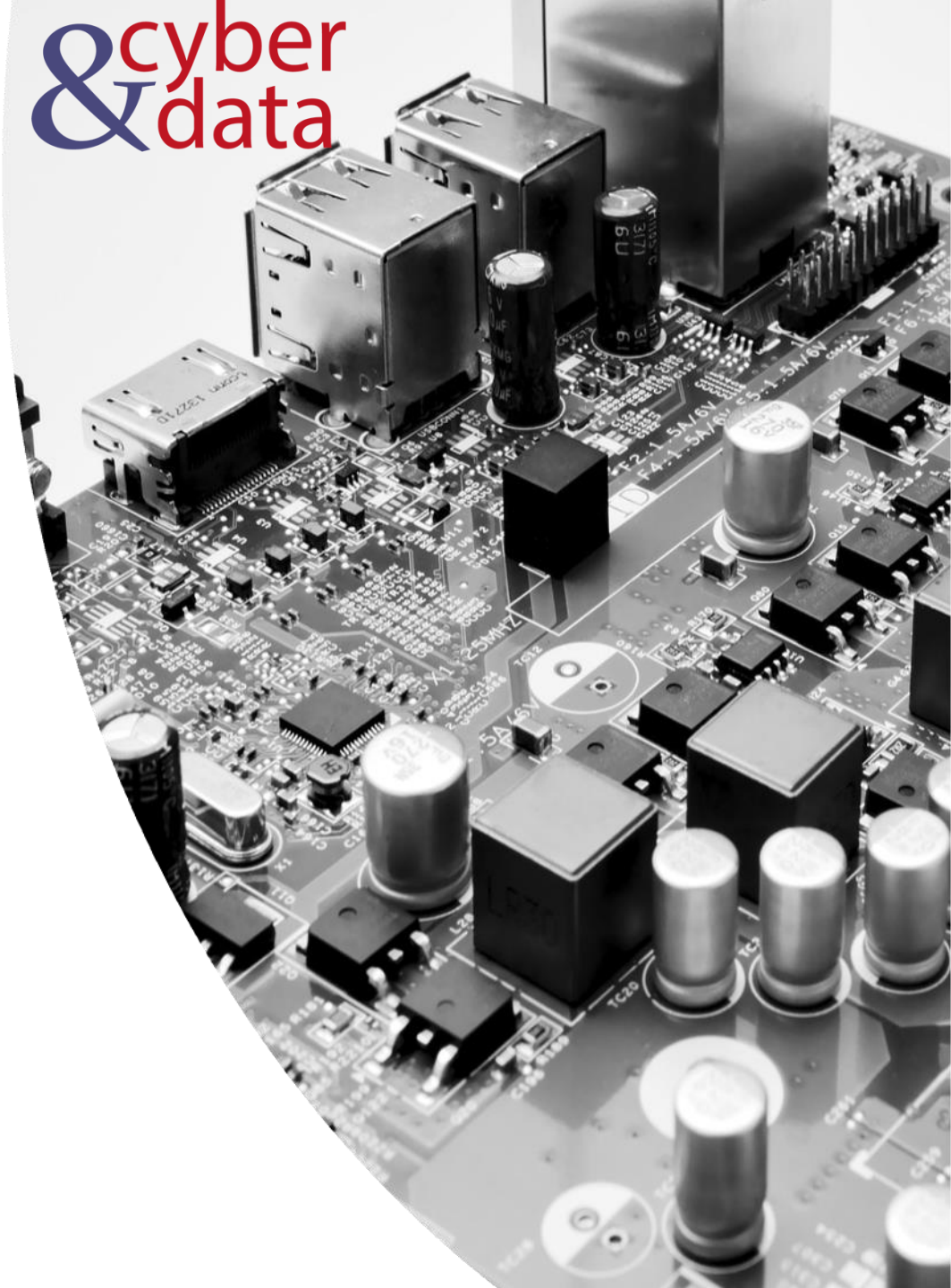
cyber & data

"From bits to information"

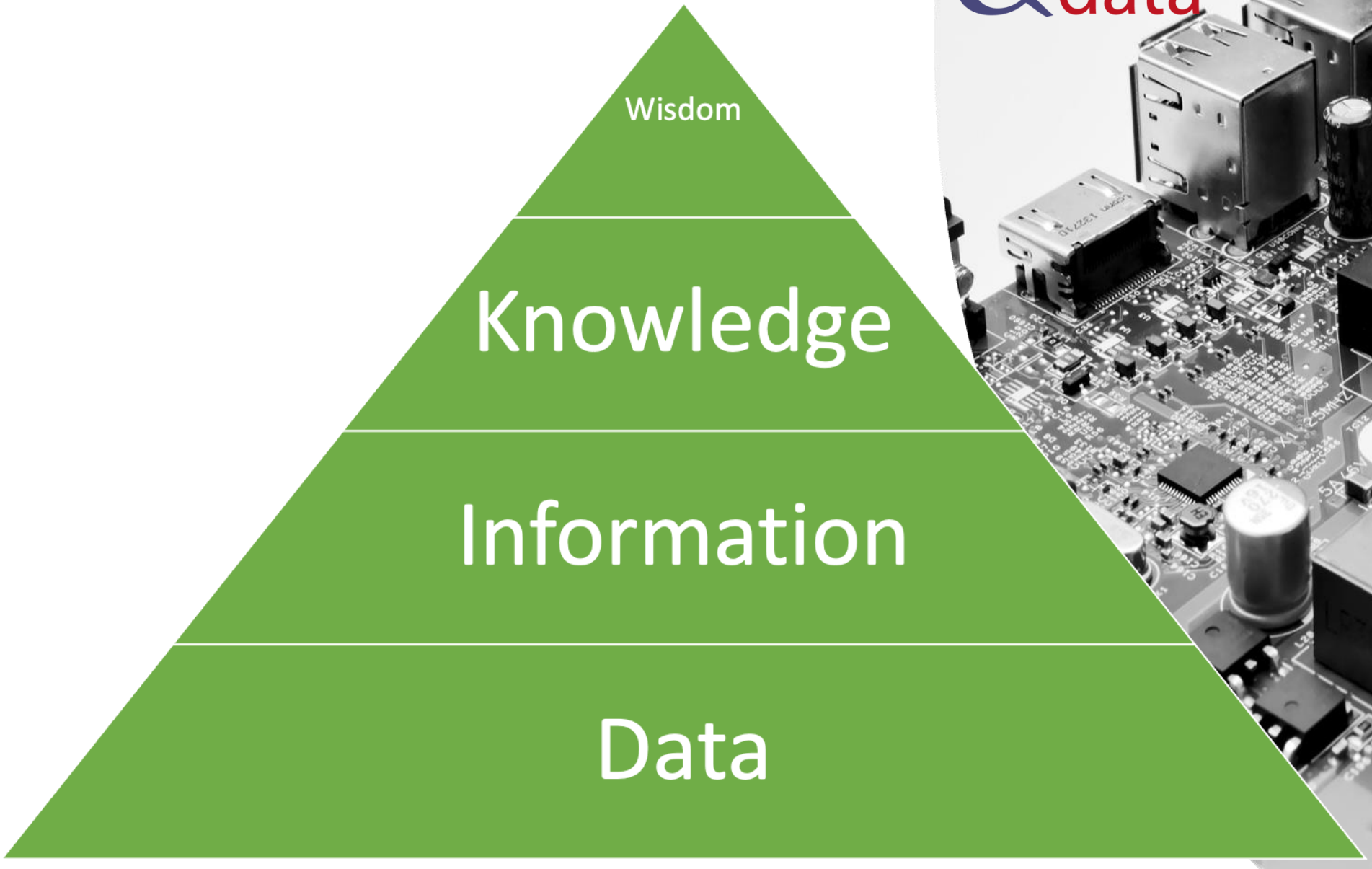
Defence Systems, Policies and Risks

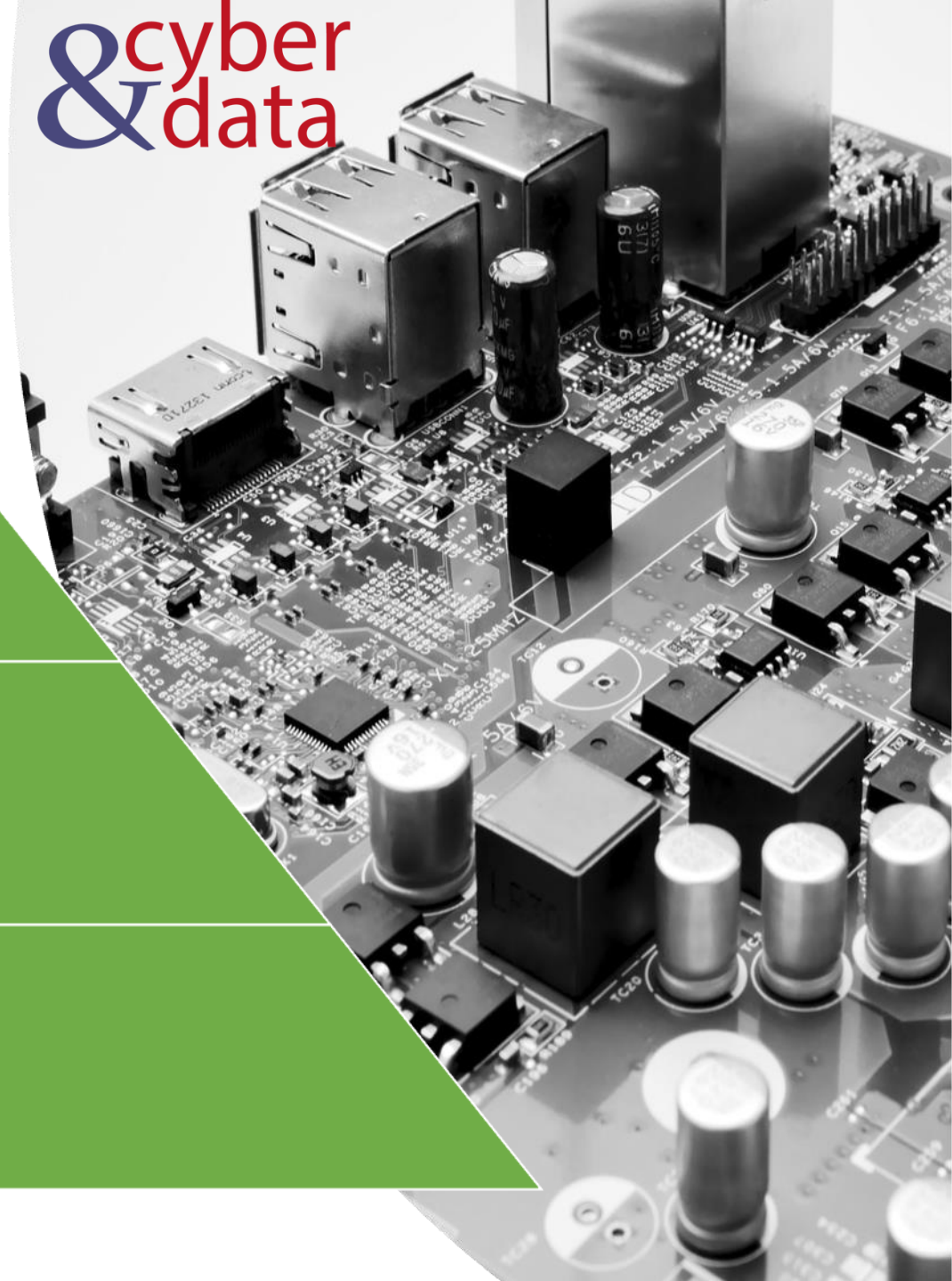
Outline

- Basics: Security Policy, Risk and Benefits.
- Kill Chain Model, MITRE ATT&CK and EMB3D.
- Basic Terms: Defence in Depth, IDS.
- Secure Infrastructures.
- Cryptography Basics.
- Secure Enclaves.
- Network Security: NAT, Stateful Firewalls.



Data to Wisdom



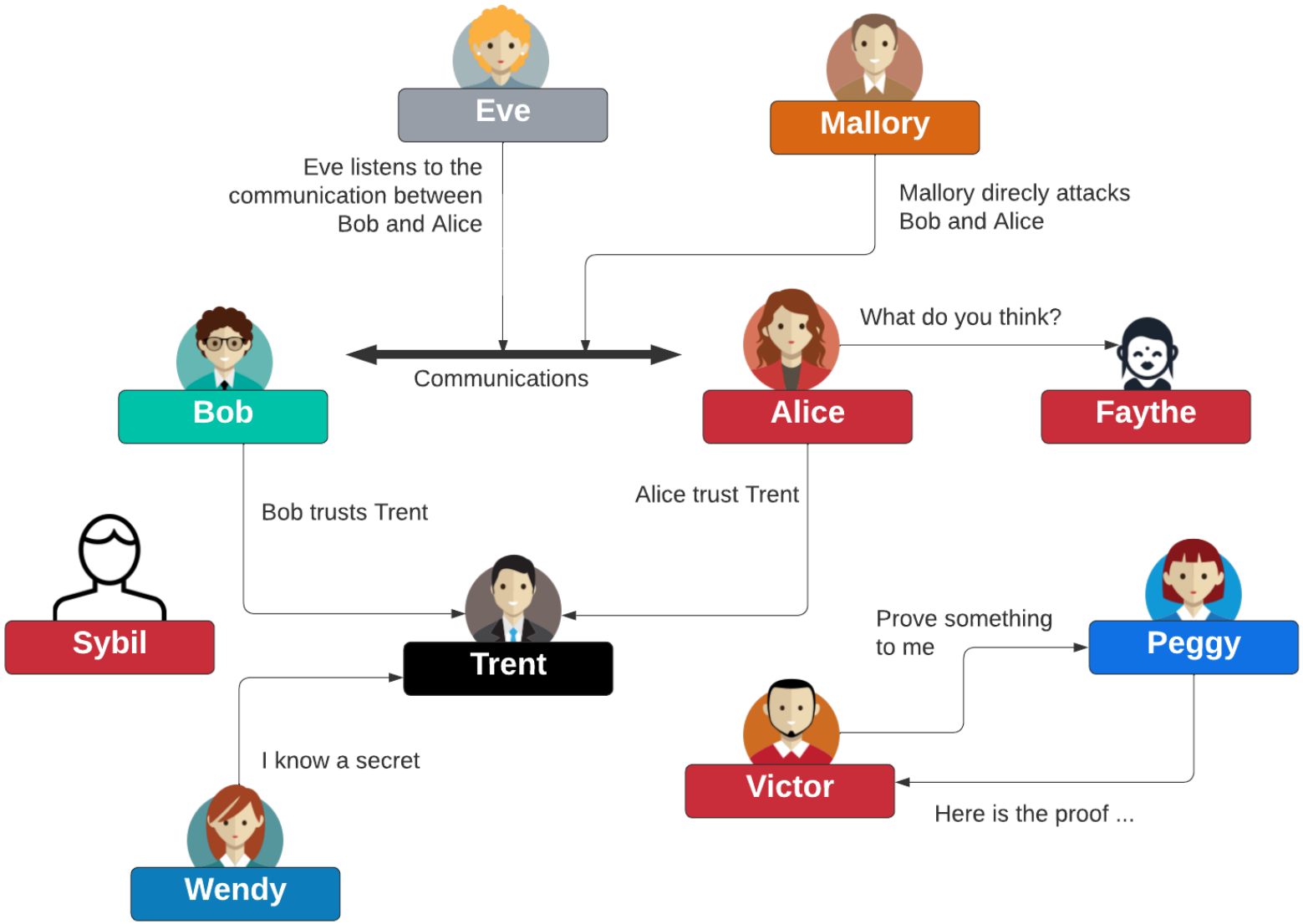


cyber & data

"From bits to information"

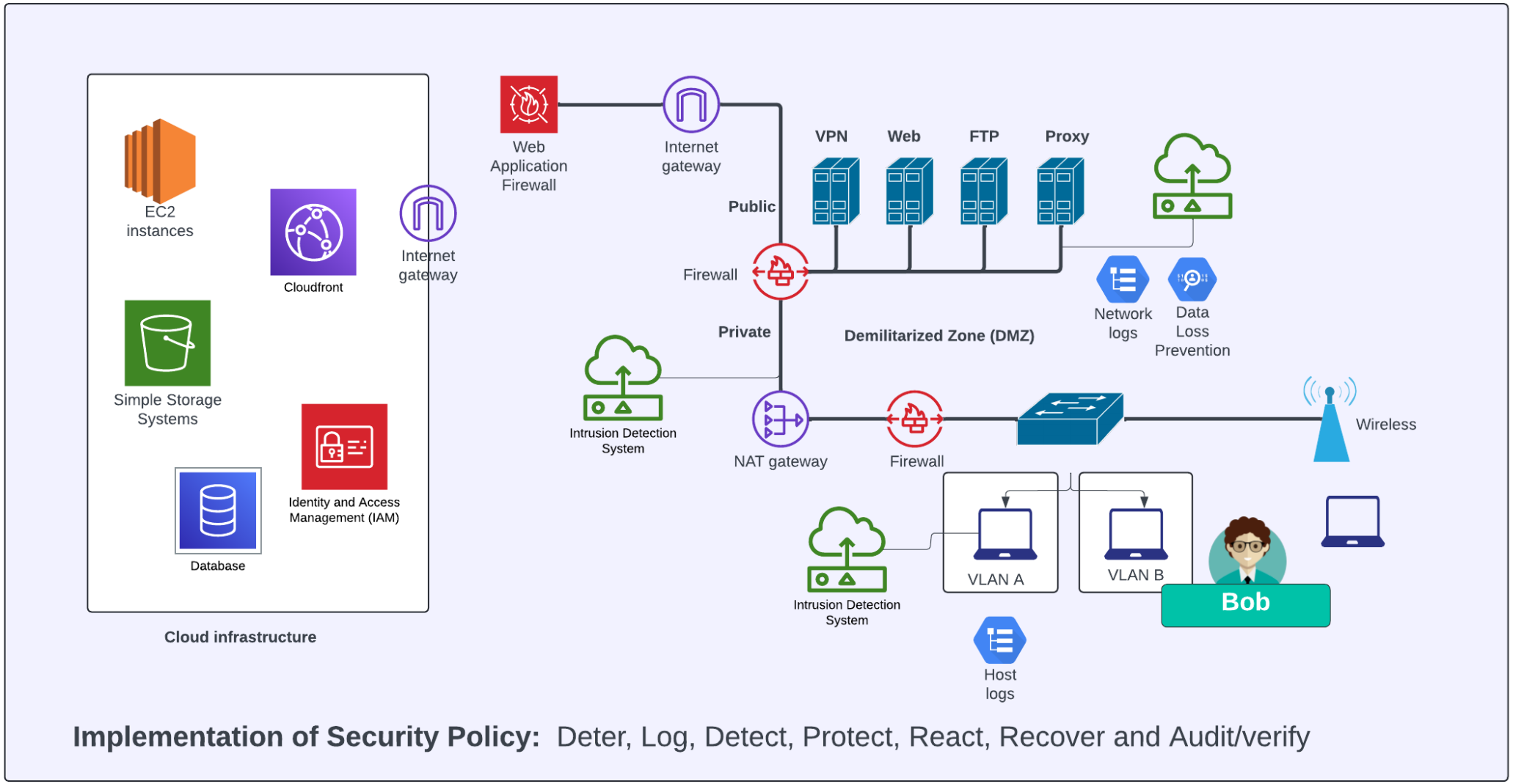
Introduction

Bob, Alice and Eve



&cyber data

Information Security



Implementation of Security Policy: Deter, Log, Detect, Protect, React, Recover and Audit/verify

&cyber&data

Due Care and Due Diligence

Due Care: Correct steps for security policy and risk analysis

Bob

Cyber Infrastructure

Testing for compliance

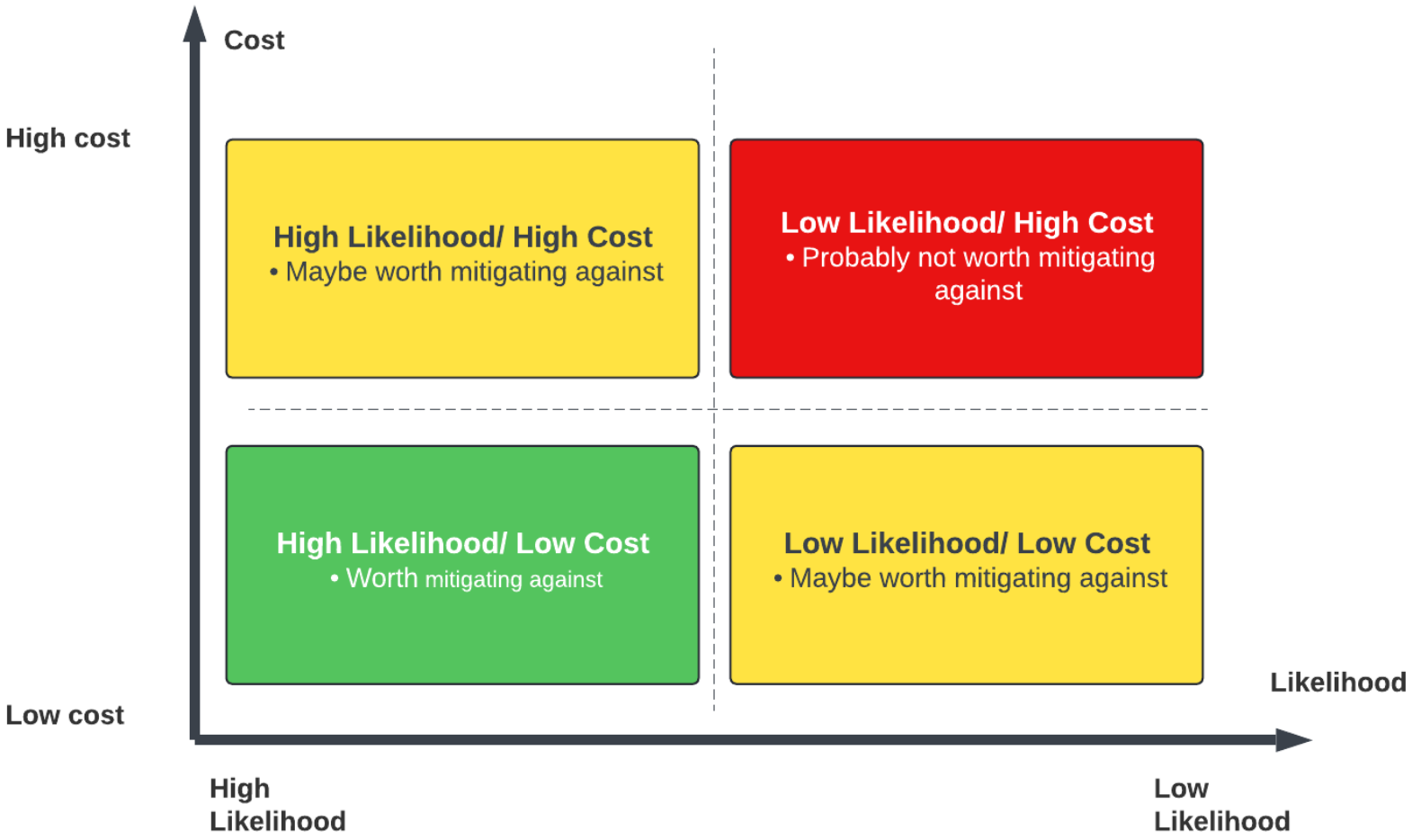
Due Diligence: Test for actions operation and maintenance of the security system, such as for vulnerability testing

&cyber data

Impact and Harm

Agrafiotis, I., Nurse, J. R., Goldsmith, M., Creese, S., & Upton, D. (2018). A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate. *Journal of Cybersecurity*, *4*(1), tyy006.

