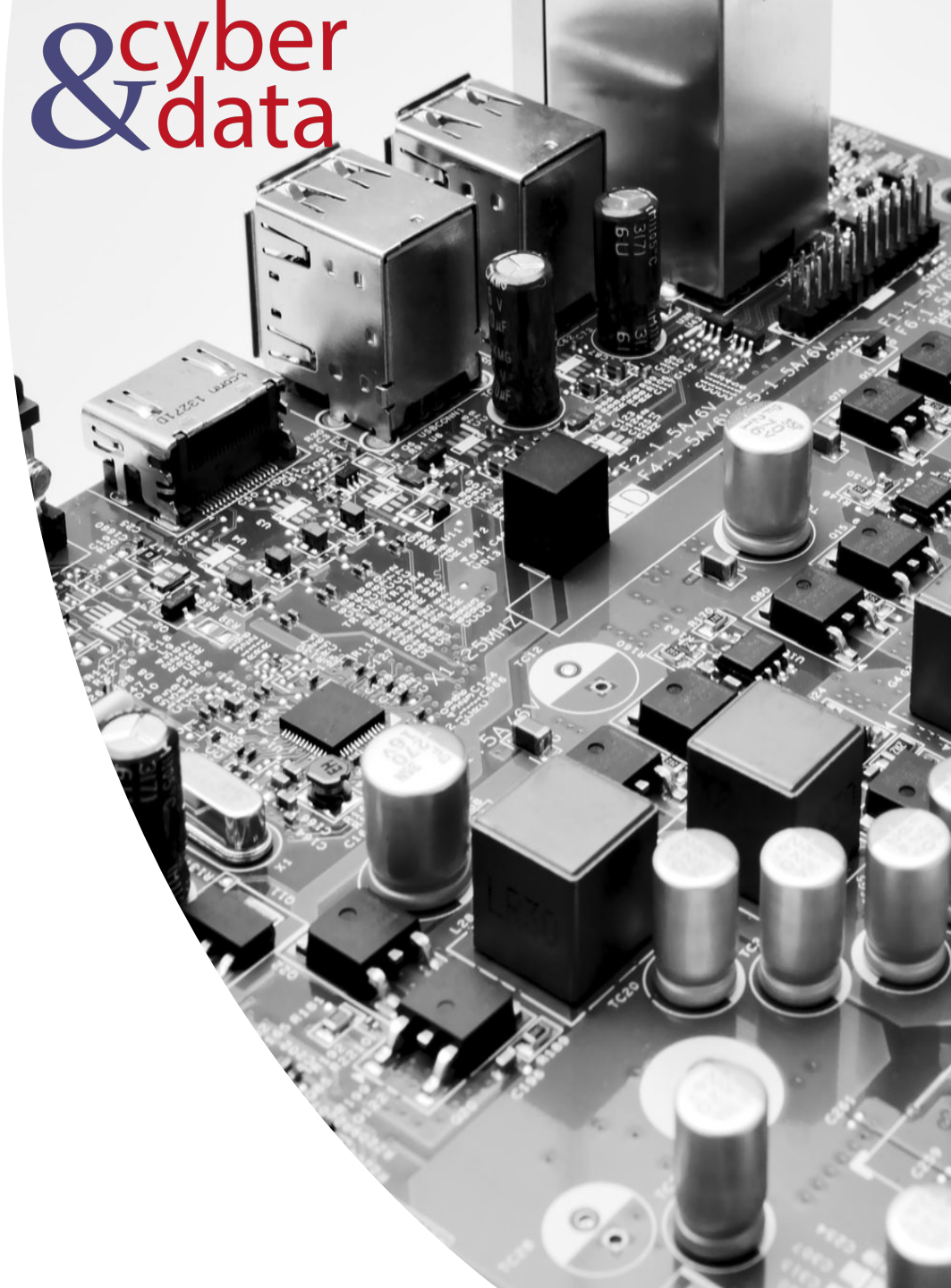
Access

Action on Objectives: Critical Asset Access

- Collection
- Exfiltration
- Target Manipulation
- Objectives

Unified Kill Chain Model

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



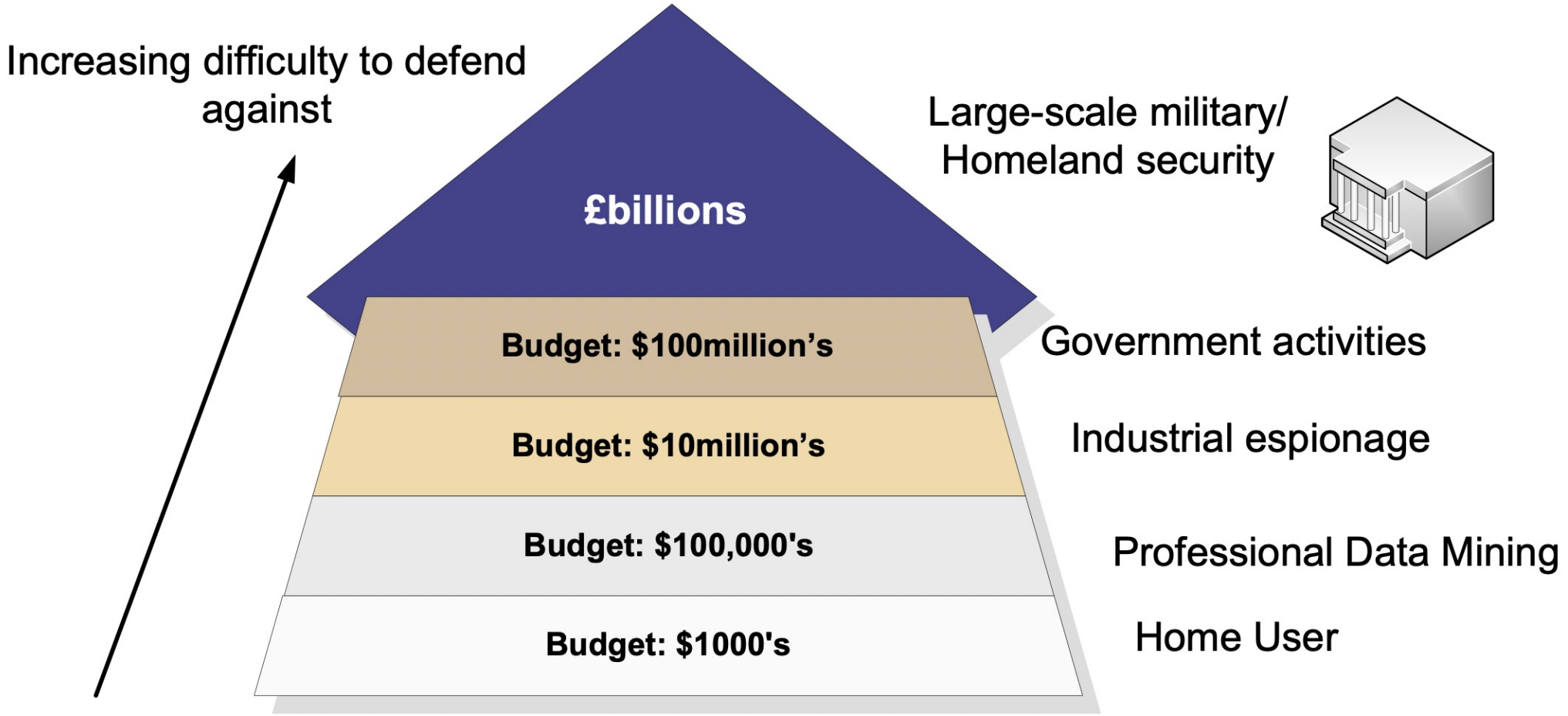
cyber & data

"From bits to information"

Defence Mechanisms

Types of intelligence

Aims/objectives



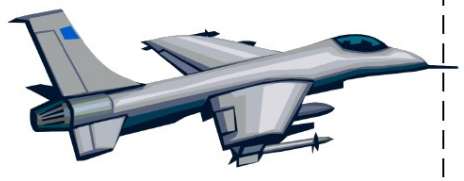
often causes the most problems

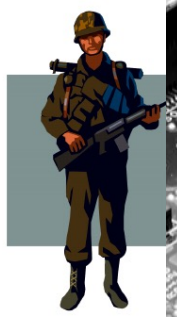
"From bits to information"

Defence in Depth

Defence in depth

&cyber data



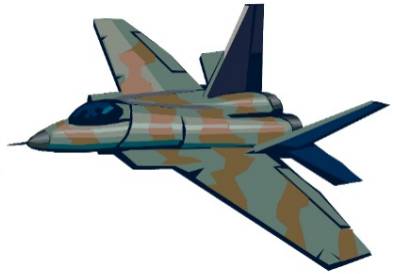


Defence

Defence

Defence

Defence



Forth-level defence

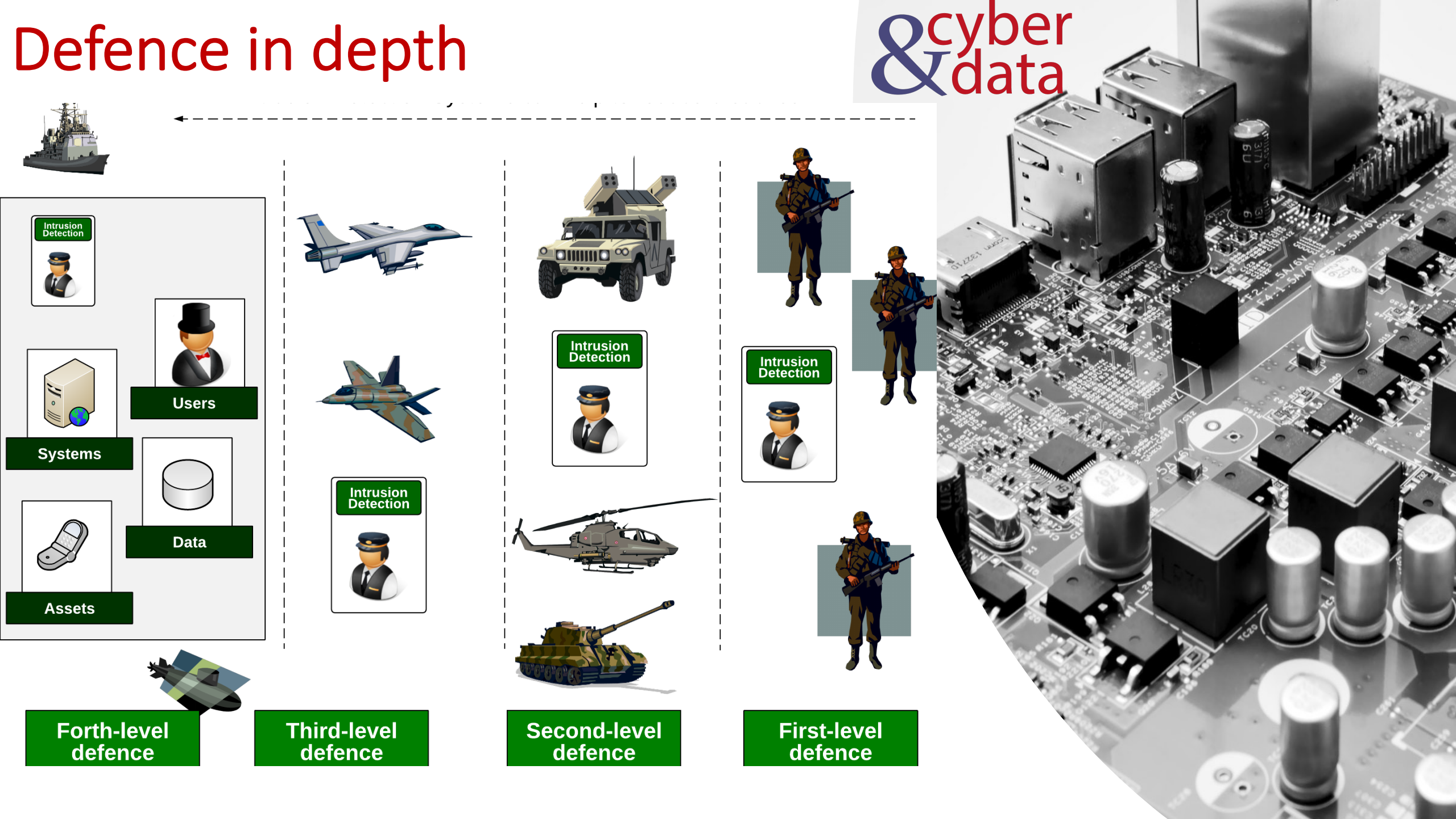
Third-level defence

Second-level defence

First-level defence

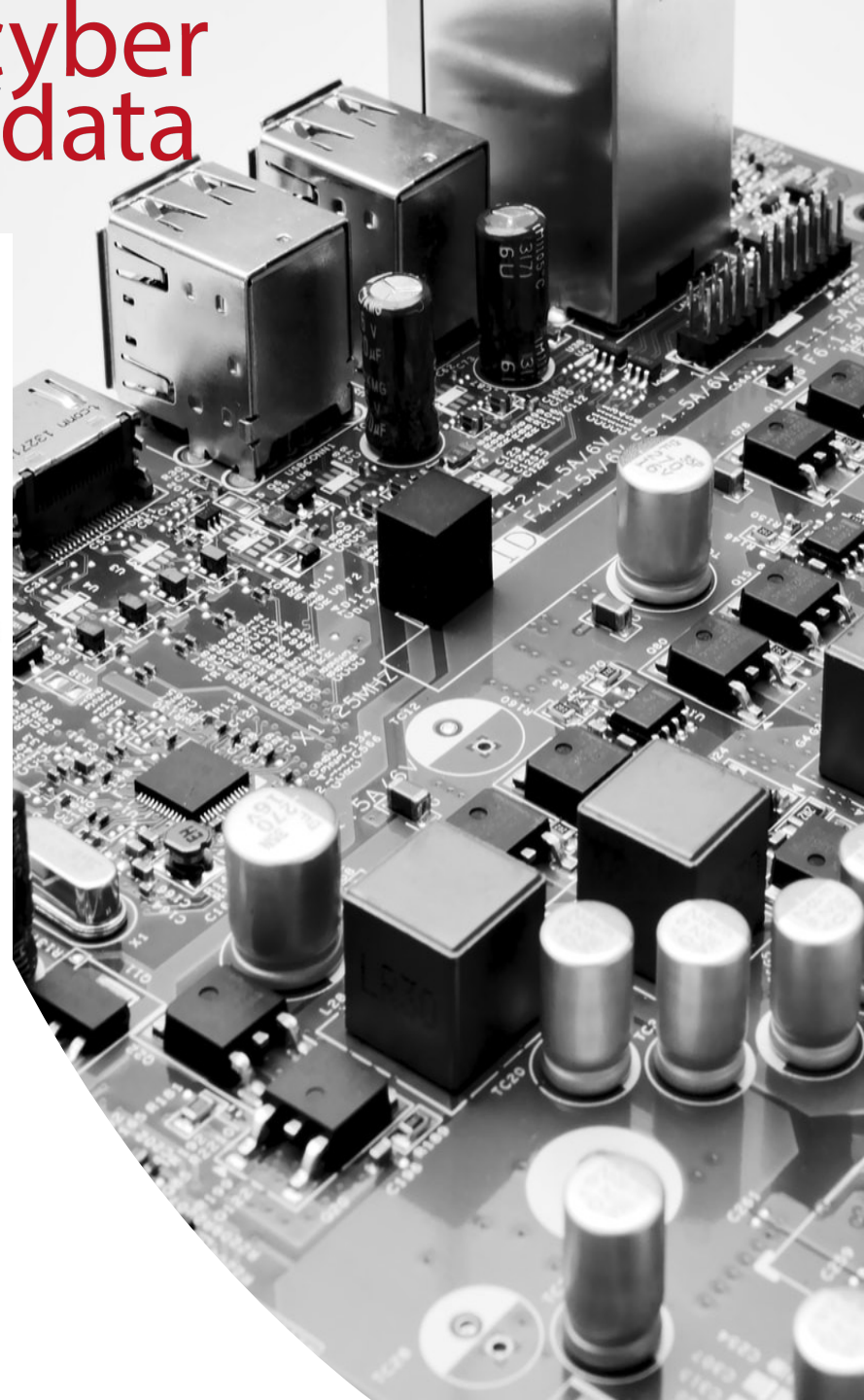
Defence in depth

&cyber data



Threats

&cyber data



Corporate access

Email access

Web access

Intrusion Detection

Users

Systems

Data

Assets

Network/Organisational perimeter

Firewall/ gateway

Data stealing

External hack

DoS (Denial-of-sevice)

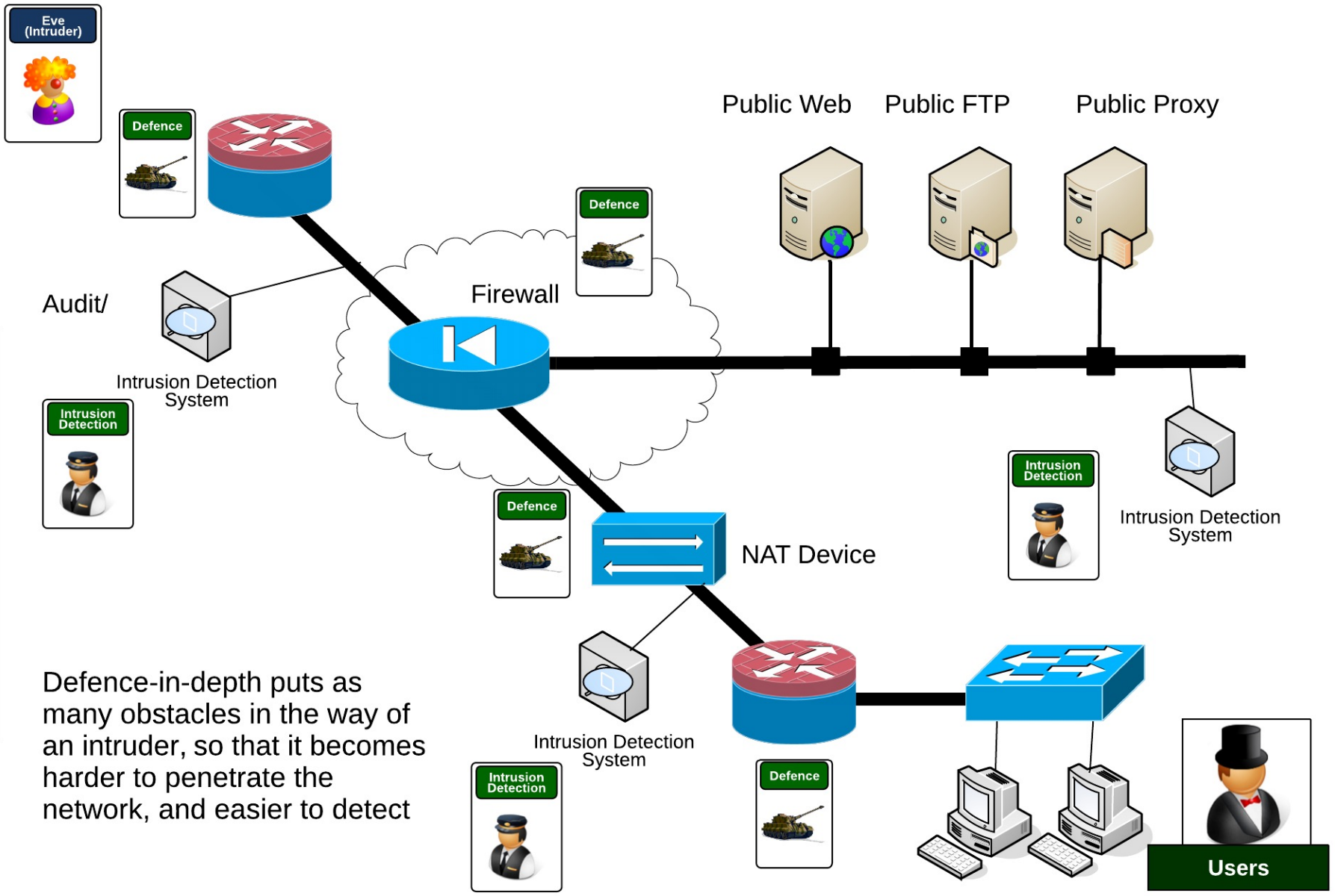
Personal abuse

Worms/viruses

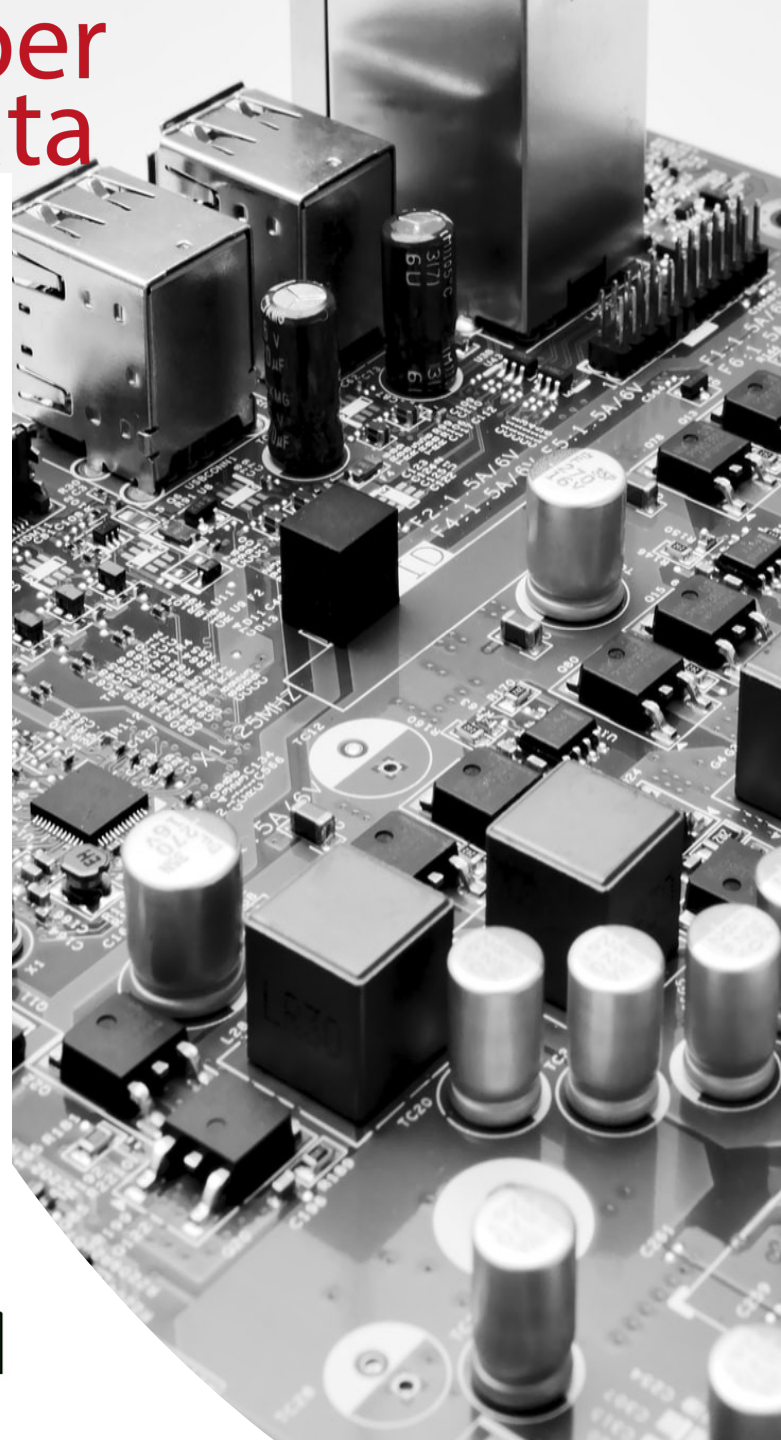
Terrorism/extortion

Fraud

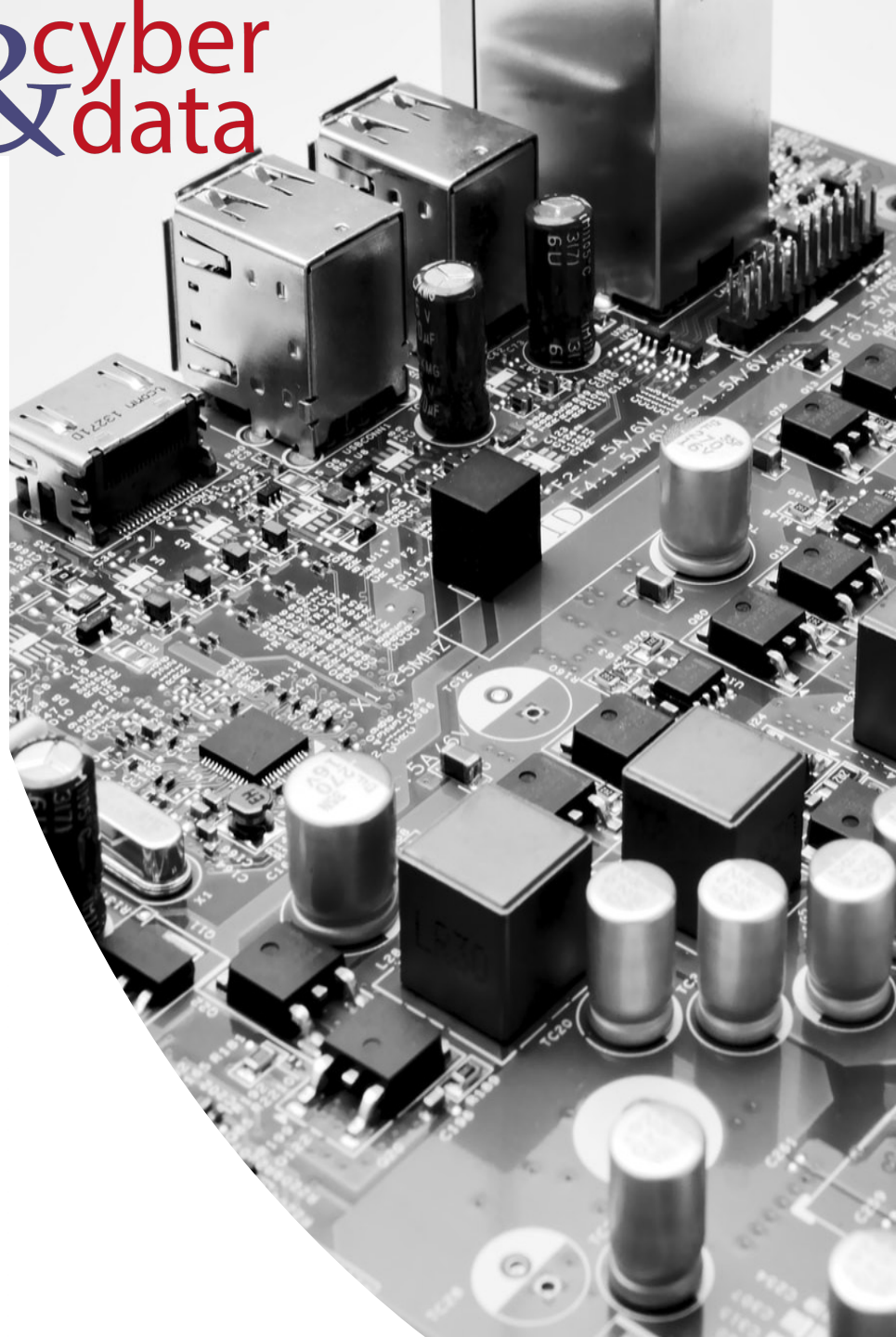
Defence in depth

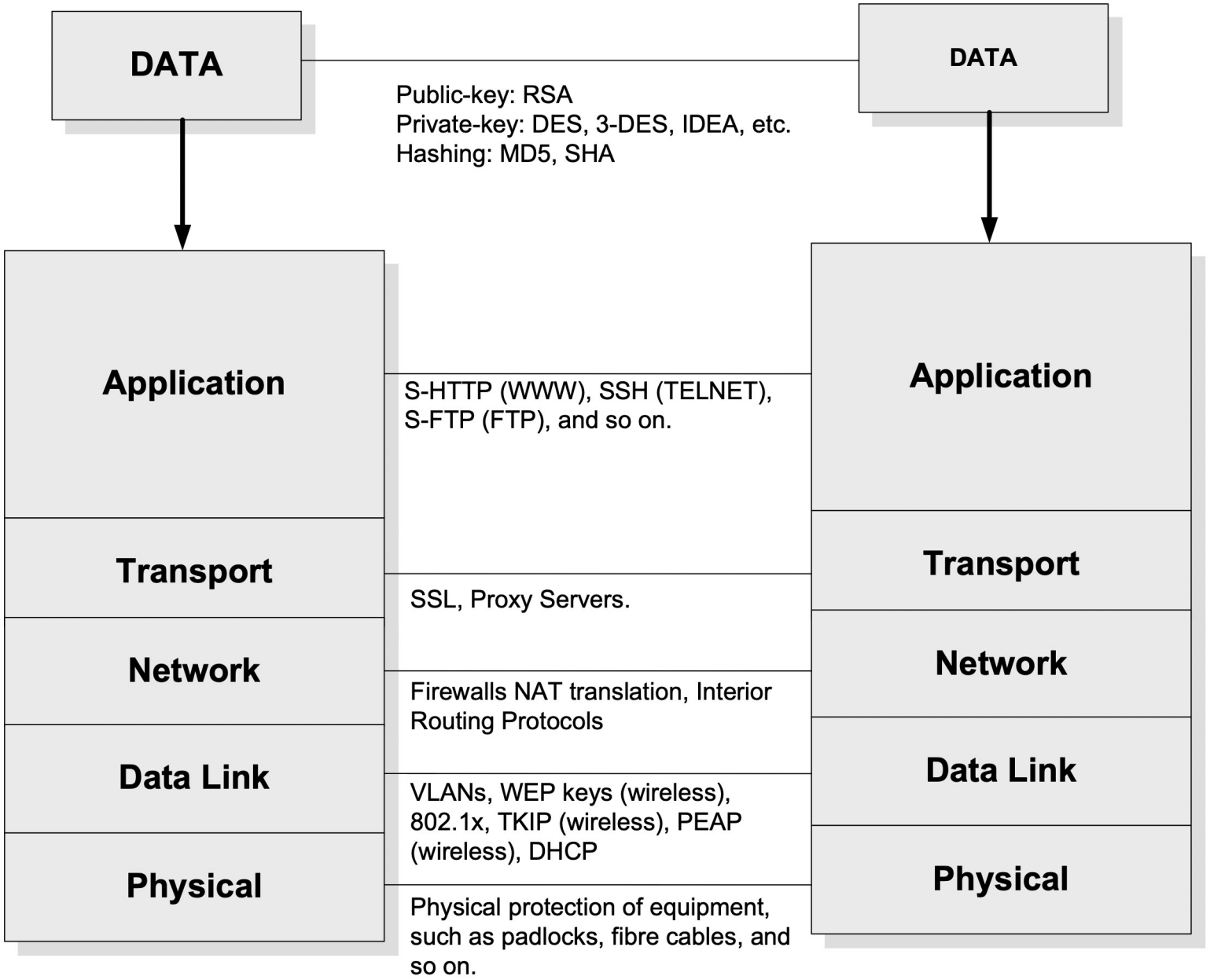


Defence-in-depth puts as many obstacles in the way of an intruder, so that it becomes harder to penetrate the network, and easier to detect



Layered Model

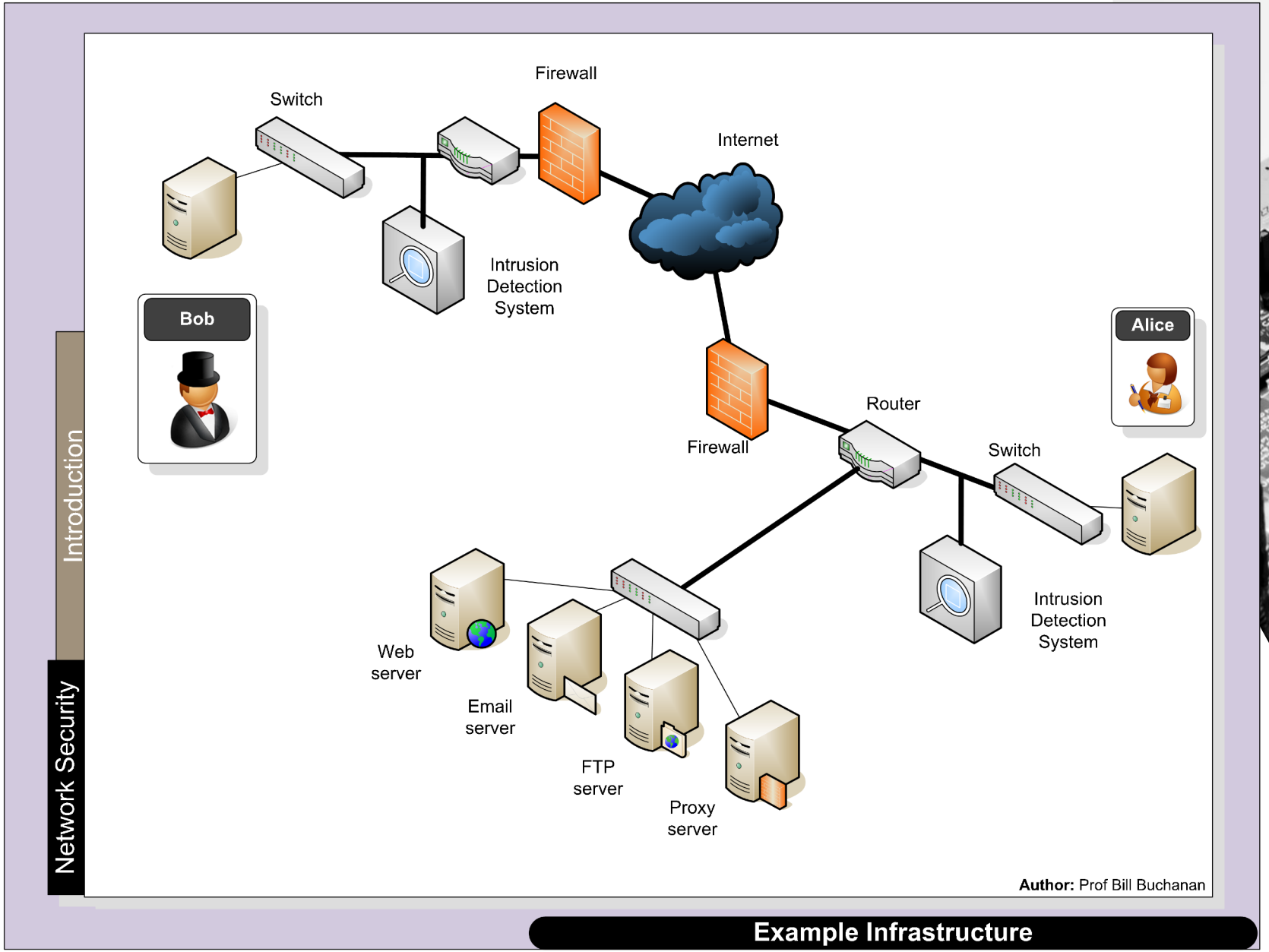


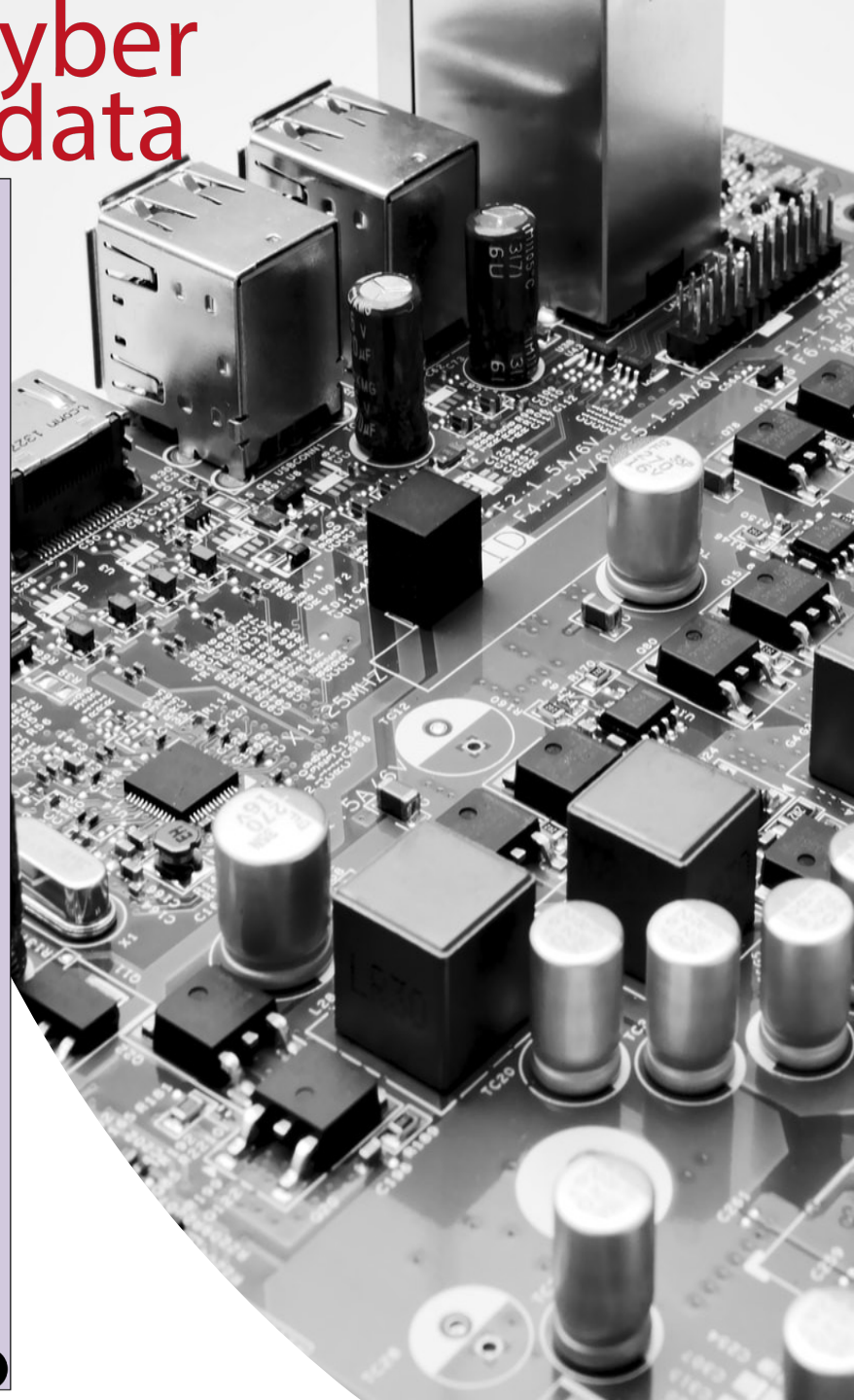


"From bits to information"