Risks, Costs and Benefits

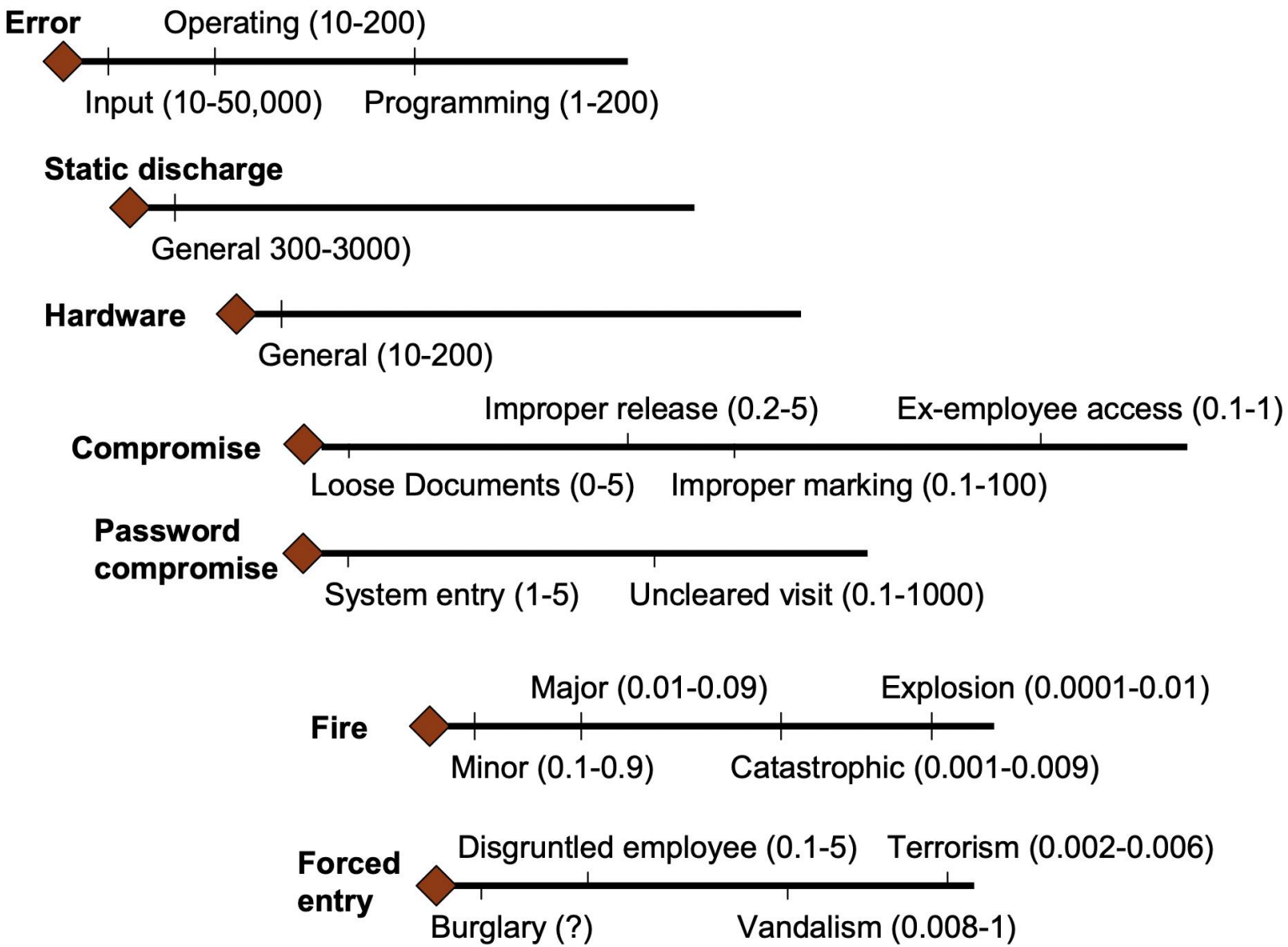


ALE = AV x ARO

ALE – Annual Loss Expectancy.
AV – Asset Value

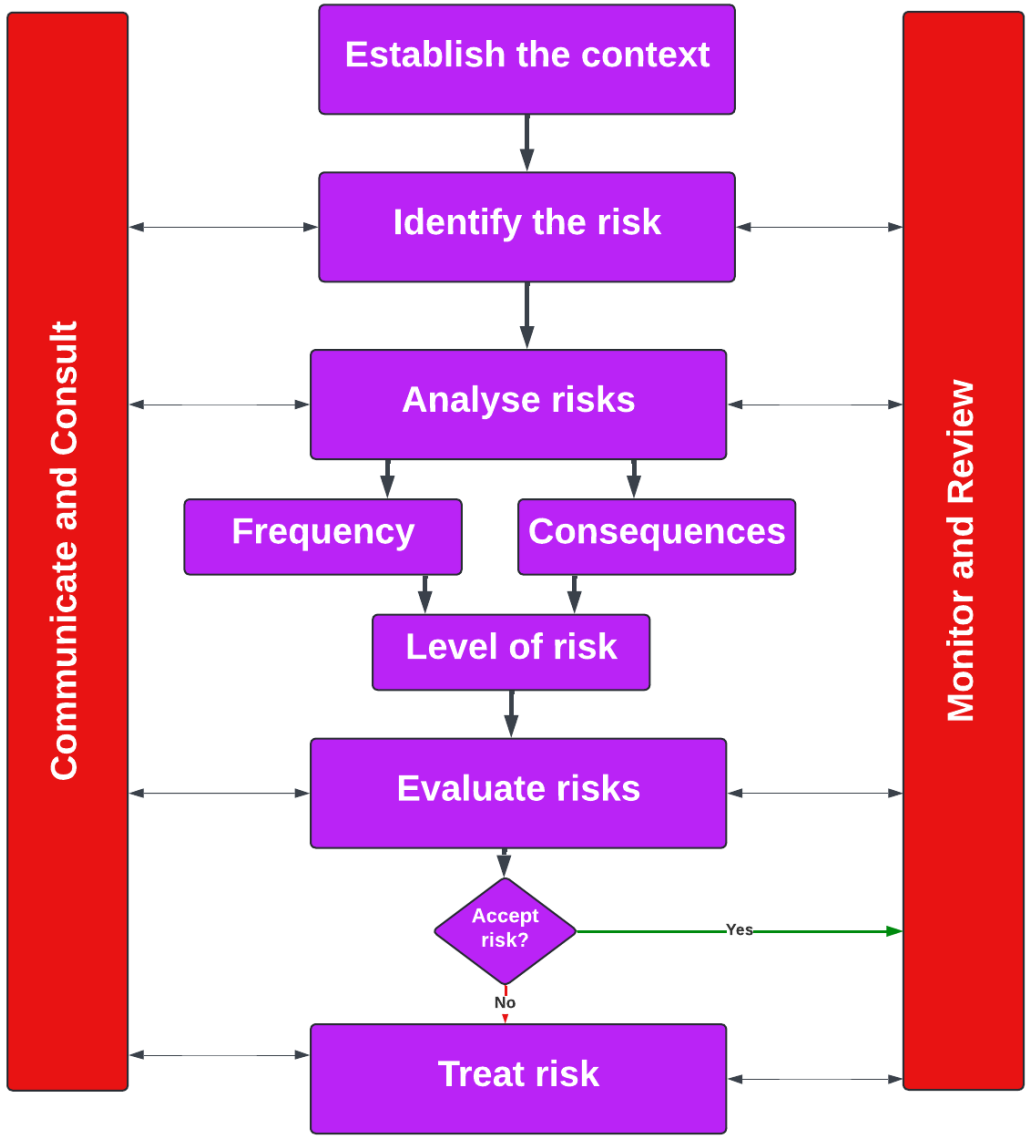
&cyber data

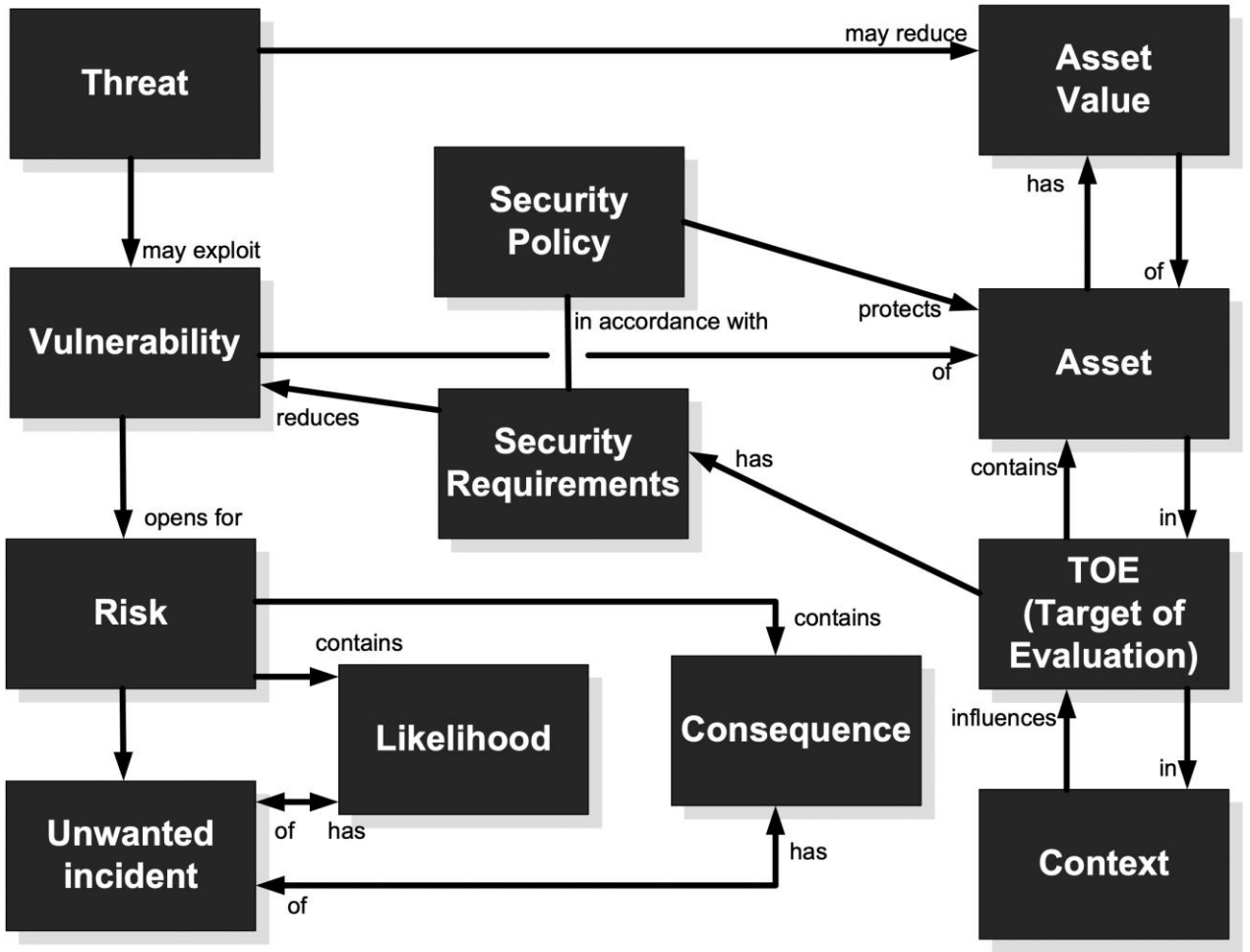
Risks, Costs and Benefits



&cyber data

CORAS Risk Management/Ontology





cyber & data

"From bits to information"

Kill Chain Model

CVE Reporting

CVE-2024-31497 PUBLISHED

View JSON | User Guide

Collapse all

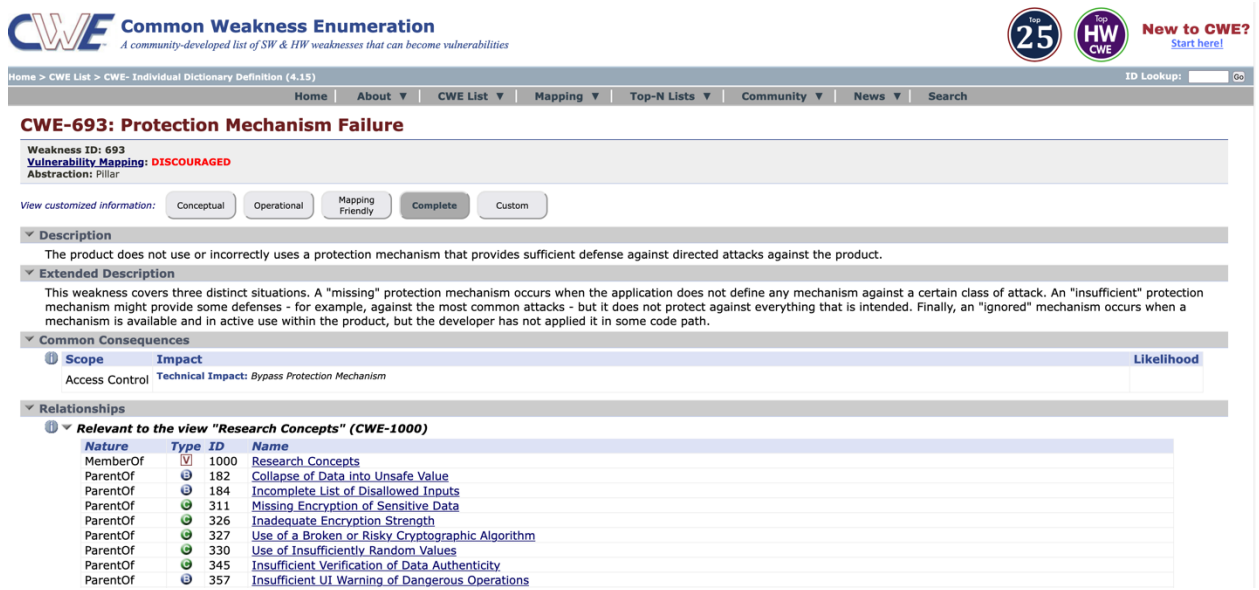
Required CVE Record Information

CNA: MITRE Corporation

Published: 2024-04-15 **Updated:** 2024-06-20

Description

In PuTTY 0.68 through 0.80 before 0.81, biased ECDSA nonce generation allows an attacker to recover a user's NIST P-521 secret key via a quick attack in approximately 60 signatures. This is especially important in a scenario where an adversary is able to read messages signed by PuTTY or Pageant. The required set of signed messages may be publicly readable because they are stored in a public Git service that supports use of SSH for commit signing, and the signatures were made by Pageant through an agent-forwarding mechanism. In other words, an adversary may already have enough signature information to compromise a victim's private key, even if there is no further use of vulnerable PuTTY versions. After a key compromise, an adversary may be able to conduct supply-chain attacks on software maintained in Git. A second, independent scenario is that the adversary is an operator of an SSH server to which the victim authenticates (for remote login or file copy), even though this server is not fully trusted by the victim, and the victim uses the same private key for SSH connections to other services operated by other entities. Here, the rogue server operator (who would otherwise have no way to determine the victim's private key) can derive the victim's private key, and then use it for unauthorized access to those other services. If the other services include Git services, then again it may be possible to conduct supply-chain attacks on software maintained in Git. This also affects, for example, FileZilla before 3.67.0, WinSCP before 6.3.3, TortoiseGit before 2.15.0.1, and TortoiseSVN through 1.14.6.



CWE Common Weakness Enumeration

A community-developed list of SW & HW weaknesses that can become vulnerabilities

New to CWE? Start here!

Home > CWE List > CWE- Individual Dictionary Definition (4.15) ID Lookup: Go

Home | About | CWE List | Mapping | Top-N Lists | Community | News | Search

CWE-693: Protection Mechanism Failure

Weakness ID: 693
Vulnerability Mapping: DISCOURAGED
Abstraction: Pillar

View customized information: Conceptual | Operational | Mapping Friendly | Complete | Custom

Description

The product does not use or incorrectly uses a protection mechanism that provides sufficient defense against directed attacks against the product.

Extended Description

This weakness covers three distinct situations. A "missing" protection mechanism occurs when the application does not define any mechanism against a certain class of attack. An "insufficient" protection mechanism might provide some defenses - for example, against the most common attacks - but it does not protect against everything that is intended. Finally, an "ignored" mechanism occurs when a mechanism is available and in active use within the product, but the developer has not applied it in some code path.

Common Consequences

Scope	Impact	Likelihood
Access Control	**Technical Impact:** *Bypass Protection Mechanism*	

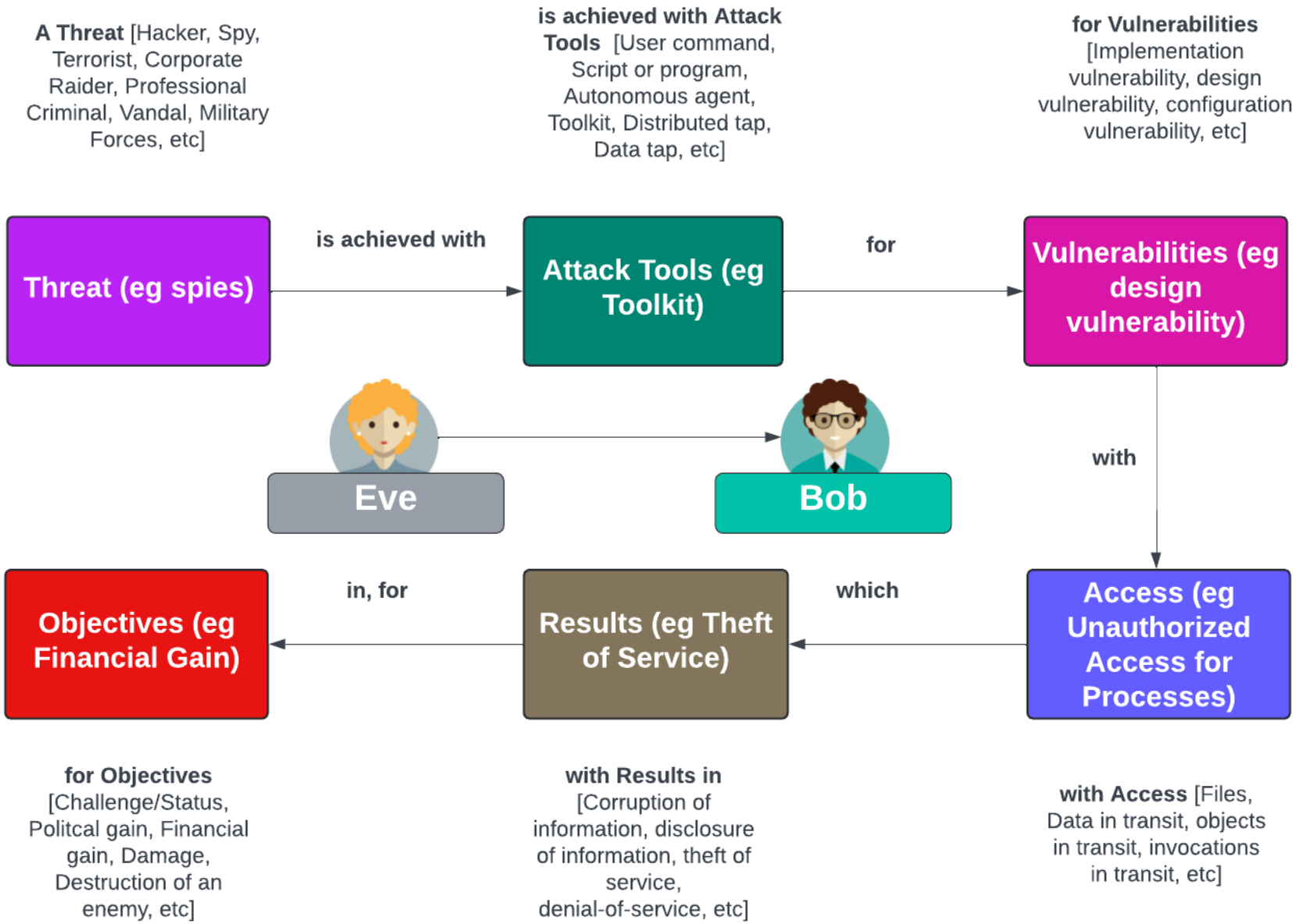
Relationships

Relevant to the view "Research Concepts" (CWE-1000)

Nature	Type	ID	Name
MemberOf	V	1000	Research Concepts
ParentOf	B	182	Collapse of Data into Unsafe Value
ParentOf	B	184	Incomplete List of Disallowed Inputs
ParentOf	C	311	Missing Encryption of Sensitive Data
ParentOf	C	326	Inadequate Encryption Strength
ParentOf	C	327	Use of a Broken or Risky Cryptographic Algorithm
ParentOf	C	330	Use of Insufficiently Random Values
ParentOf	C	345	Insufficient Verification of Data Authenticity
ParentOf	B	357	Insufficient UI Warning of Dangerous Operations

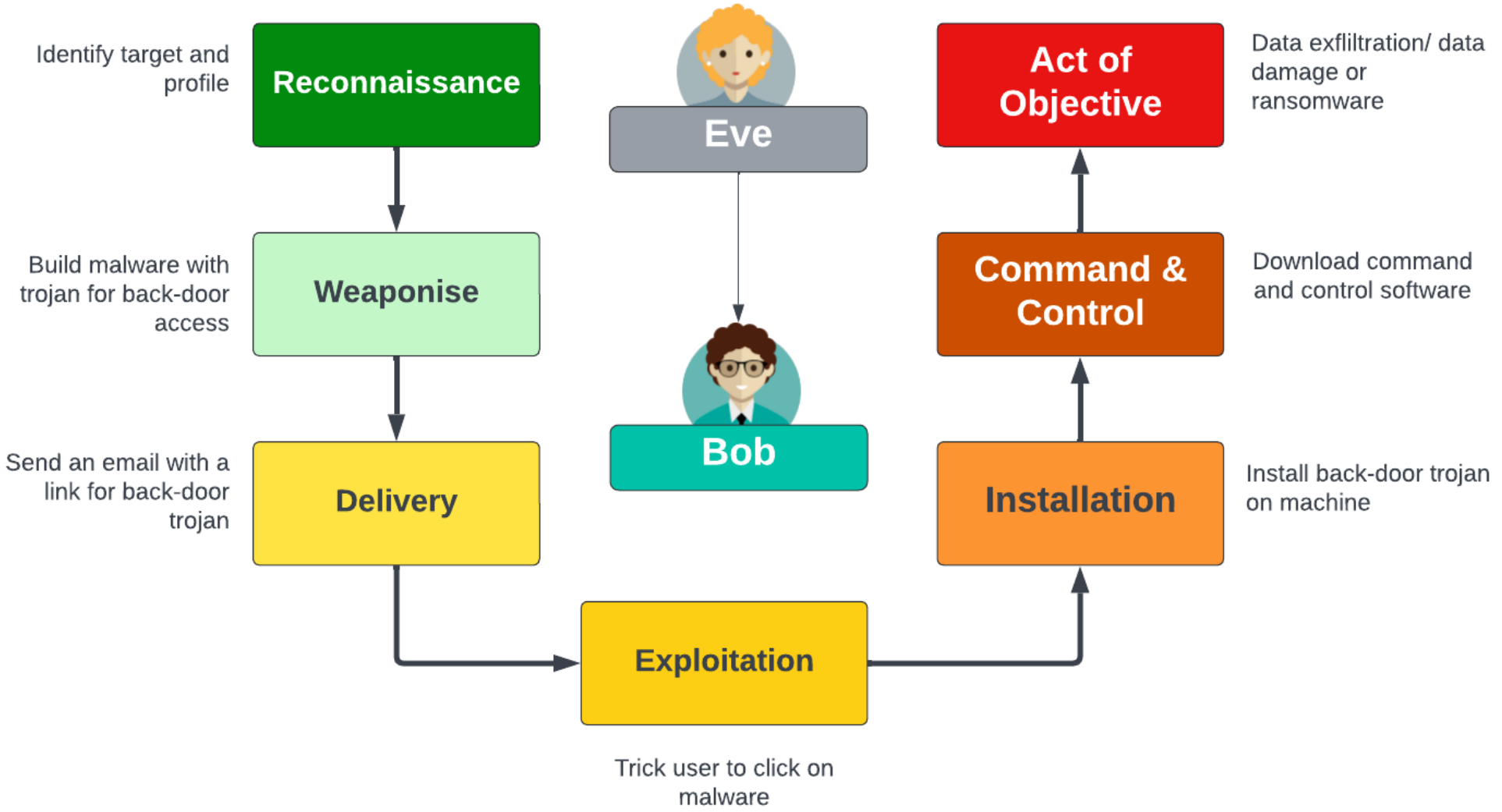
&cyber&data

Incident Taxonomy



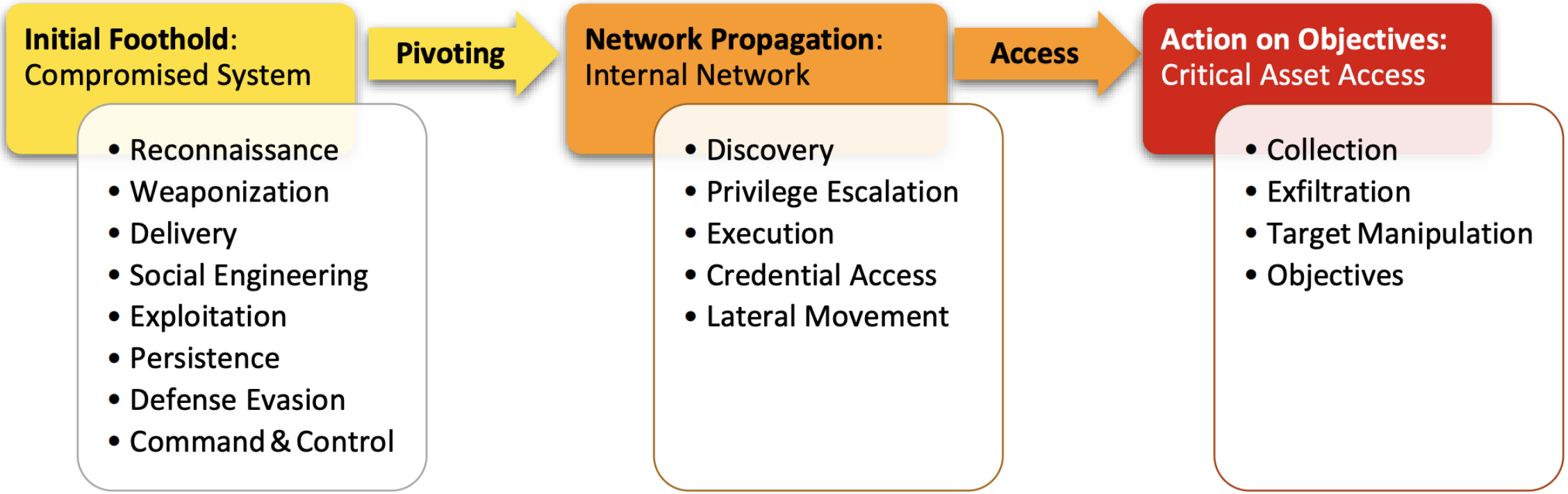
&cyber data

Kill Chain Model



&cyber data

Unified Kill Chain Phases



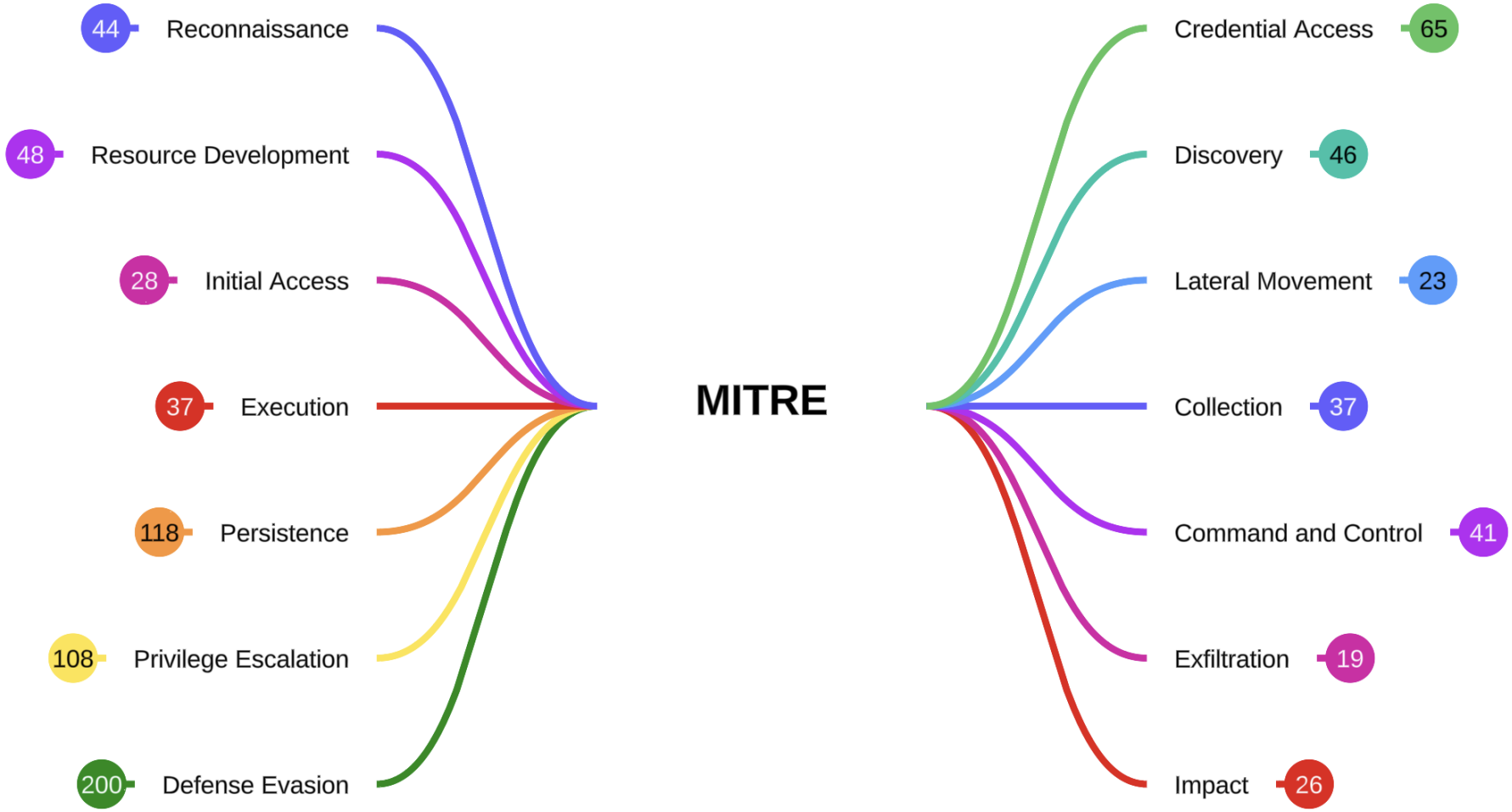
Pols, P., & van den Berg, J. (2017). The unified kill chain. *CSA Thesis, Hague*, 1-104.

&cyber data

"From bits to information"

MITRE ATT&CK

MITRE ATT&CK (Enterprise)



&cyber data

MITRE ATT&CK (Enterprise)

Techniques

Techniques: 10

ID	Name	Description
T1595	Active Scanning	Adversaries may execute active reconnaissance scans to gather information that can be used during targeting. Active scans are those where the adversary probes victim infrastructure via network traffic, as opposed to other forms of reconnaissance that do not involve direct interaction.
.001	Scanning IP Blocks	Adversaries may scan victim IP blocks to gather information that can be used during targeting. Public IP addresses may be allocated to organizations by block, or a range of sequential addresses.
.002	Vulnerability Scanning	Adversaries may scan victims for vulnerabilities that can be used during targeting. Vulnerability scans typically check if the configuration of a target host/application (ex: software and version) potentially aligns with the target of a specific exploit the adversary may seek to use.
.003	Wordlist Scanning	Adversaries may iteratively probe infrastructure using brute-forcing and crawling techniques. While this technique employs similar methods to Brute Force, its goal is the identification of content and infrastructure rather than the discovery of valid credentials. Wordlists used in these scans may contain generic, commonly used names and file extensions or terms specific to a particular software. Adversaries may also create custom, target-specific wordlists using data gathered from other Reconnaissance techniques (ex: Gather Victim Org Information, or Search Victim-Owned Websites).

Procedure Examples

ID	Name	Description
C0030	Triton Safety Instrumented System Attack	In the Triton Safety Instrumented System Attack, TEMP.Veles engaged in network reconnaissance against targets of interest.[3]

Mitigations

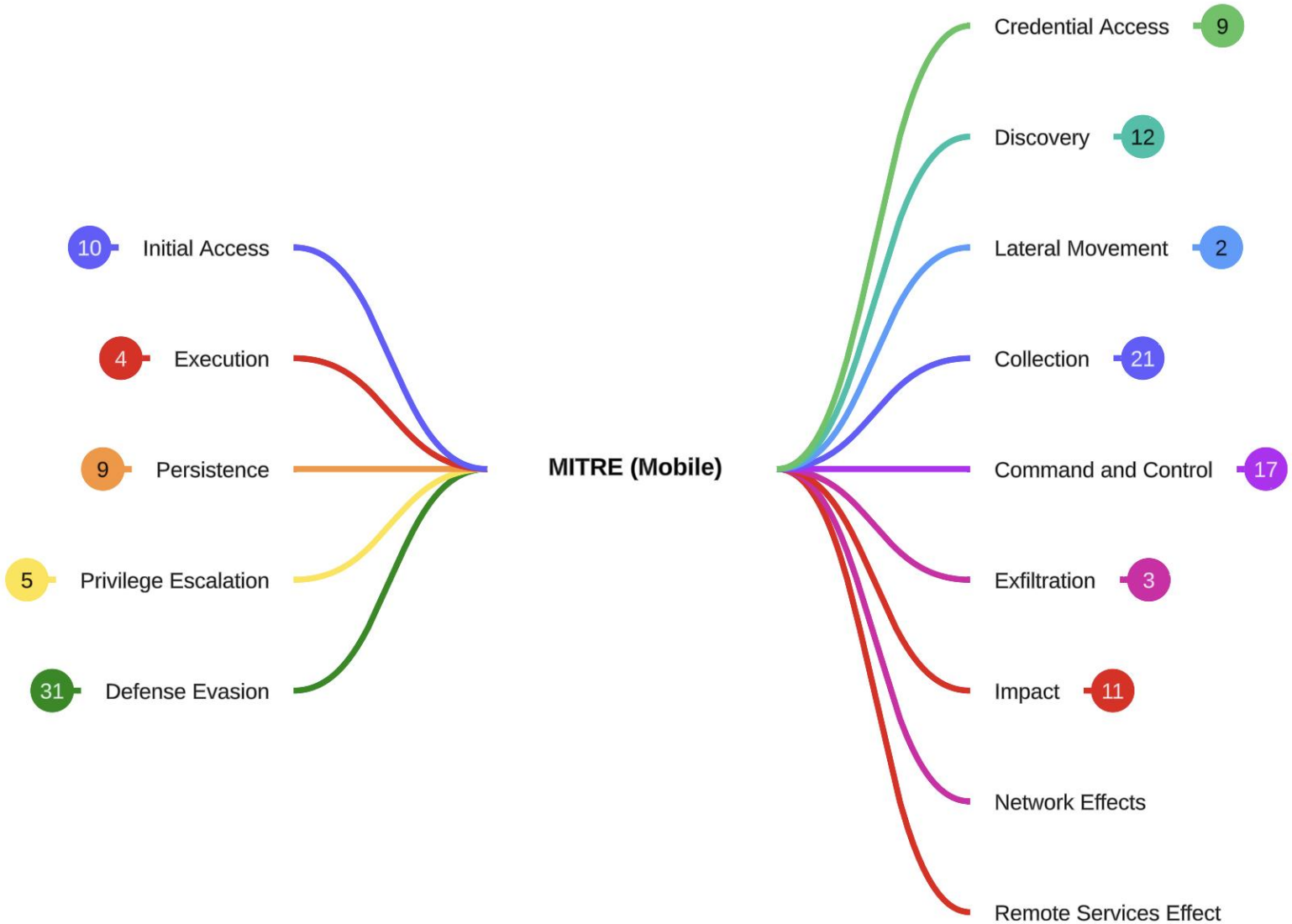
ID	Mitigation	Description
M1056	Pre-compromise	This technique cannot be easily mitigated with preventive controls since it is based on behaviors performed outside of the scope of enterprise defenses and controls. Efforts should focus on minimizing the amount and sensitivity of data available to external parties.

Detection

ID	Data Source	Data Component	Detects
DS0029	Network Traffic	Network Traffic Content	Monitor and analyze traffic patterns and packet inspection associated to protocol(s) that do not follow the expected protocol standards and traffic flows (e.g extraneous packets that do not belong to established flows, gratuitous or anomalous traffic patterns, anomalous syntax, or structure). Consider correlation with process monitoring and command line to detect anomalous processes execution and command line arguments associated to traffic patterns (e.g. monitor anomalies in use of files that do not normally initiate connections for respective protocol(s)).
		Network Traffic Flow	Monitor network data for uncommon data flows. Processes utilizing the network that do not normally have network communication or have never been seen before are suspicious.

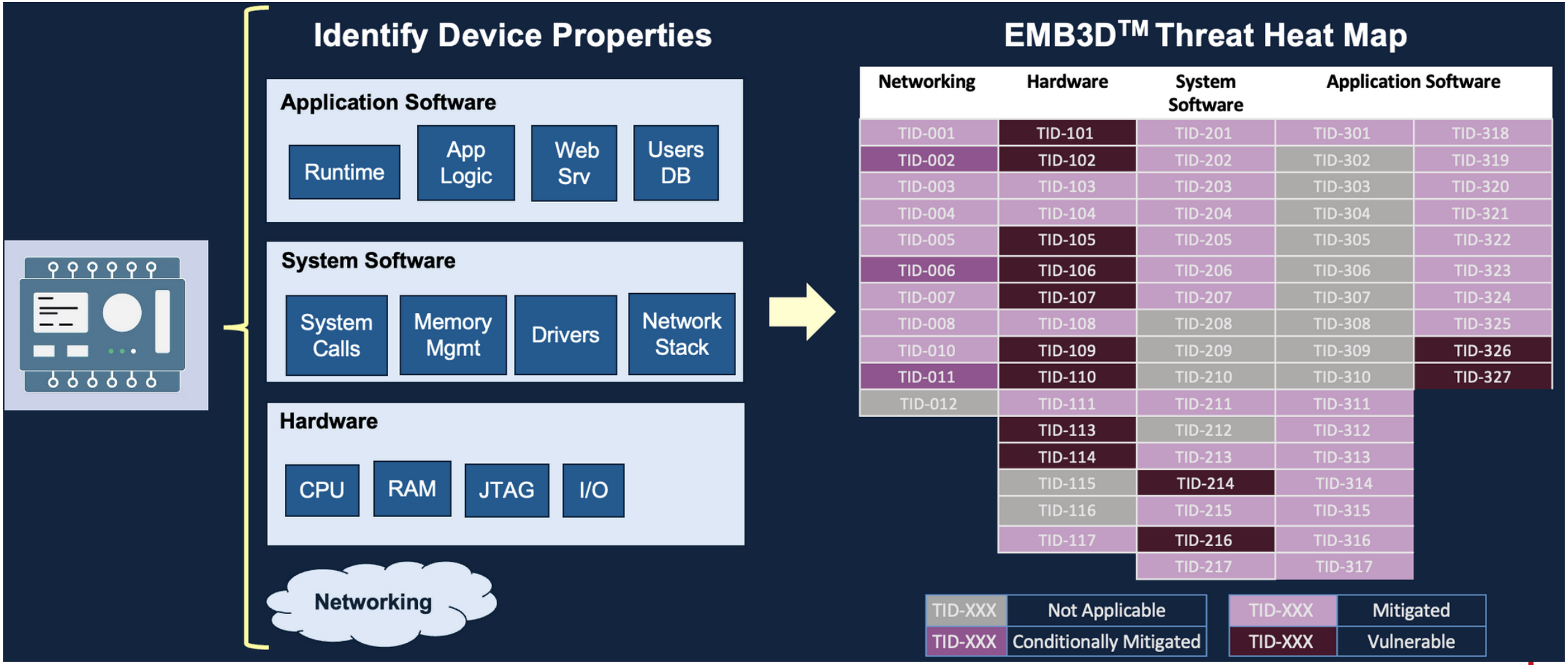
&cyber &data

MITRE ATT&CK (Mobile)



&cyber data

MITRE EMB3D (Embedded Devices)

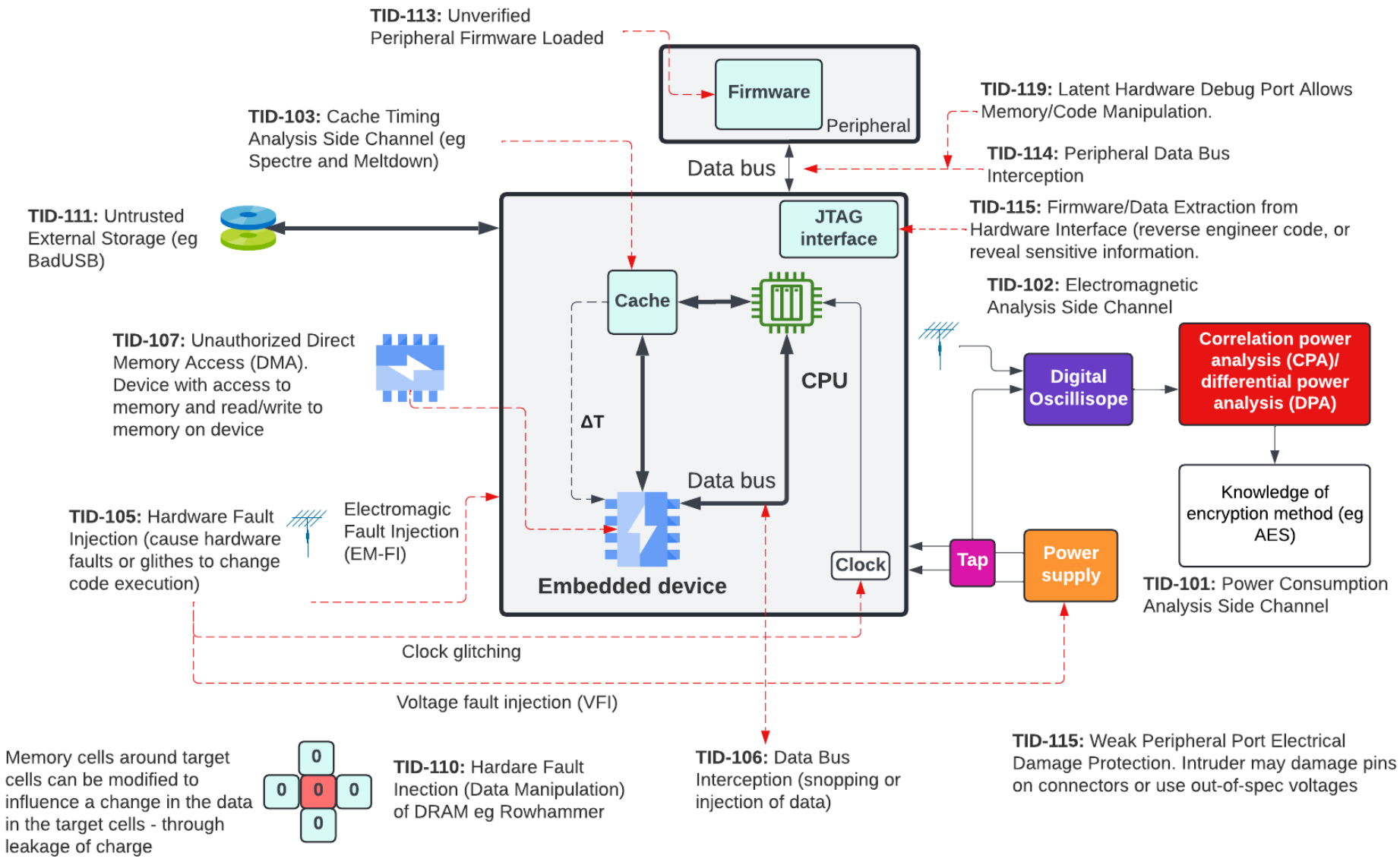


&cyber data

MITRE EMB3D (Embedded Devices)

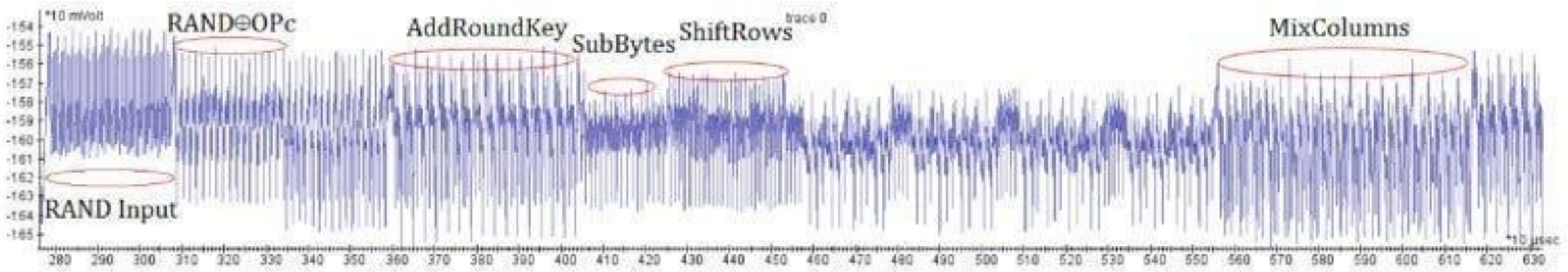
MITRE EMB3D (Embedded Devices)

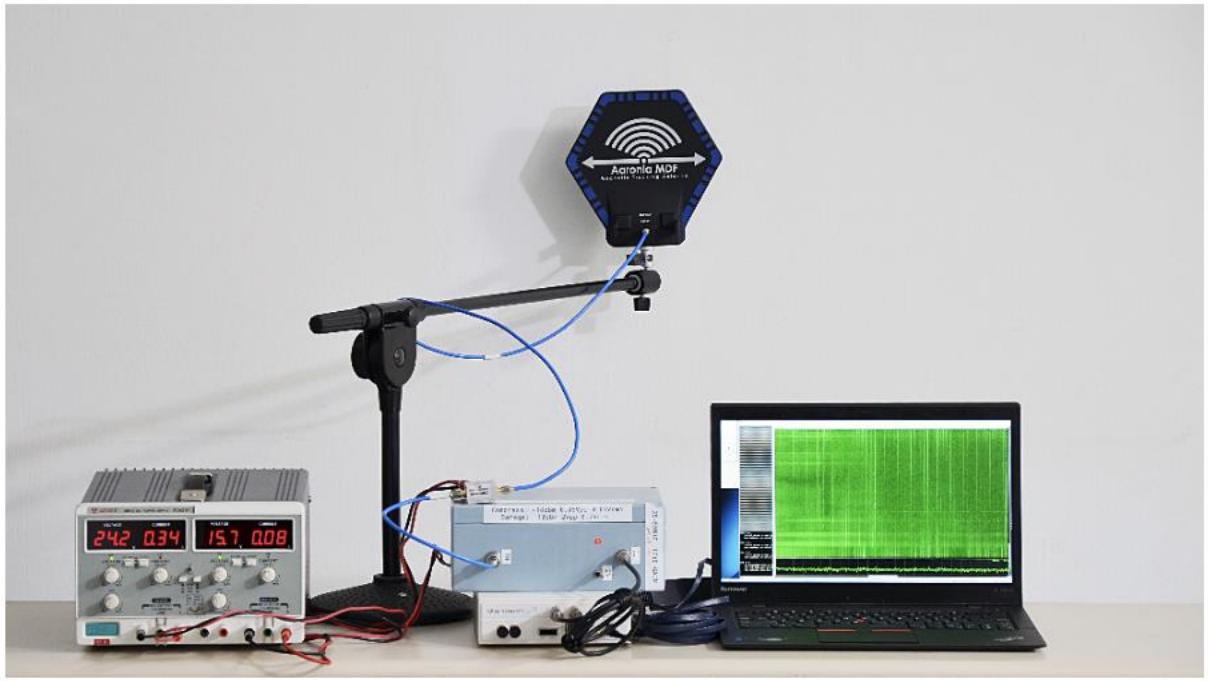
MITRE EMB3D (Embedded Devices)



&cyber data

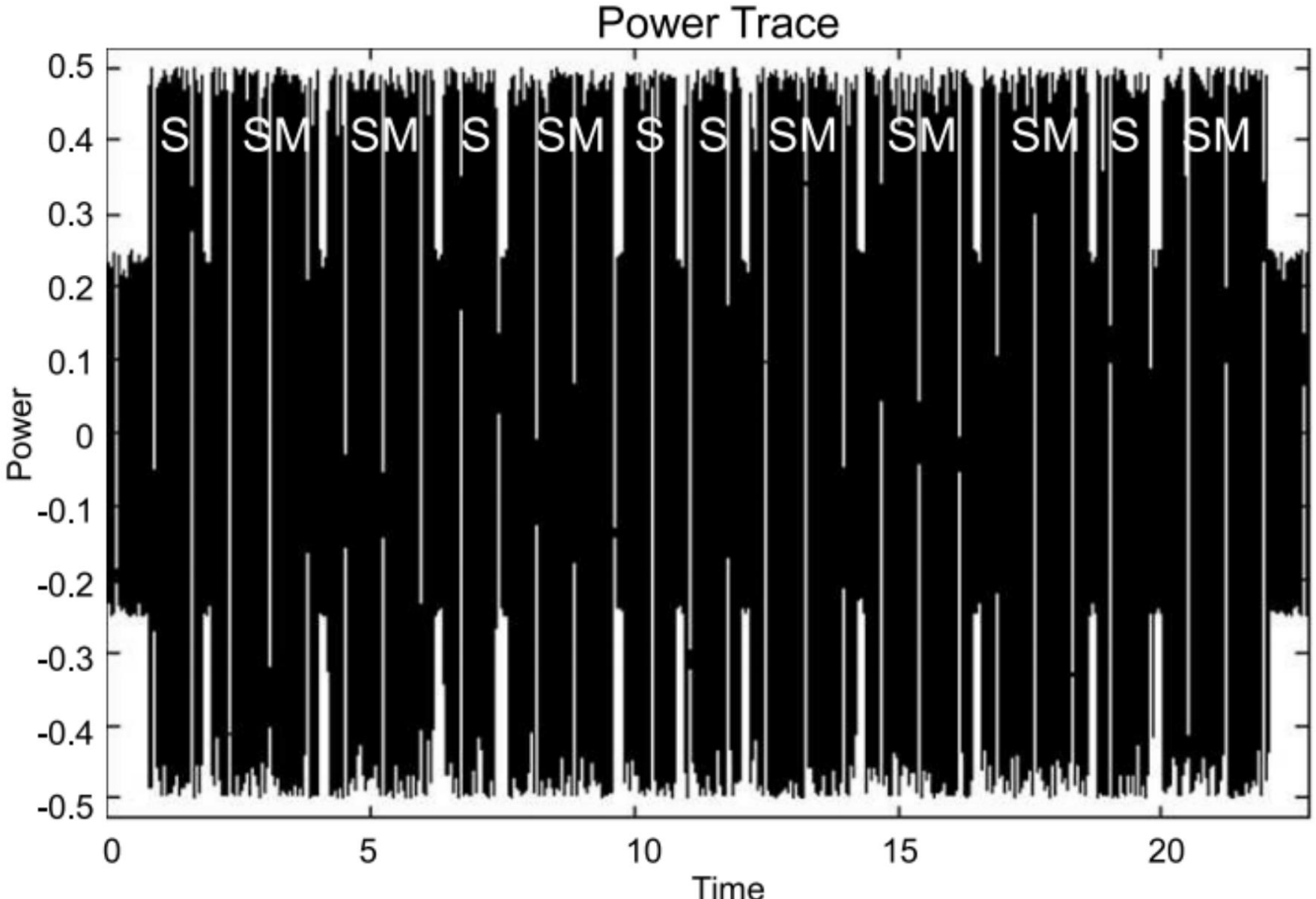
MITRE EMB3D (Embedded Devices) – Symmetric Key Crack





&cyber data

MITRE EMB3D (Embedded Devices) – RSA Crack



&cyber data

MITRE EMB3D (Embedded Devices)

EUCLEAK

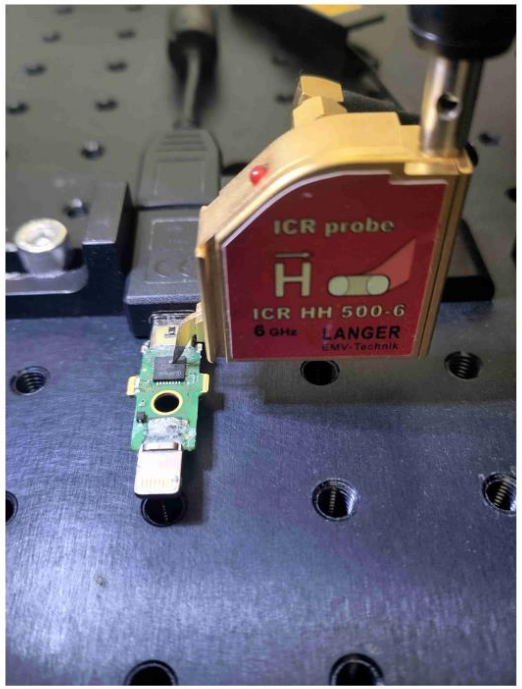
Side-Channel Attack on the YubiKey 5 Series

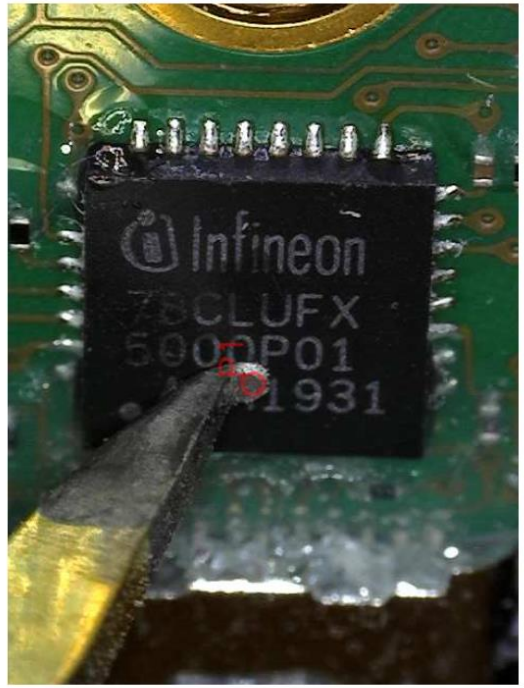
(Revealing and Breaking Infineon ECDSA Implementation on the Way)