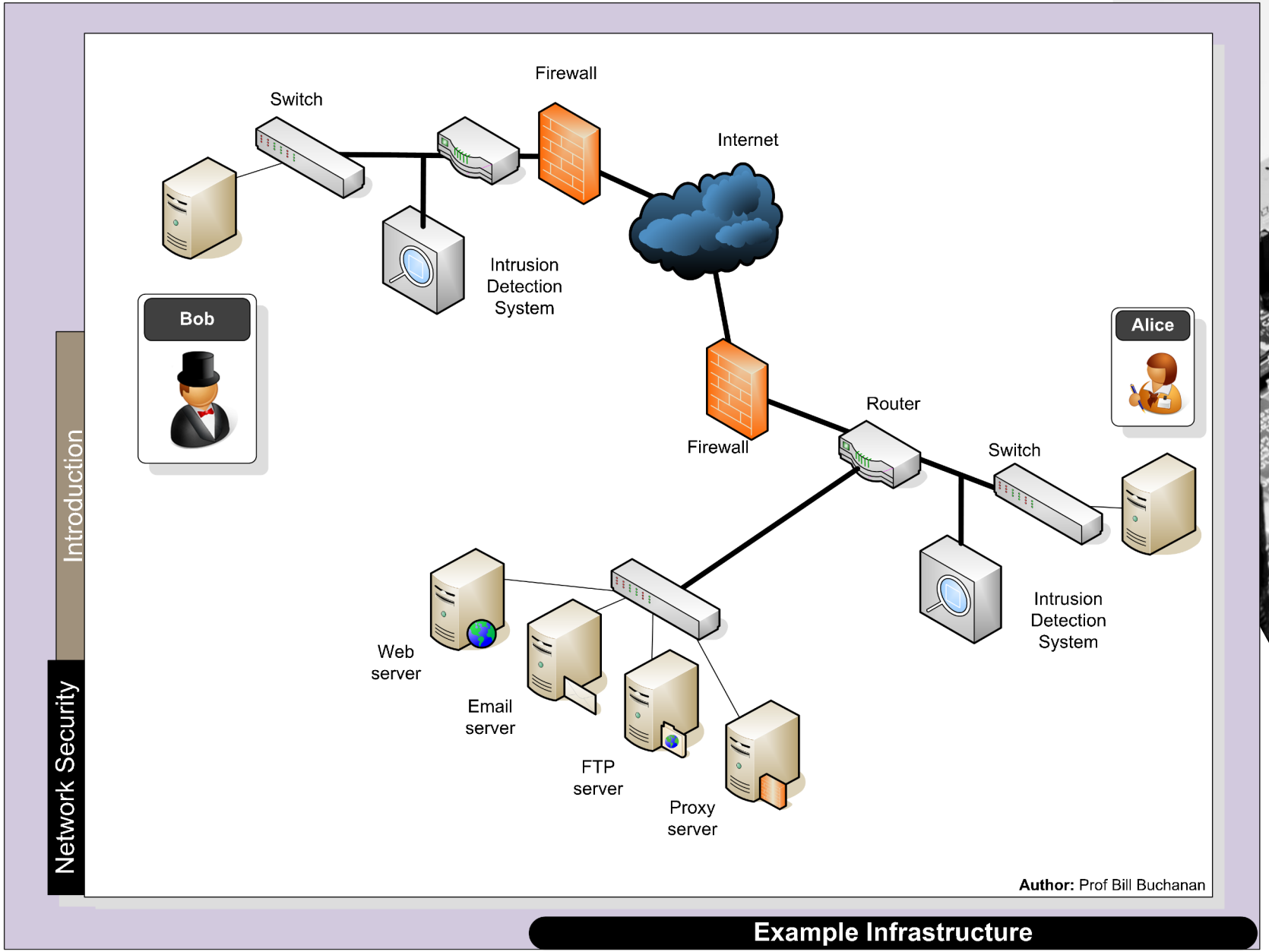
Network Security

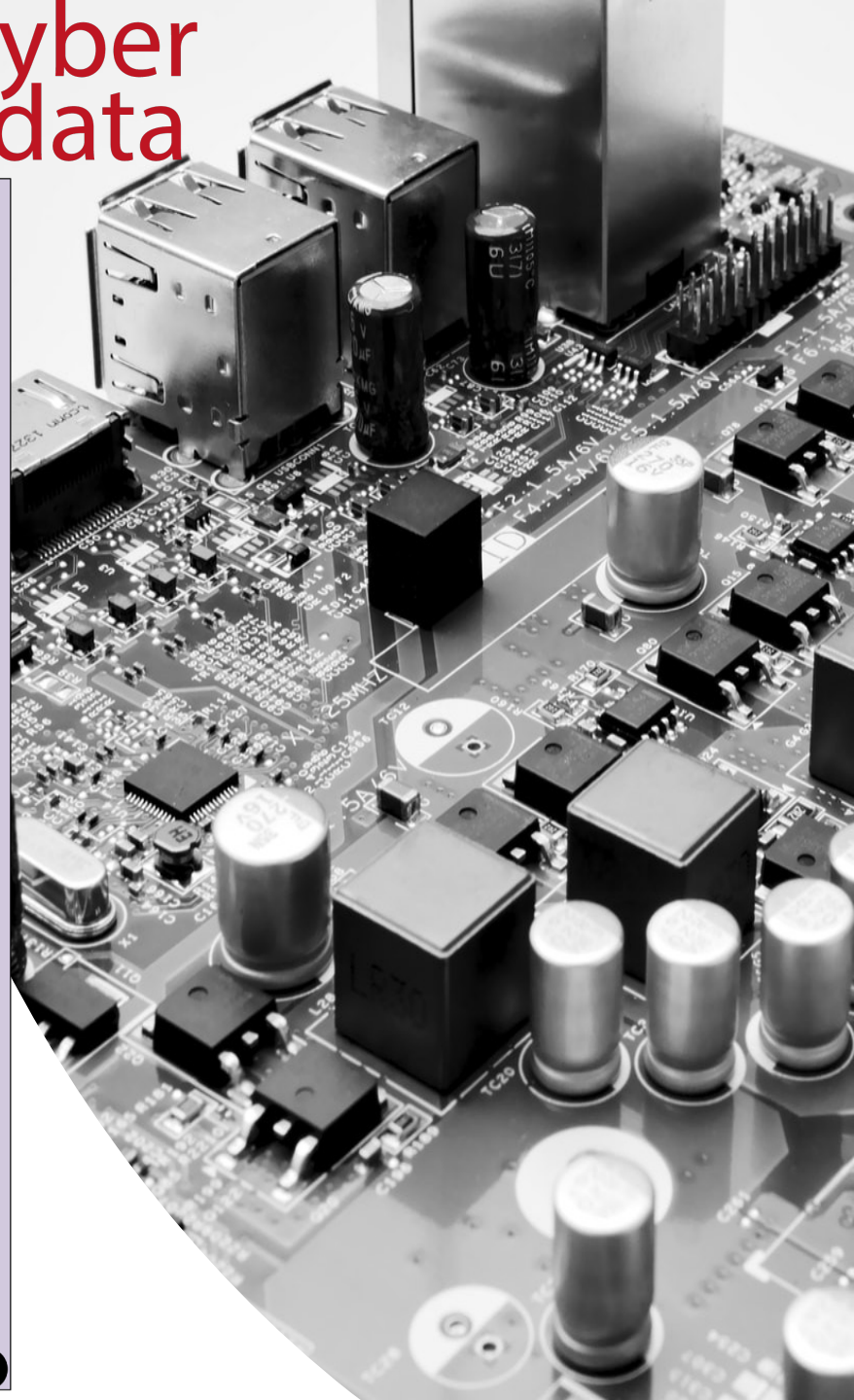
Layered Model



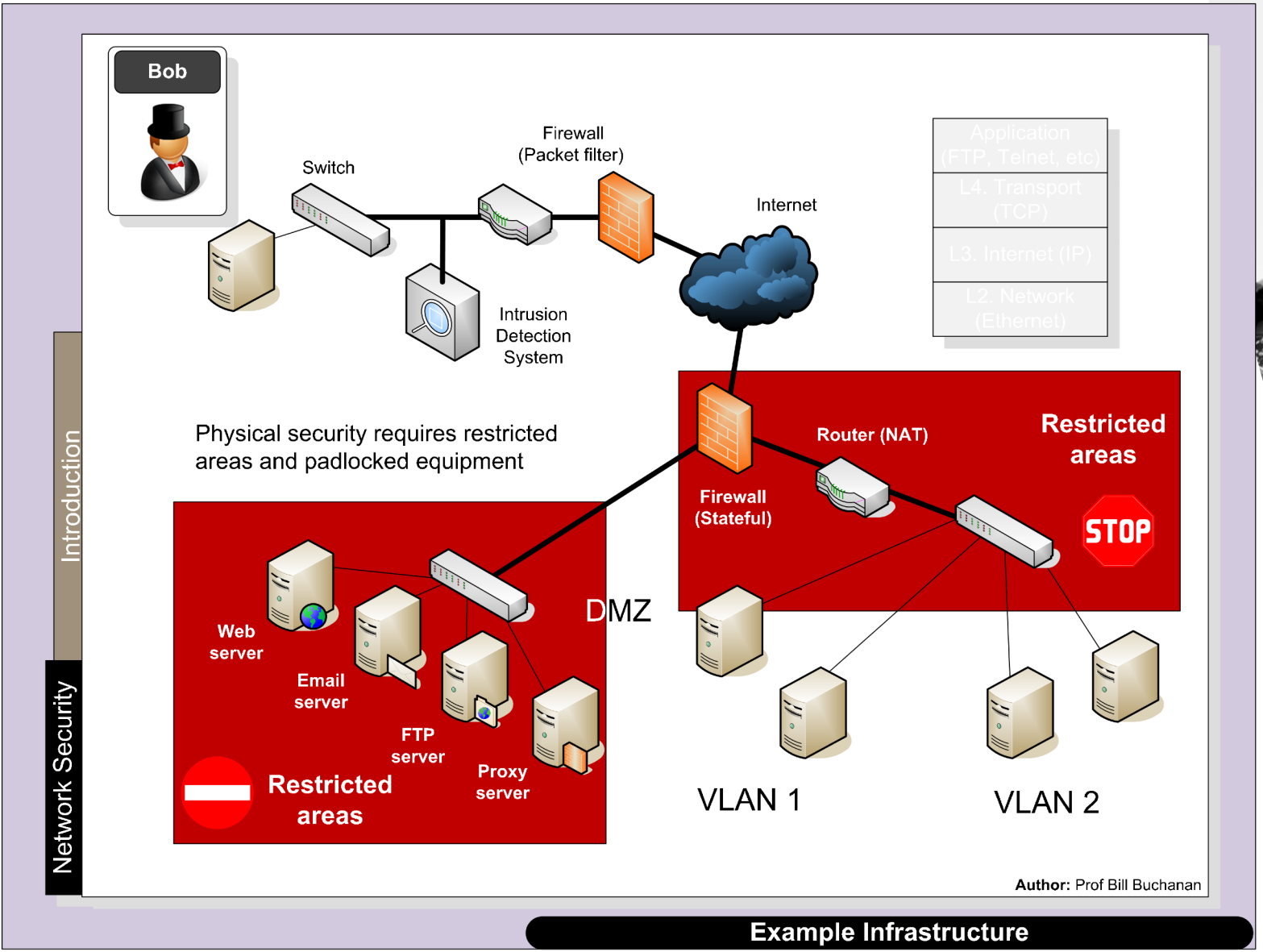


Layered Model

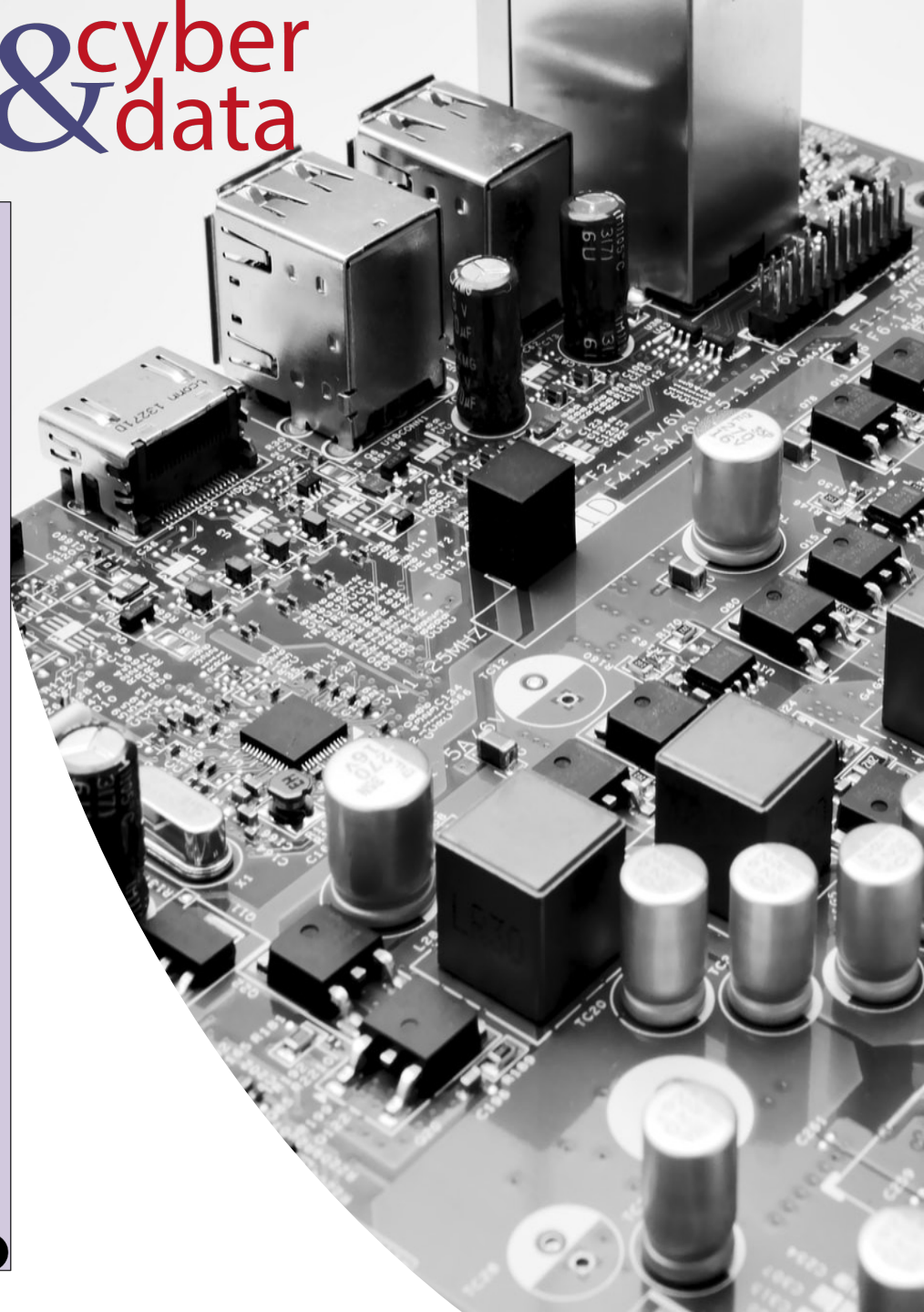




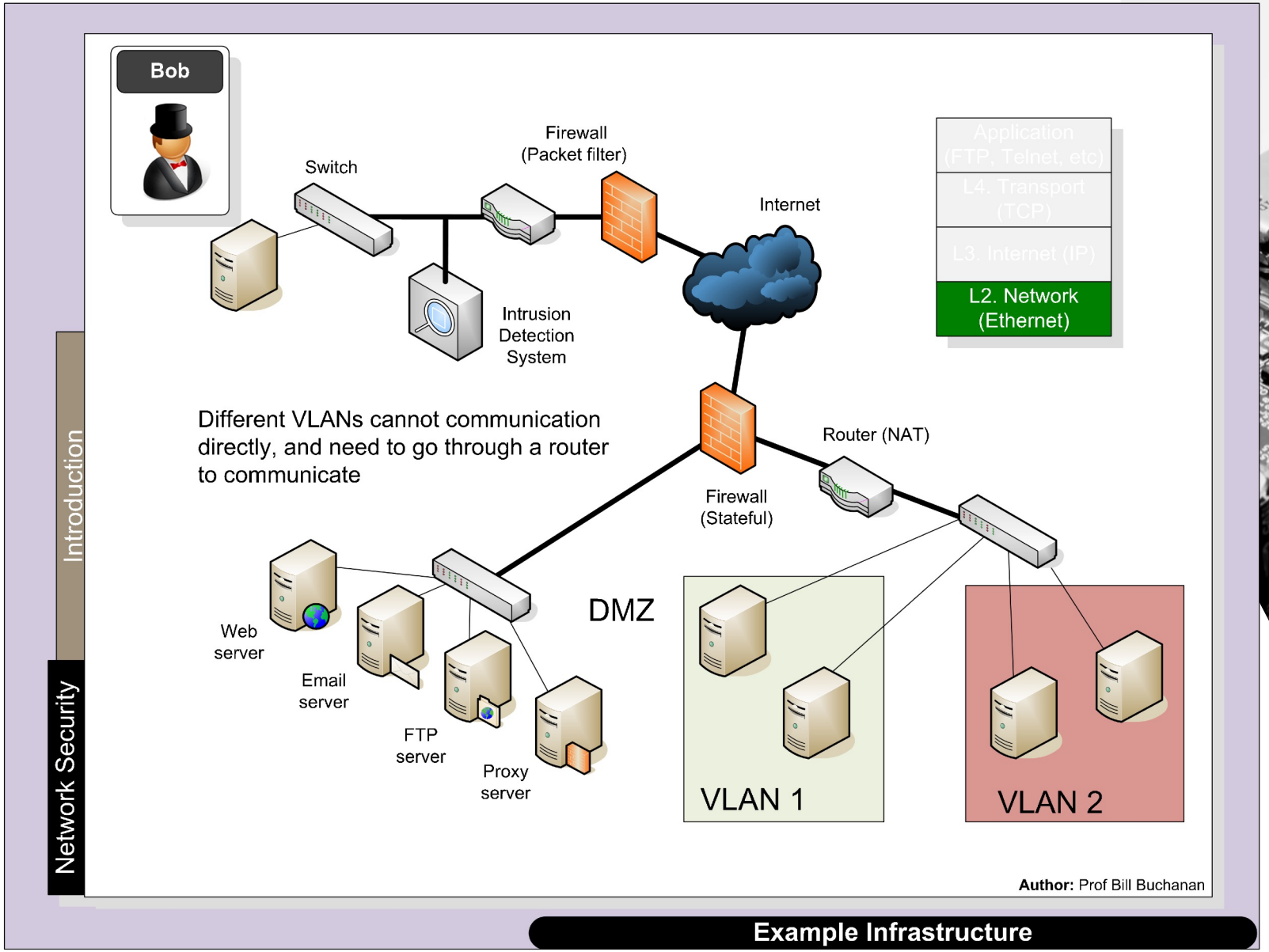
Layered Model

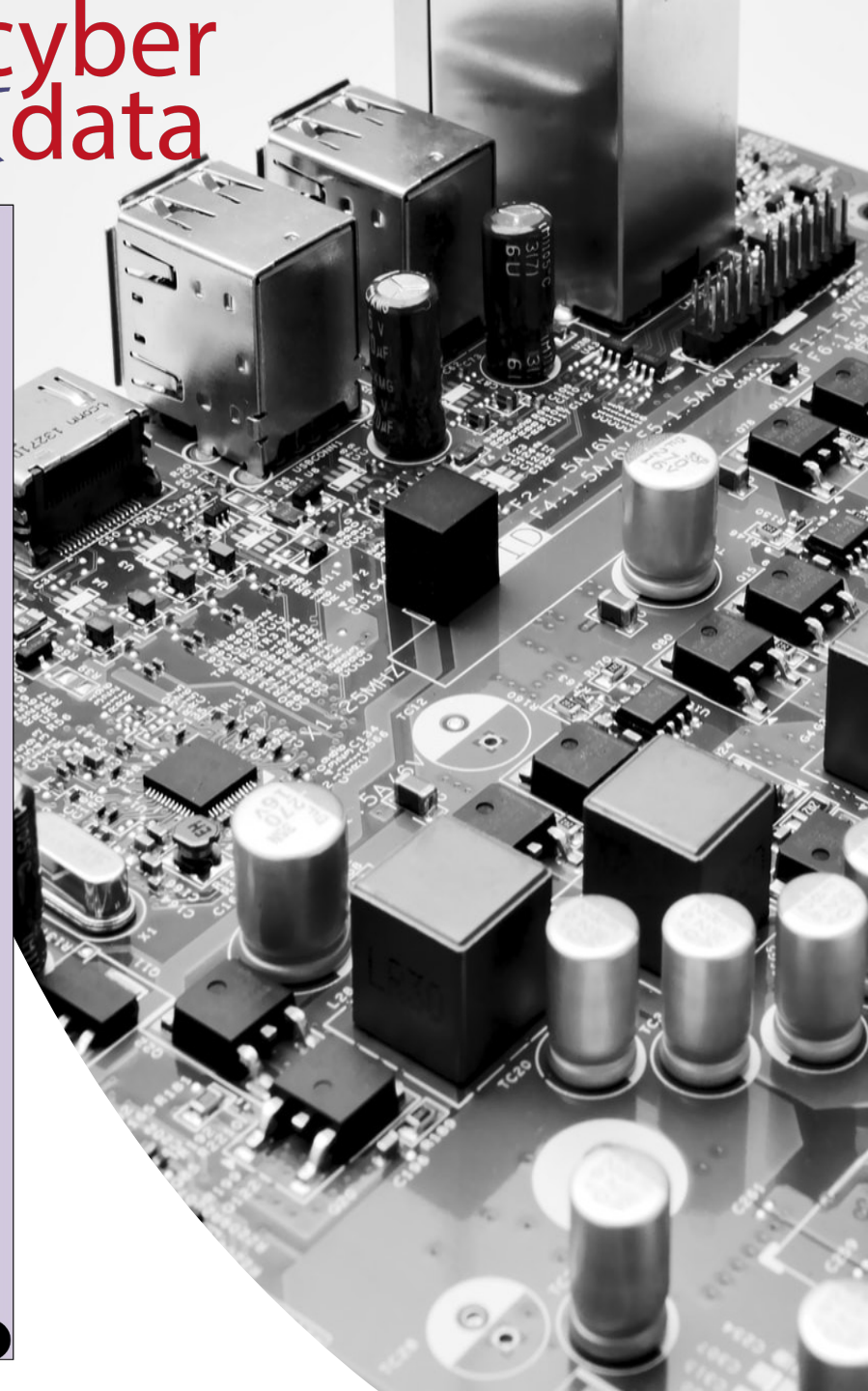


Example Infrastructure

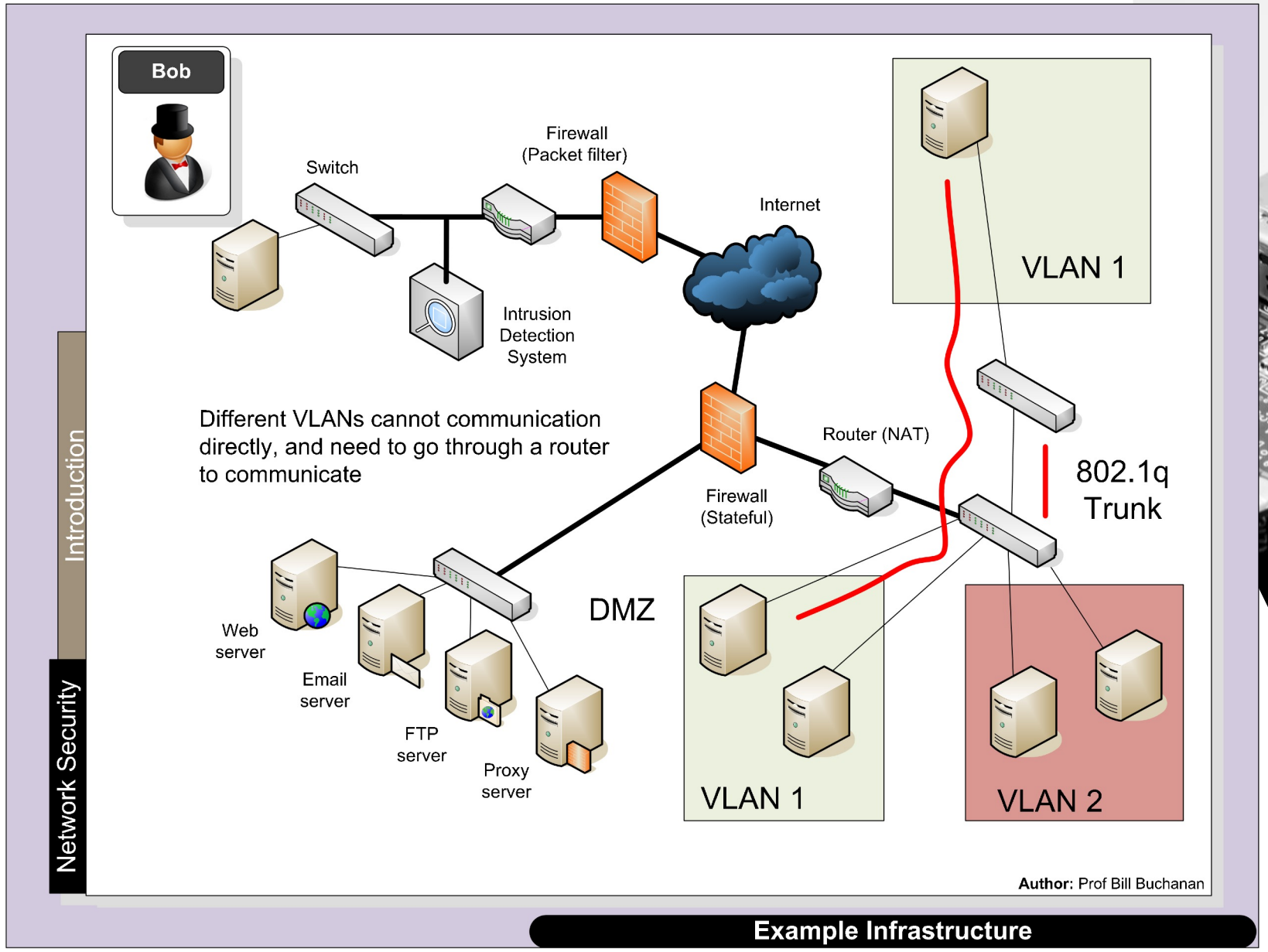


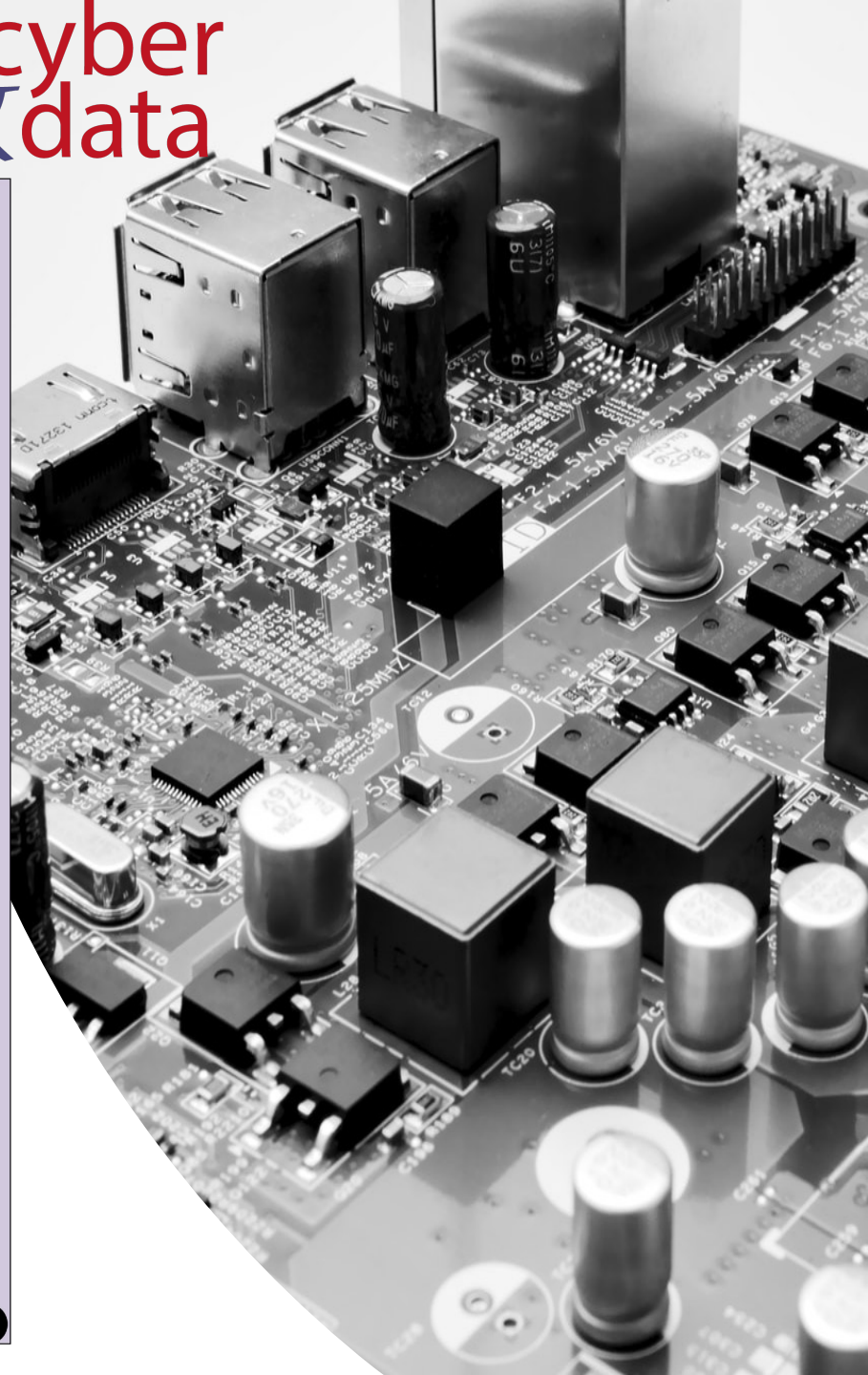
Layered Model



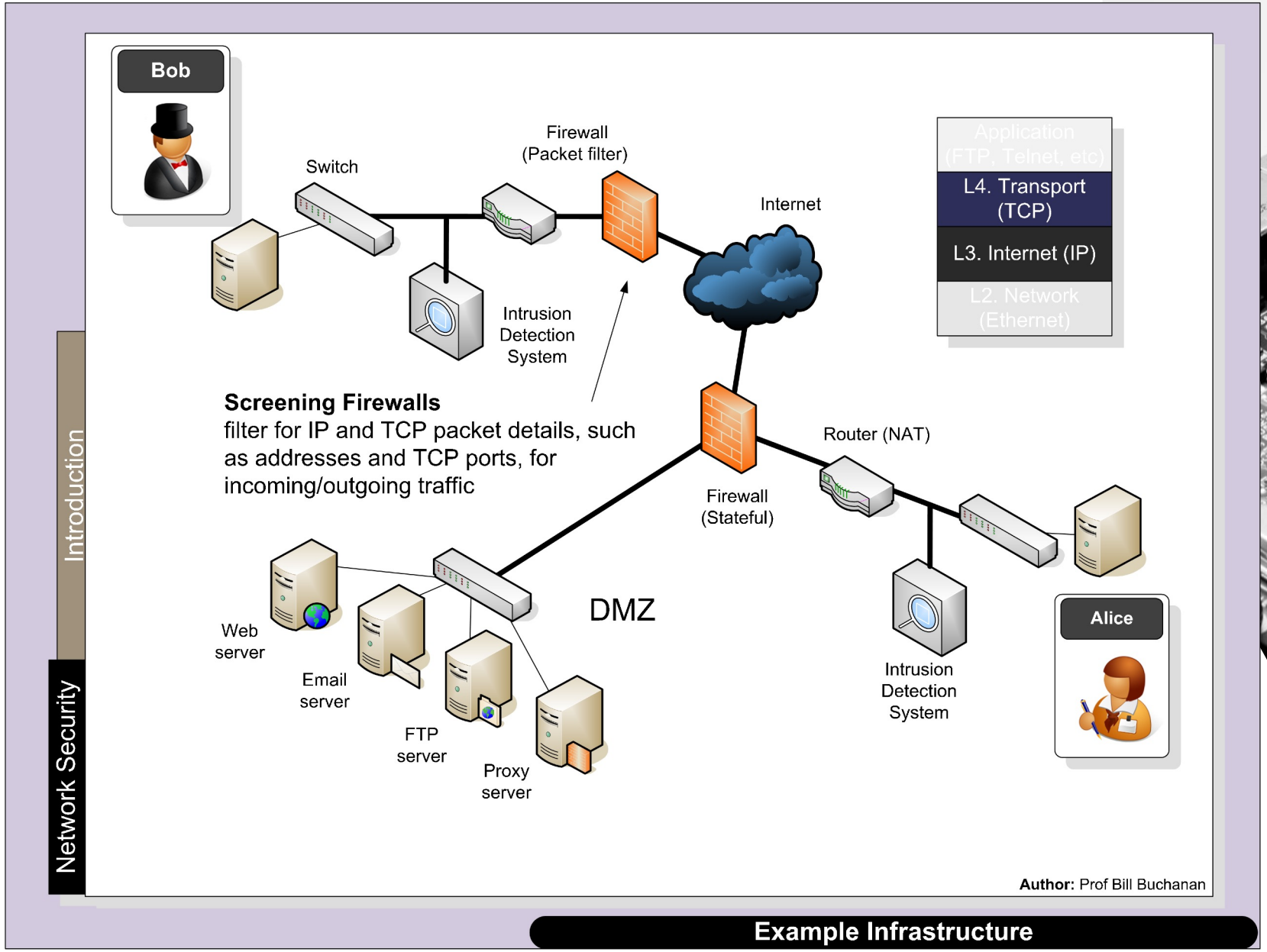


Layered Model

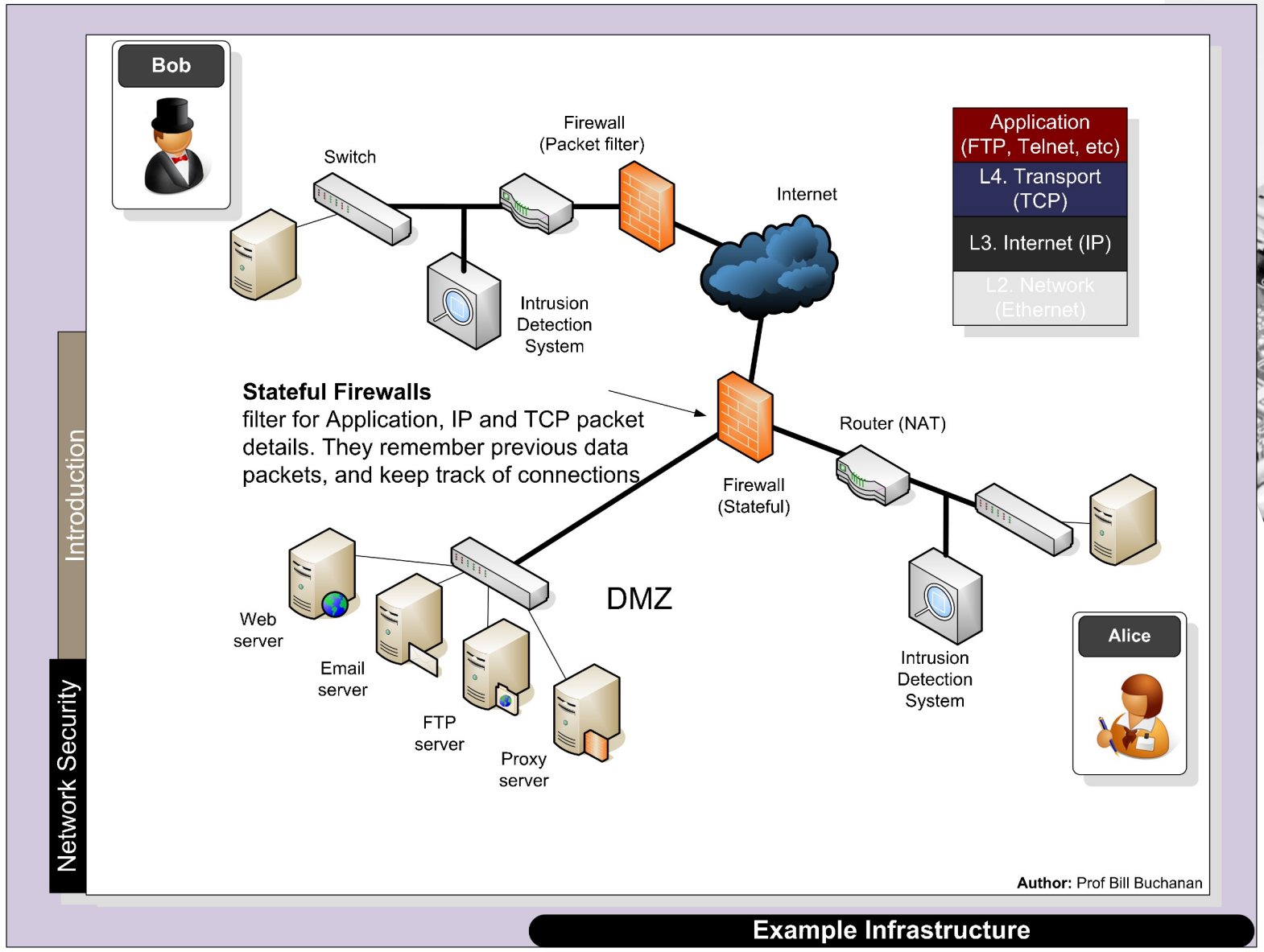


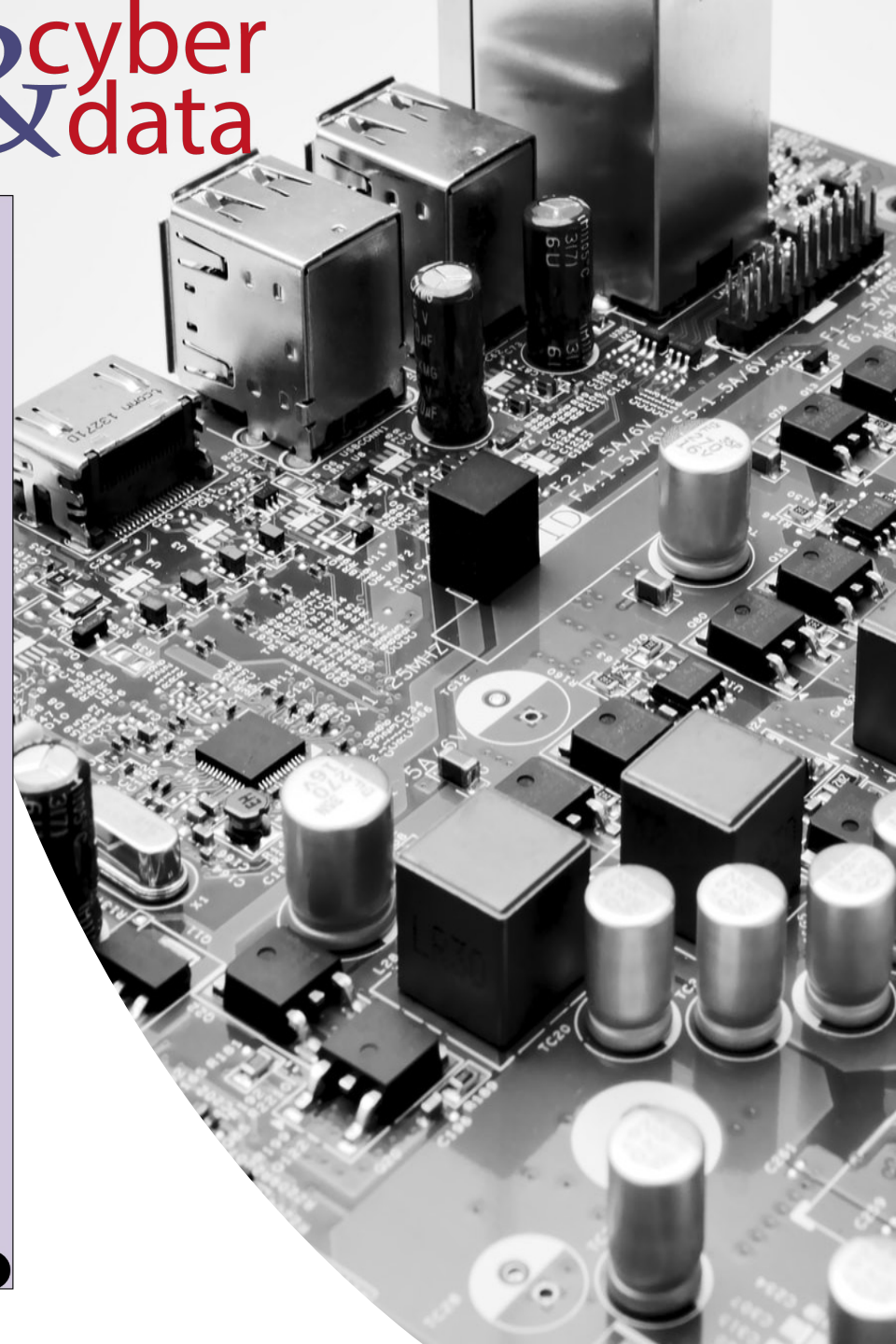


Layered Model

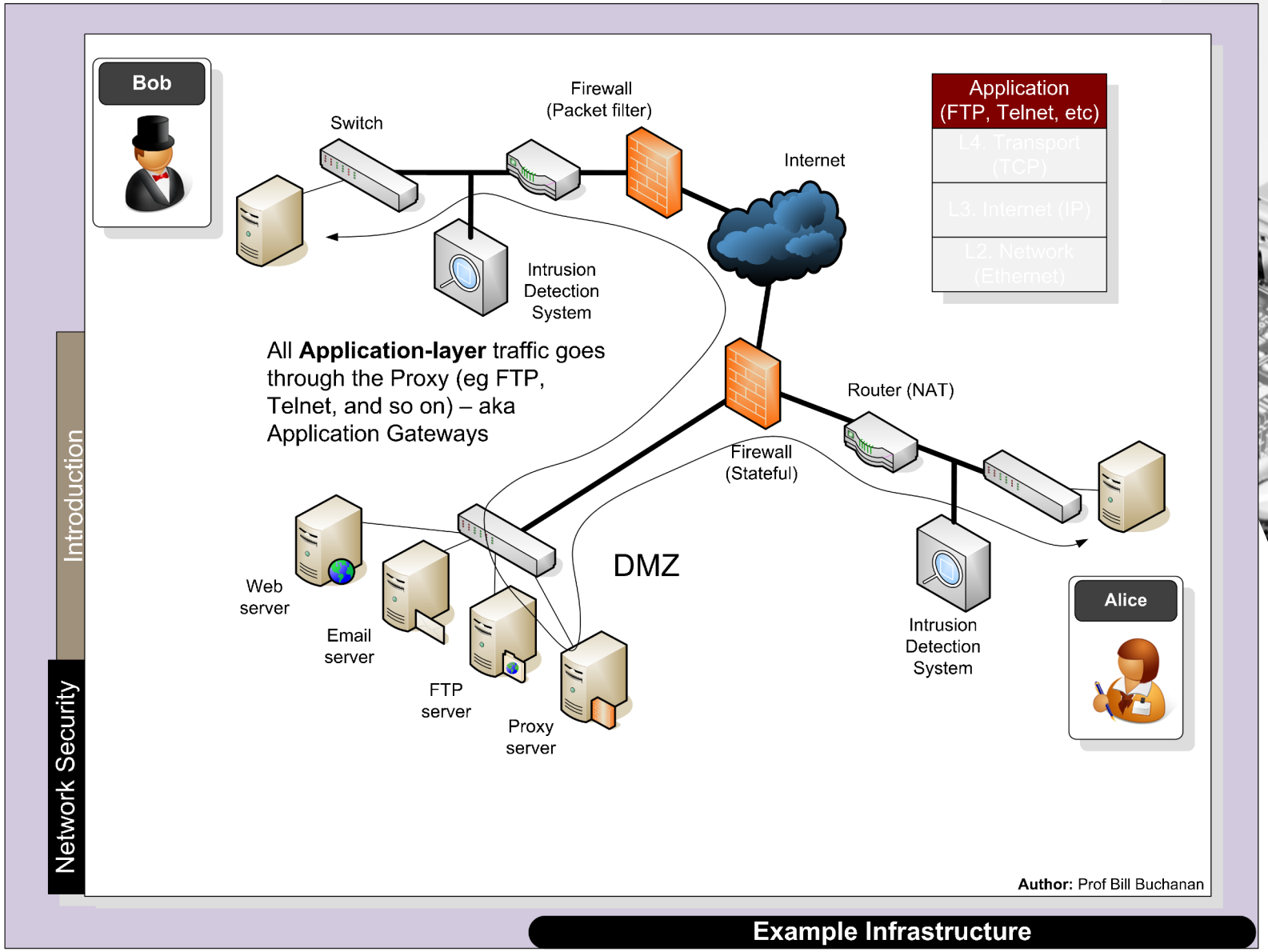


Layered Model

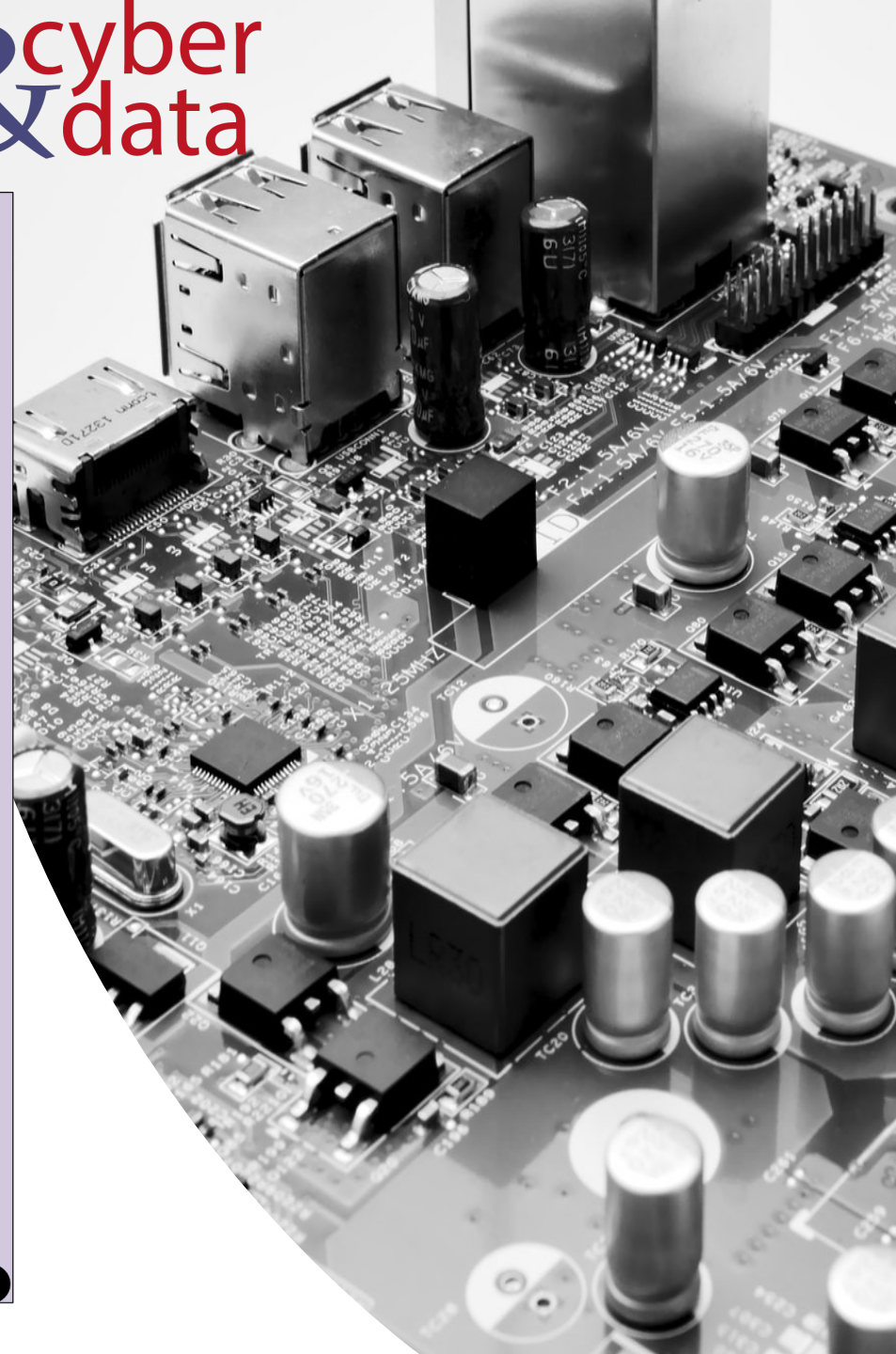




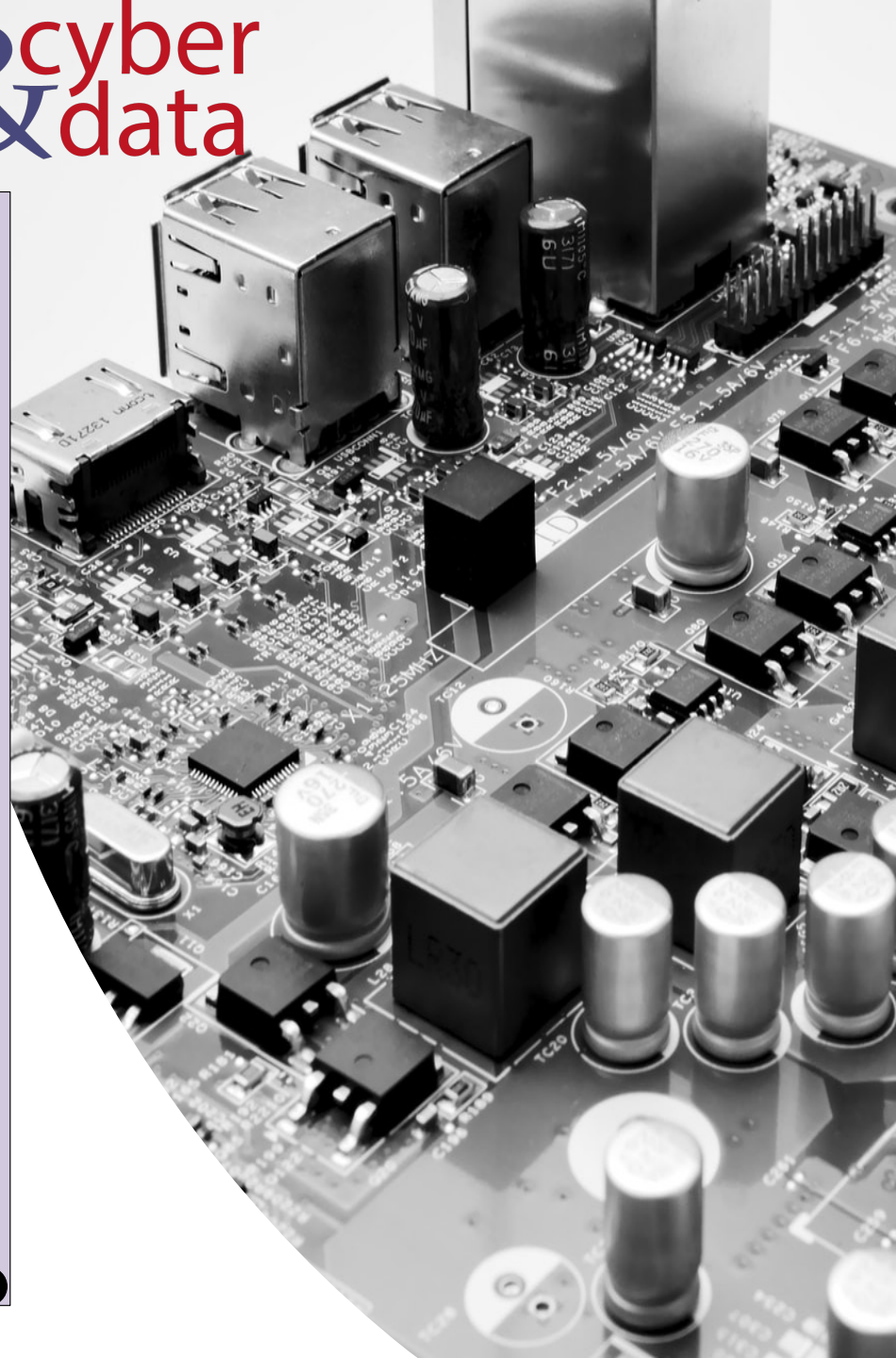
Layered Model



Example Infrastructure



Layered Model



Introduction

Network Security

Software firewall

Check Point SOFTWARE TECHNOLOGIES LTD.
We Secure the Internet.