Thomas ROCHE

NinjaLab, Montpellier, France
thomas@ninjalab.io

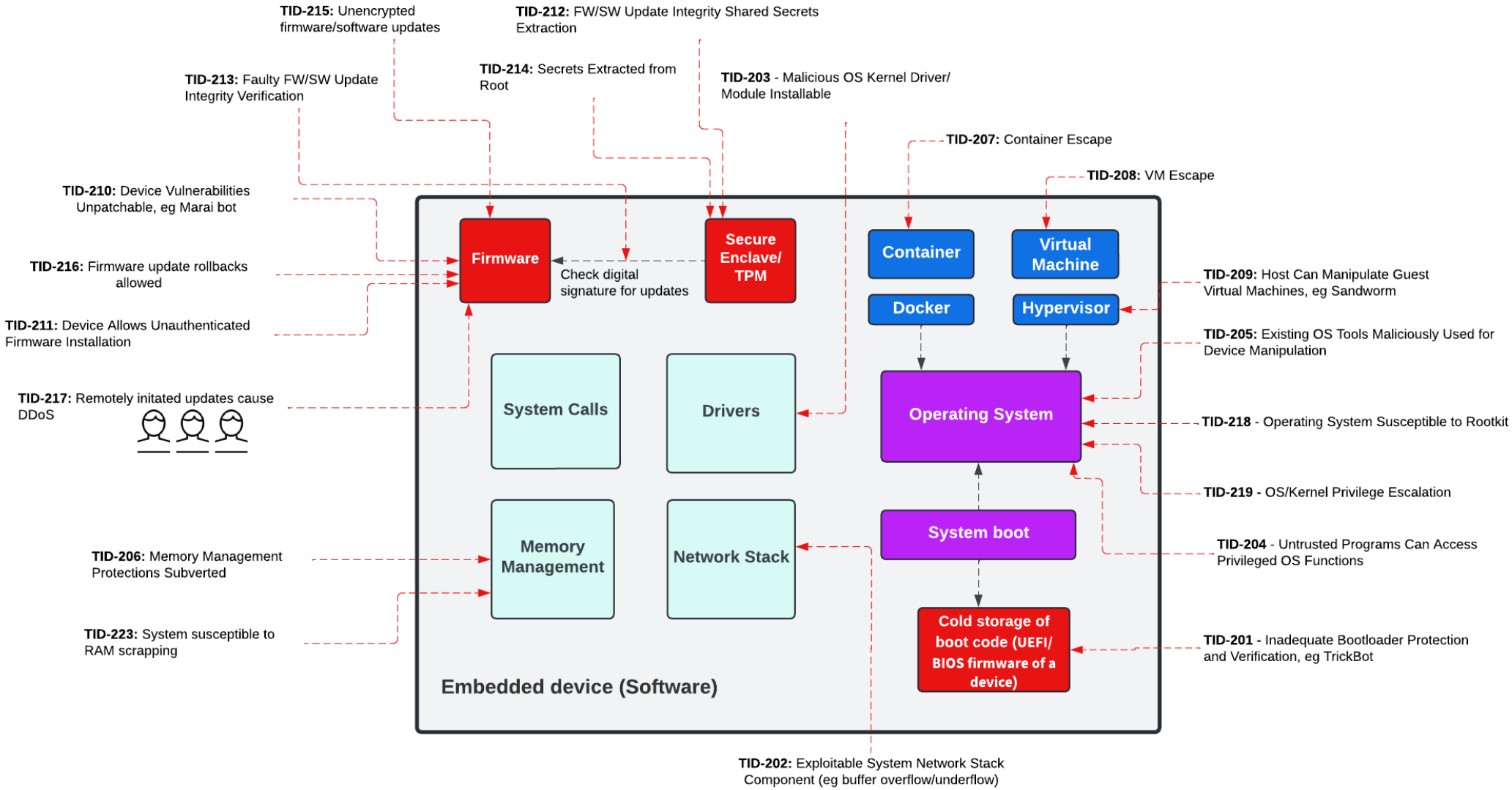
September 3rd, 2024





&cyber data

MITRE EMB3D (Embedded Devices)



&cyber data

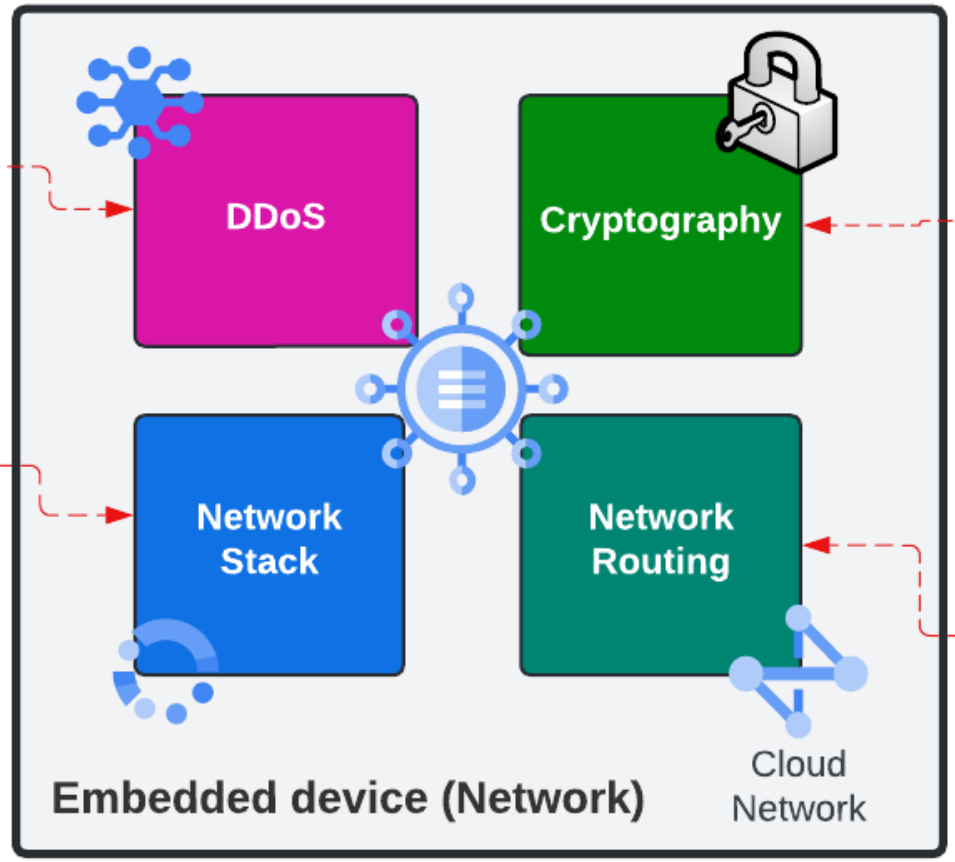
MITRE EMB3D (Embedded Devices)

TID-404 - Remotely Triggerable Deadlock/DoS

TID-405 - Network Stack Resource Exhaustion

TID-406 - Unauthorized Messages or Connections

TID-407 - Missing Message Replay Protection



TID-408 - Unencrypted Sensitive Data Communication

TID-410 - Cryptographic Protocol Side Channel

TID-411 - Weak/Insecure Cryptographic Protocol

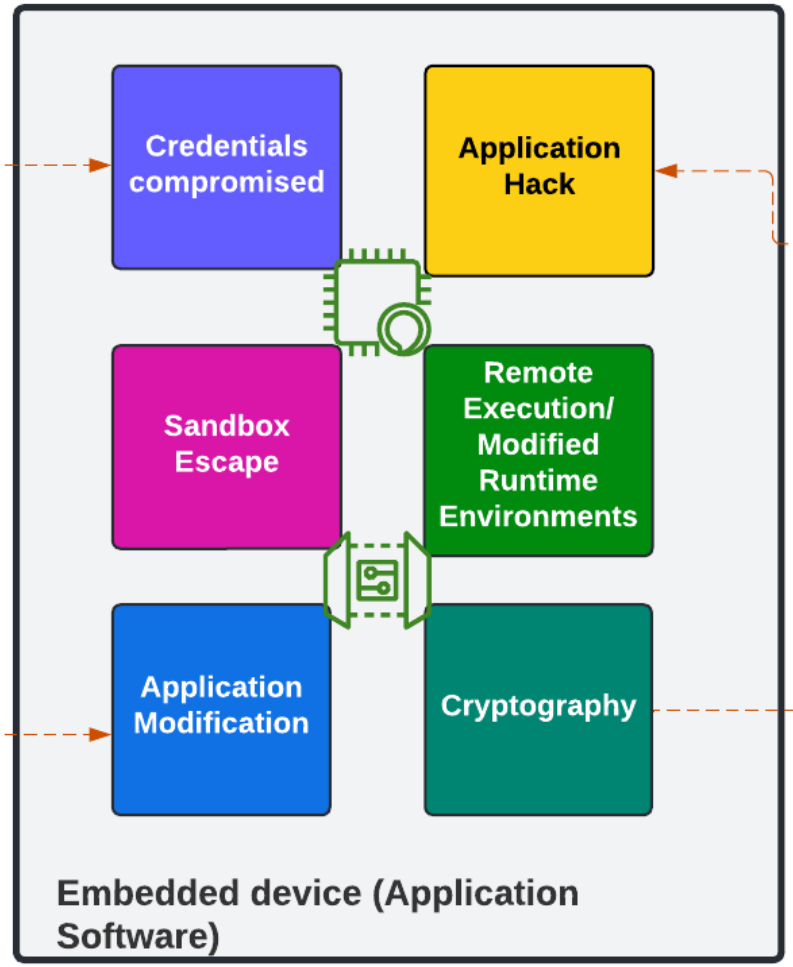
TID-412 - Network Routing Capability Abuse

TID-412 - Network Routing Capability Abuse

&cyber data

MITRE EMB3D (Embedded Devices)

TID-328 - Hardcoded Credentials
TID-311 - Default Credentials
TID-312 - Credential Change Mechanism Can Be Abused



TID-318 - Insecure Cryptographic Implementation
TID-319 - Cross Site Scripting (XSS)
TID-320 - SQL Injection
TID-321 - HTTP Application Session Hijacking
TID-322 - Cross Site Request Forgery (CSRF)
TID-323 - HTTP Path Traversal
TID-324 - HTTP Direct Object Reference
TID-325 - HTTP Injection/Response Splitting
TID-326 - Insecure Deserialization
TID-327 - Out of Bounds Memory Access

TID-301 - Applications Binaries Modified
TID-302 - Install Untrusted Application
TID-303 - Excessive Trust in Offboard Management/IDE Software

TID-317 - Predictable Cryptographic Key
TID-330 - Cryptographic Timing Side-Channel

&cyber&data

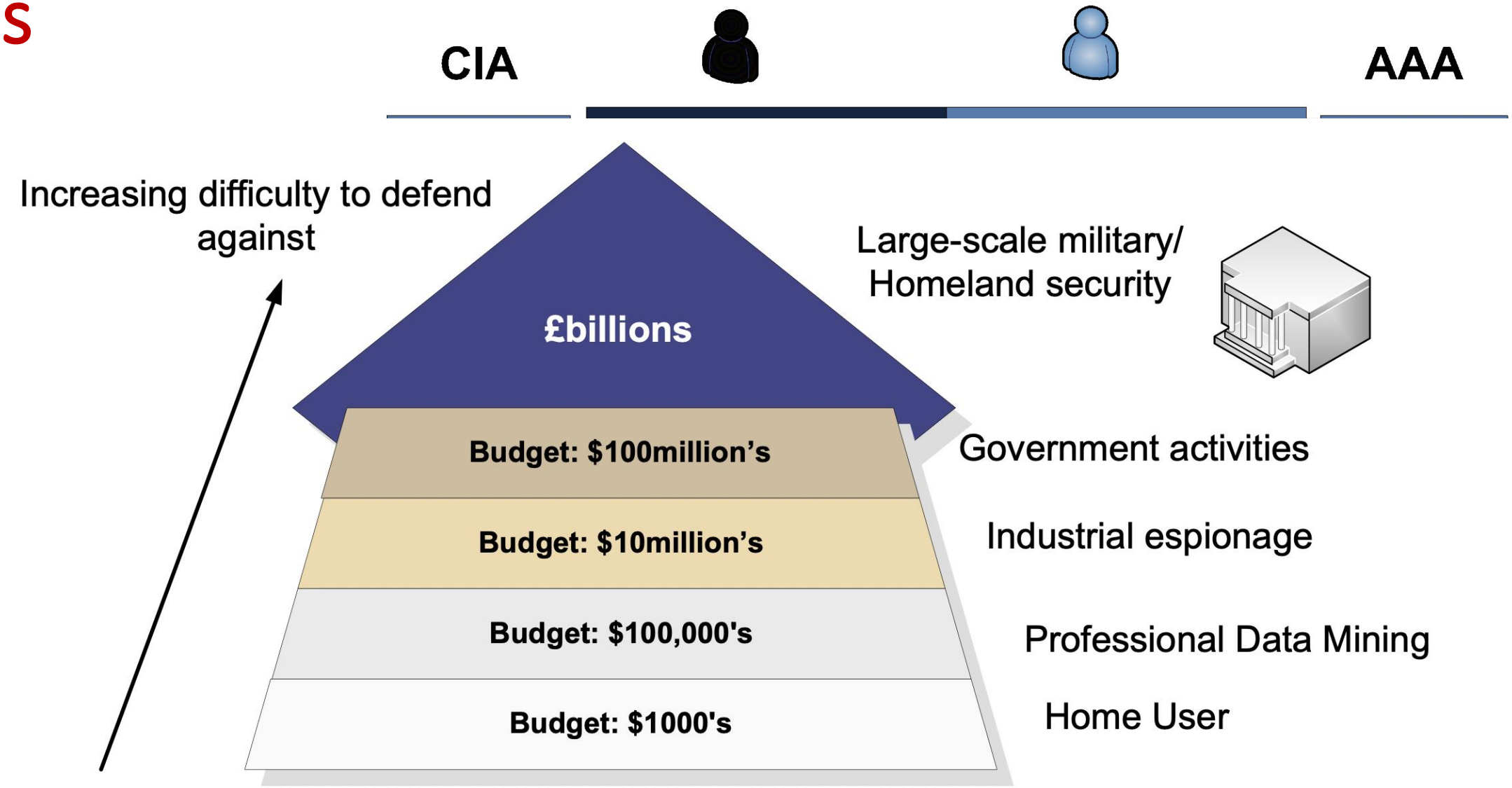
cyber & data

"From bits to information"

Basic Terms

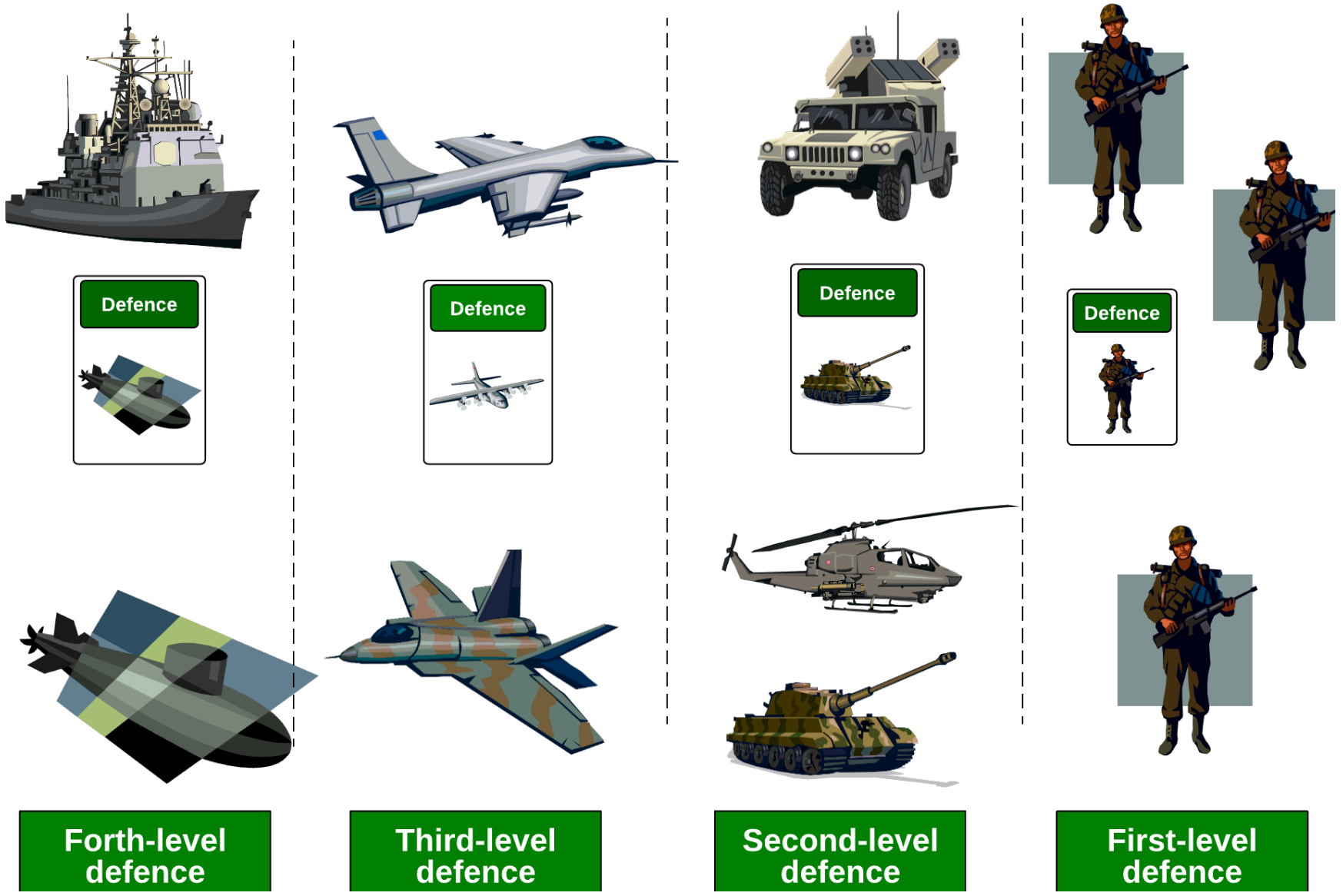
Policies

- **Dete**
  orde
  first
- **Log.**
  som
  logg
  can
- **Dete**
  netw
  ever
  in a
  futu
  dete
- **Prot**
  user
  dam
  acci
  prev
- **Read**
  intru
  Ofte
  activ
  metl
  ever
- **Recc**
  syste
  of us
- **Audi**
  audi



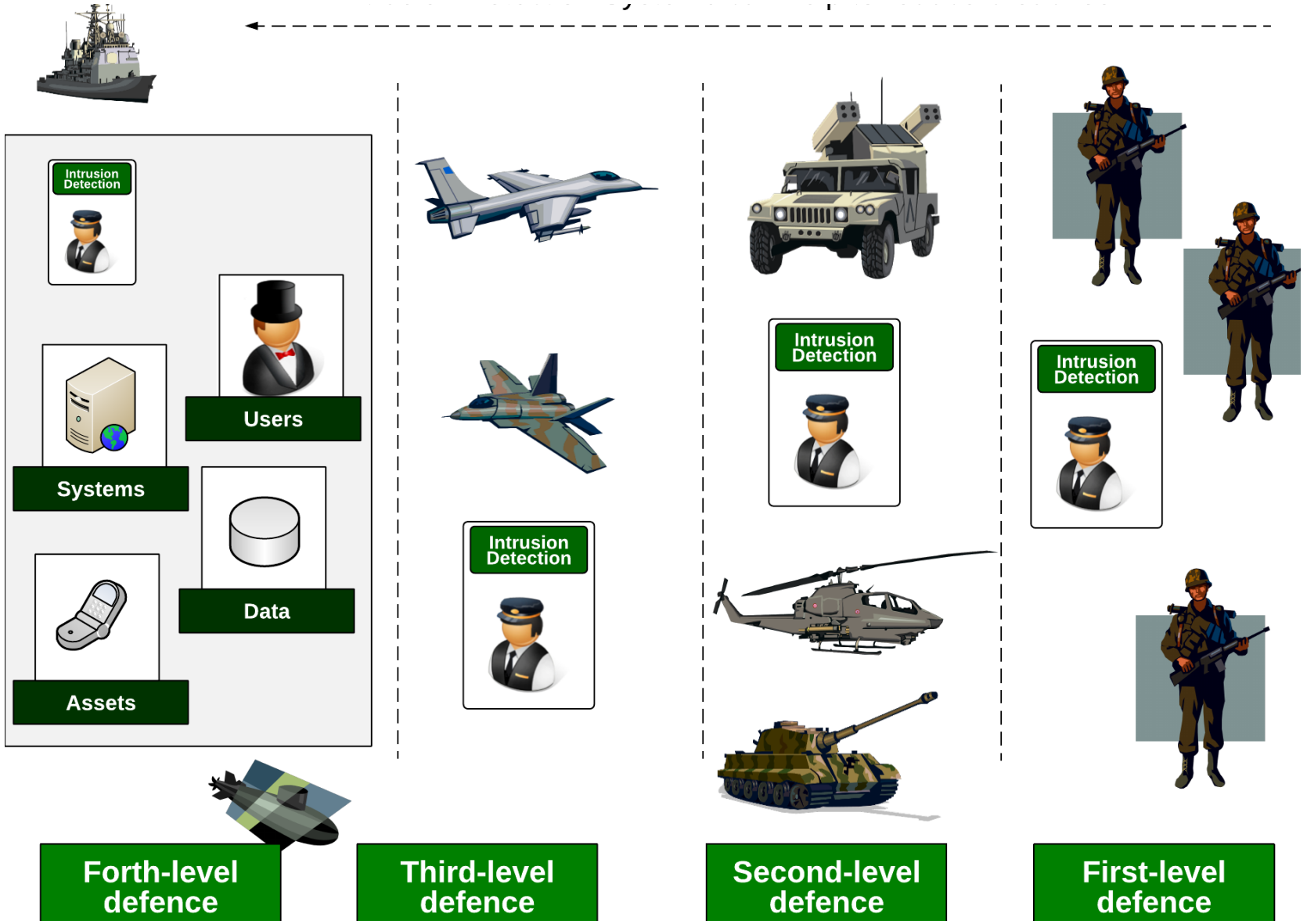
&cyber data

Defence in depth



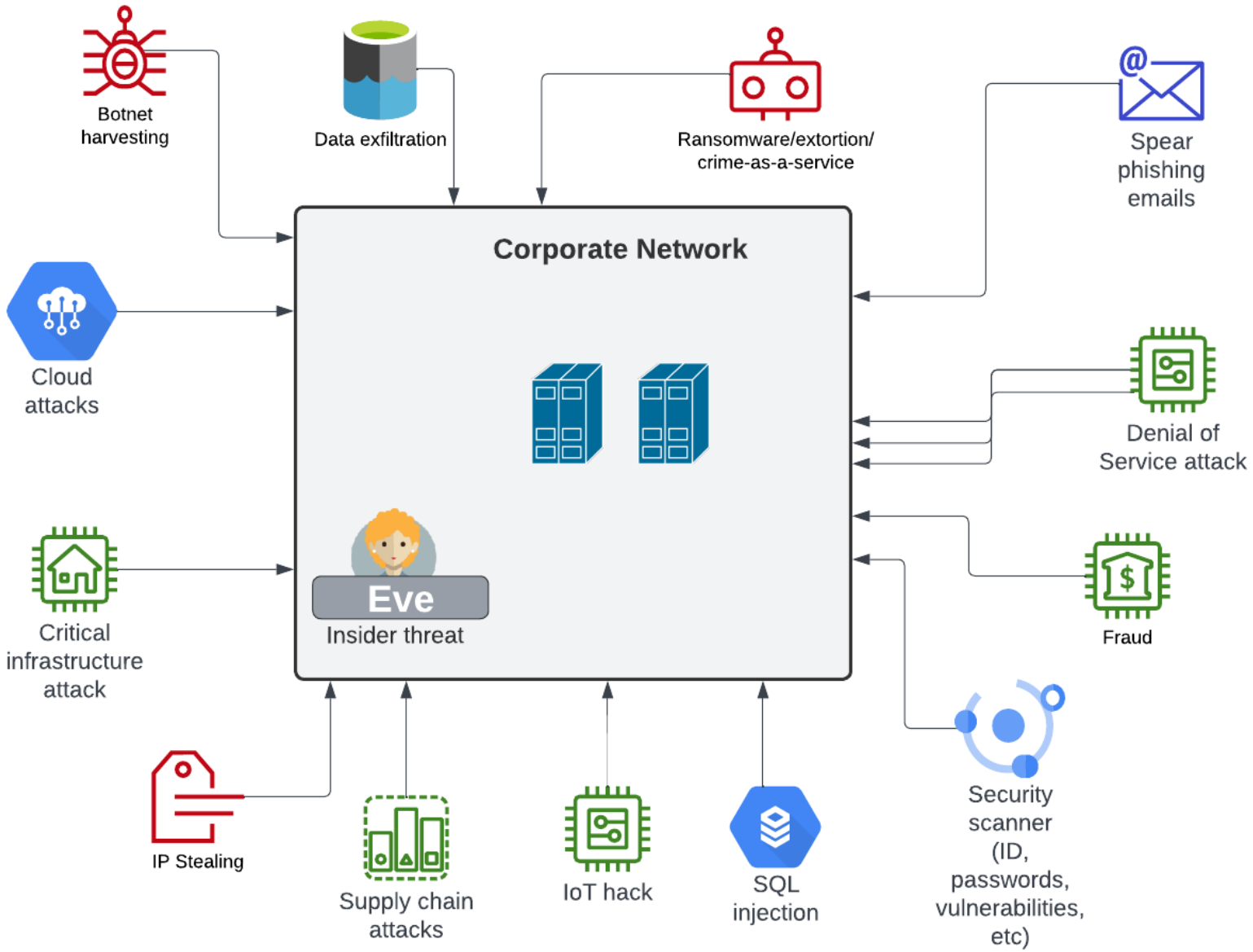
cyber & data

Intrusion Detection Systems (IDS)



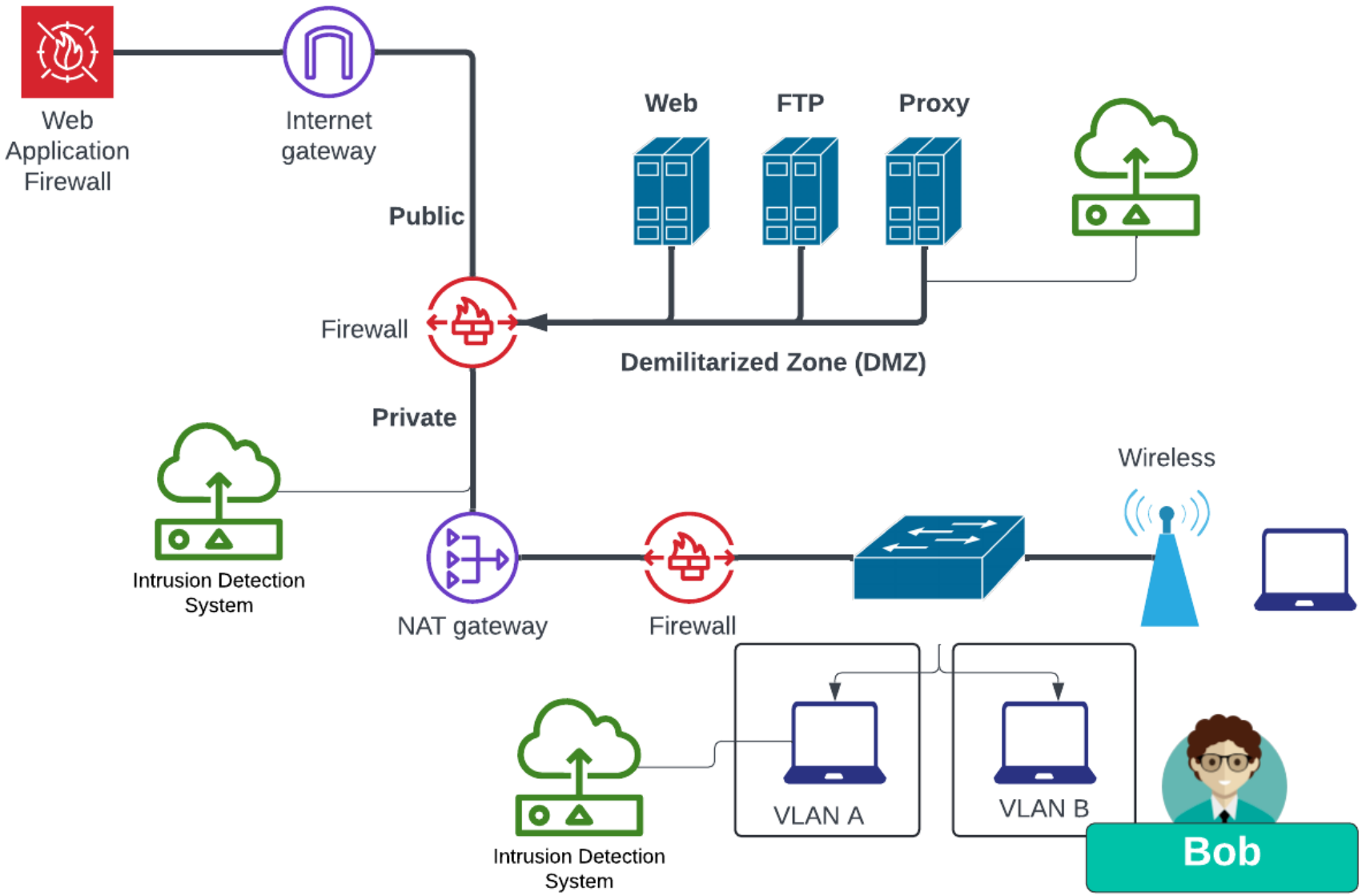
cyber &data

Threats



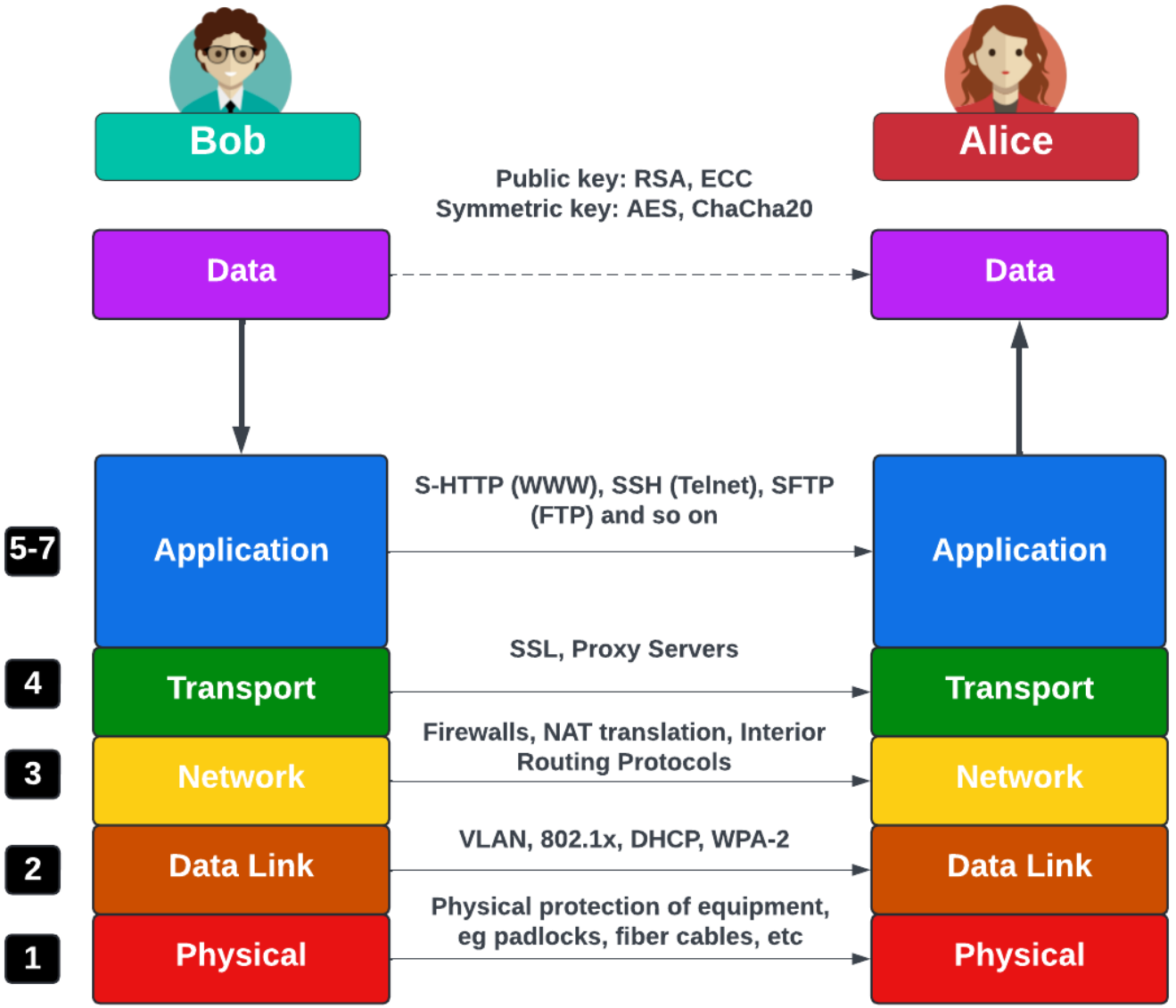
&cyber data

Defence in depth



&cyber data

OSI 7-Layered Model

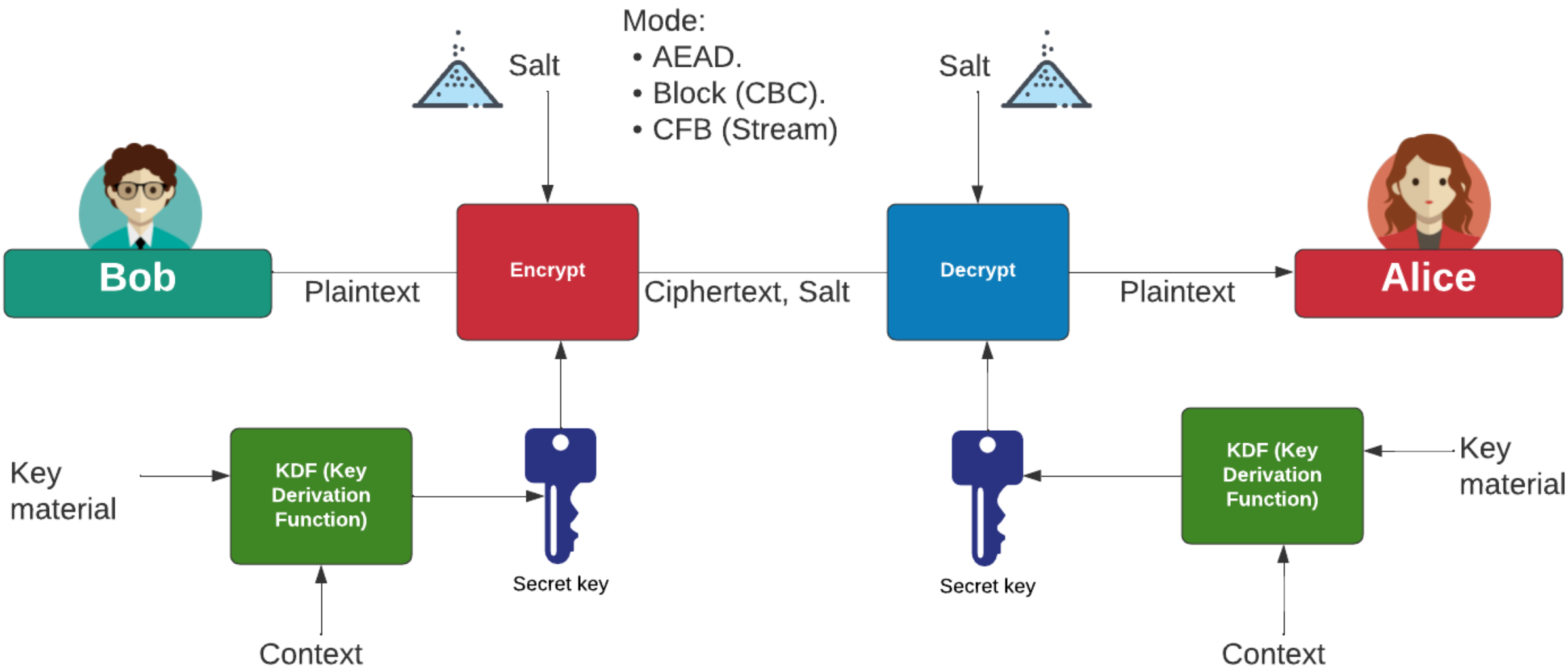


cyber & data

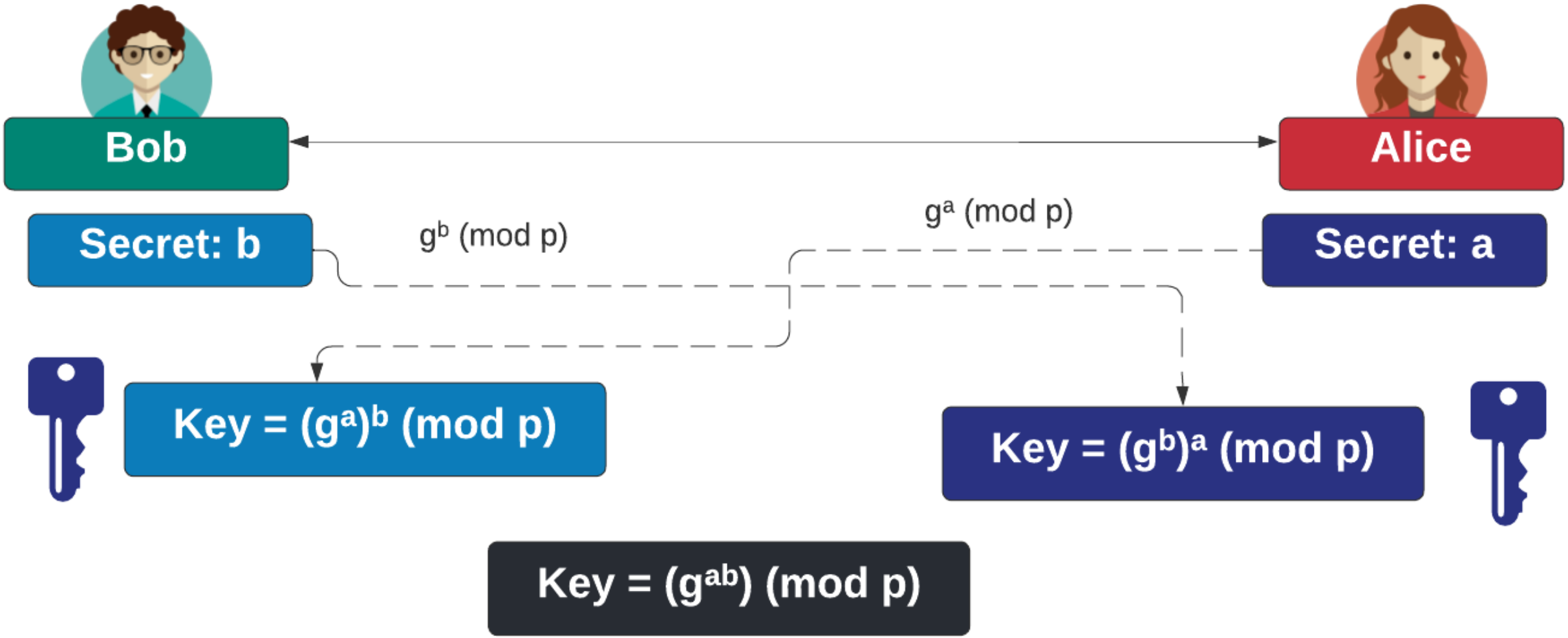
"From bits to information"

Basics of Cryptography

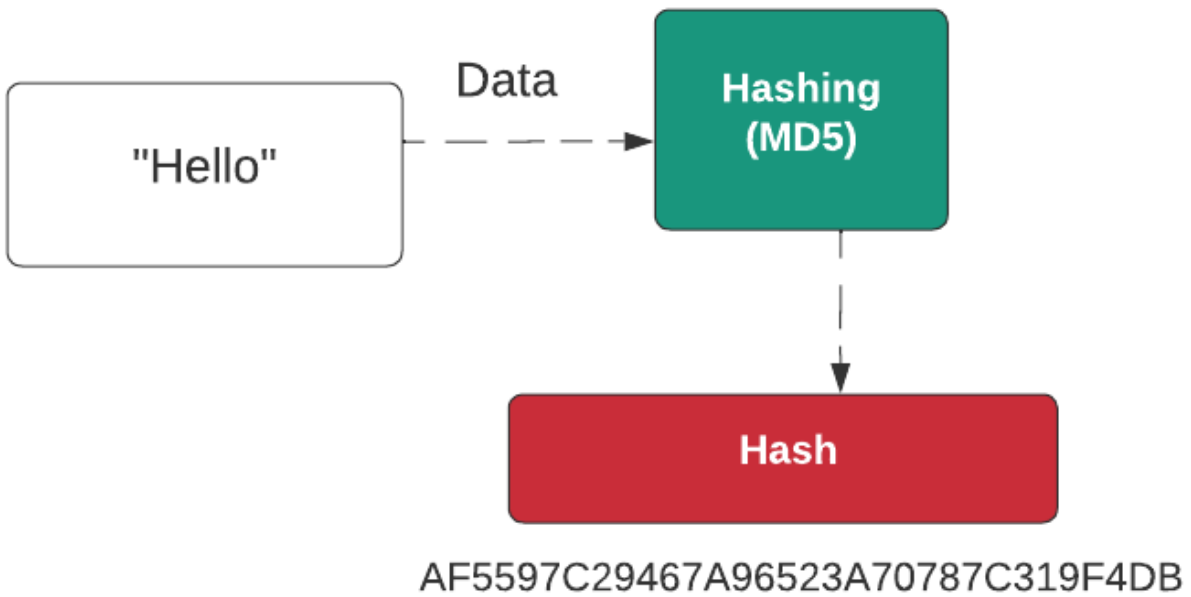
Symmetric Key Encryption



Key Exchange



Hashing



Hashed password

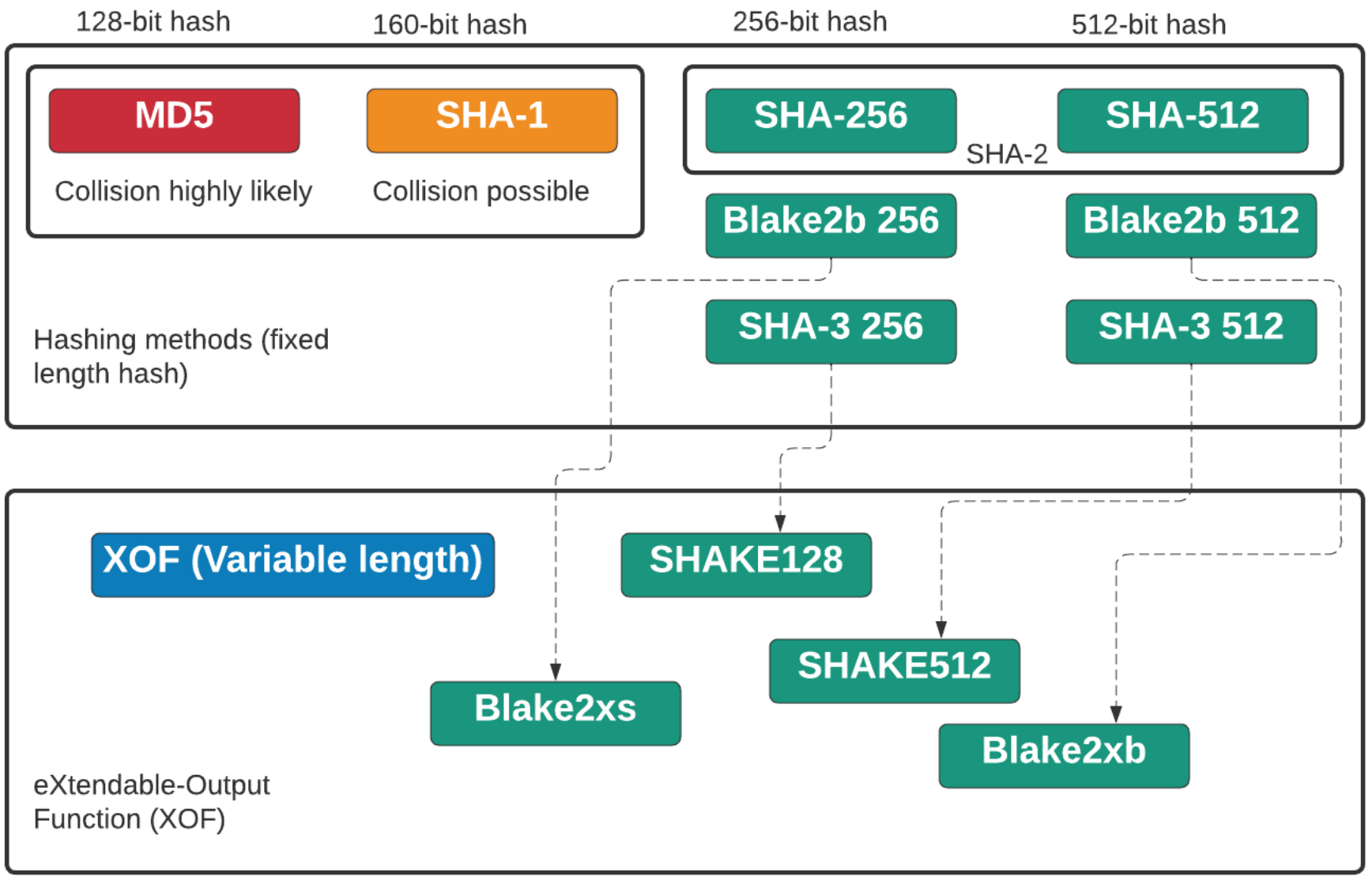
Bob: AF5597C29467A96523A70787C319F4DB

Hashed password with salt (hellozj8n)

Bob: zj8n:51A7C663A3BDCD06D6CE21E2BCB2AD5A

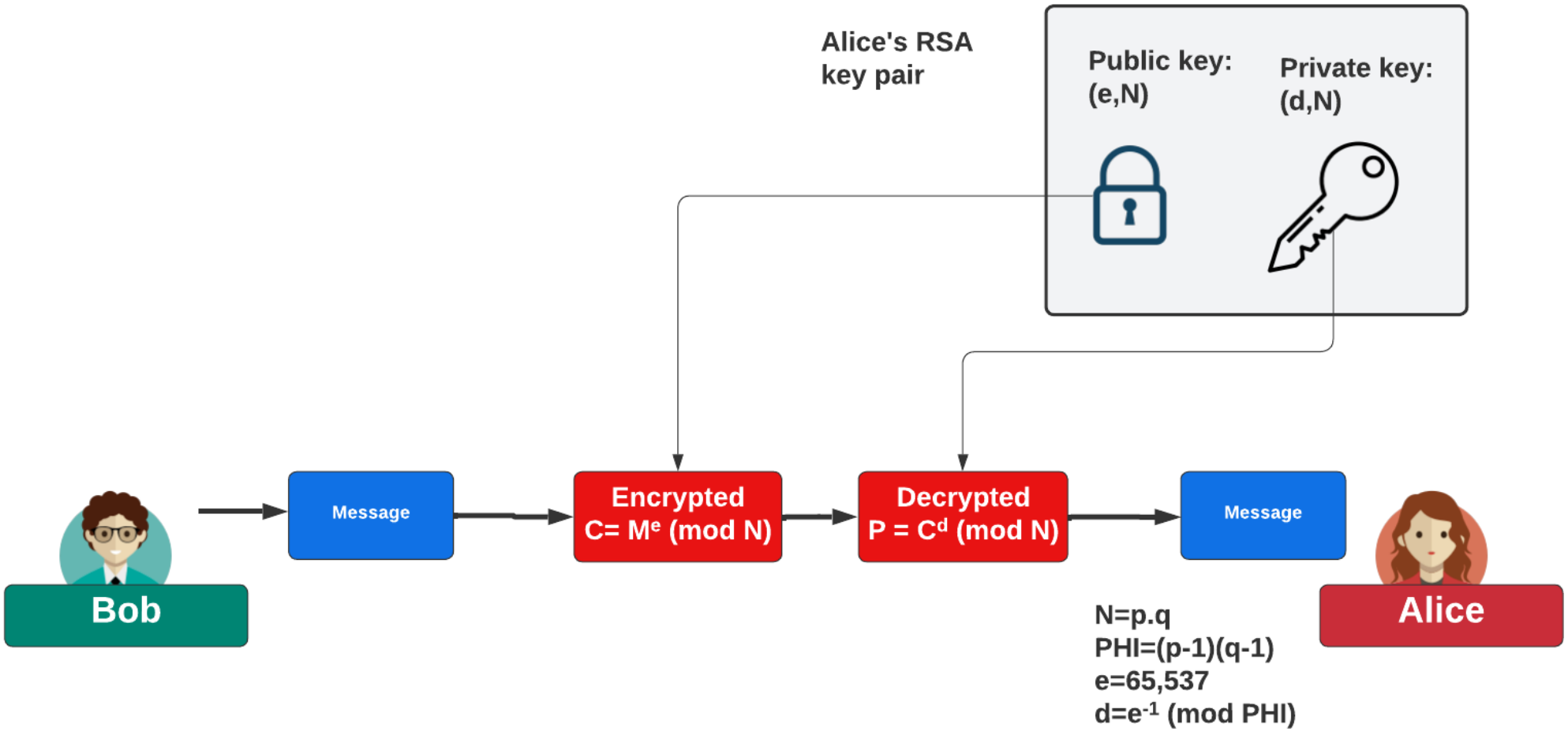
&cyber data

Hashing



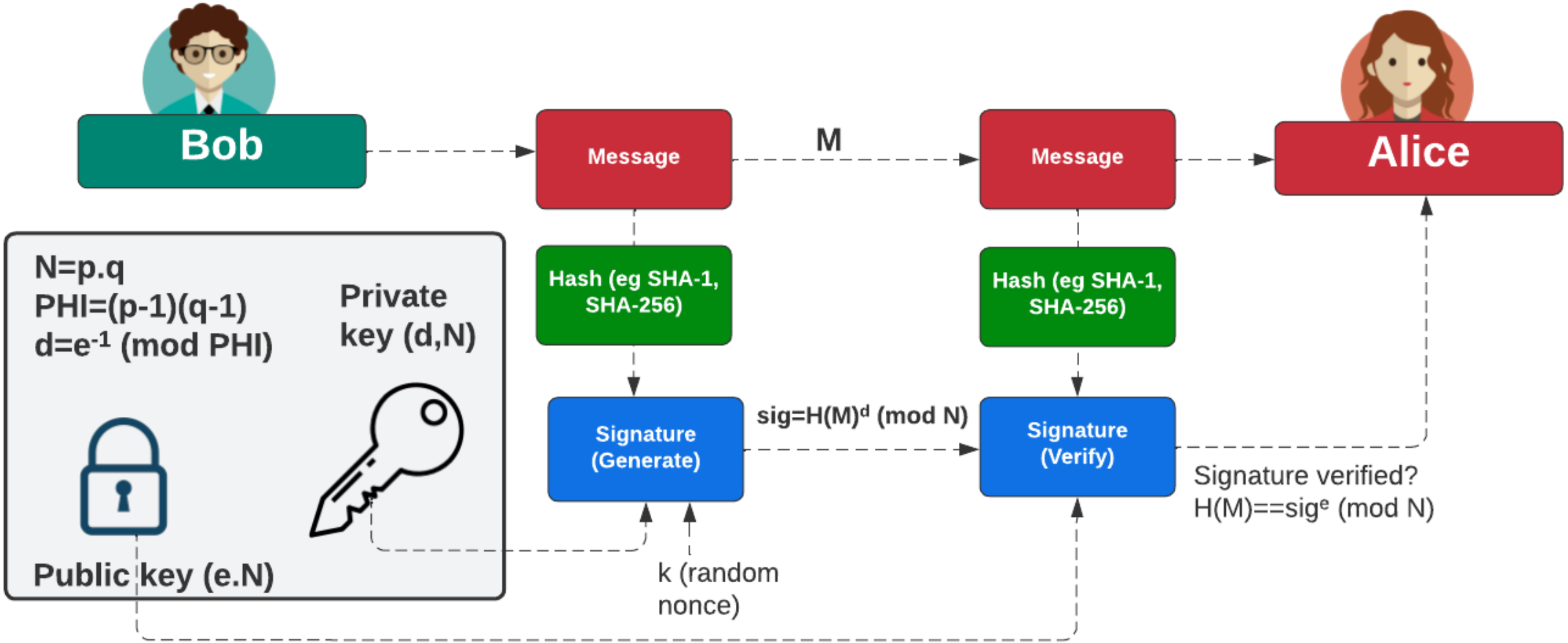
cyber & data

Public Key Encryption



&cyber data

Public Key (Digital Signing)