Host-based: Zone alarm

ZONEALARM FOR YOUR HOME AND SMALL BUSINESS

CheckPoint firewall (software)

Runs within: Windows Server, VMWare LINUX

CheckPoint firewall (dedicated) Nokia

LINUX iptables

Hardware firewall

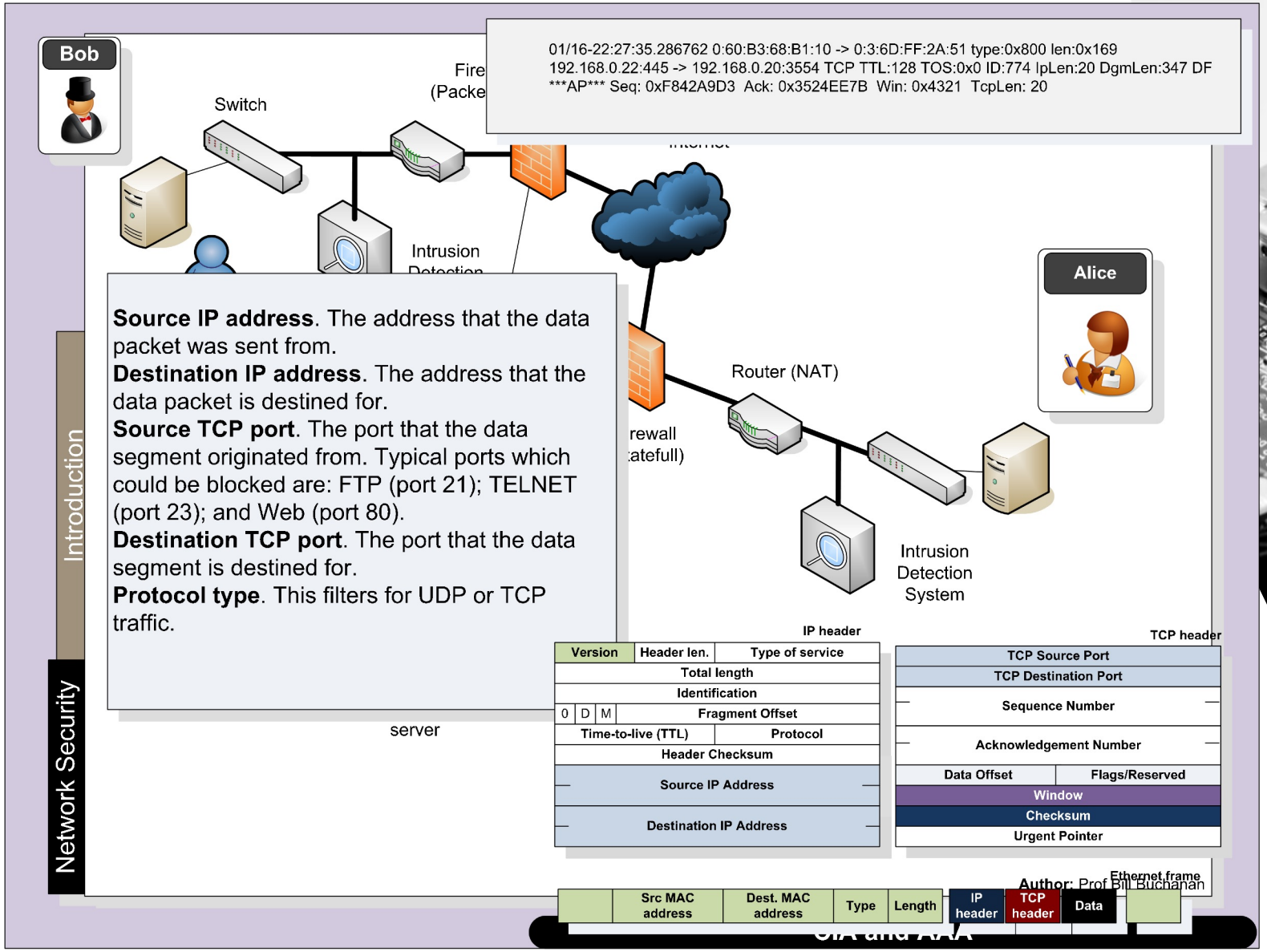
Cisco router With firewall (non-stateful)

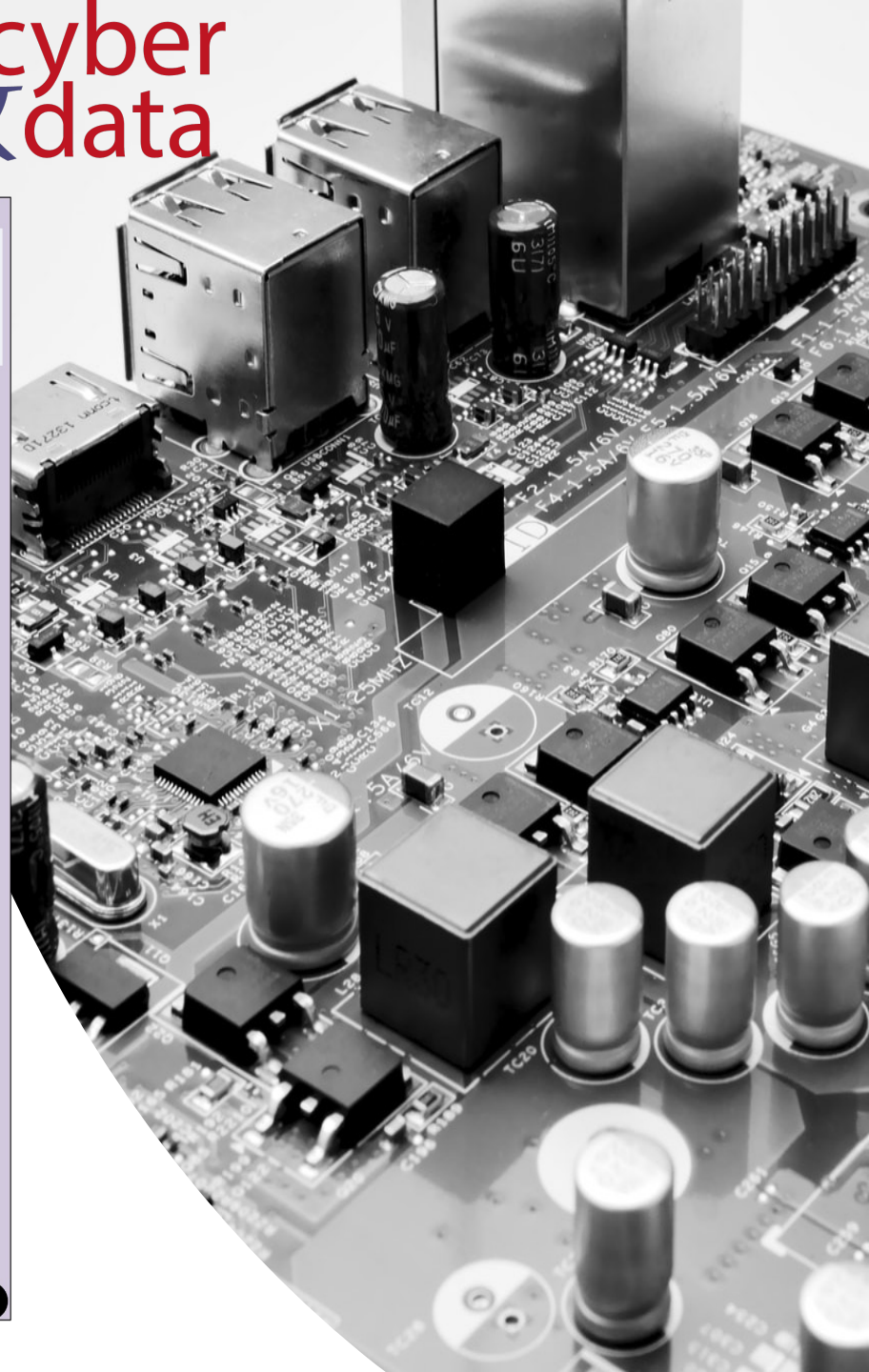
Cisco PIX/ASA (stateful)

Software firewall:
- Easy to reconfigure
- Slower
- Less expensive
- Can be used with a range of computers/OSs

Hardware firewall:
- Optimized engine/architecture
- Copes better with large traffic conditions
- Improved failover

Layered Model





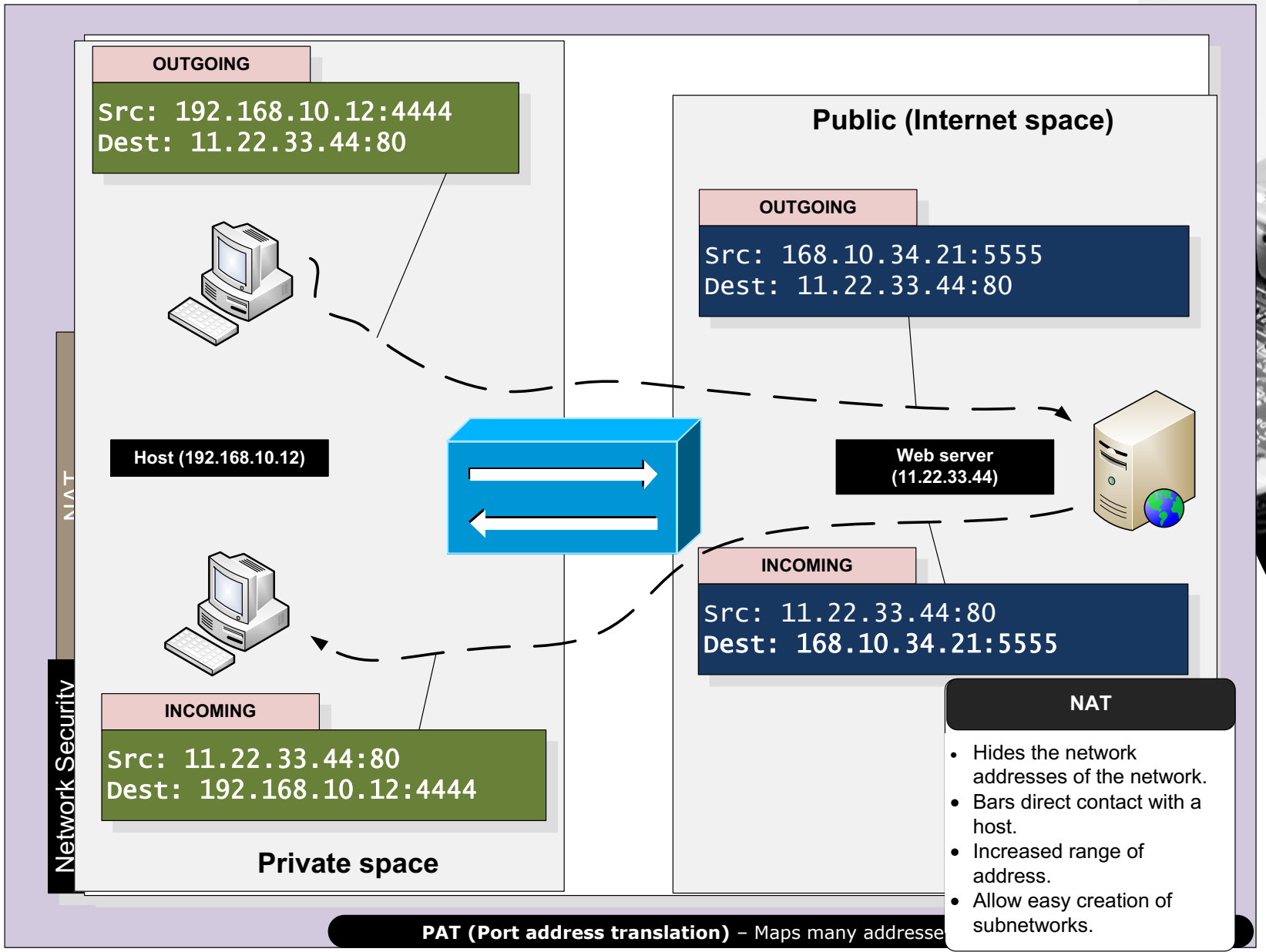
cyber & data

"From bits to information"

NAT

Layered Model

&cyber data

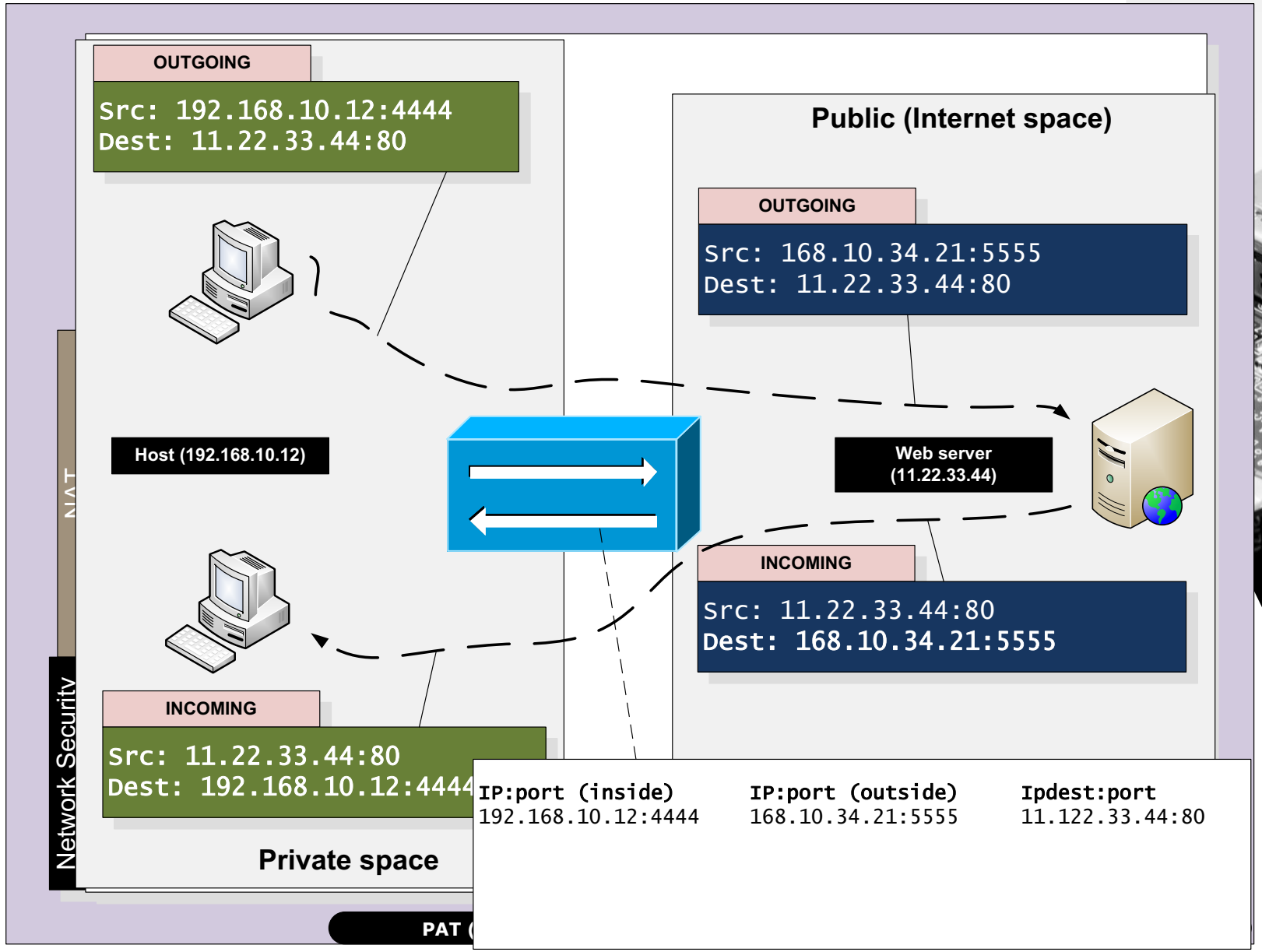


NAT

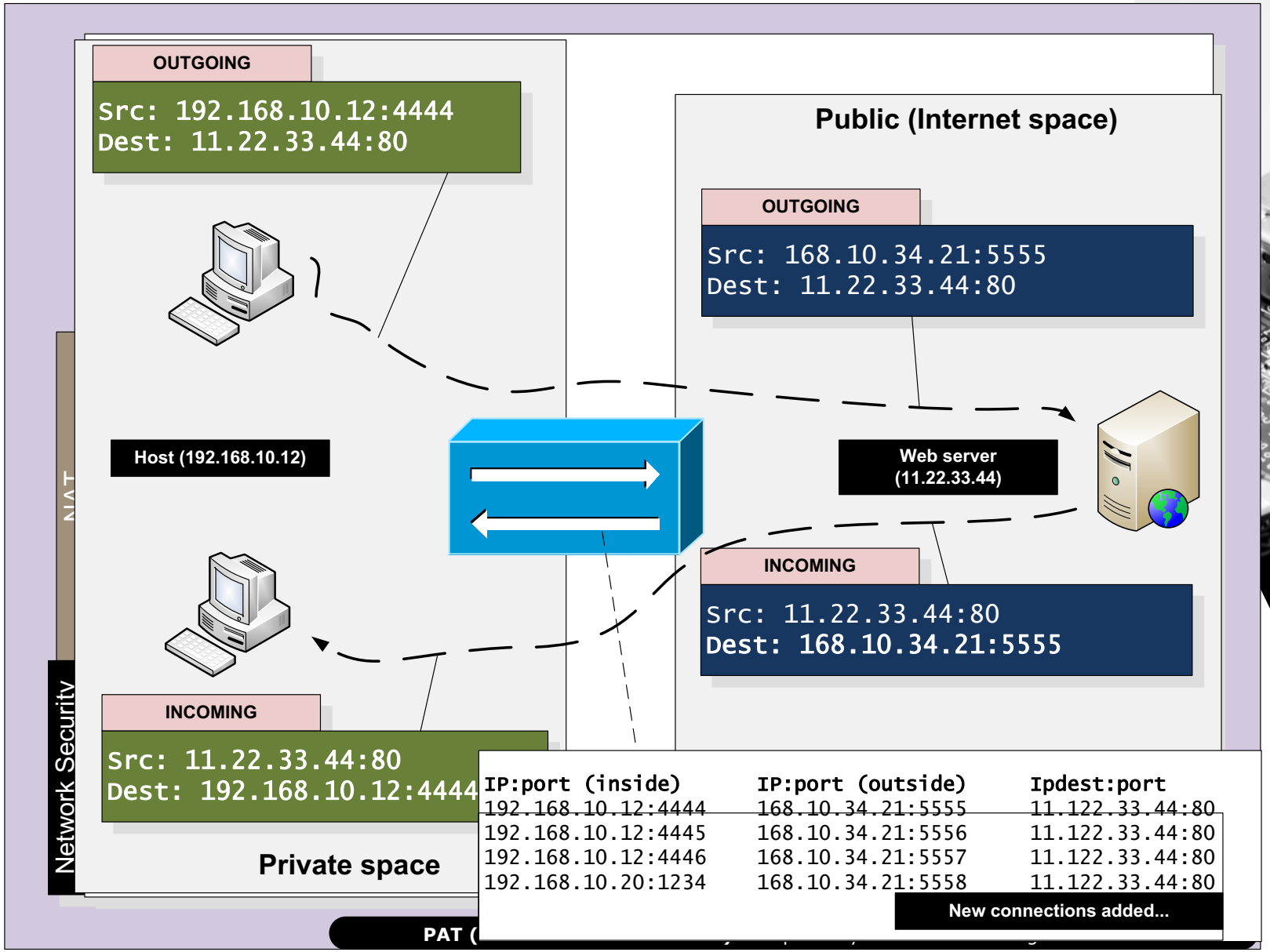
- Hides the network addresses of the network.
- Bars direct contact with a host.
- Increased range of address.
- Allow easy creation of subnetworks.

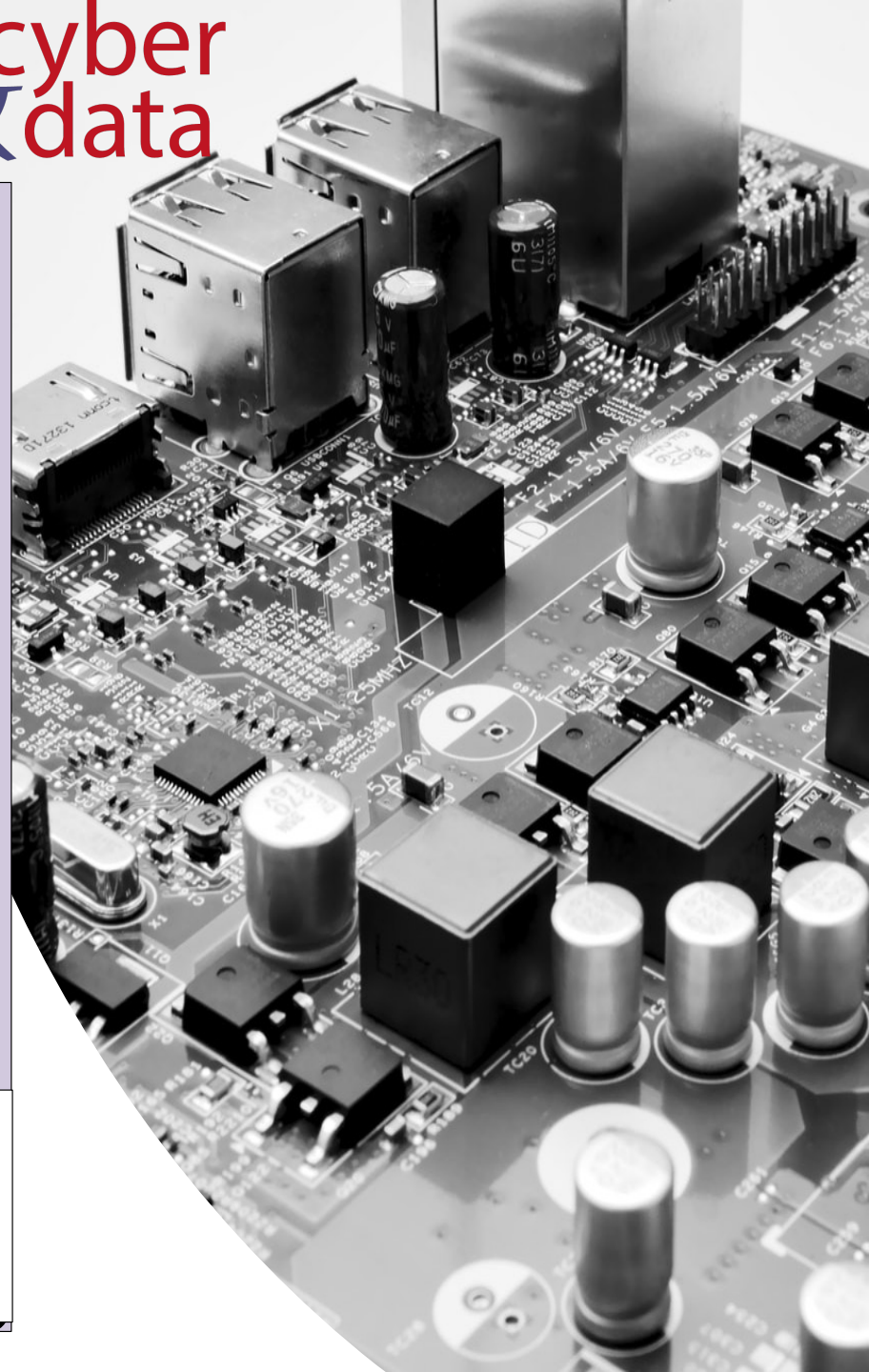
Layered Model

&cyber data

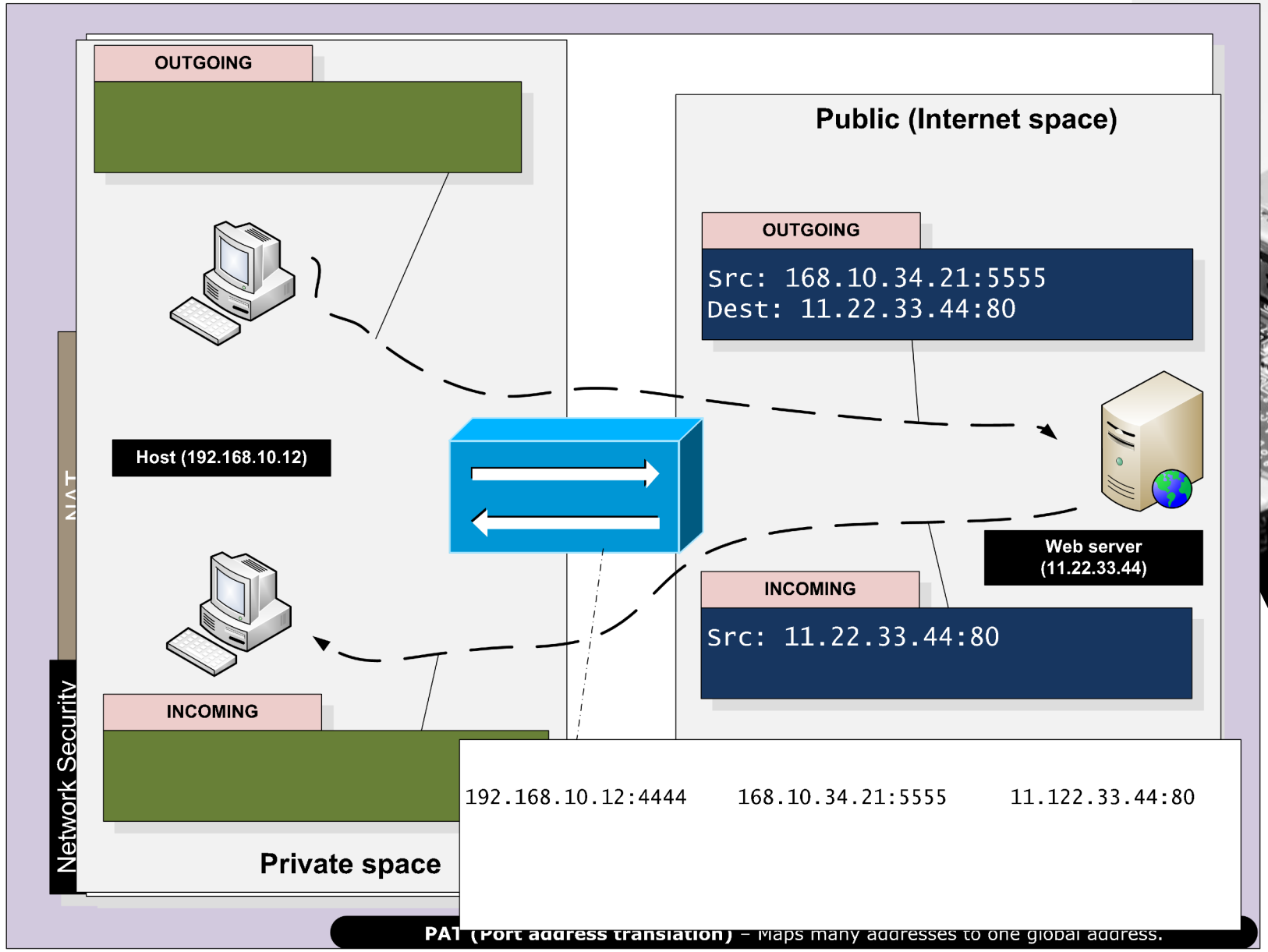


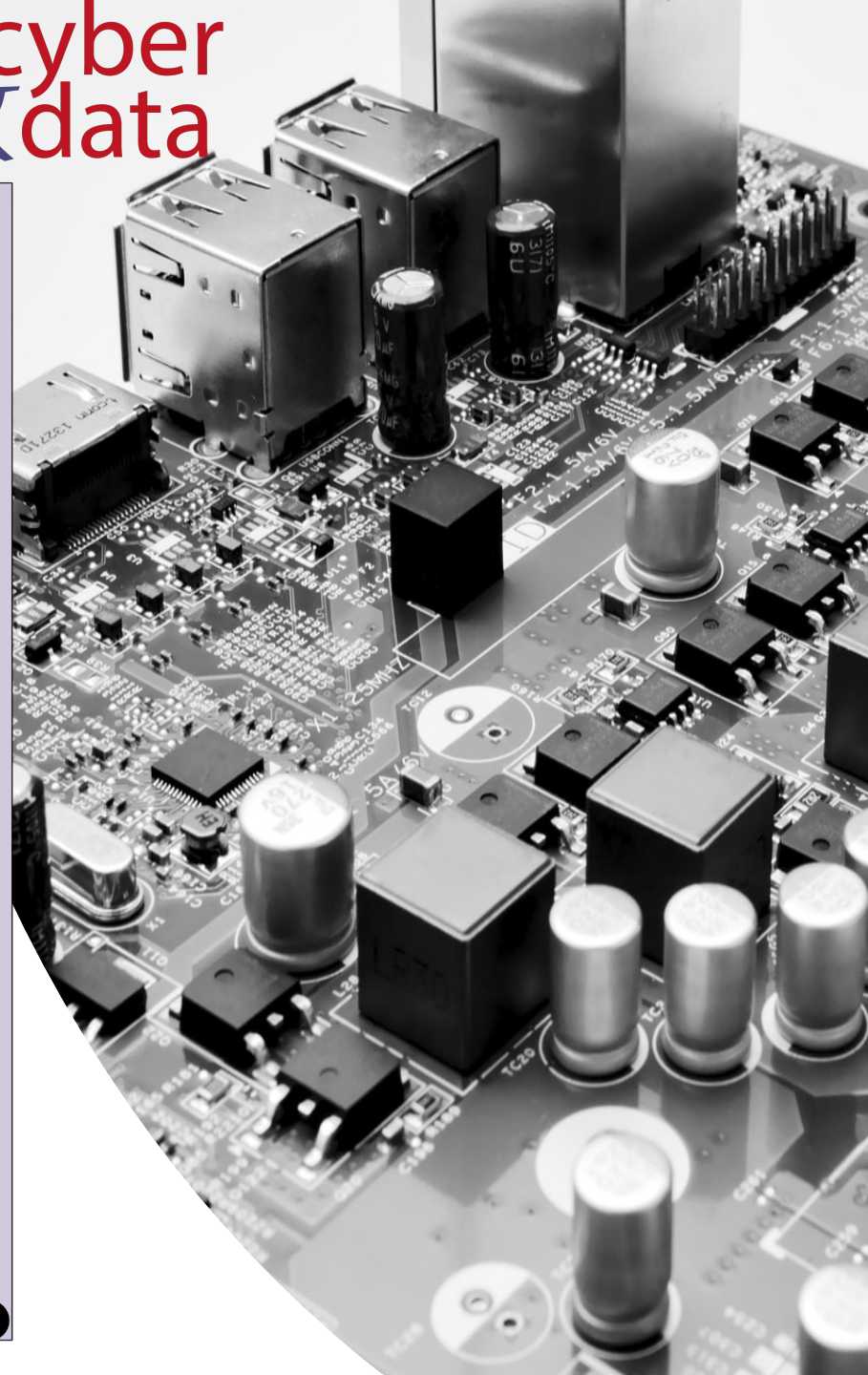
Layered Model



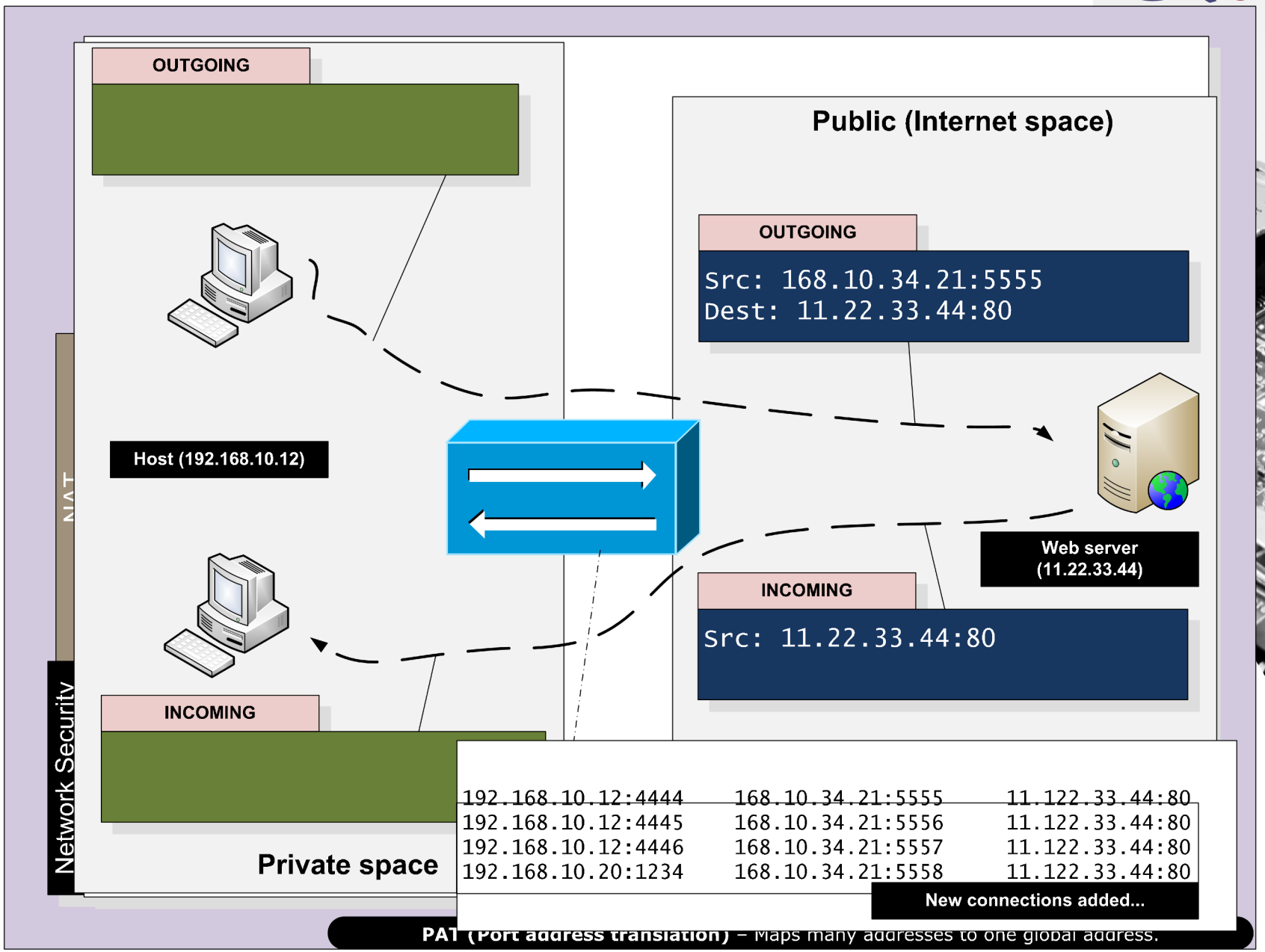


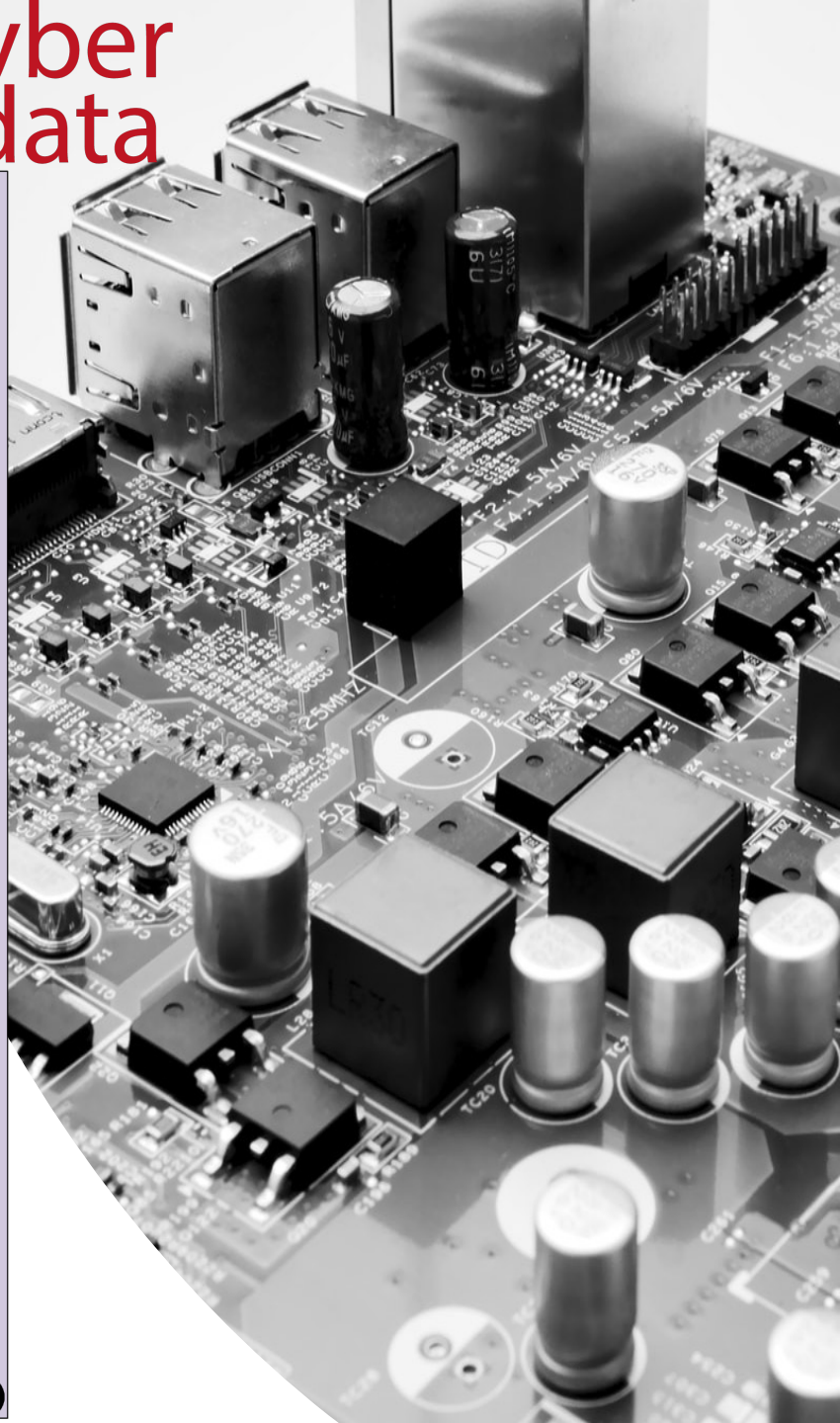
Layered Model





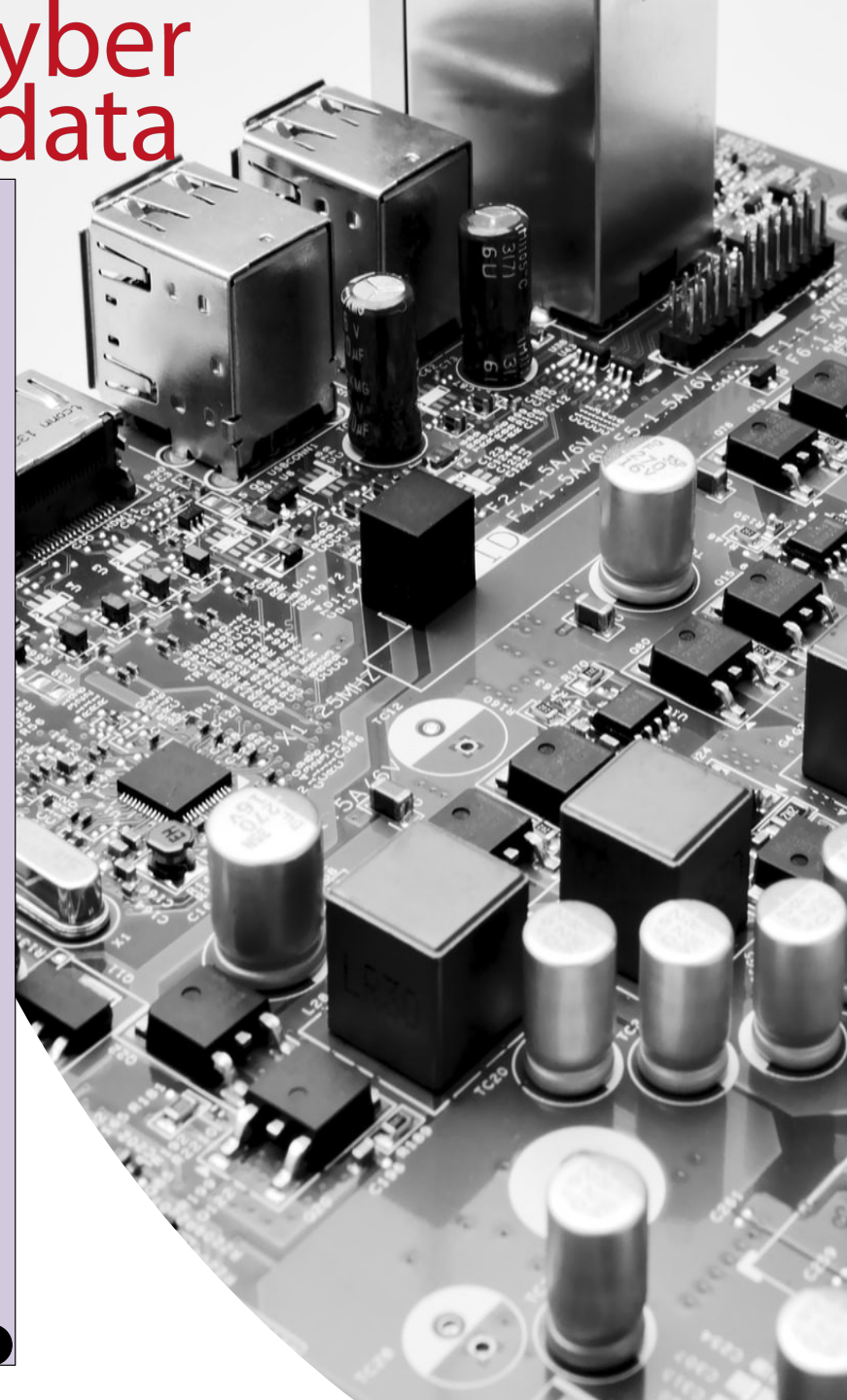
Layered Model



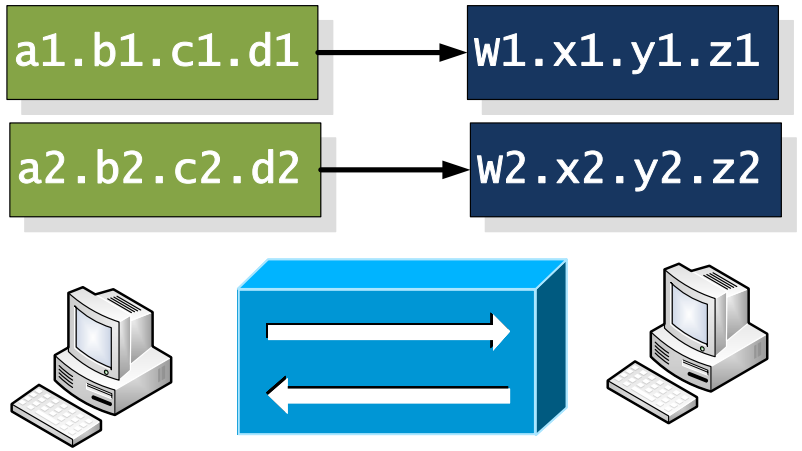


Layered Model

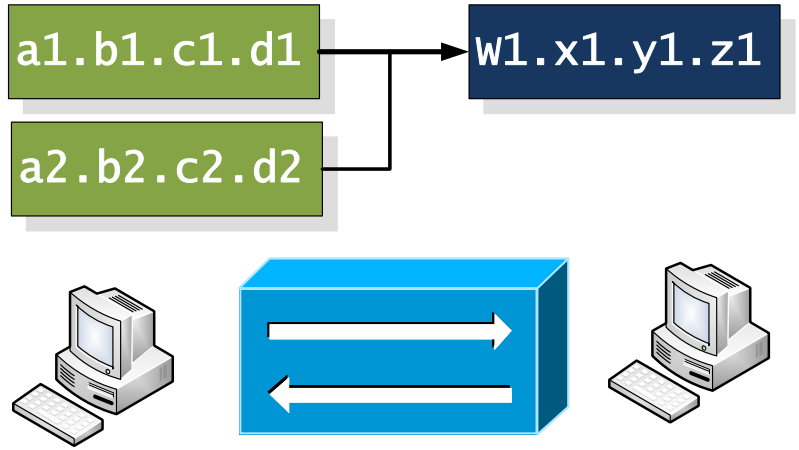
&cyber data



Static translation.
Each public IP address translates to a private one through a static table.
Good for security/logging/traceability.
Bad, as it does not hide the internal network.



IP Masquerading (Dynamic Translation).
A single public IP address is used for the whole network. The table is thus dynamic.



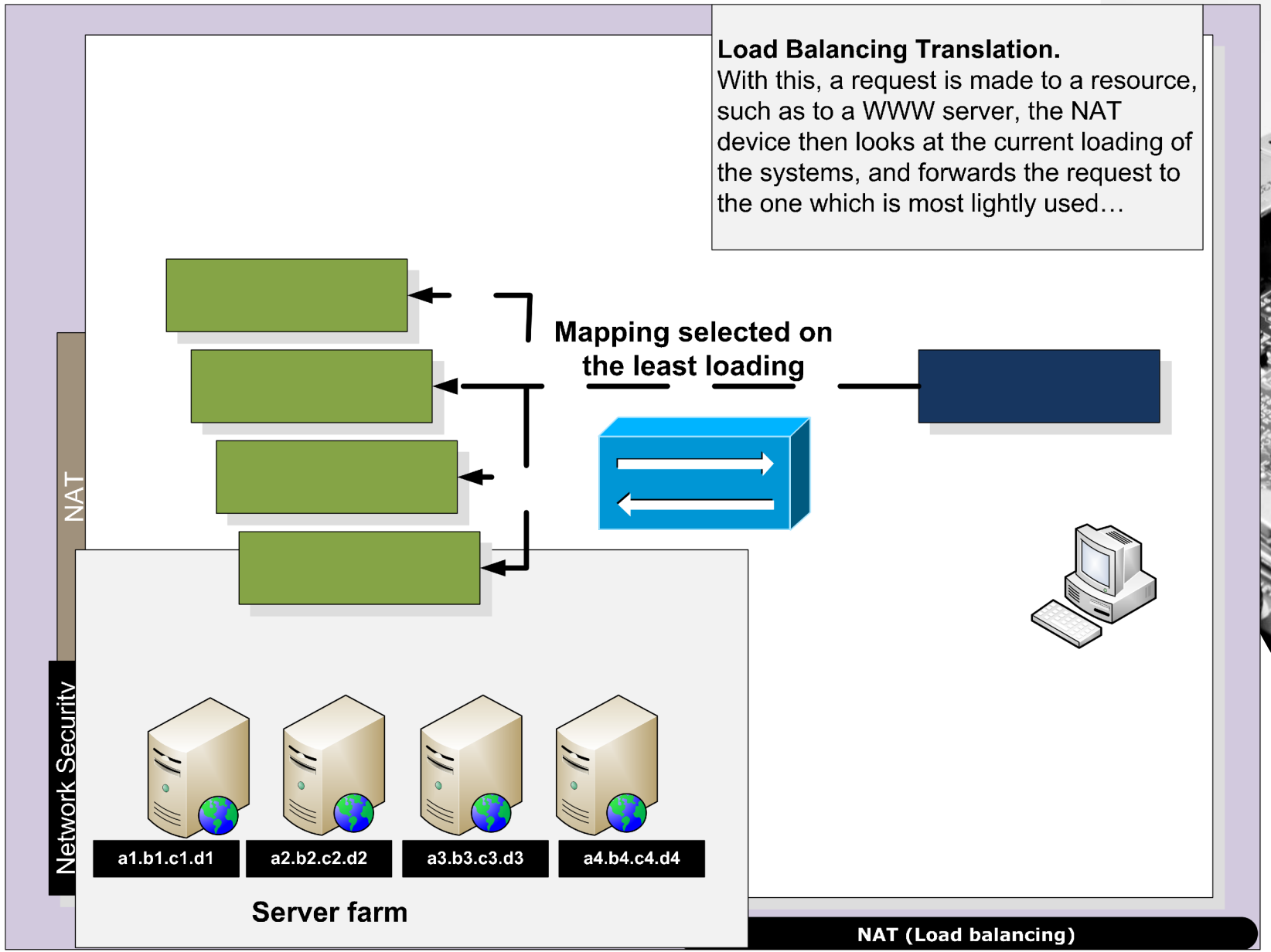
NAT

Network Security

NAT

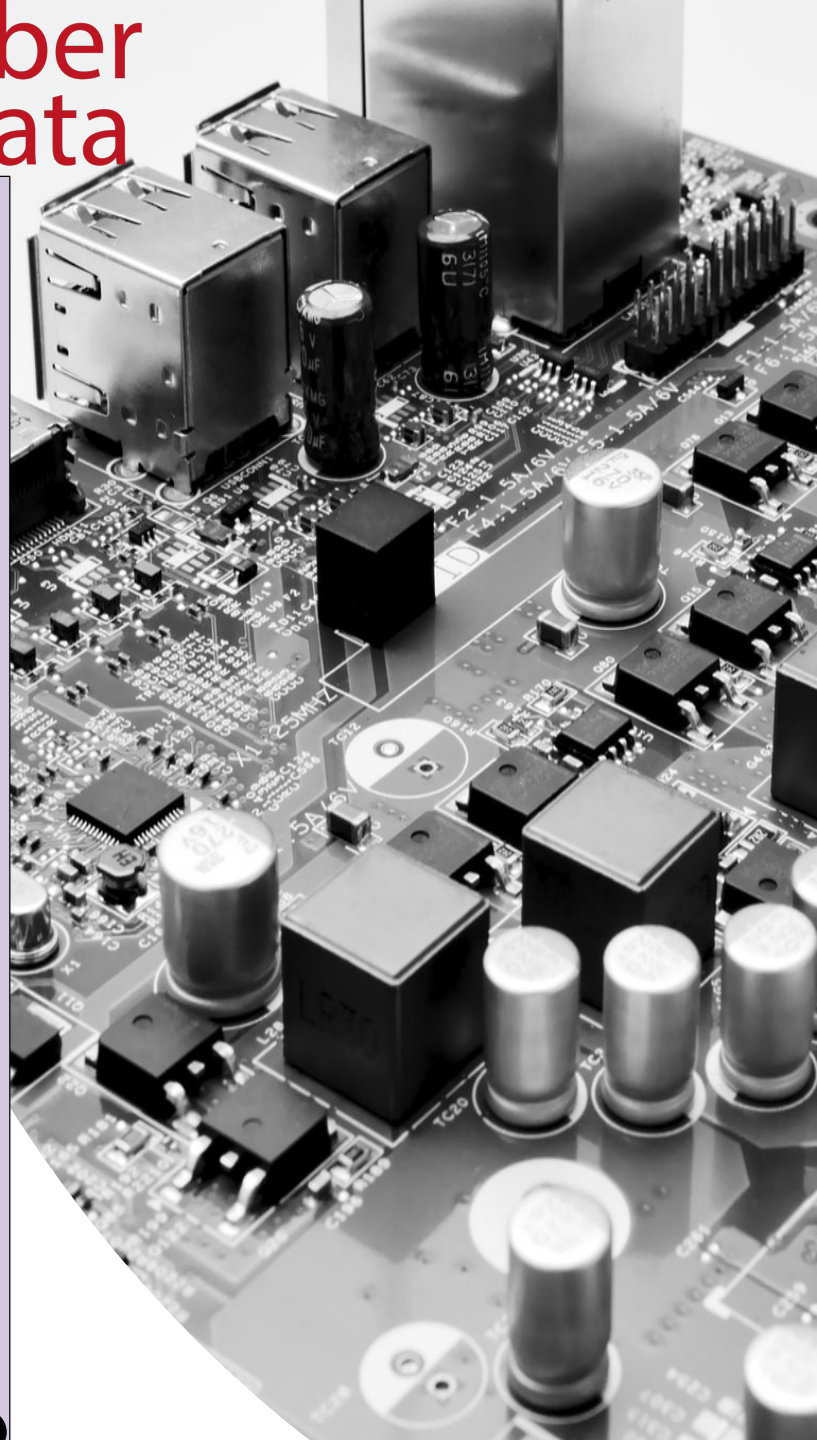
Layered Model

&cyber data

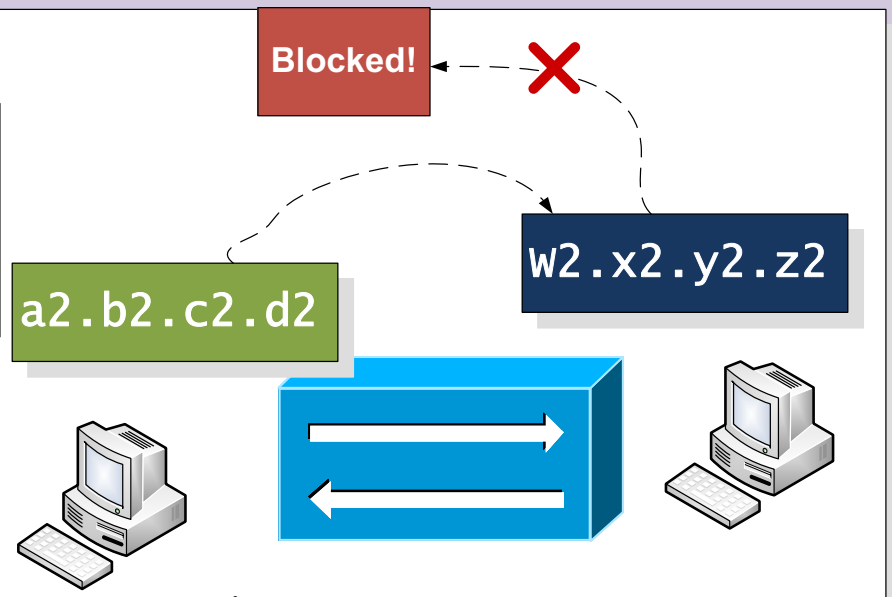


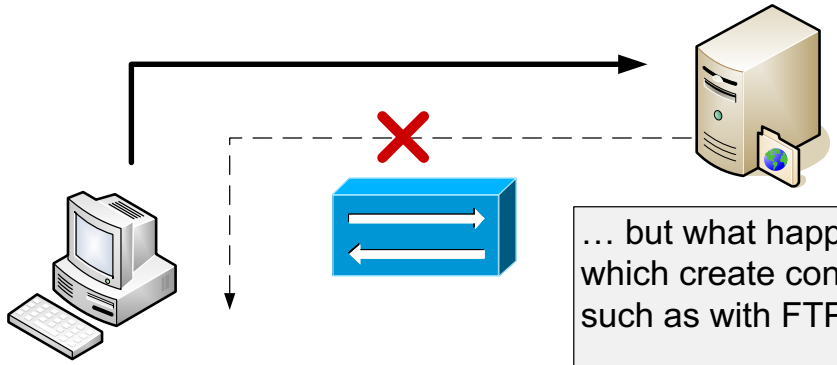
Layered Model

&cyber data



NAT is good as we are isolated from the external public network, where our hosts make the **initiate** connections





FTP creates a local server port

… but what happens if we use applications which create connections in the reverse direction, such as with FTP and IRC?

.. we thus need some form of **backtracking** of connections in the NAT device. Where the NAT device remembers the initial connection, and then allows direct connections to the initiator.

NAT

Network Security

Backtracking

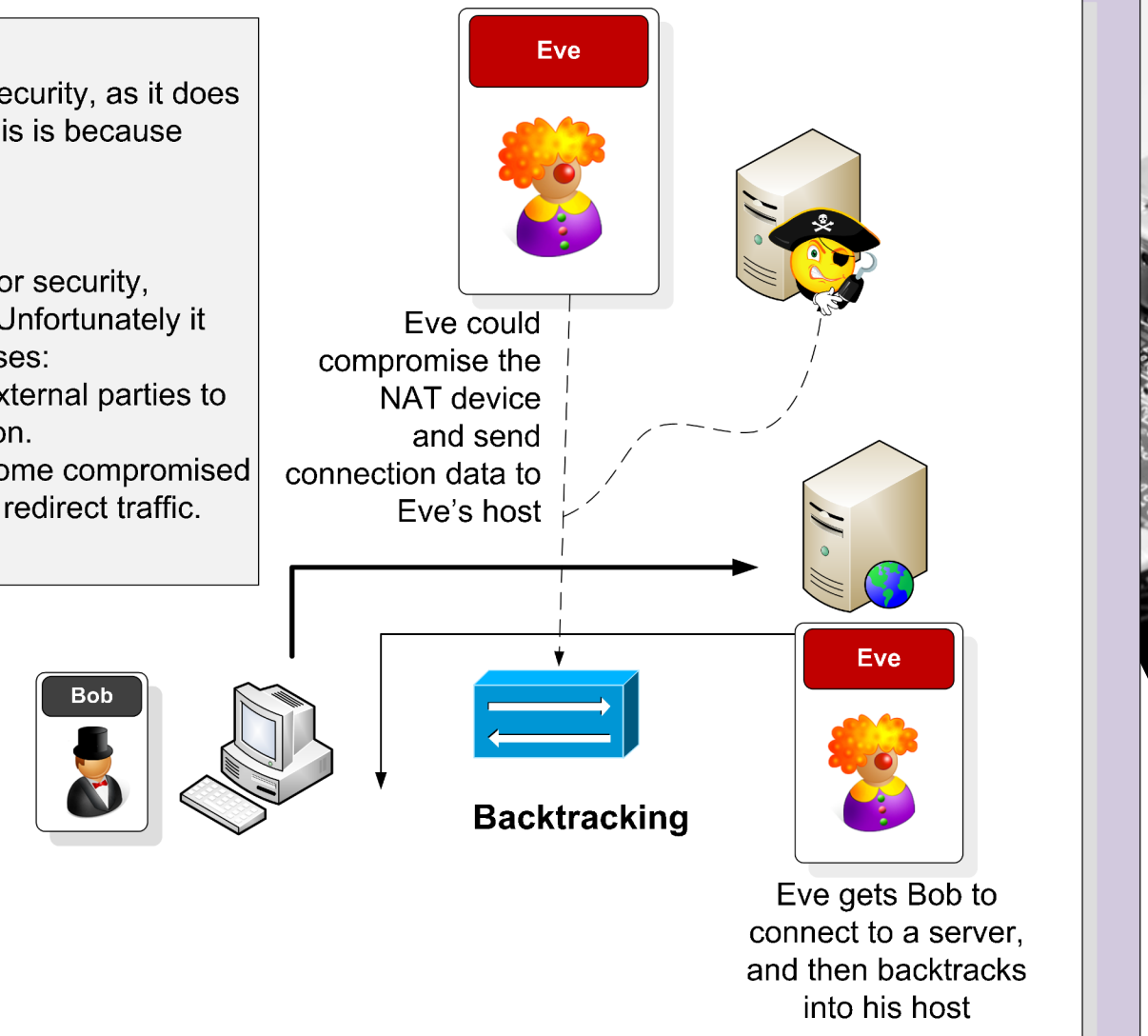
Layered Model

&cyber data

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.