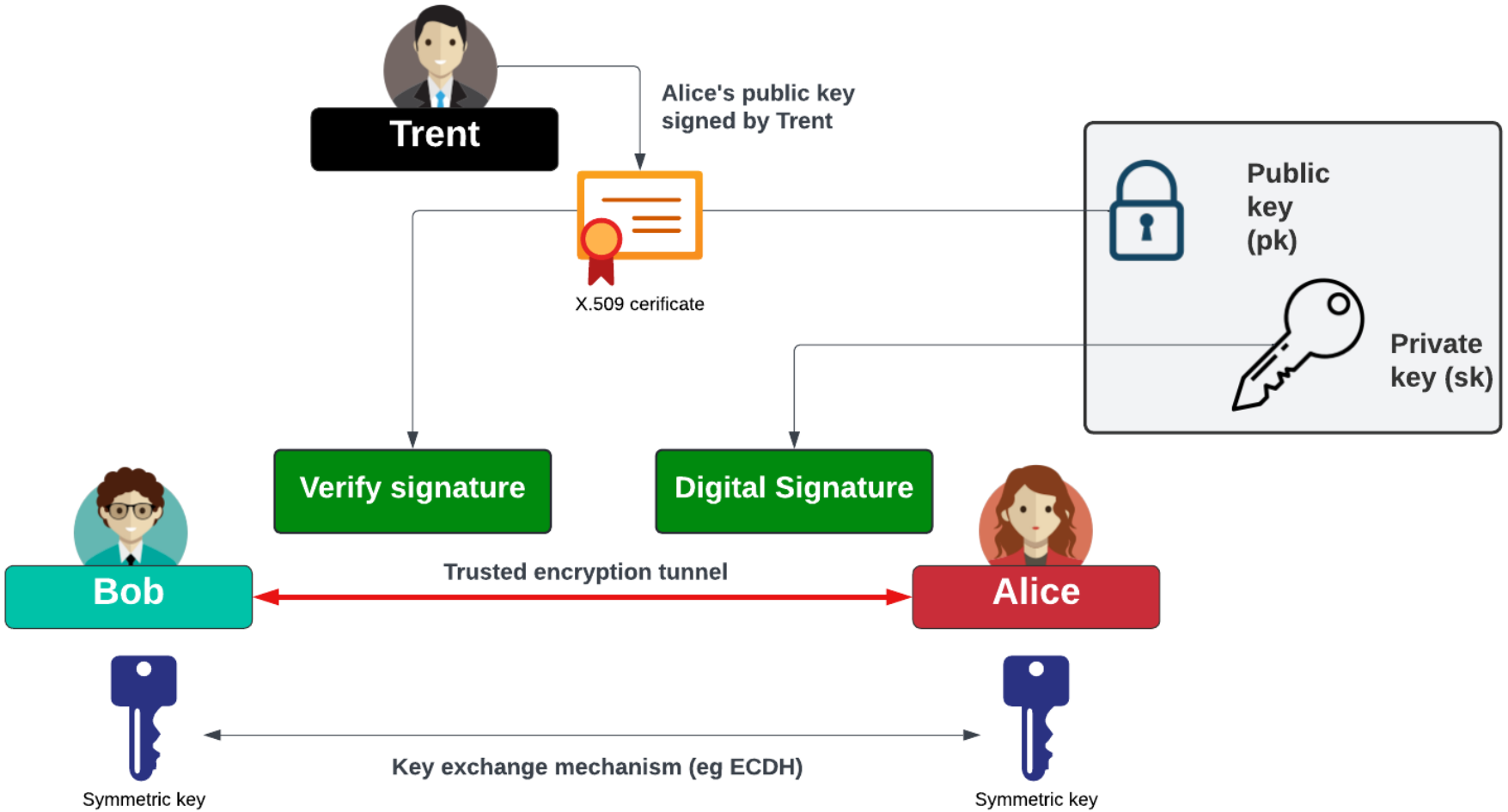
&cyber data

cyber & data

"From bits to information"

Outline of Secure Architectures

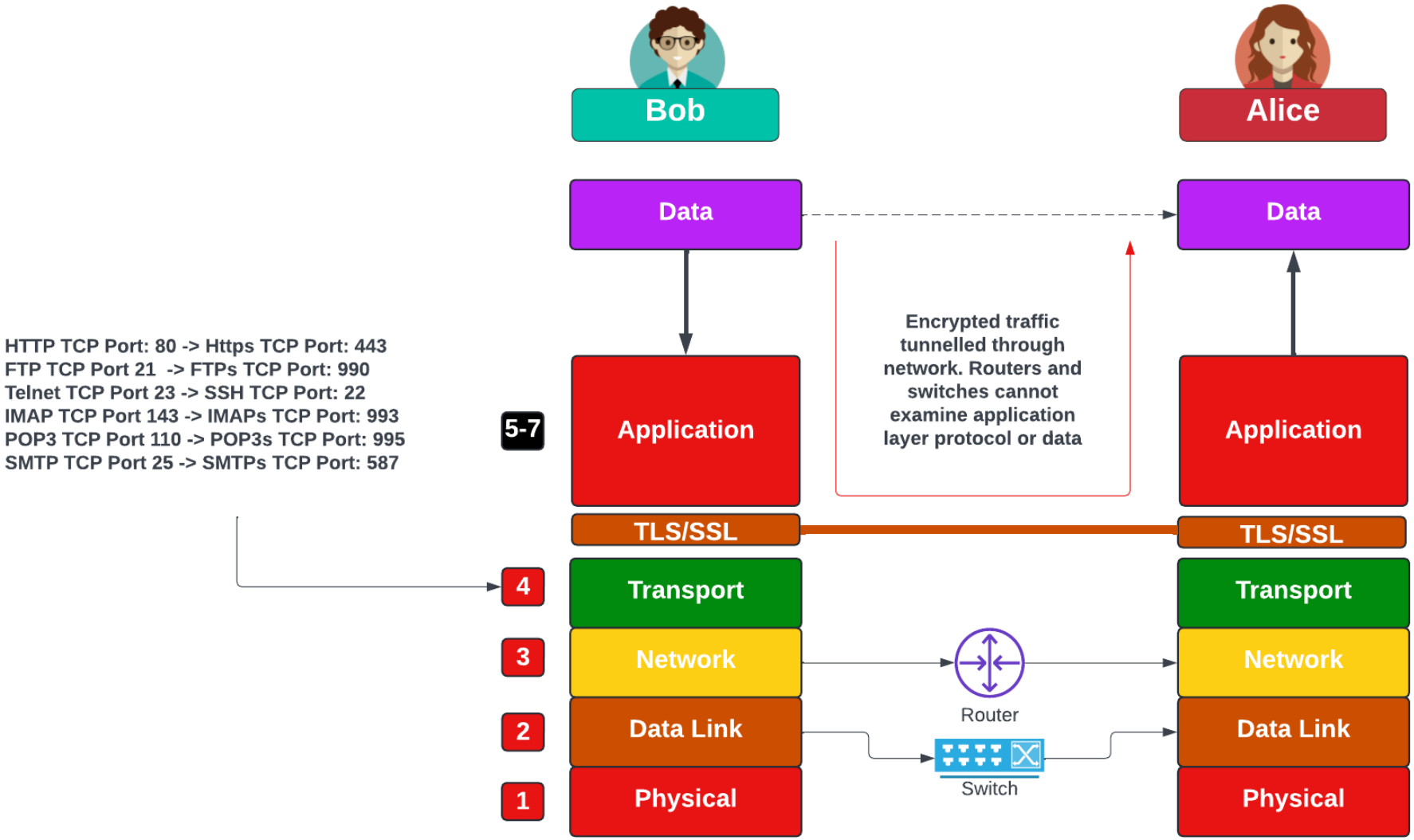
Trust, Privacy and Integrity



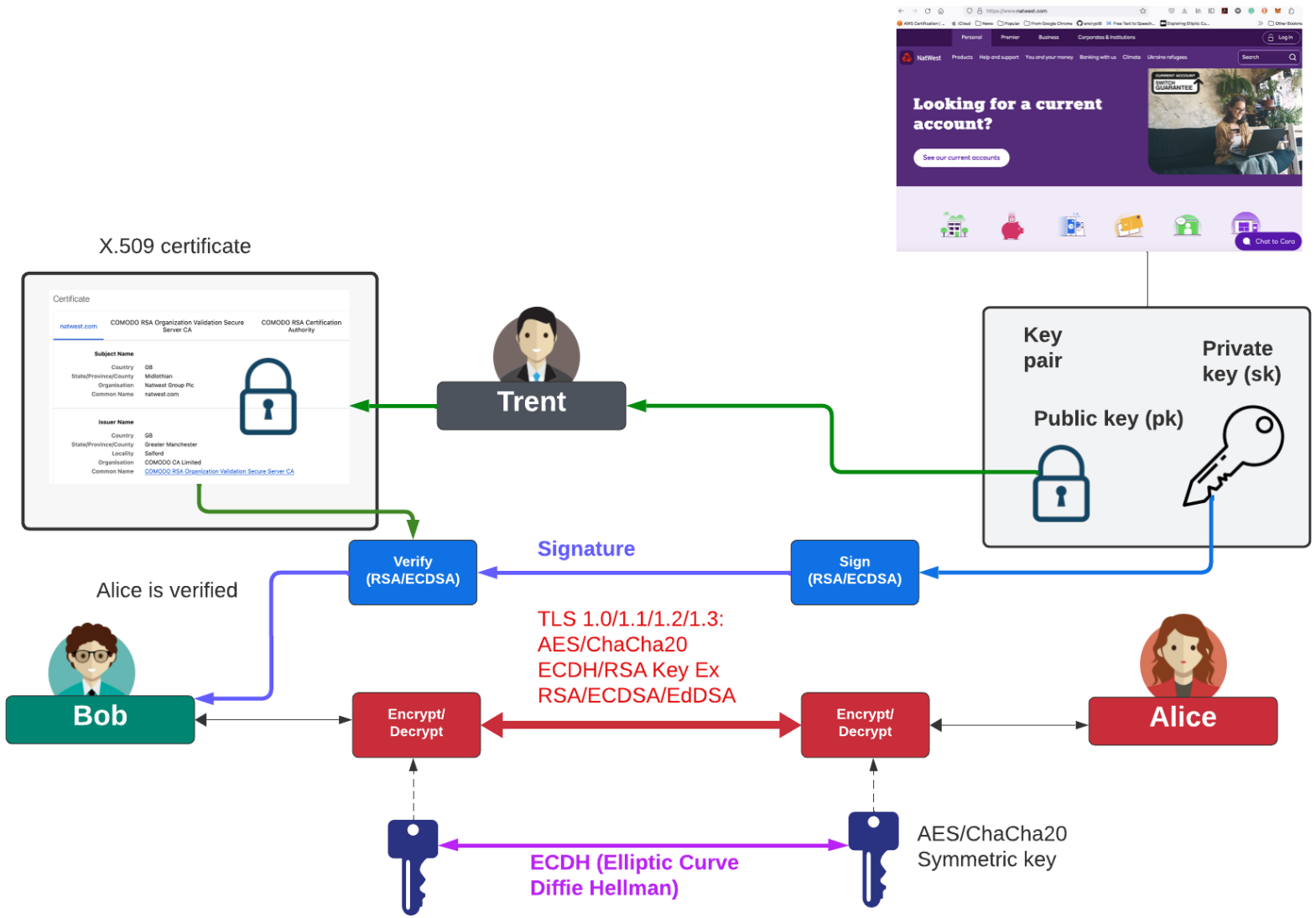
Public key method: RSA, ECDSA
Symmetric Key method: AES, ChaCha20
Integrity checking: SHA-1, SHA-256

&cyber data

Tunneled Traffic

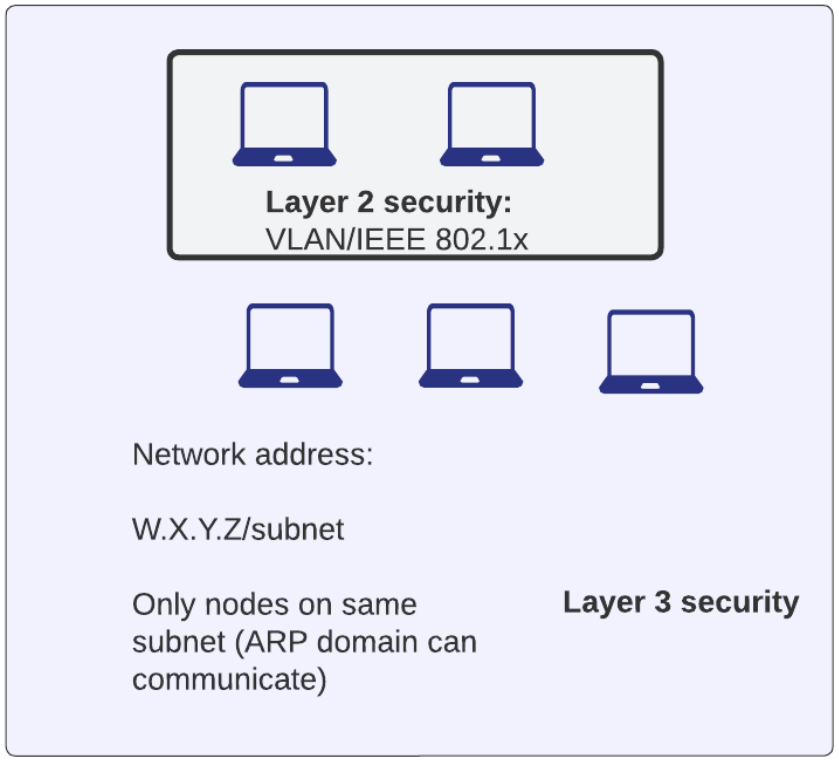


Tunneled Traffic

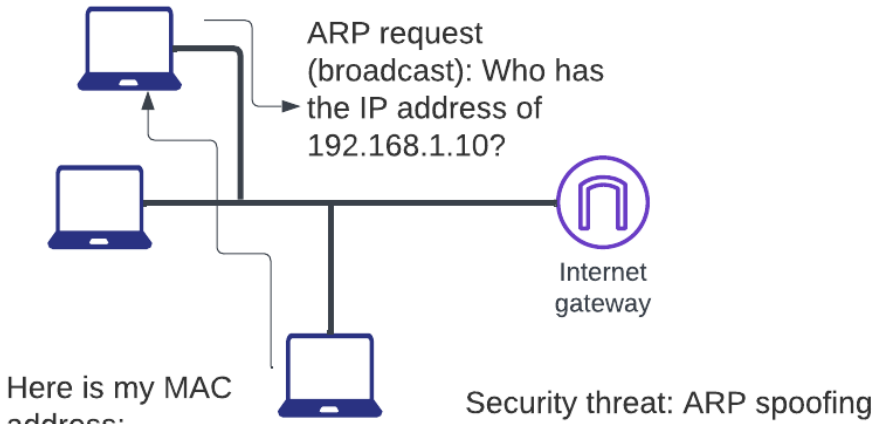


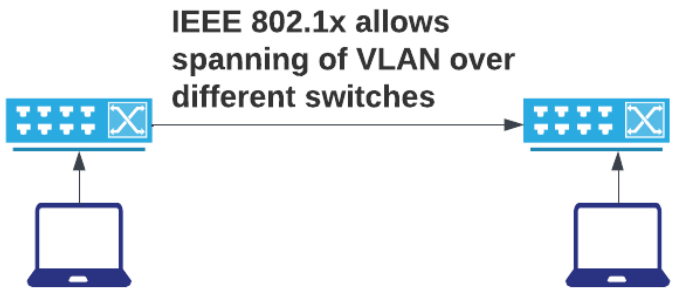
&cyber data

Layer 2 and Layer 3 Security



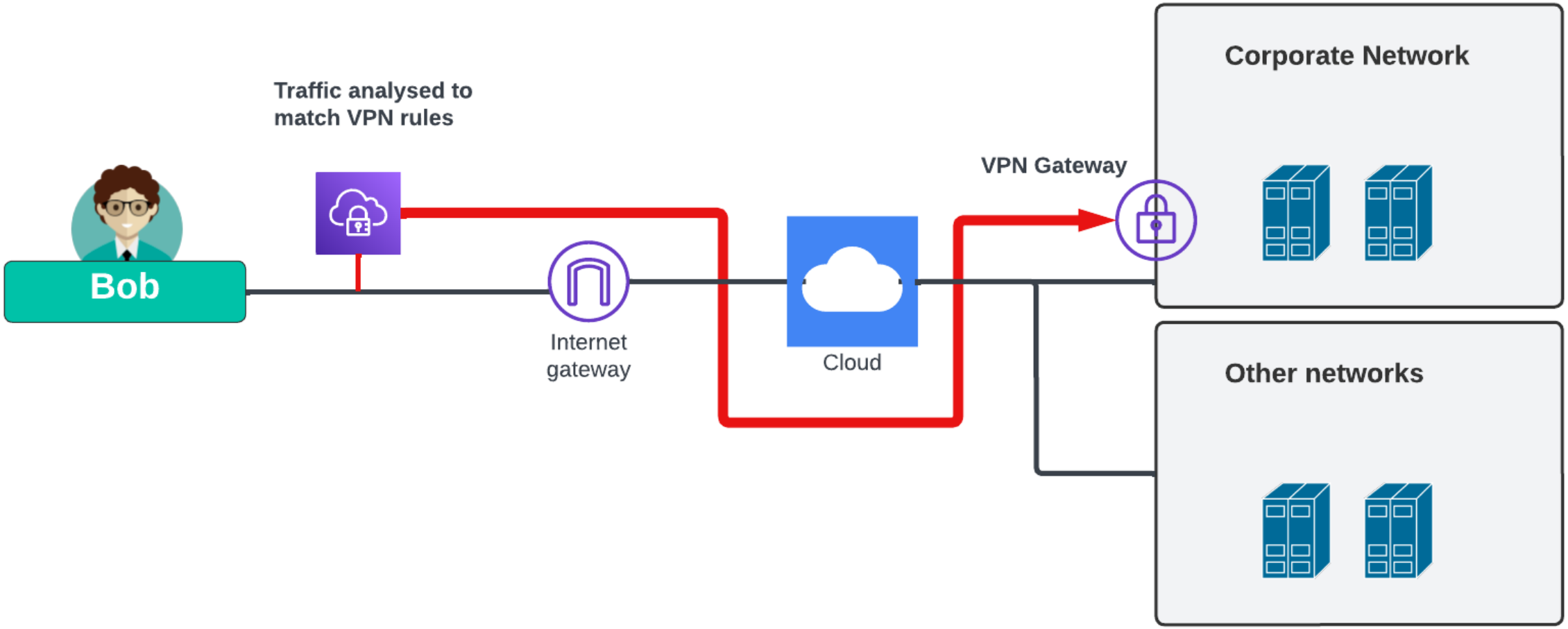
ARP Cache:
192.168.1.0 -> 11:22:33:44:55:66