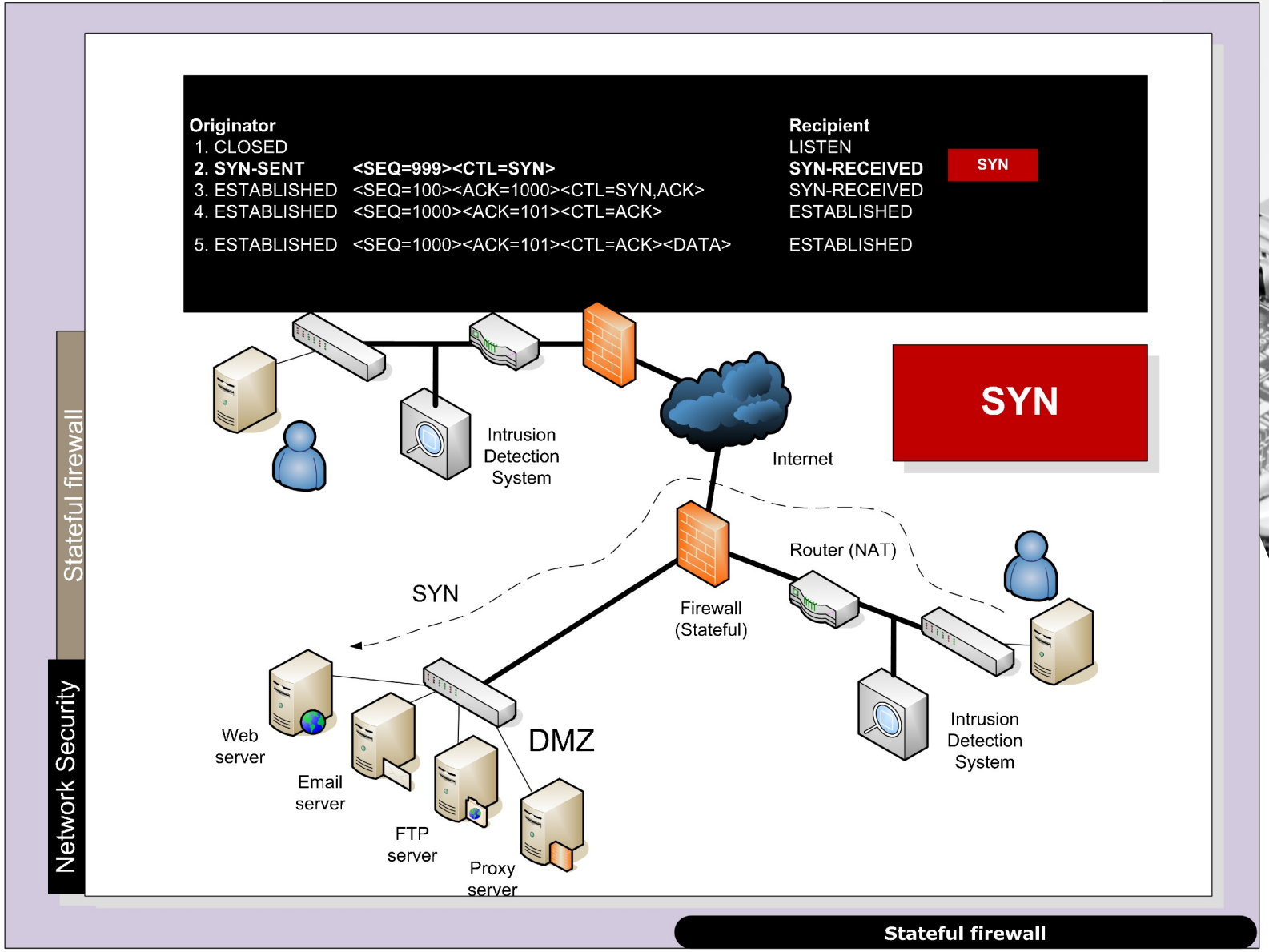
Network Security

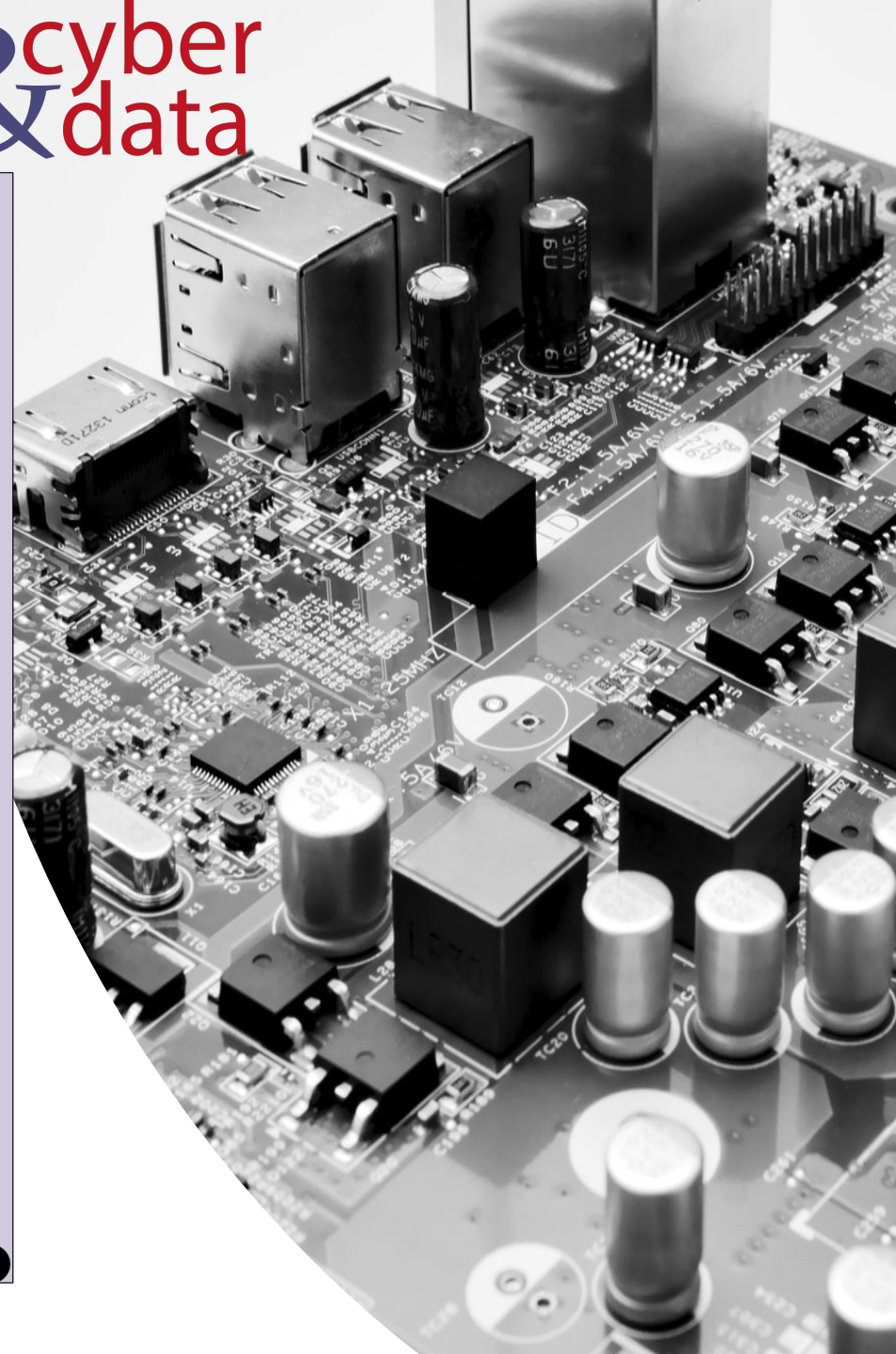
cyber & data

"From bits to information"

Stateful Firewalls

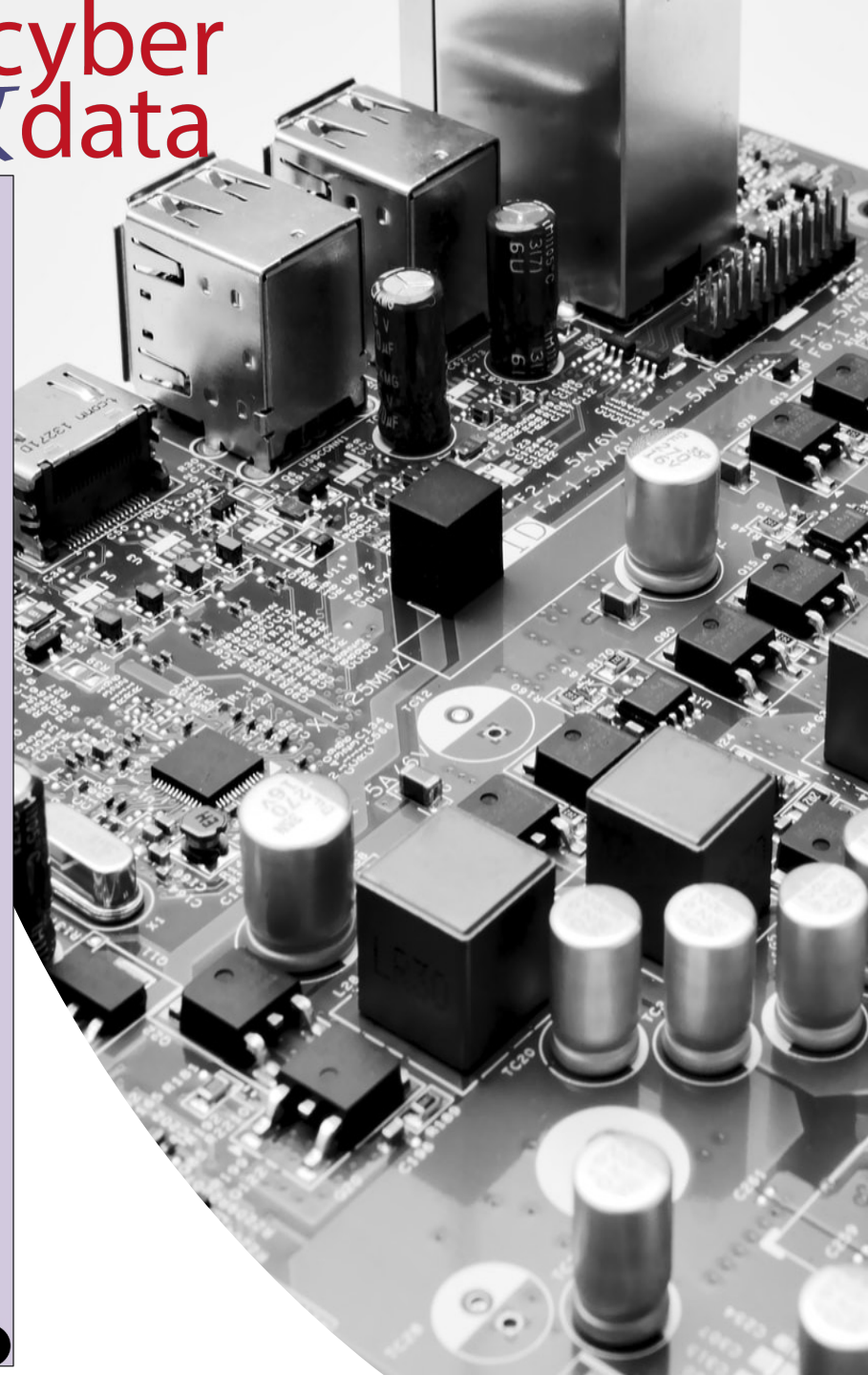
Layered Model



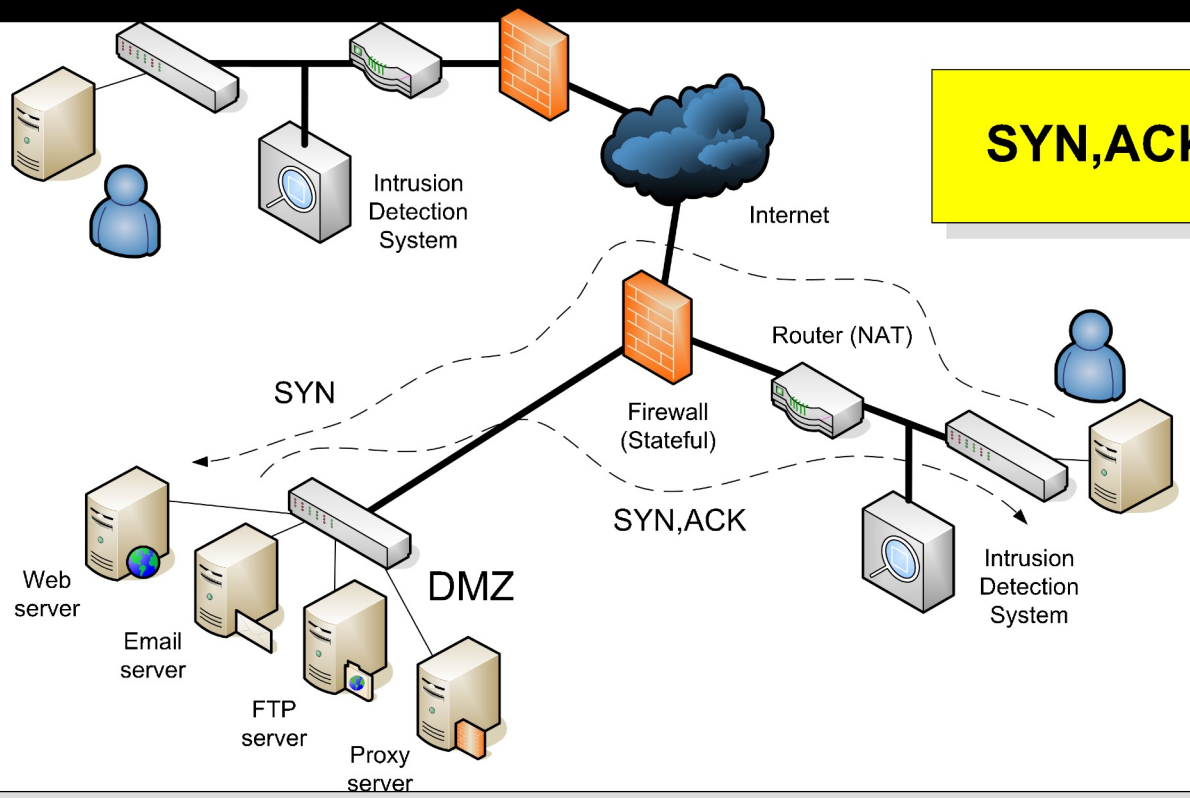


Layered Model

&cyber data

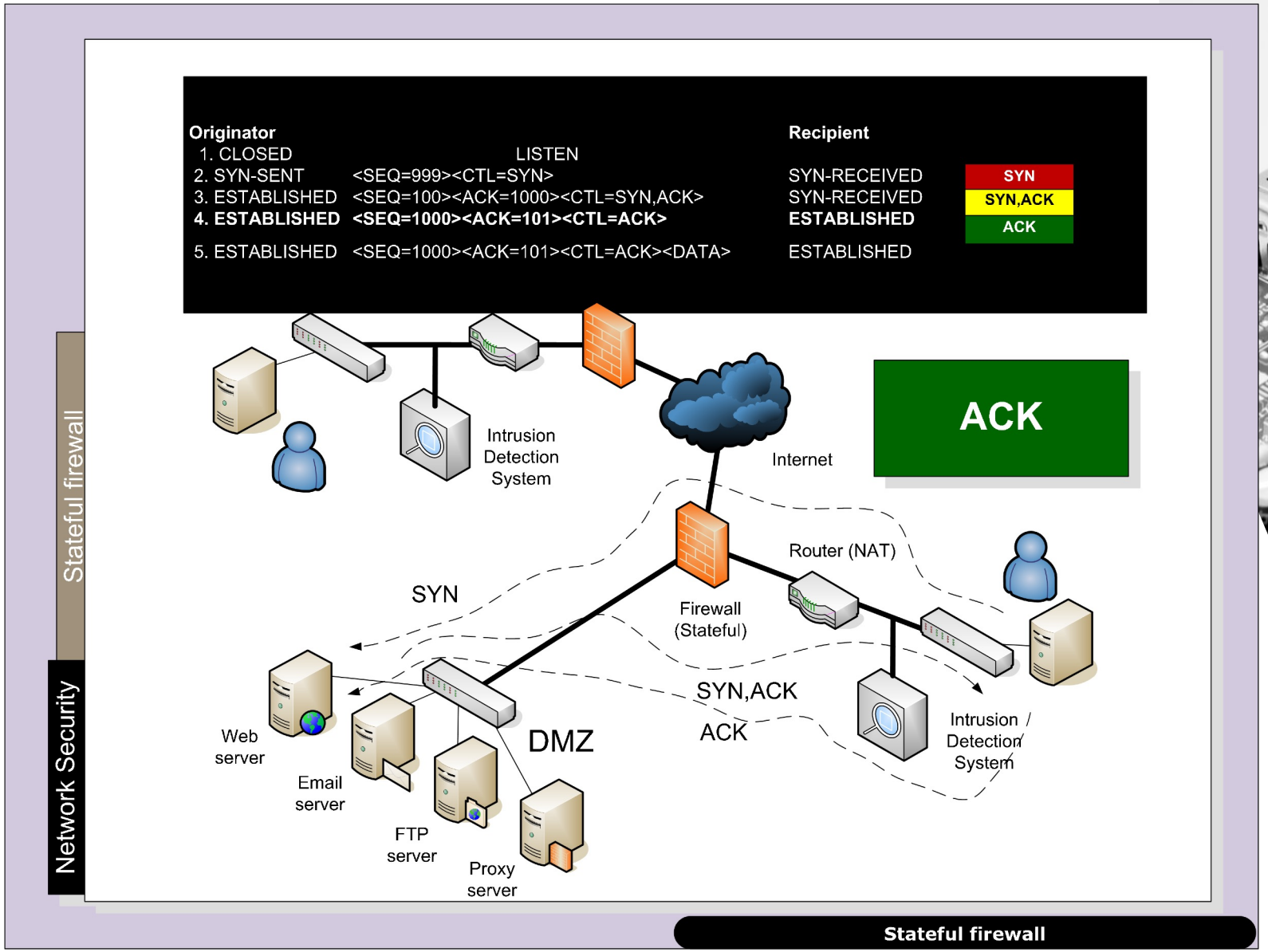


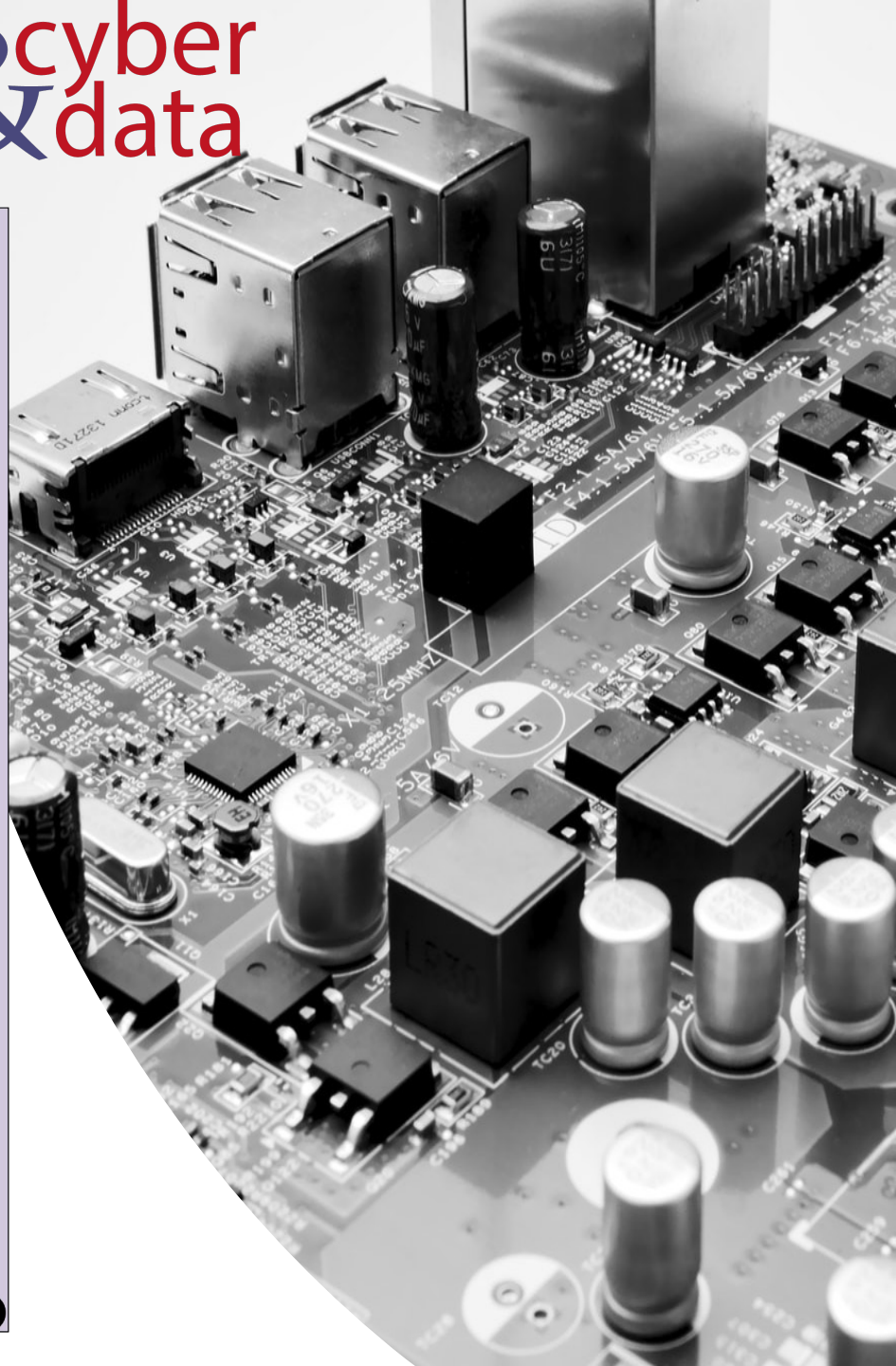
Originator		Recipient	
1. CLOSED		LISTEN	
2. SYN-SENT	<SEQ=999><CTL=SYN>	SYN-RECEIVED	SYN
3. ESTABLISHED	**<SEQ=100><ACK=1000><CTL=SYN,ACK>**	**SYN-RECEIVED**	**SYN,ACK**
4. ESTABLISHED	<SEQ=1000><ACK=101><CTL=ACK>	ESTABLISHED	
5. ESTABLISHED	<SEQ=1000><ACK=101><CTL=ACK><DATA>	ESTABLISHED	



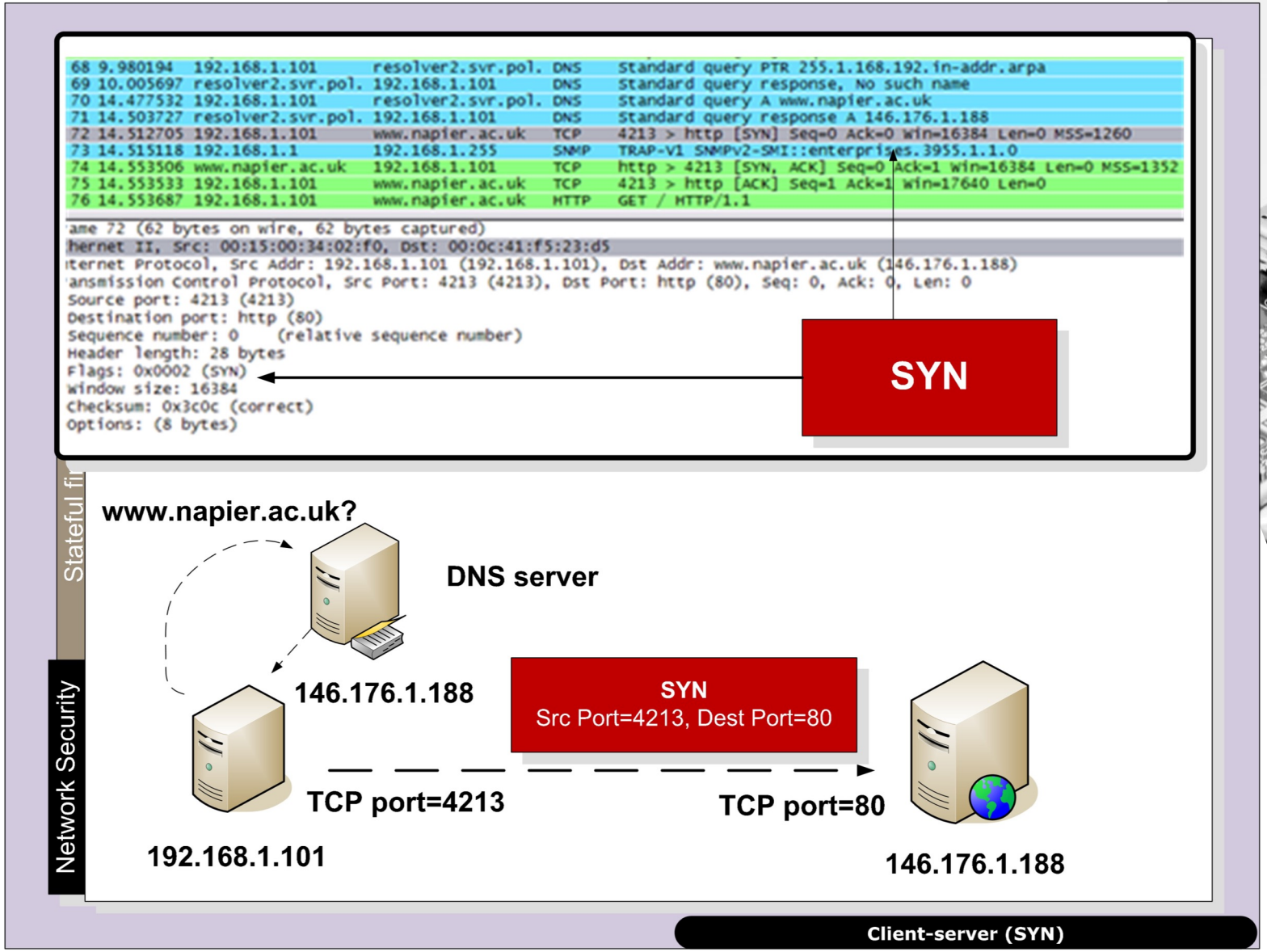
Stateful firewall

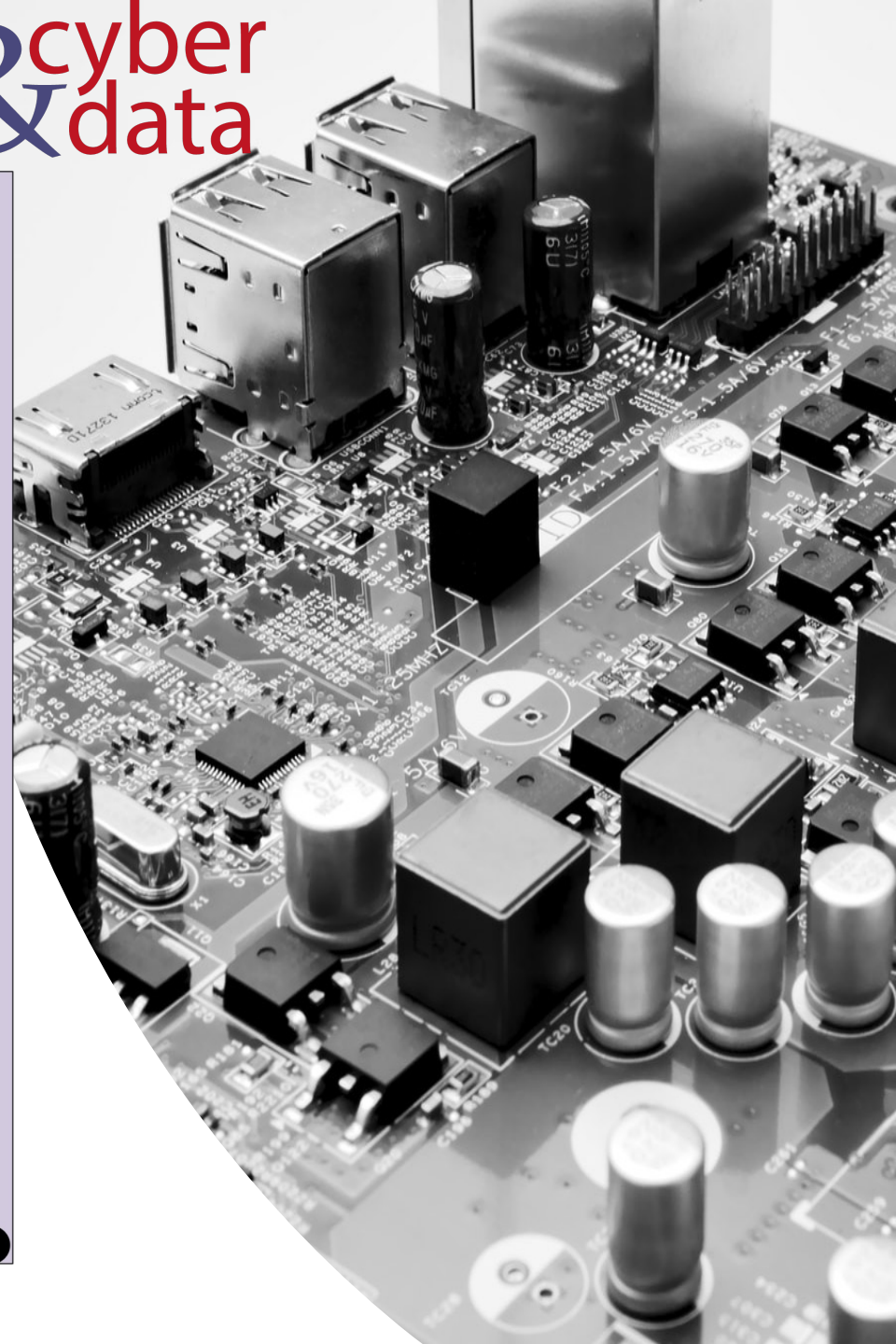
Layered Model





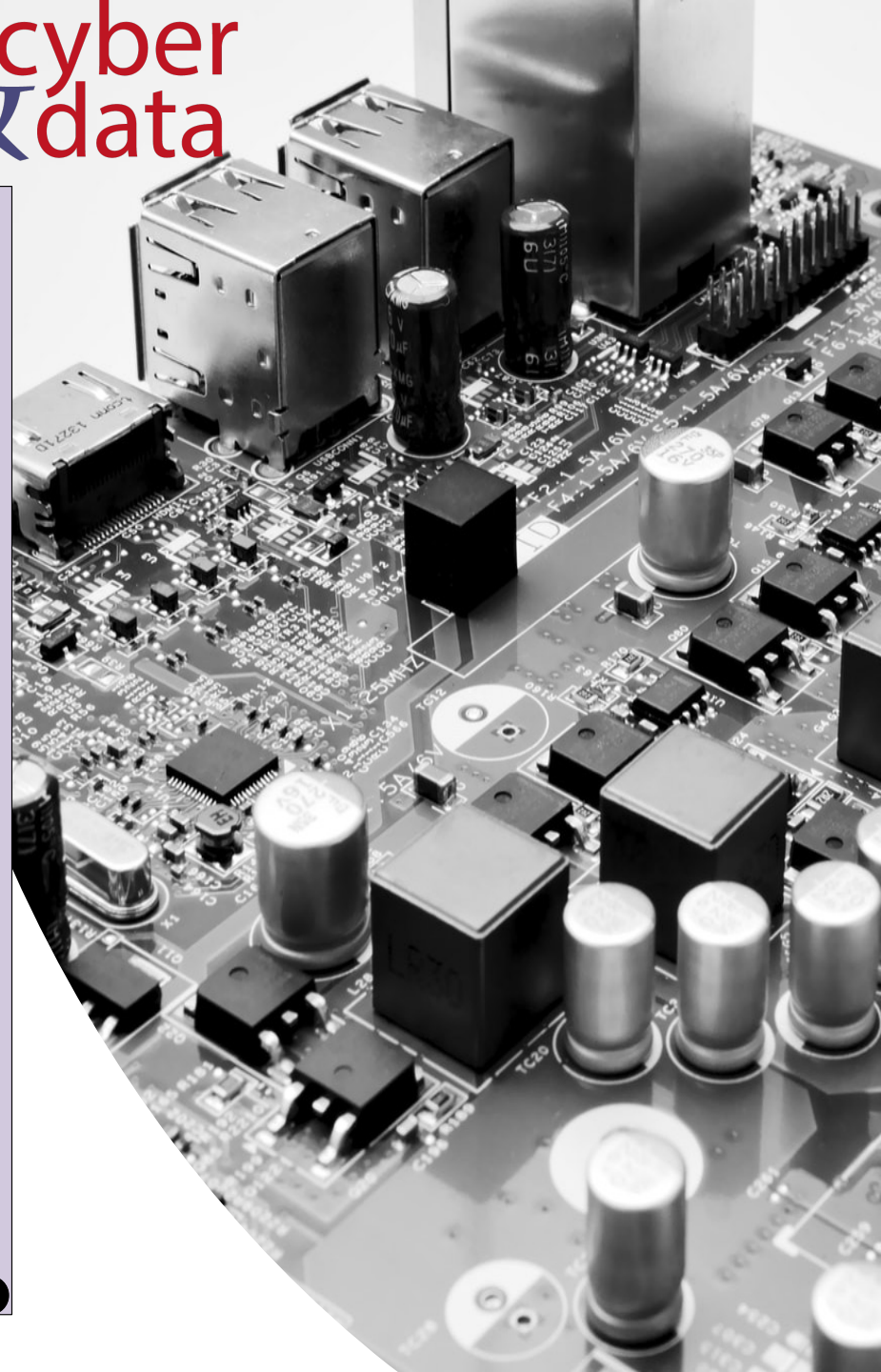
Layered Model





Layered Model

&cyber data



Stateful firewall

```
68 9.980194   192.168.1.101    resolver2.svr.pol. DNS    Standard query PTR 255.1.168.192.in-addr.arpa
69 10.005697  resolver2.svr.pol. 192.168.1.101    DNS    Standard query response, No such name
70 14.477532  192.168.1.101    resolver2.svr.pol. DNS    Standard query A www.napier.ac.uk
71 14.503727  resolver2.svr.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

rame 74 (62 bytes on wire, 62 bytes captured)
thernet II, Src: 00:0c:41:f5:23:d5, Dst: 00:15:00:34:02:f0
nternet Protocol, Src Addr: www.napier.ac.uk (146.176.1.188), Dst Addr: 192.168.1.101 (192.168.1.101)
ransmission Control Protocol, Src Port: http (80), Dst Port: 4213 (4213), Seq: 0, Ack: 1, Len: 0
 Source port: http (80)
 Destination port: 4213 (4213)
 Sequence number: 0    (relative sequence number)
 Acknowledgement number: 1    (relative ack number)
 Header length: 28 bytes
 Flags: 0x0012 (SYN, ACK)
 Window size: 16384
 Checksum: 0xa97c (correct)
 Options: (8 bytes)
 [SEQ/ACK analysis]
```