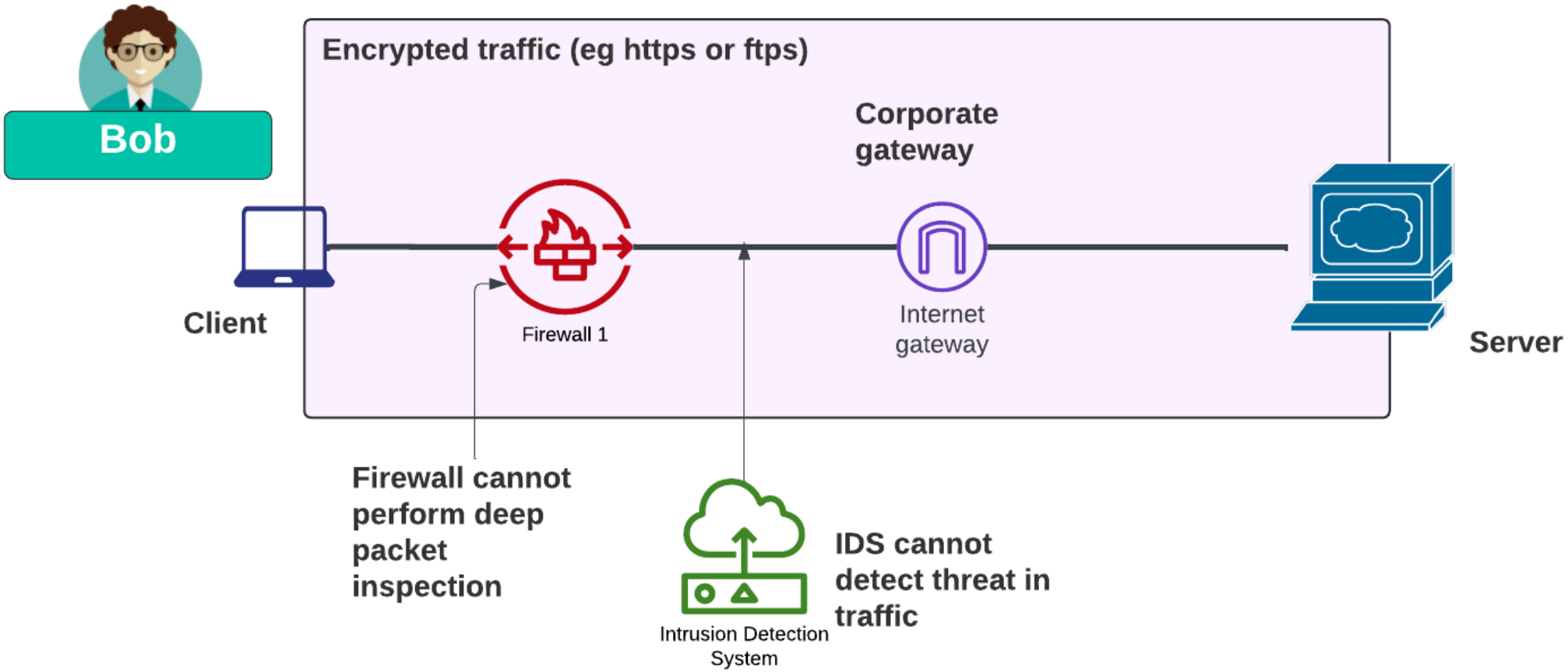


&cyber data

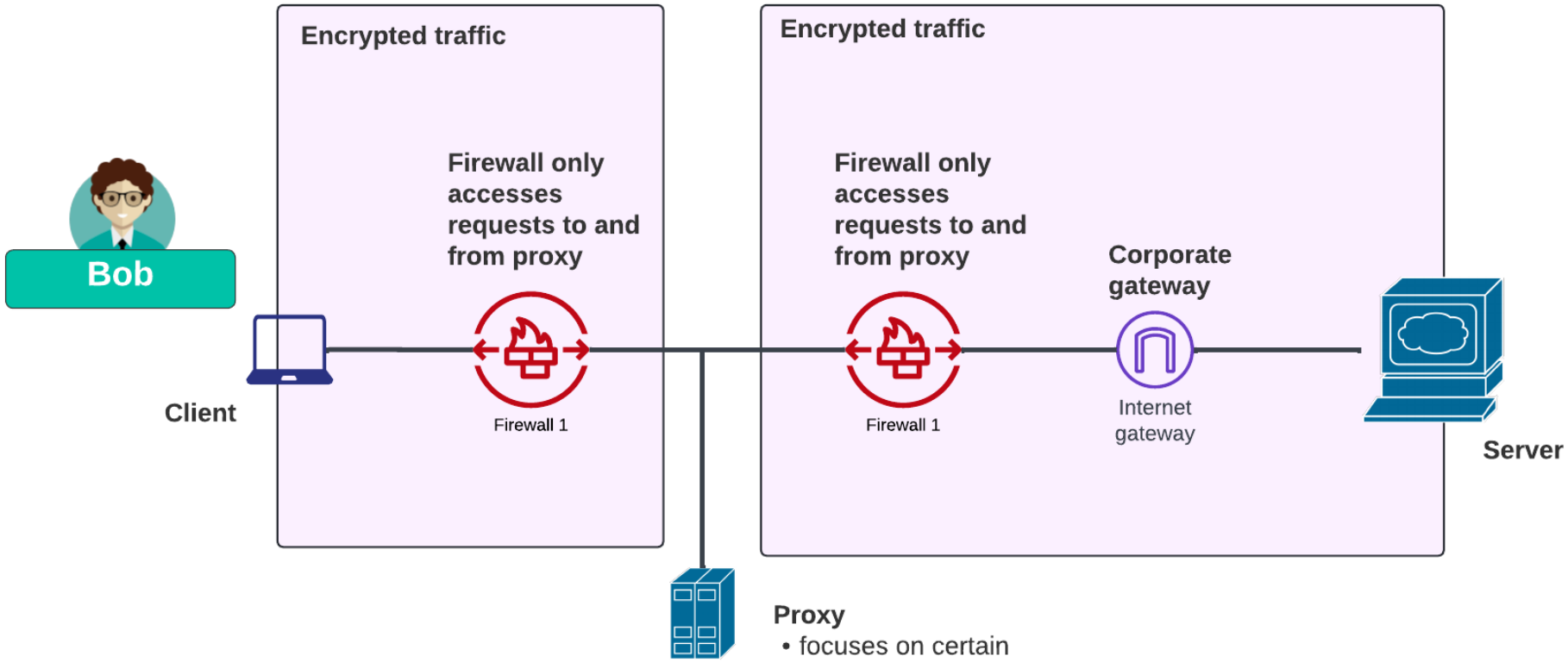
VPN (Virtual Private Network) Tunneling



Tunneled Traffic

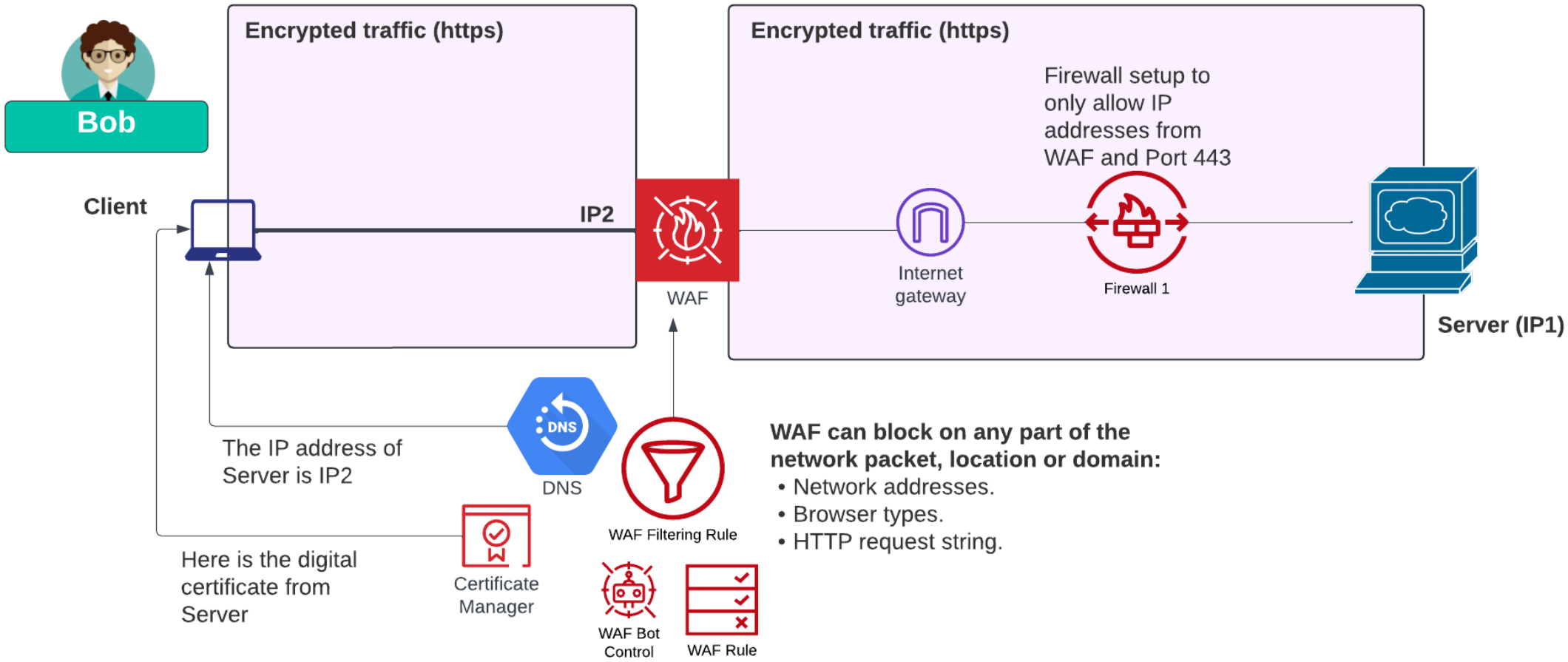


Dual-homed Architecture



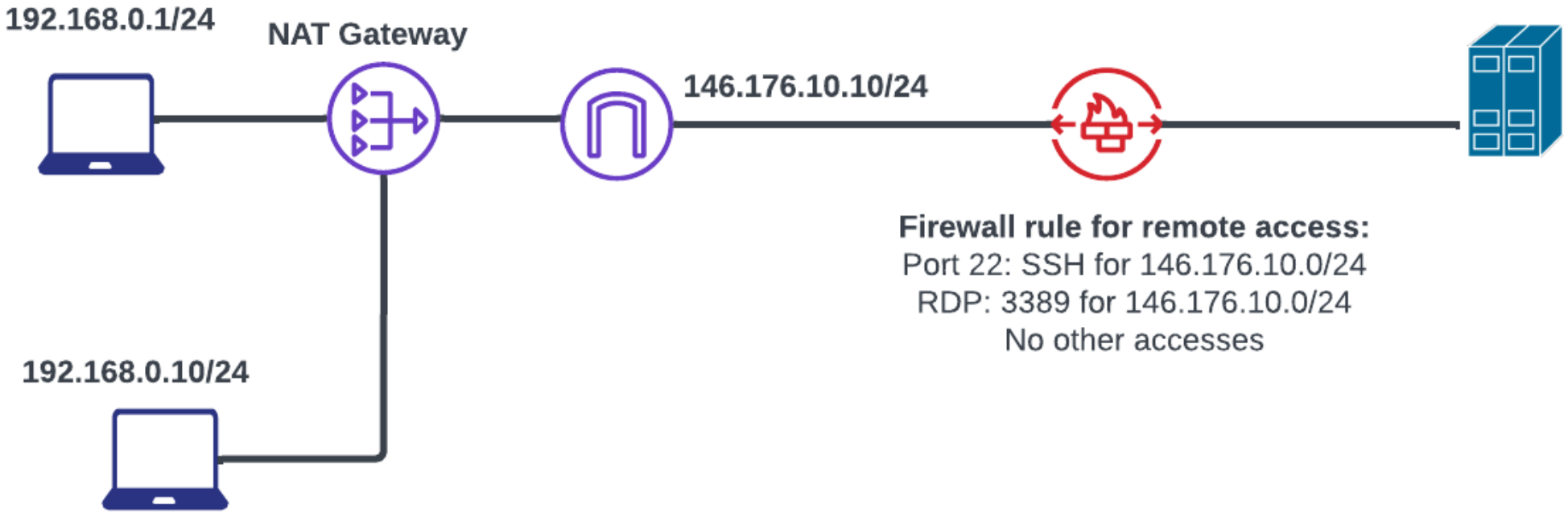
&cyber data

Web Application Firewall (WAF)



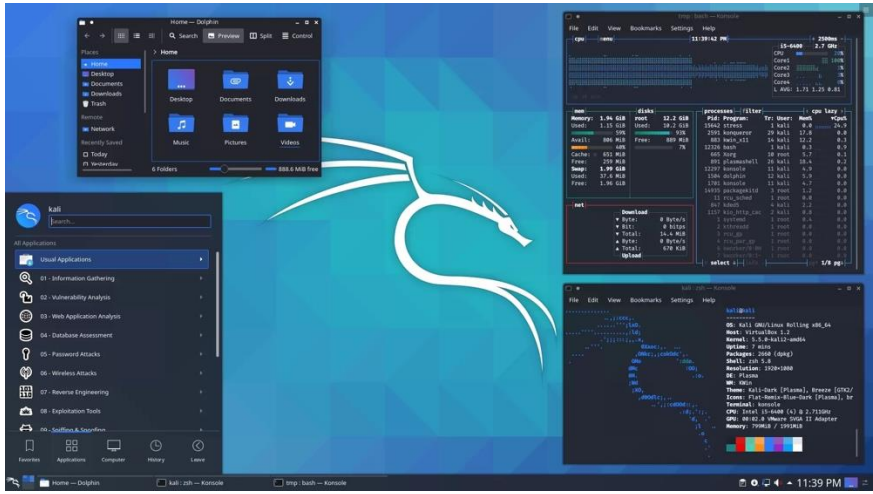
cyber &data

Remote Access to Device/Server



&cyber data

Pen Testing Tools



hydra -L list_user -P list_password 10.10.y.9 ftp

Hydra

nmap -O 10.10.10.10

Discover services
OS operating system
Devices connected

Creating exploits

metasploit

IP

BURPSUITE

Client setup for proxy at IP

Firewall

bill:$apr1$waZS/8Tm$jDZmiZBct/c2hysERc

Password database

Discoverting messages passed from client to server

Nessus

Scanning for know vulnerabilities

WIRESHARK

OWASP ZAP

Hashcat

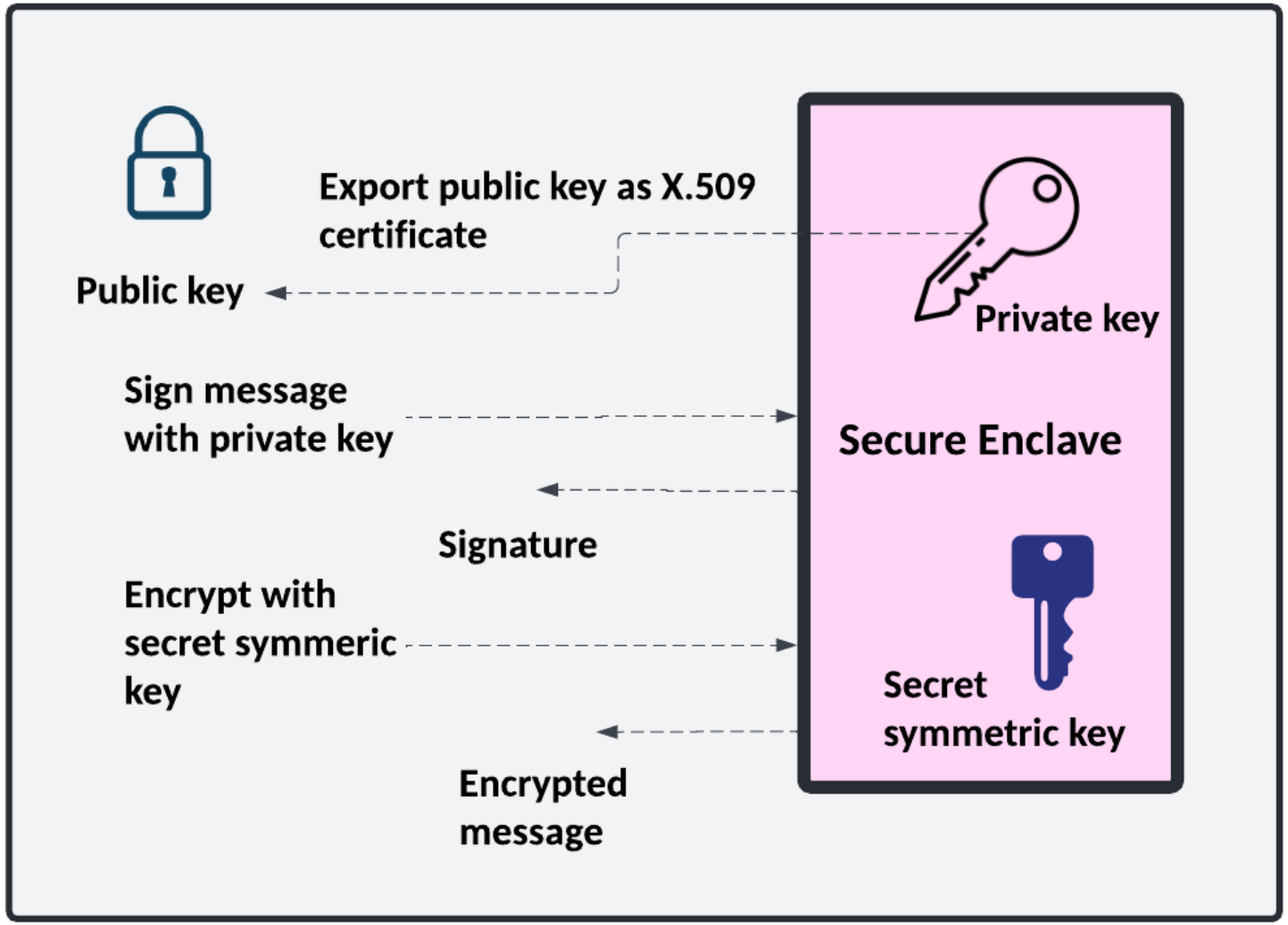
hashcat –m 0 hash1 words

&cyber data

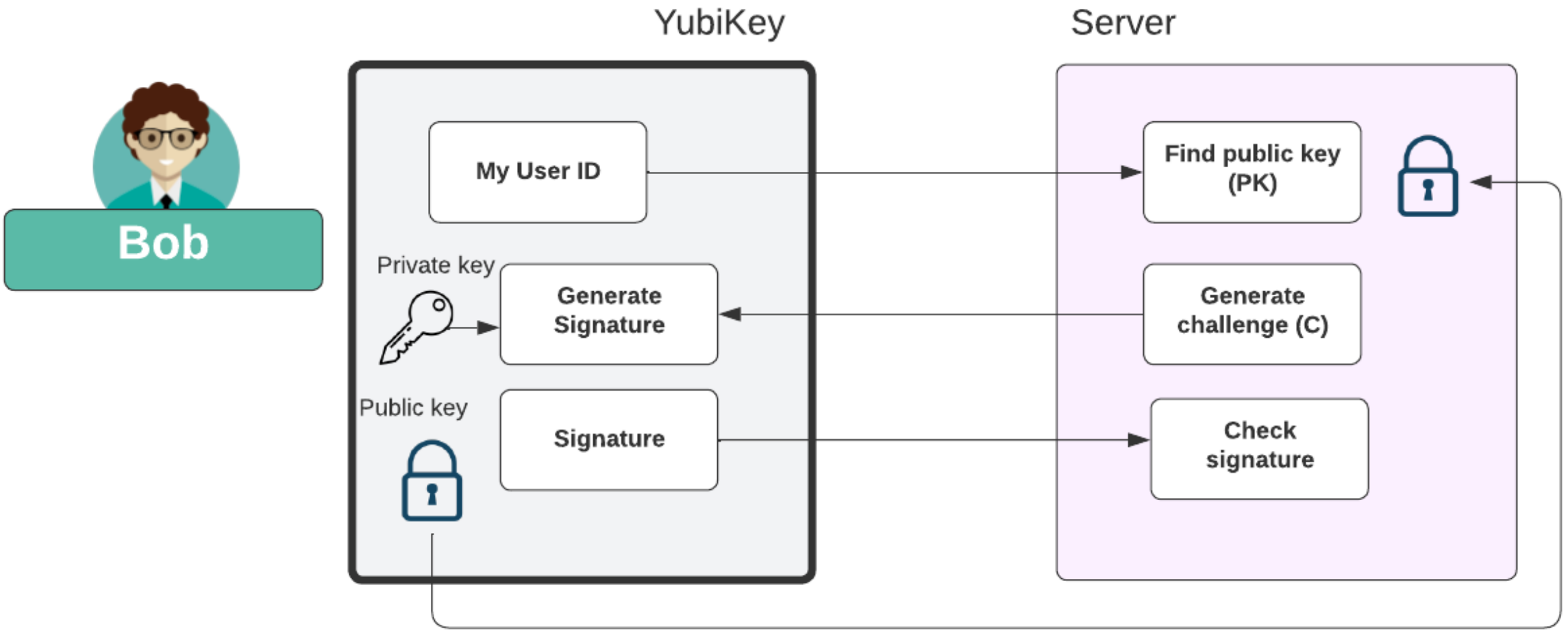
"From bits to information"

Secure Enclaves

Secure Enclaves

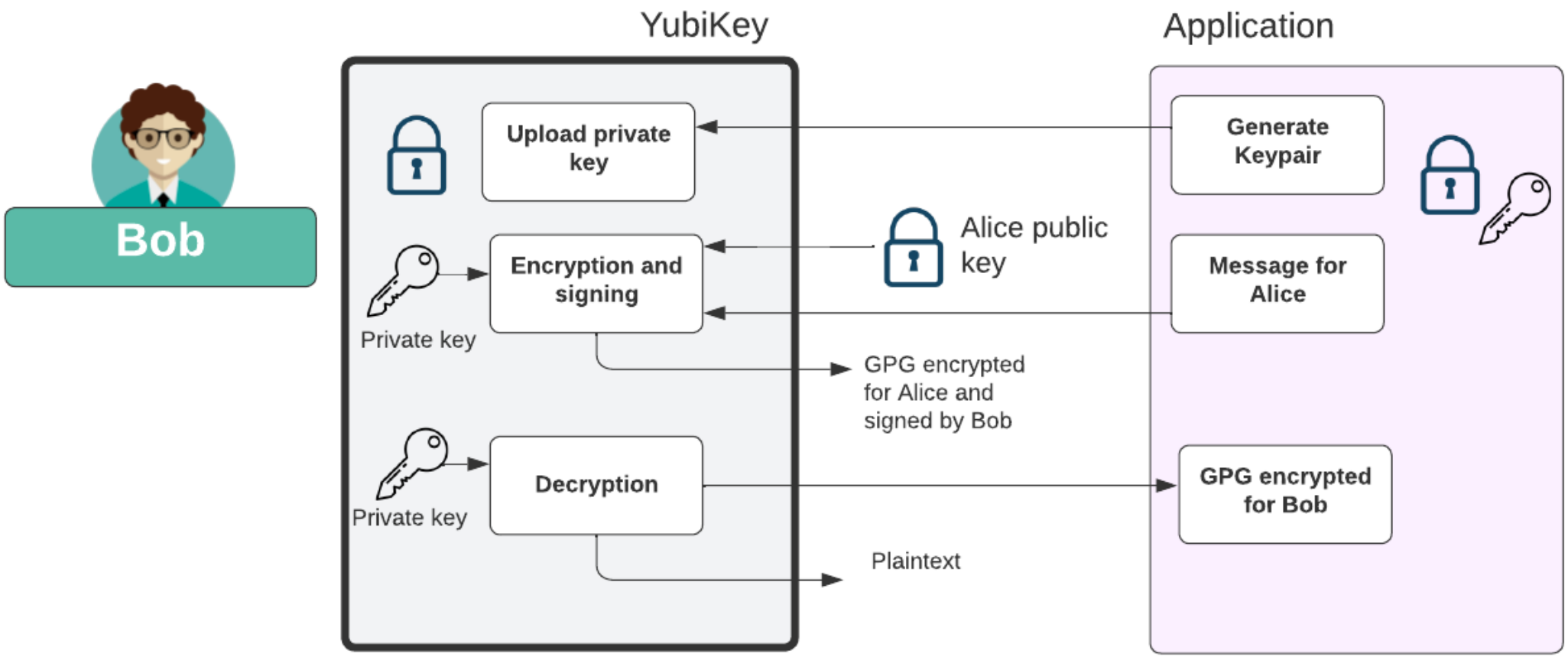


Secure Enclaves



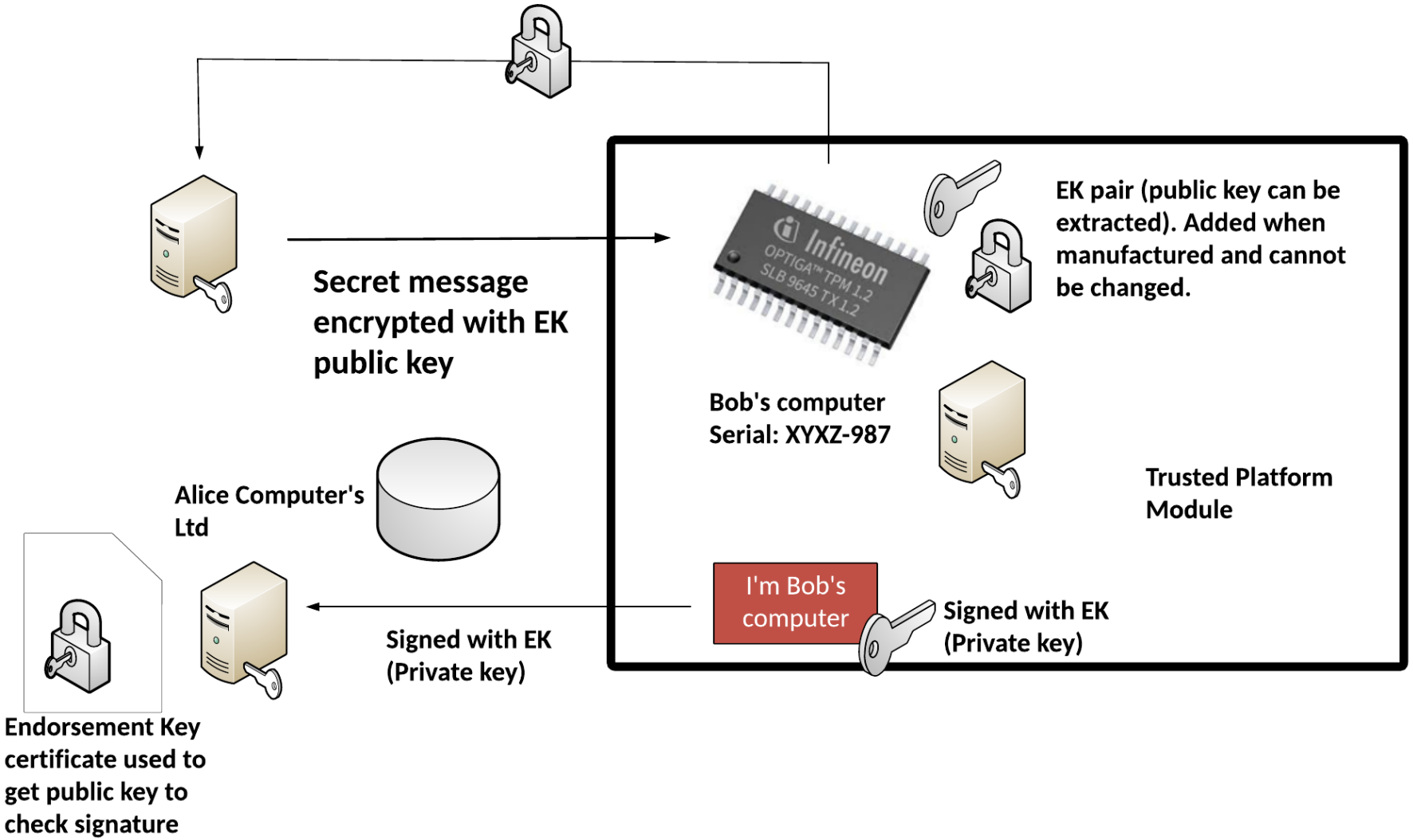
&cyber data

Secure Enclaves



&cyber data

MITRE EMB3D (Embedded Devices)



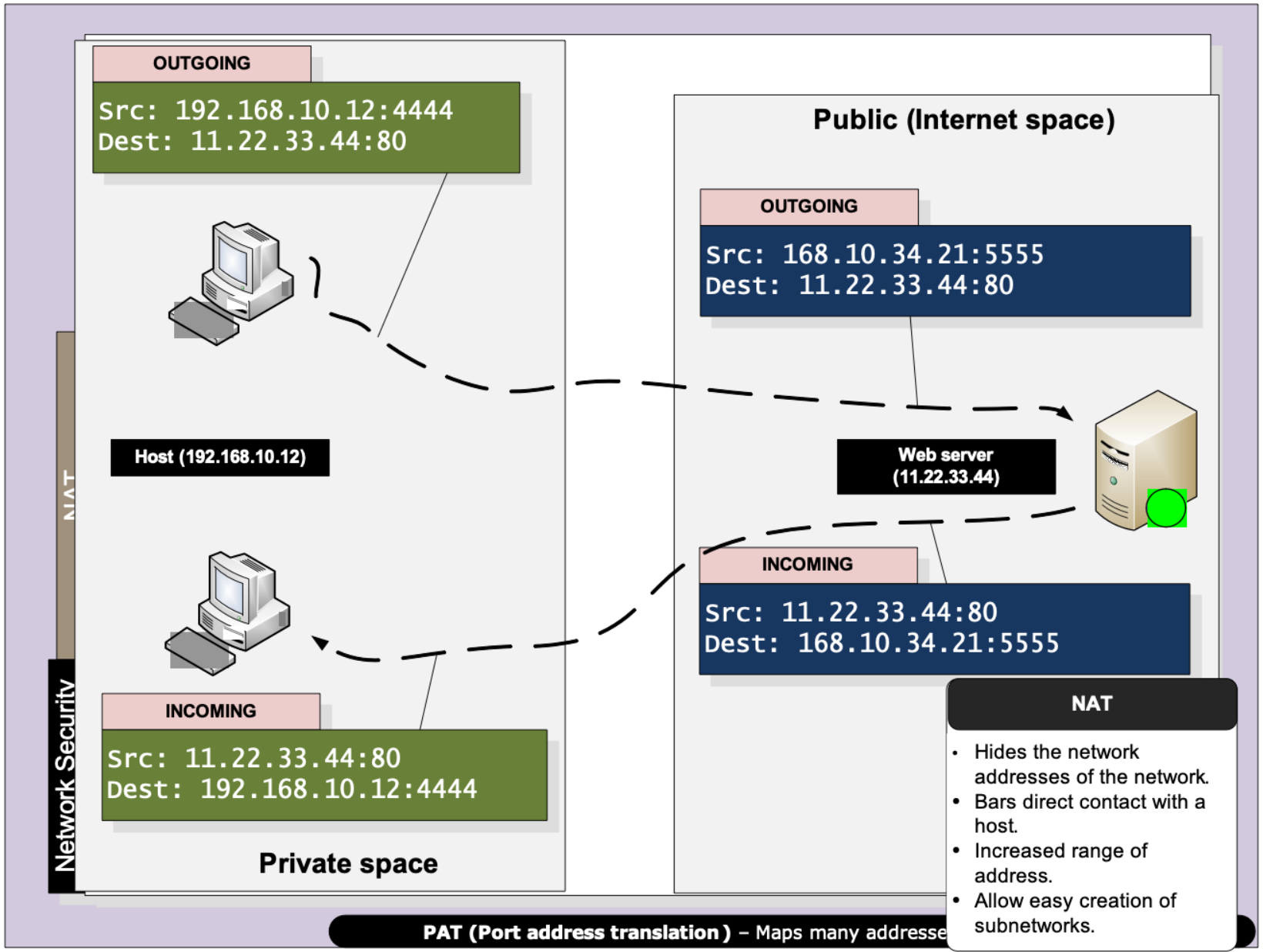
cyber &data

cyber & data

"From bits to information"