SYN,ACK

Network Security

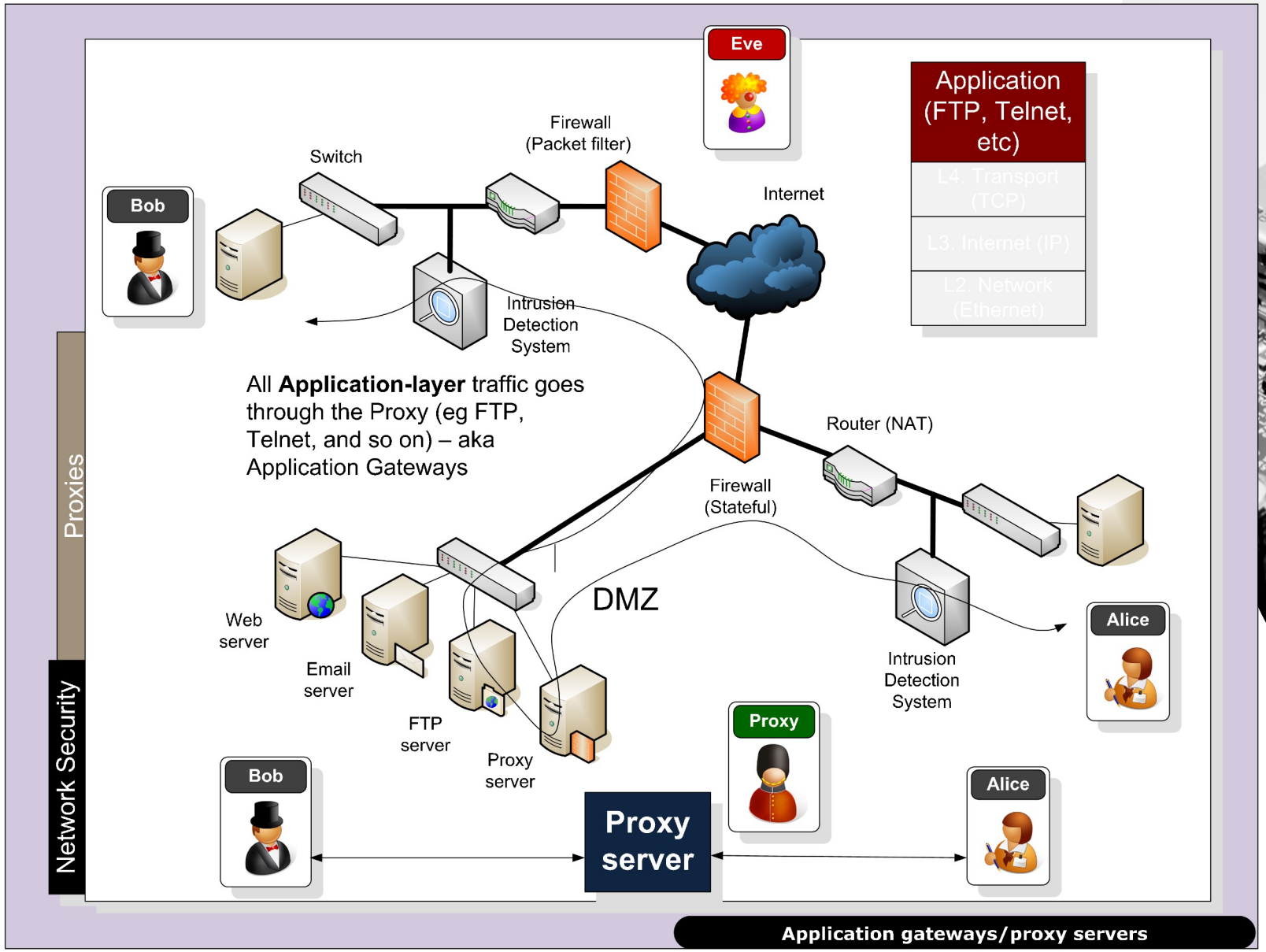
```
69 10.005697  resolver2.svr.pol. 192.168.1.101    DNS    Standard query response, No such name
70 14.477532  192.168.1.101    resolver2.svr.pol. DNS    Standard query A www.napier.ac.uk
71 14.503727  resolver2.svr.pol. 192.168.1.101    DNS    Standard query response A 146.176.1.188
72 14.512705  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

rame 75 (54 bytes on wire, 54 bytes captured)
thernet II, Src: 00:15:00:34:02:f0, Dst: 00:0c:41:f5:23:d5
nternet Protocol, Src Addr: 192.168.1.101 (192.168.1.101), Dst Addr: www.napier.ac.uk (146.176.1.188)
ransmission Control Protocol, Src Port: 4213 (4213), Dst Port: http (80), Seq: 1, Ack: 1, Len: 0
 Source port: 4213 (4213)
 Destination port: http (80)
 Sequence number: 1    (relative sequence number)
 Acknowledgement number: 1    (relative ack number)
 Header length: 20 bytes
 Flags: 0x0010 (ACK)
 Window size: 17640
 Checksum: 0xd0ec (correct)
 [SEQ/ACK analysis]
```

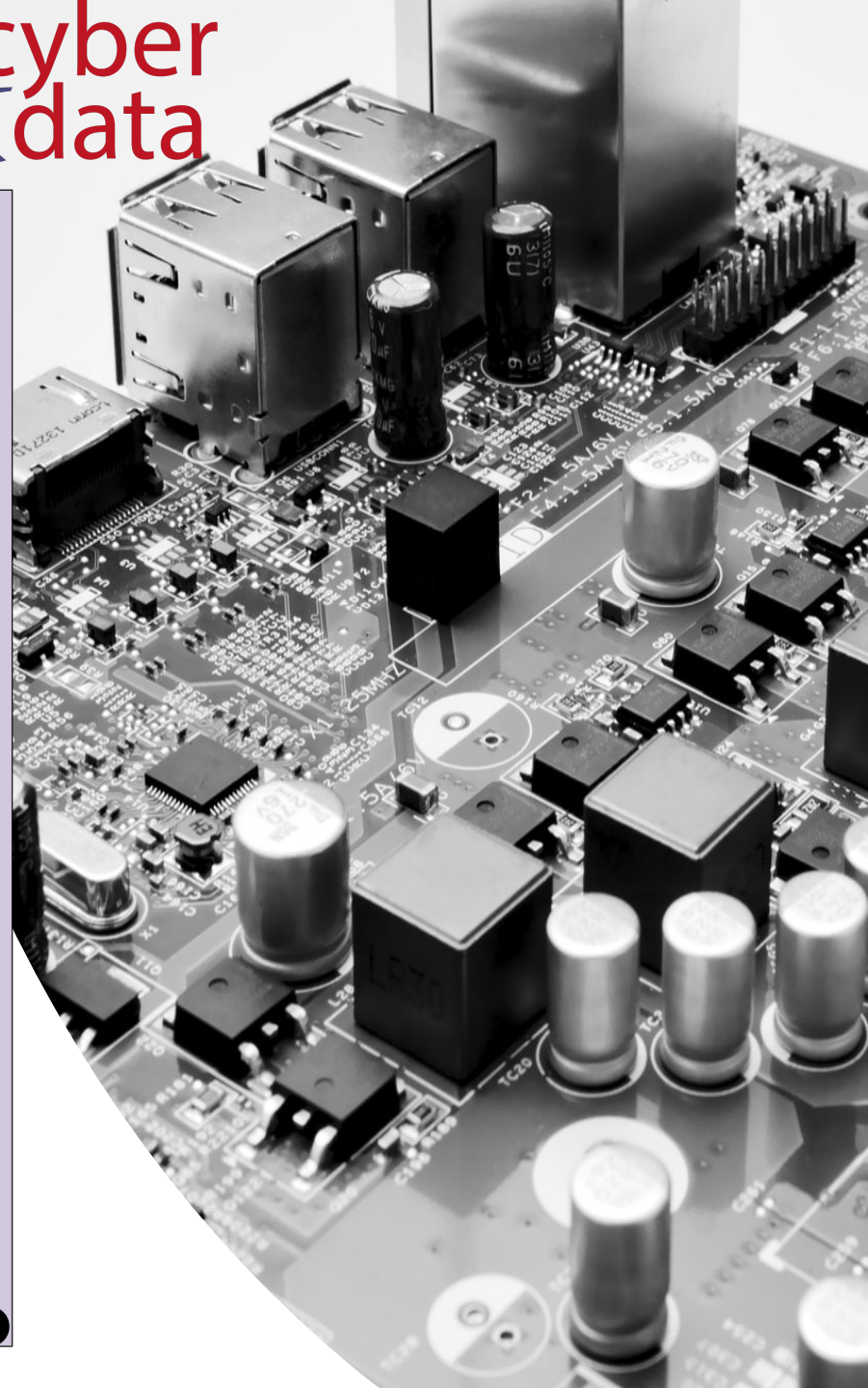
ACK

"From bits to information"

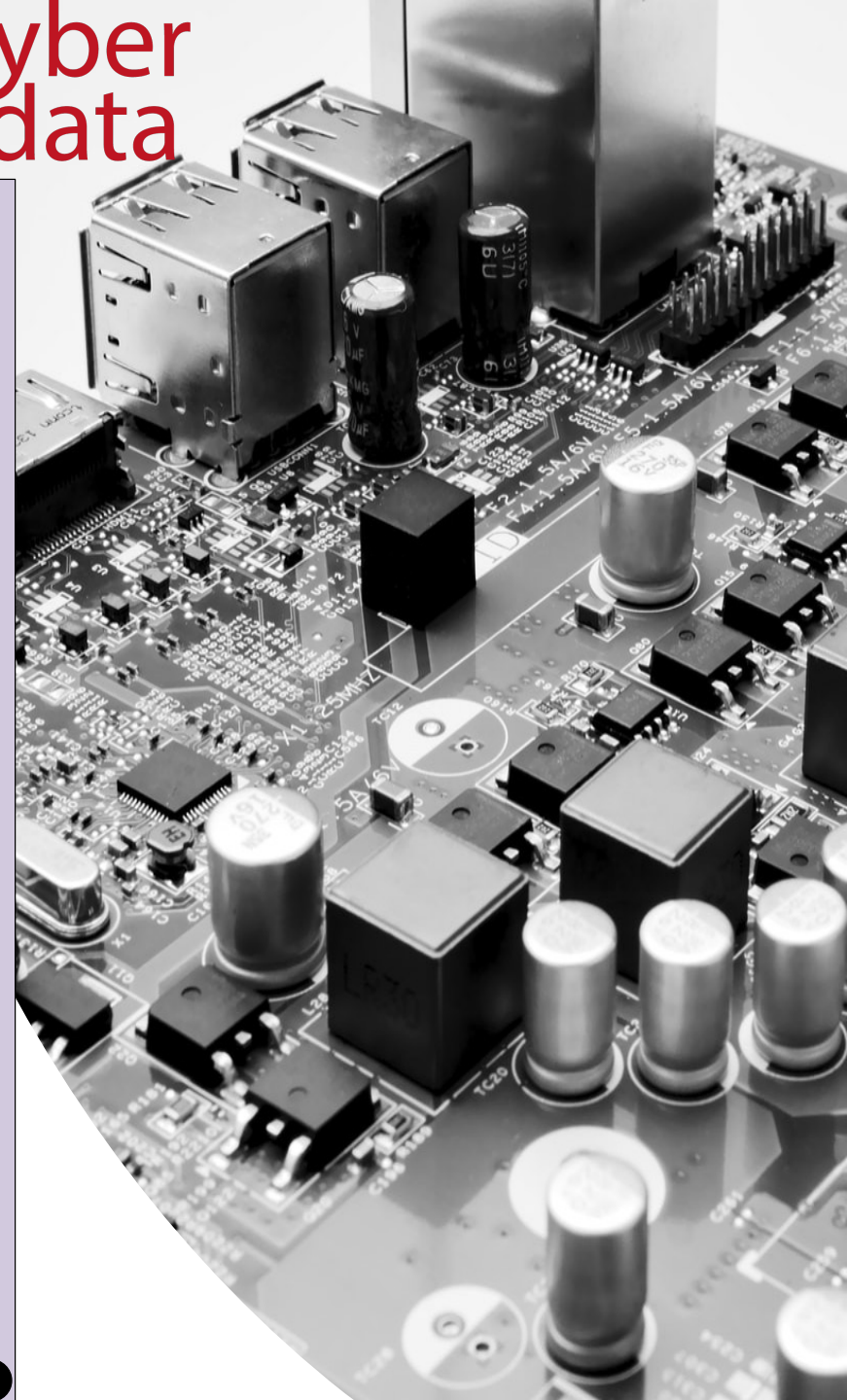
Proxies

Layered Model





Layered Model



Eve

Communications on certain application protocols (such as HTTP for Web) go through the proxy.

Bob

Proxy

Trusted

Untrusted

Alice

Proxies

Network Security

Proxy (Application Gateway):

Advantages:

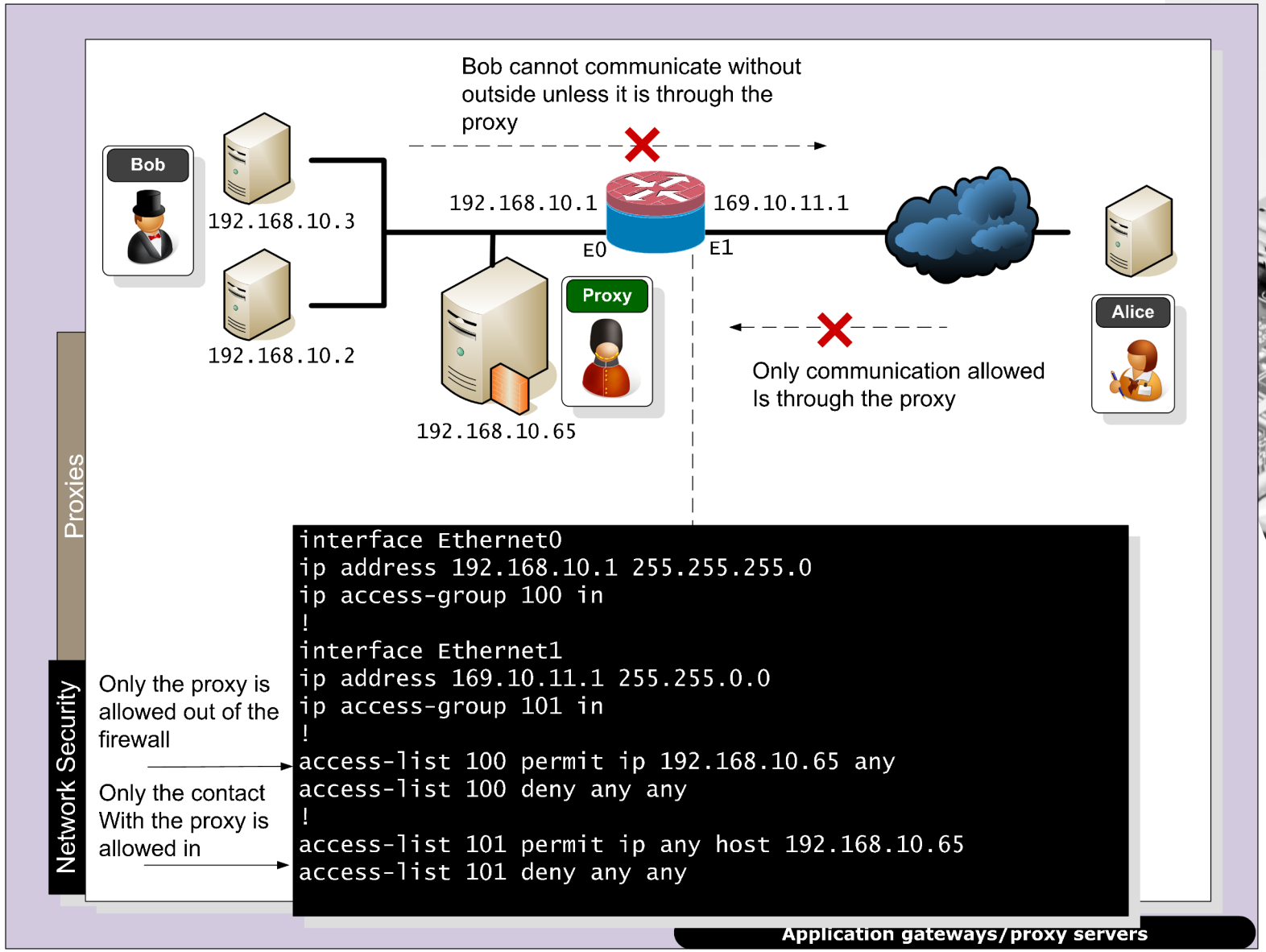
- User-oriented authentication.
- User-oriented logging.
- User-oriented accounting.

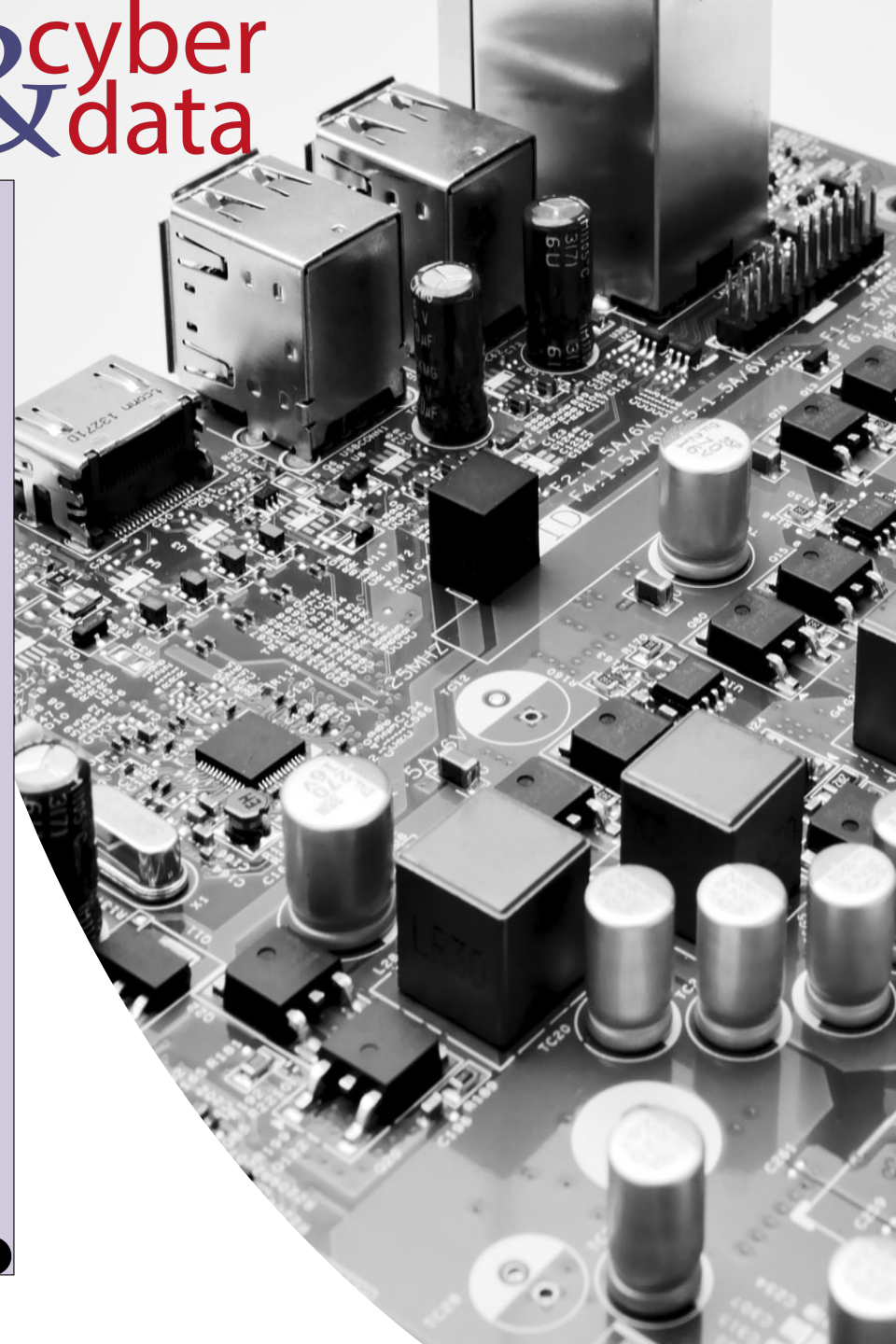
Disadvantages:

- Build specifically for each application (although the SOCKS protocol has been designed, which is an all-one proxy).
- Slower than without proxy.
- Central point-of-failure

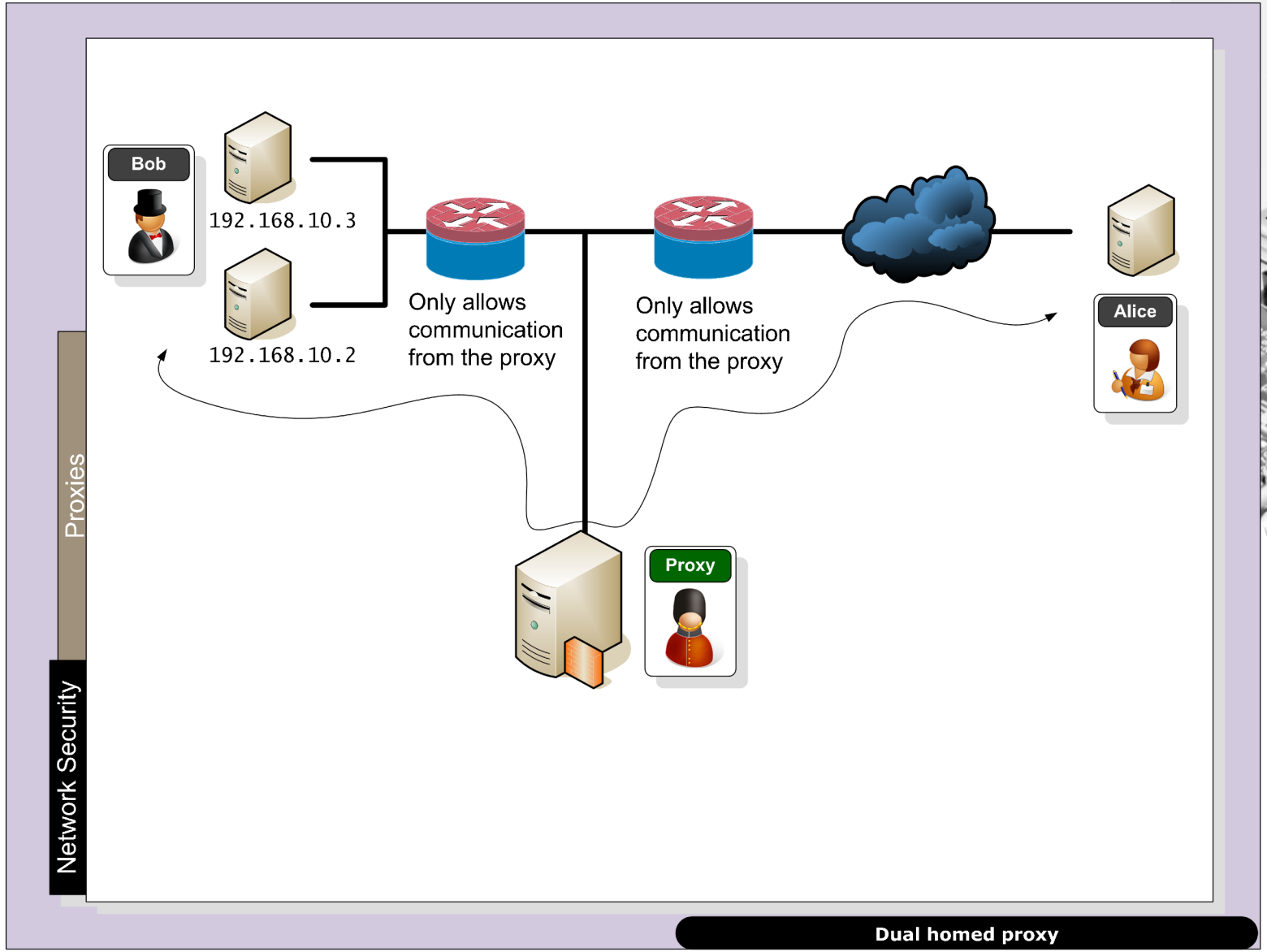
Application gateways/proxy servers

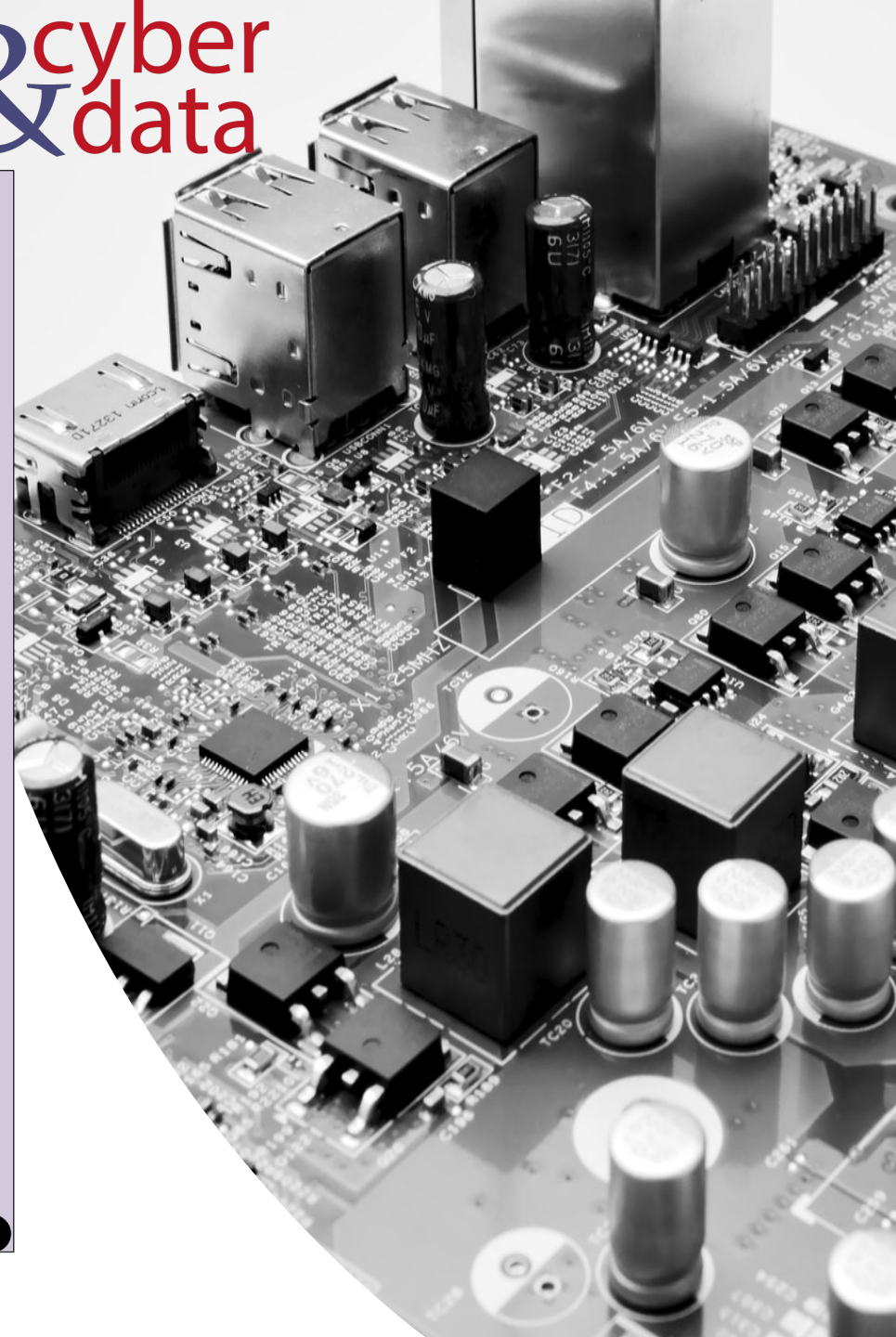
Layered Model



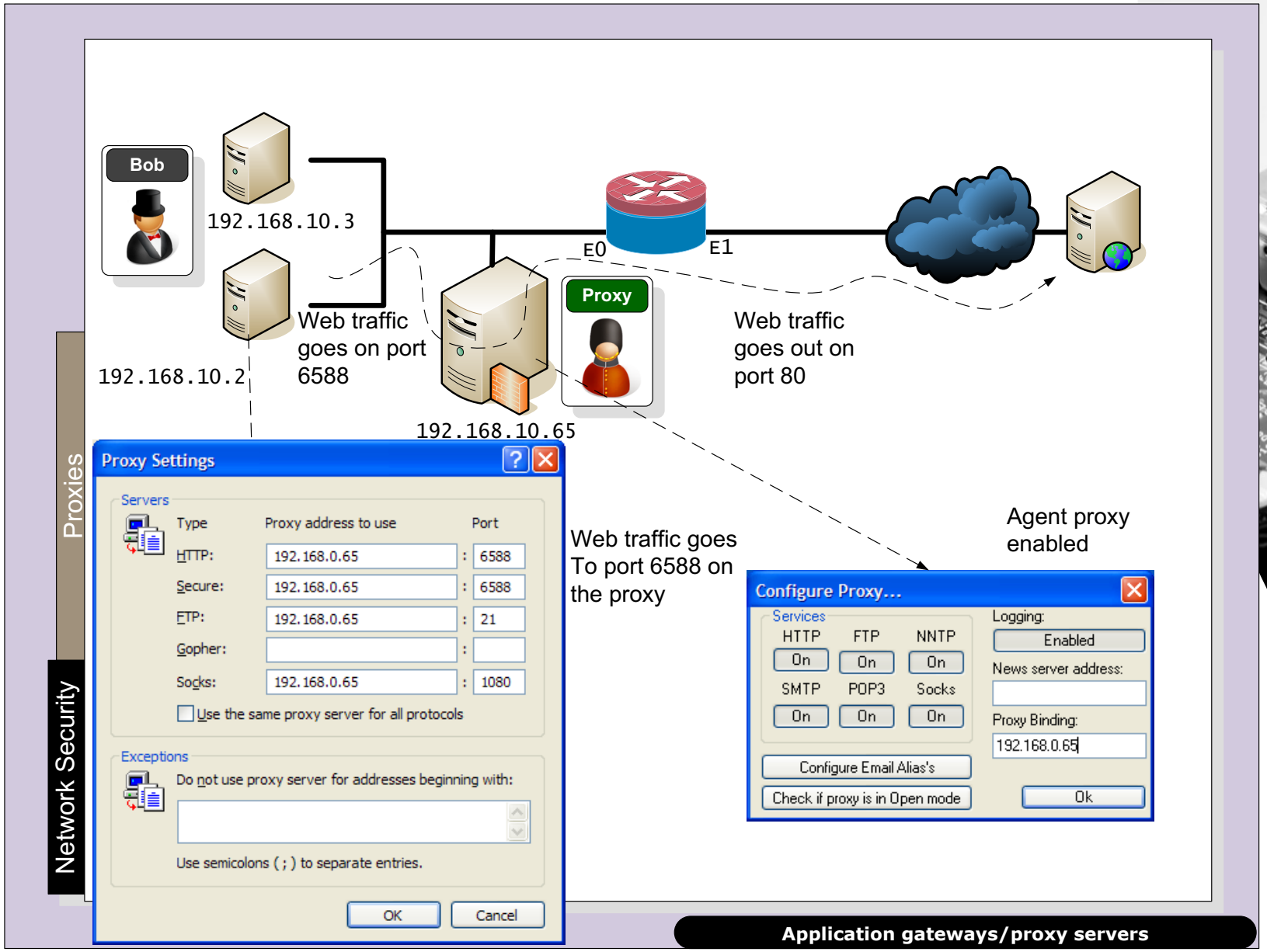


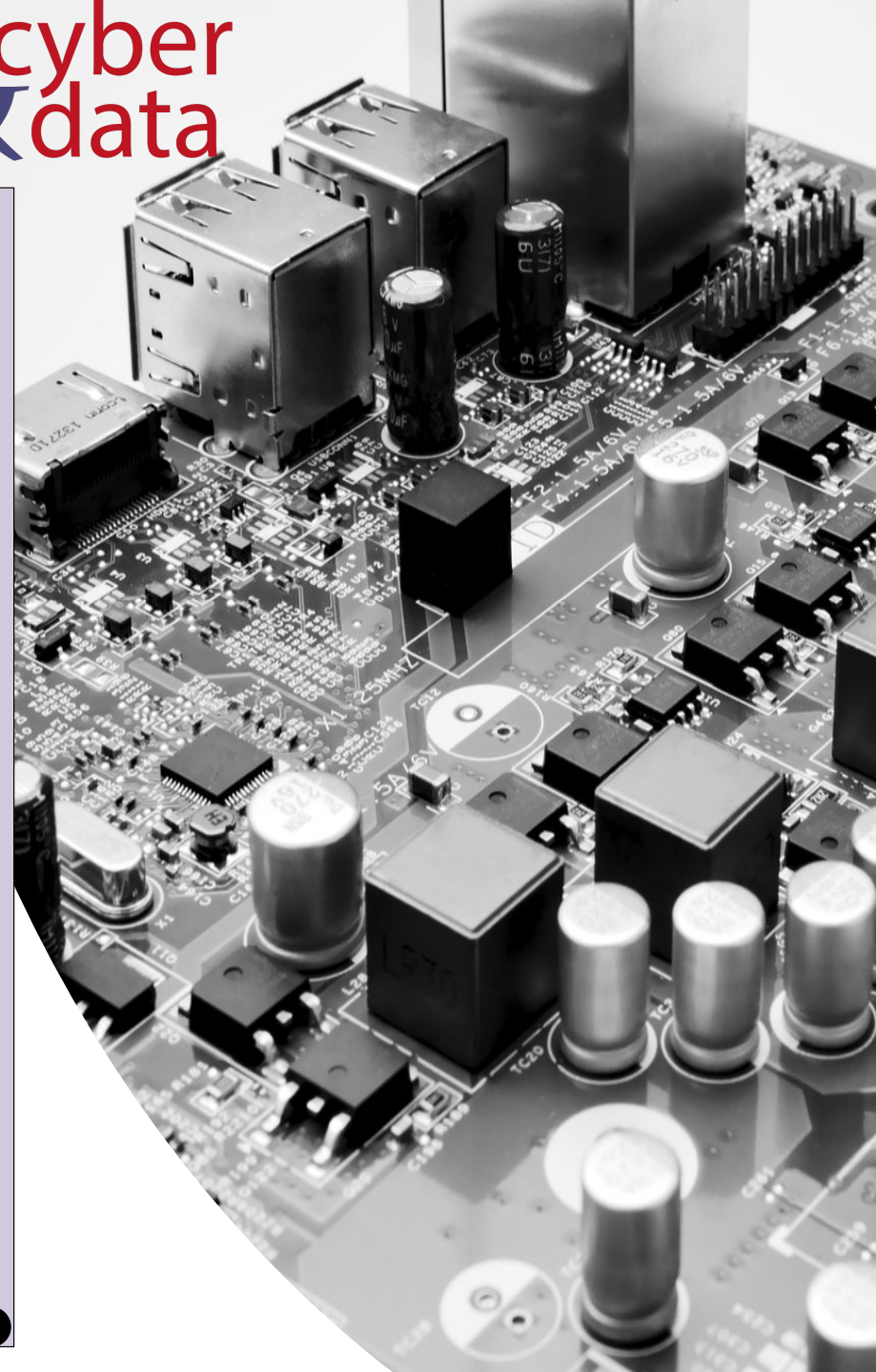
Layered Model



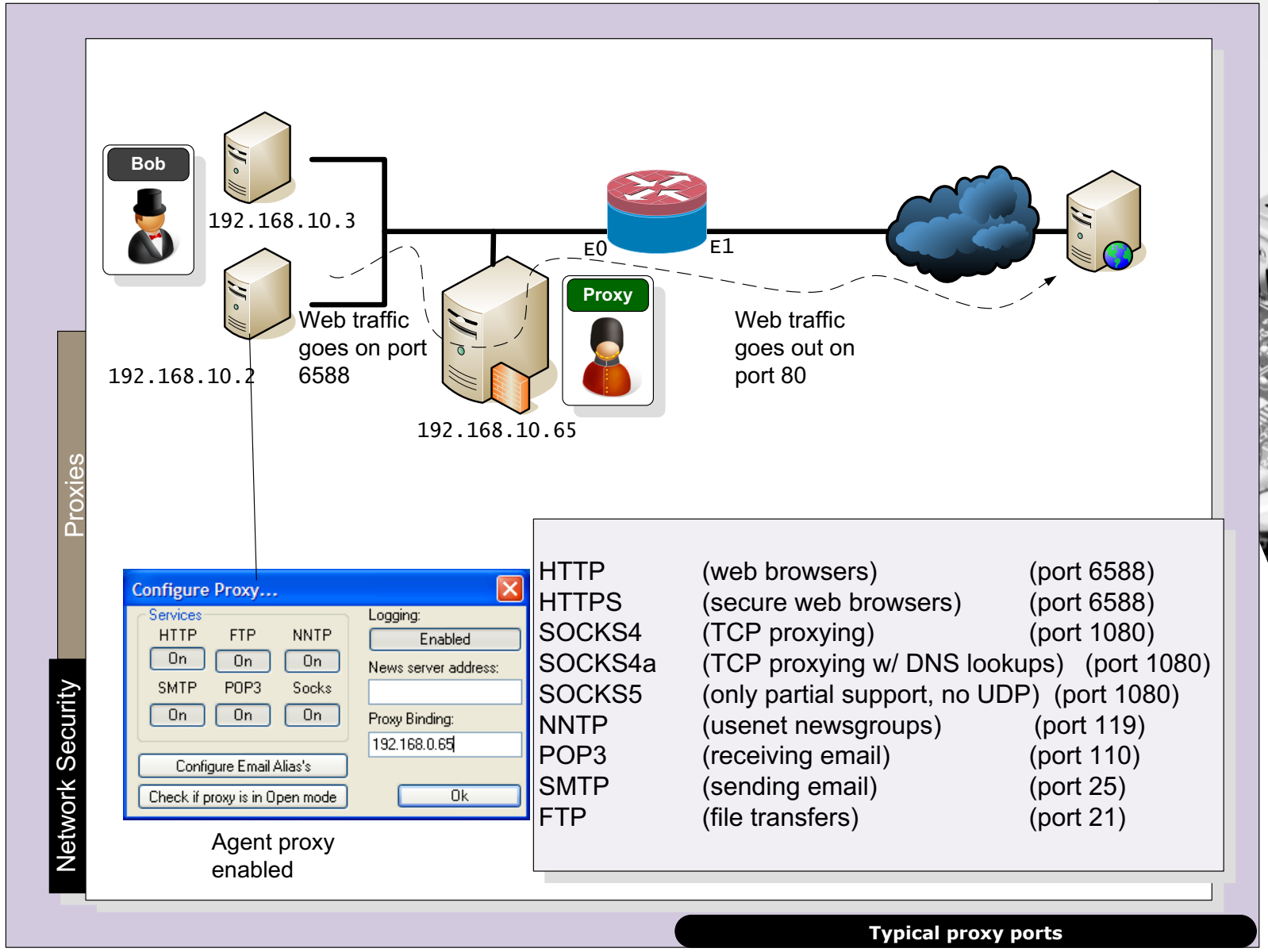


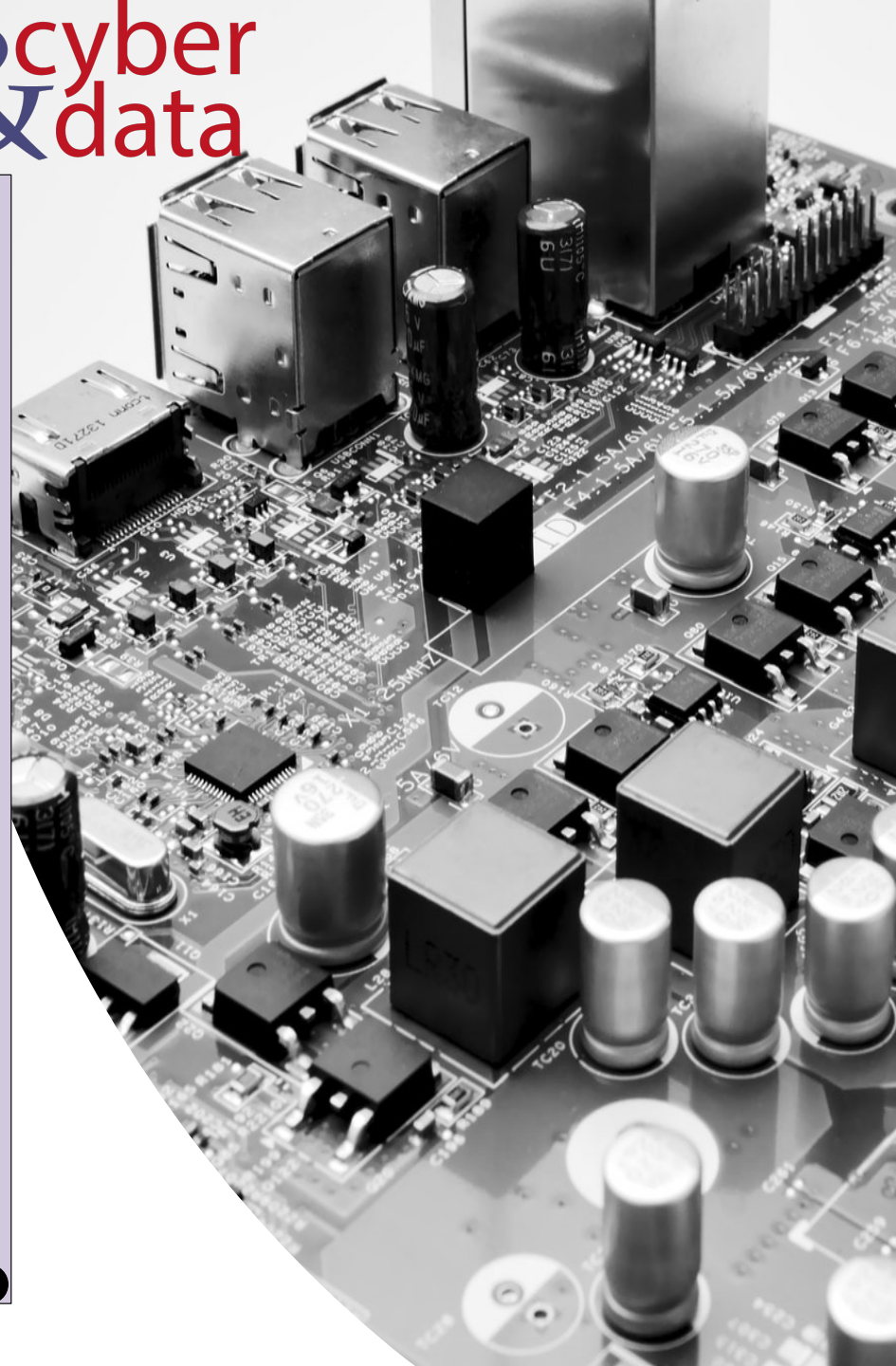
Layered Model





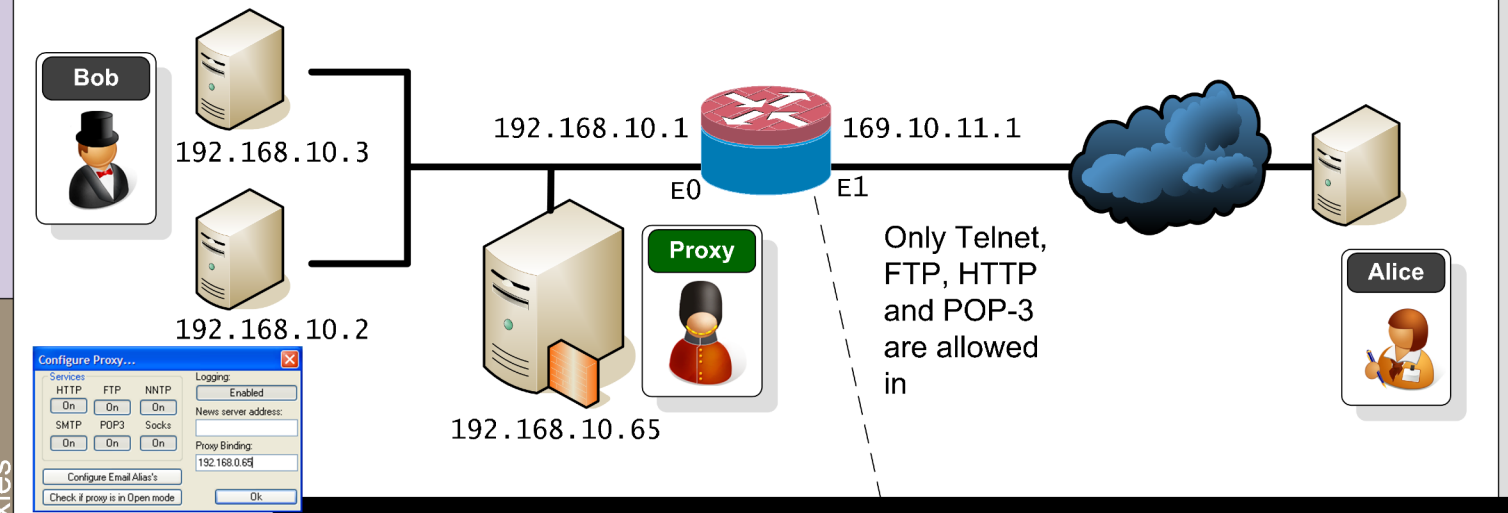
Layered Model





Layered Model

&cyber data



Proxies

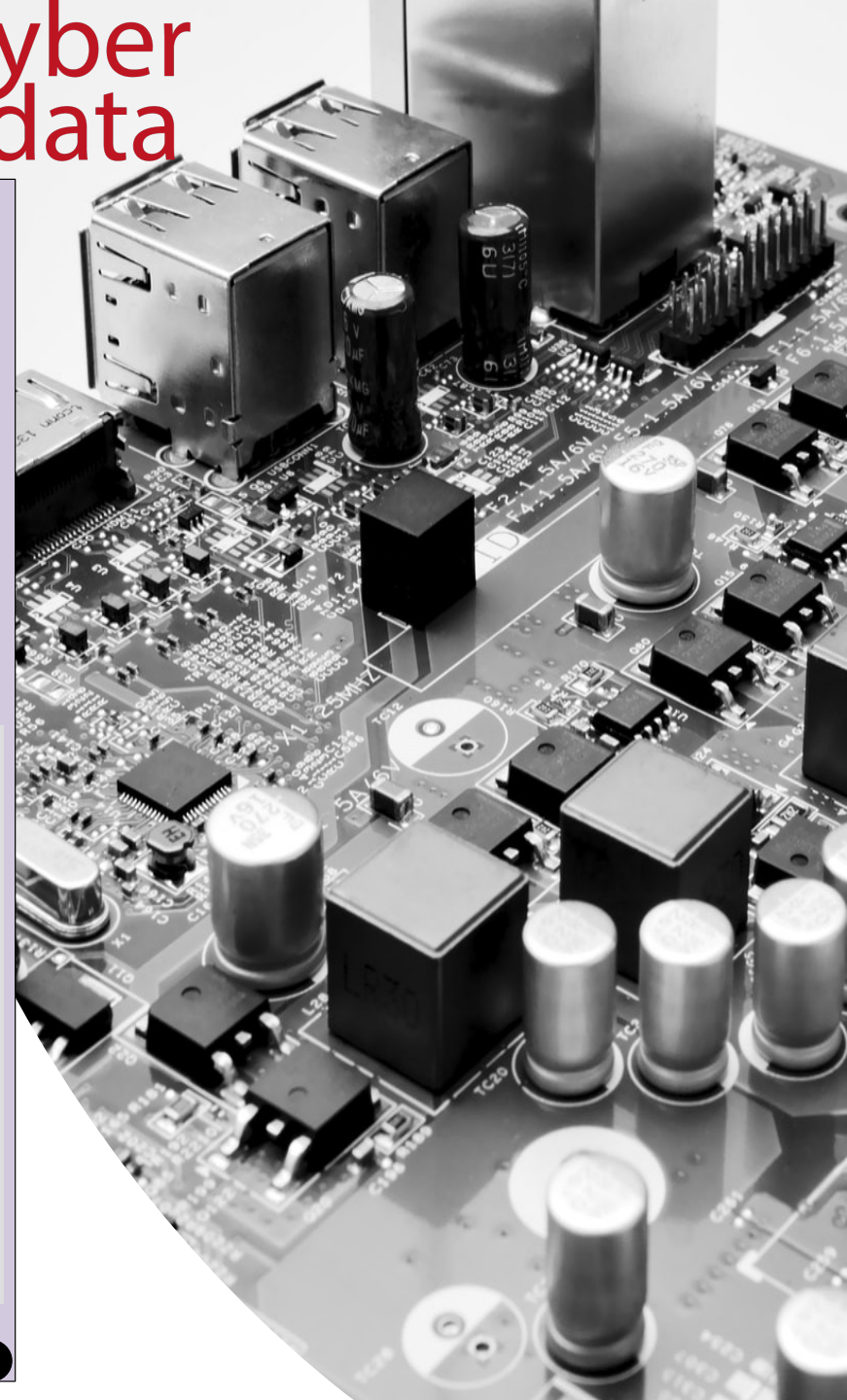
Network Security

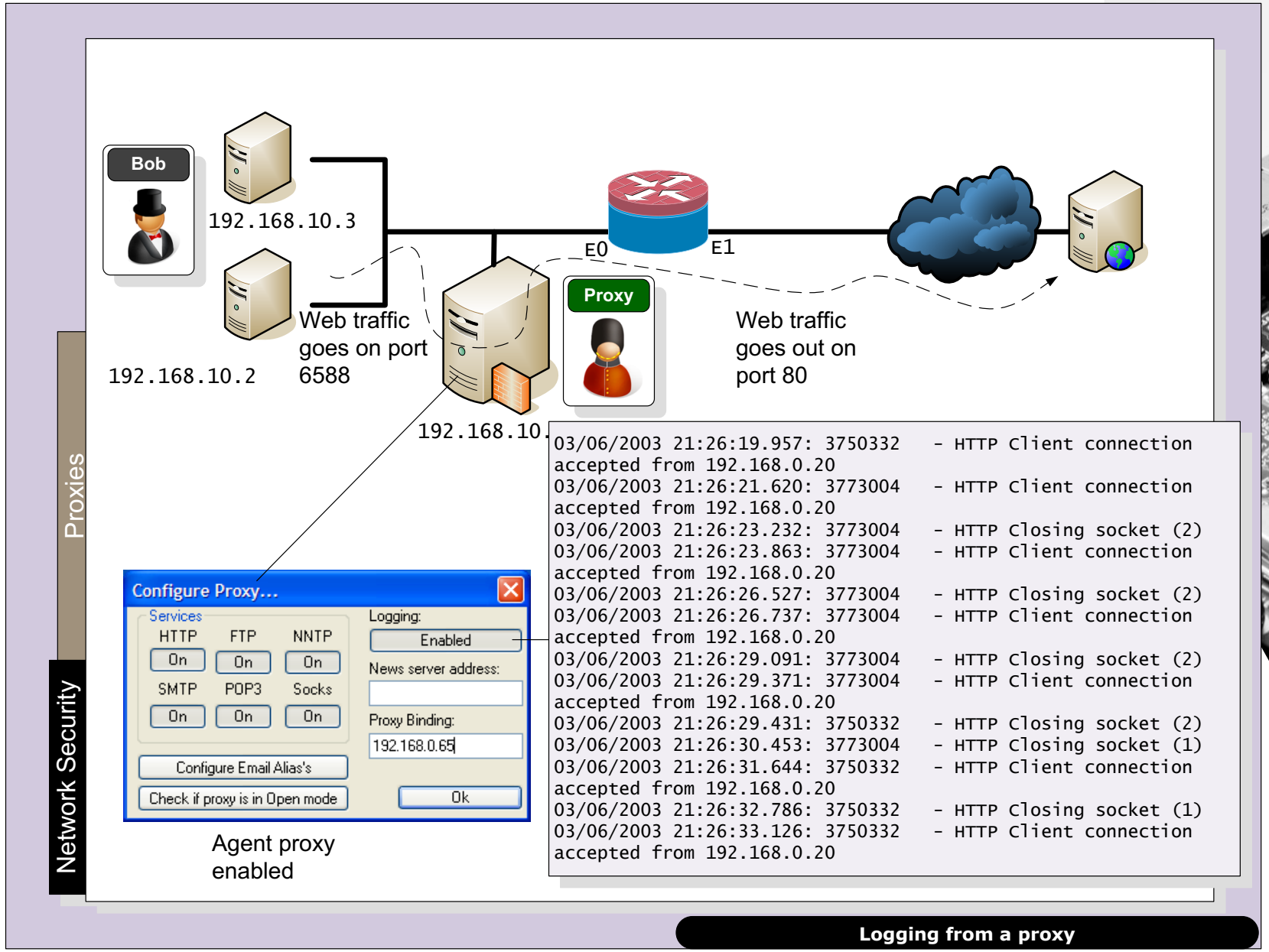
Only traffic on certain ports are allowed, and only if they are destined for the proxy

```
interface Ethernet1
ip address 169.10.11.1 255.255.0.0
ip access-group 101 in
!
access-list 101 permit tcp any any eq telnet host 192.168.10.65
access-list 101 permit tcp any any eq ftp host 192.168.10.65
access-list 101 permit tcp any any eq http host 192.168.10.65
access-list 101 permit tcp any any eq pop3 host 192.168.10.65
access-list 101 deny any any
```

Application gateways/proxy servers

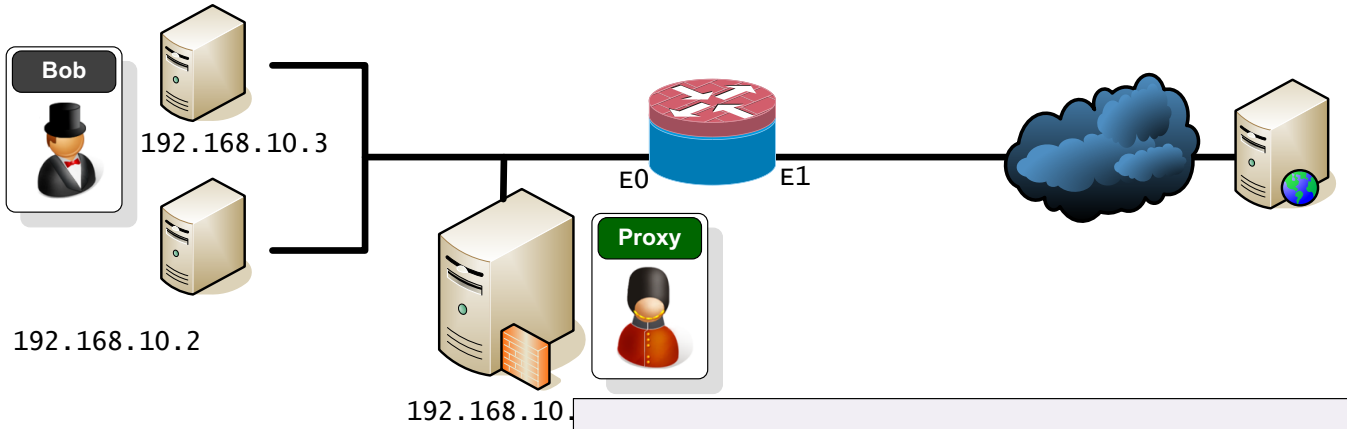
Layered Model





Logging from a proxy

Layered Model



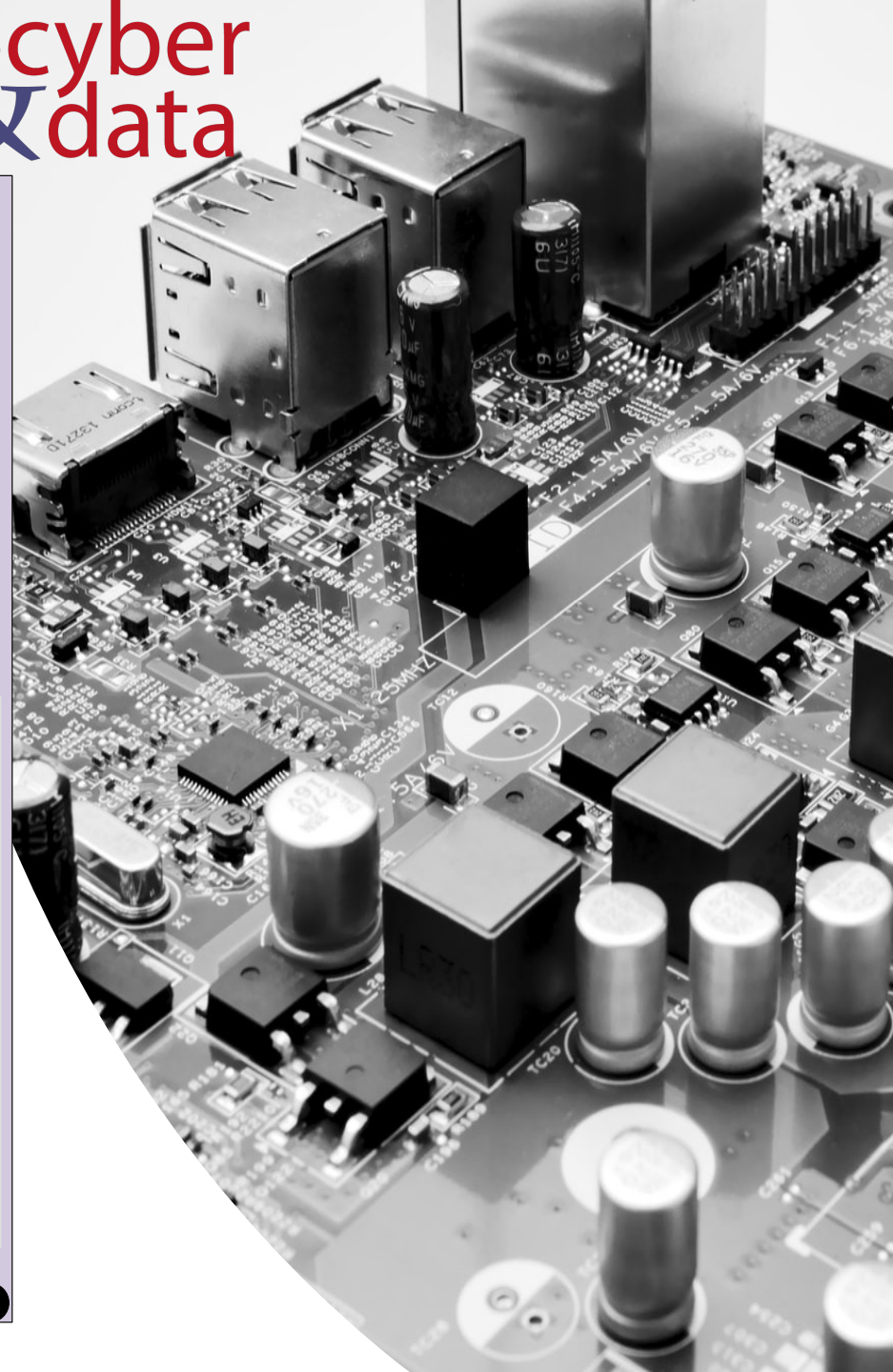
Proxies

Network Security

Proxy allows:

- The hosts to be hidden from the outside.
- Private addresses can be used for the internal network.
- Logging of data packets.
- User-level authentication, where users may require a username and a password.
- Isolation of nodes inside the network, as they cannot be directly contacted.

Strengths of a proxy



cyber & data

"From bits to information"

Defence Systems, Policies and Risks