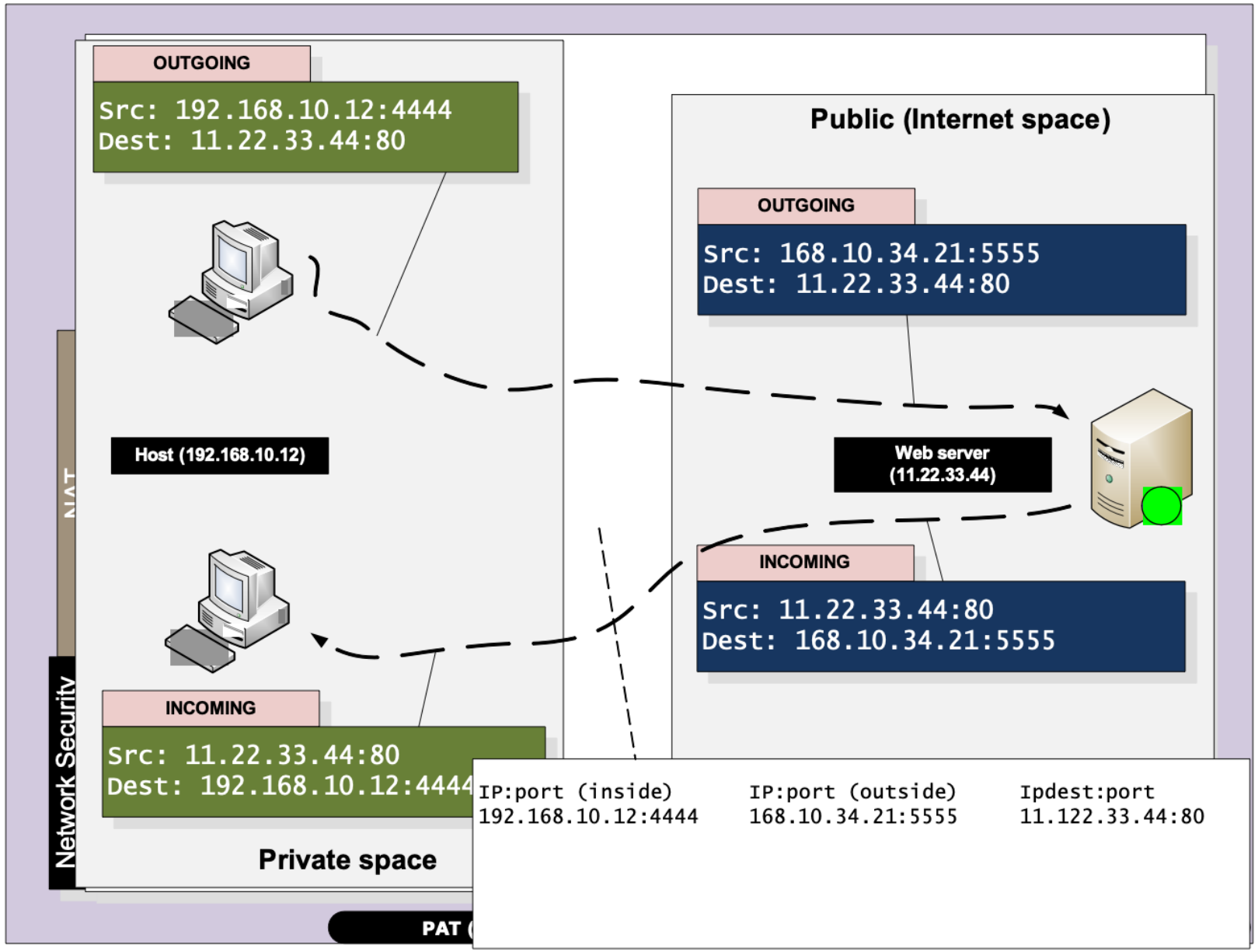
NAT

Layered Model



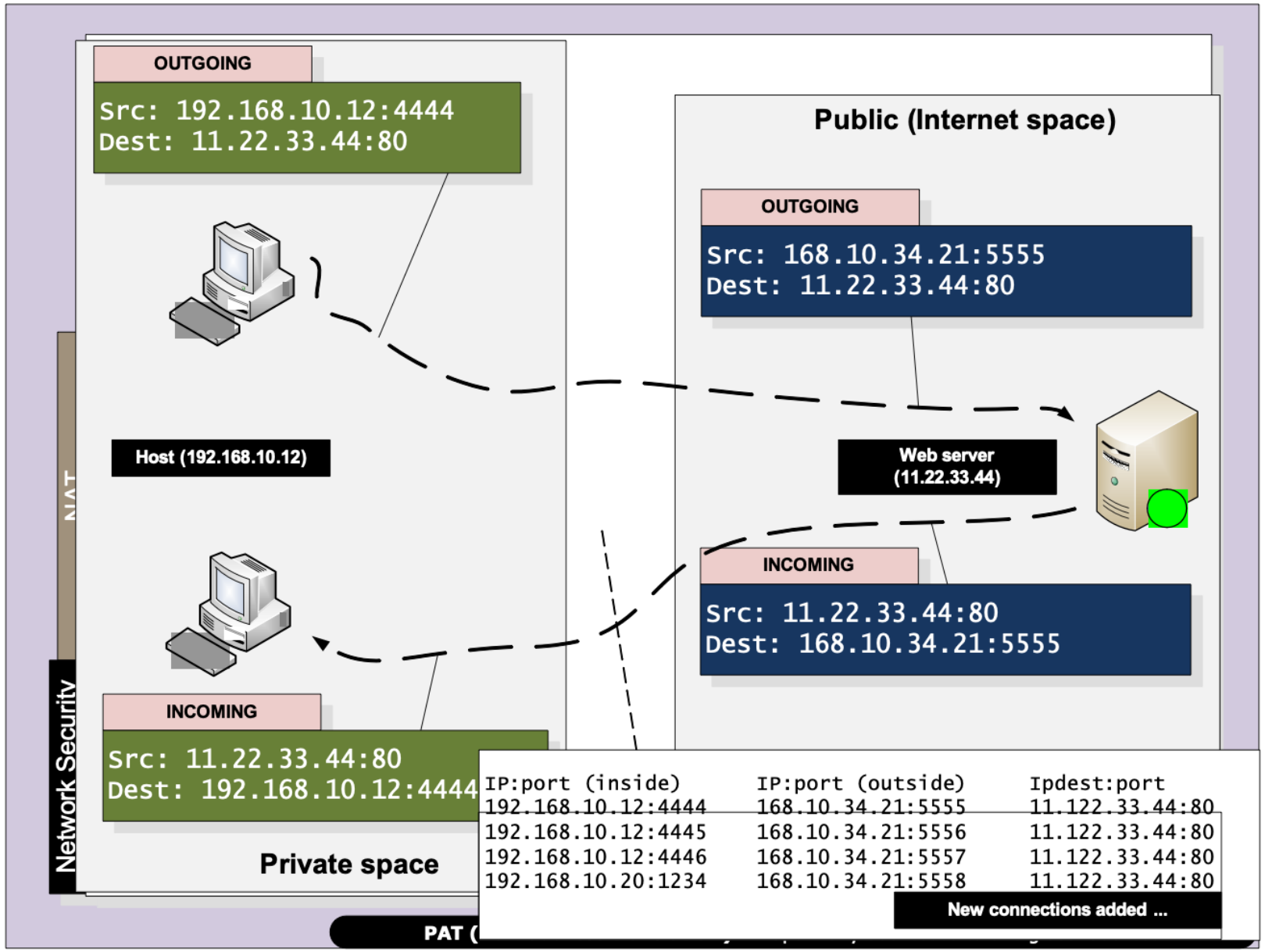
&cyber data

Layered Model



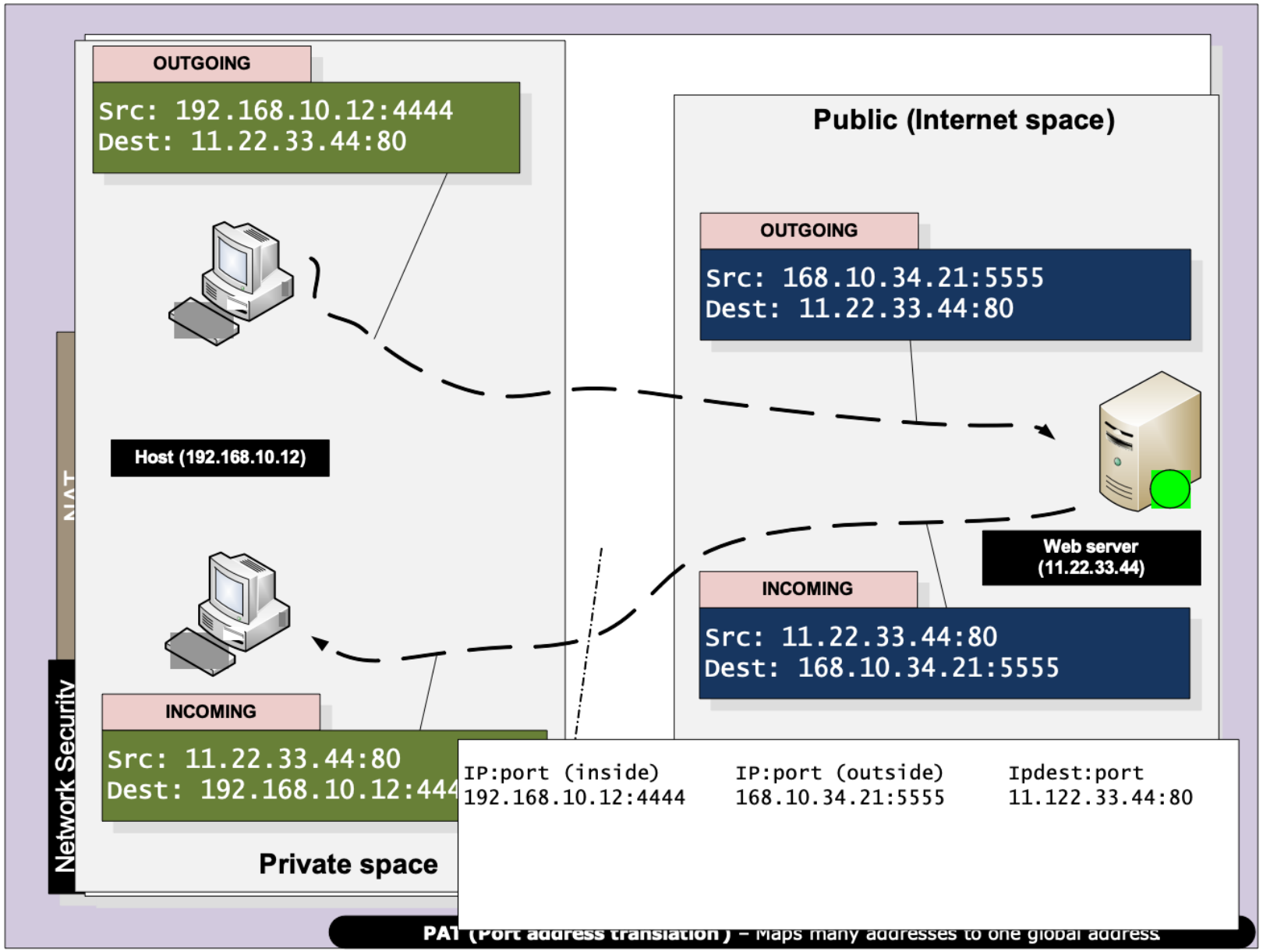
&cyber data

Layered Model



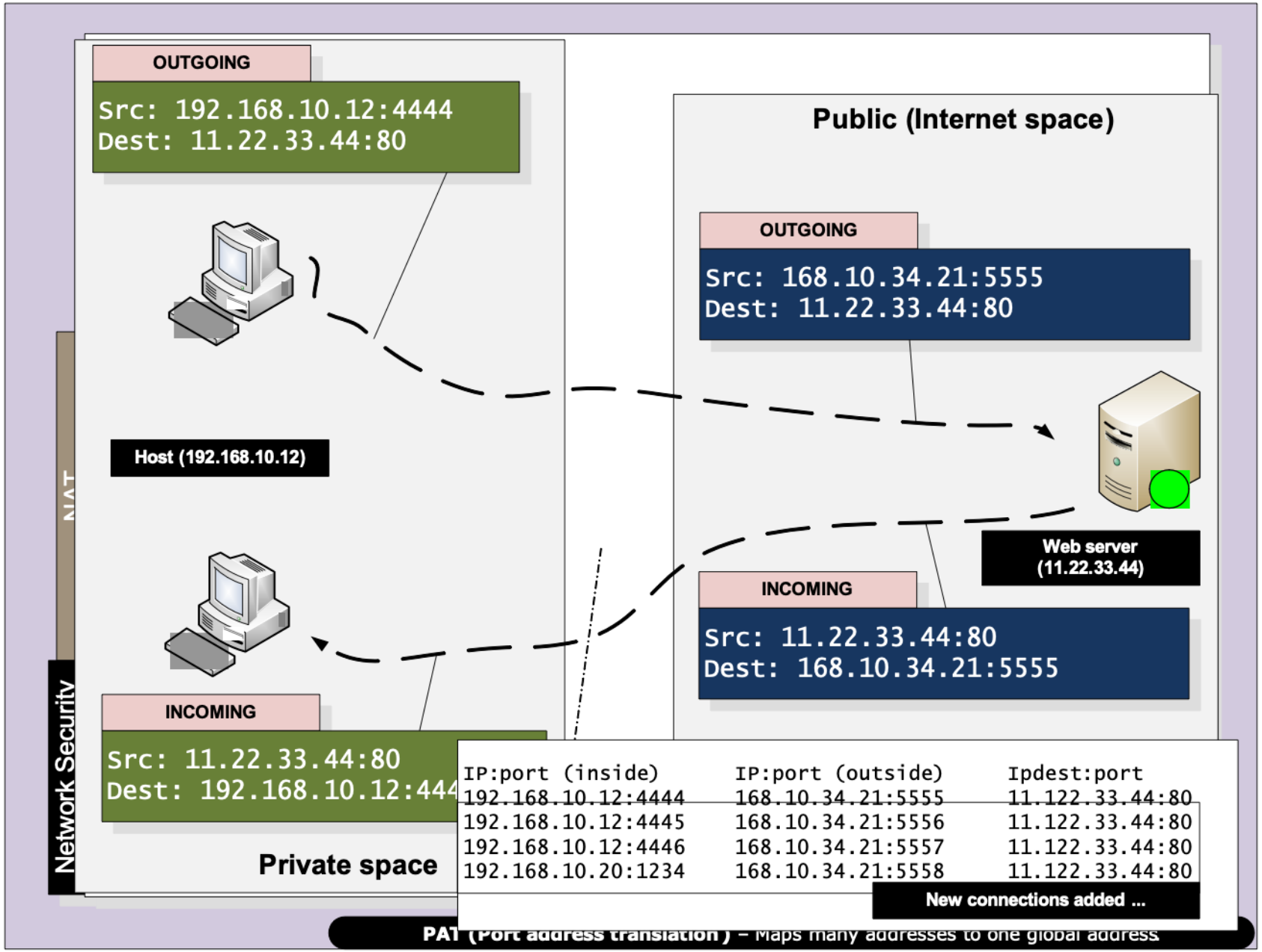
&cyber data

Layered Model



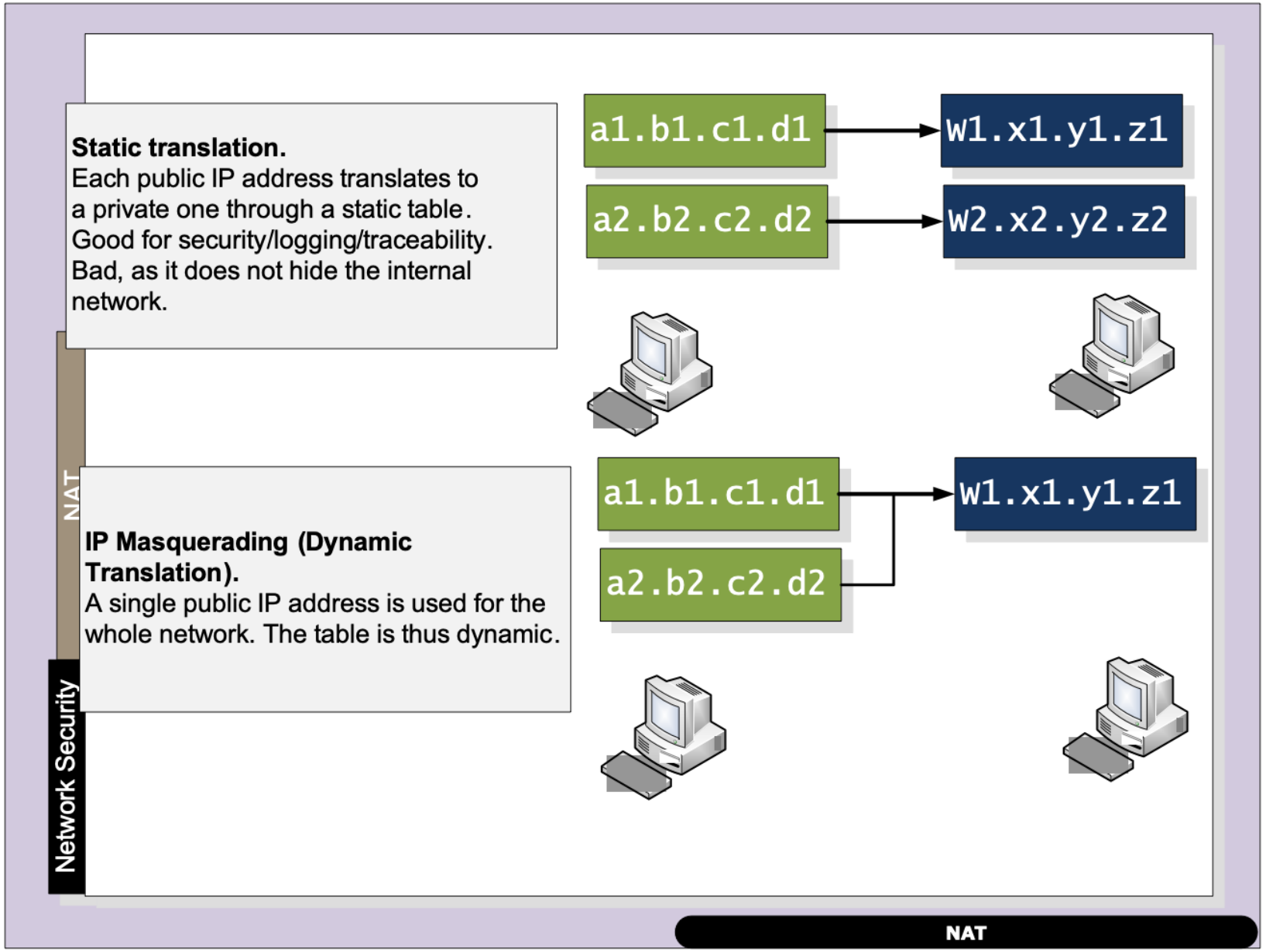
&cyber data

Layered Model



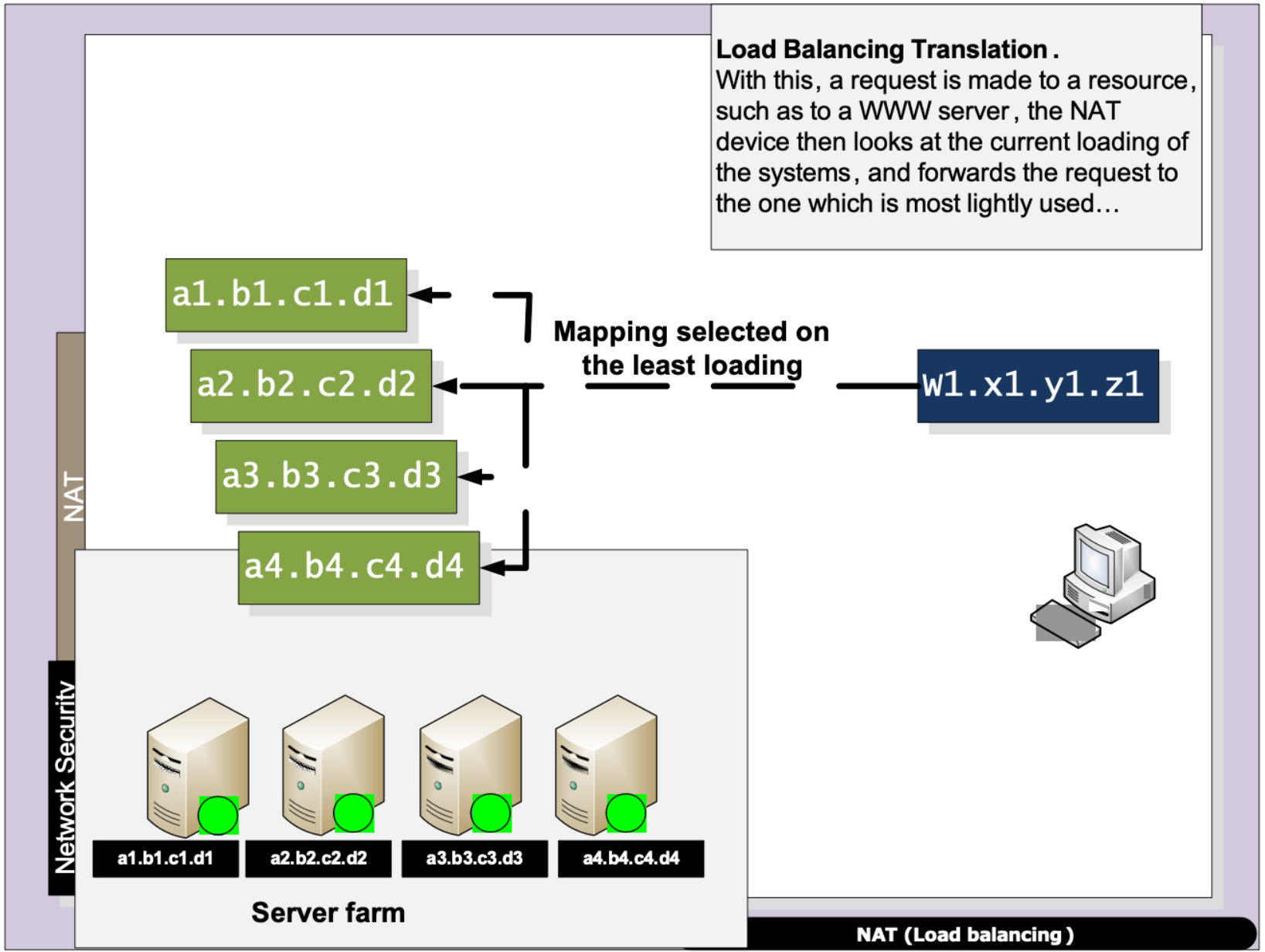
&cyber data

Layered Model



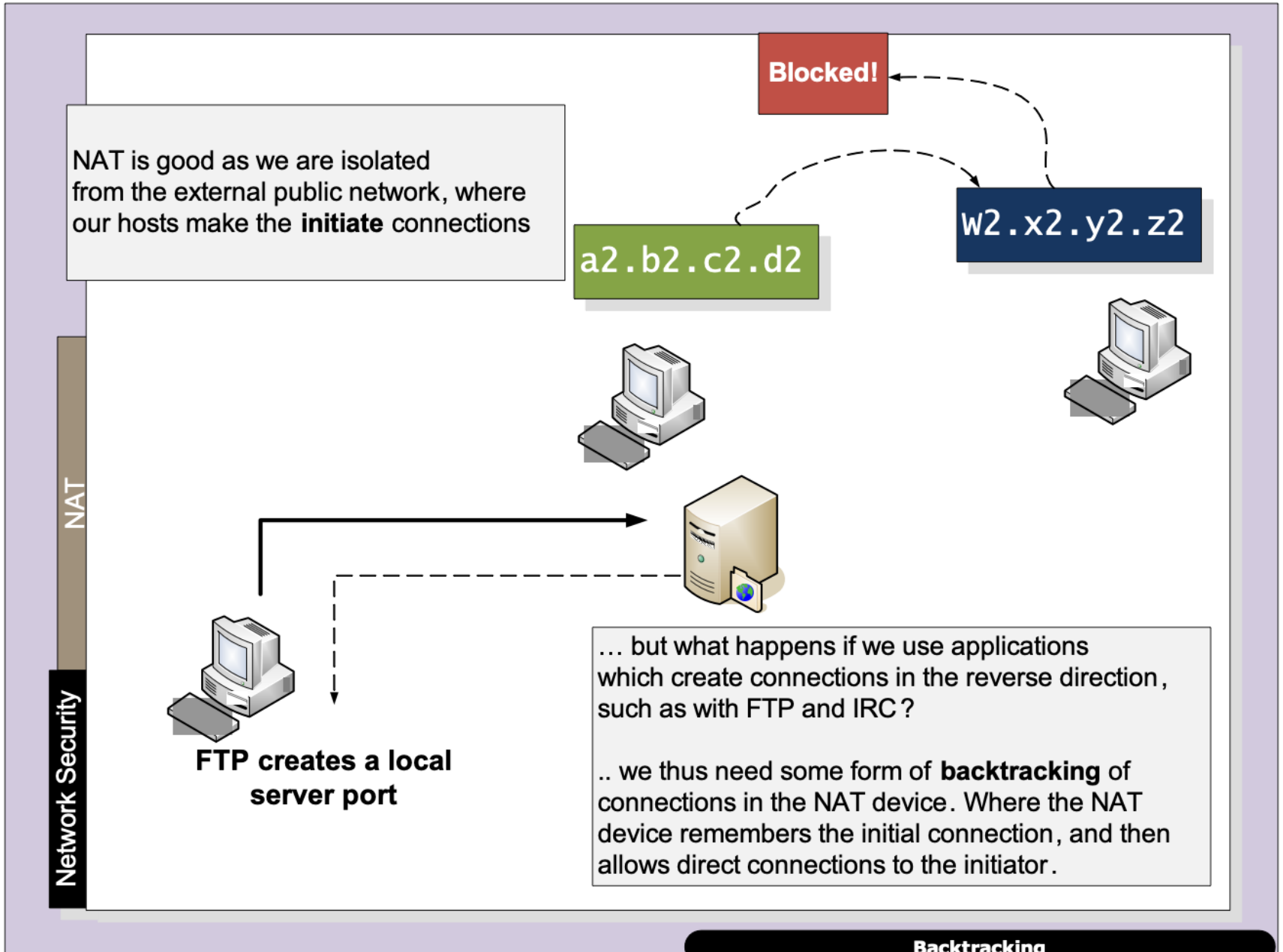
&cyber data

Layered Model



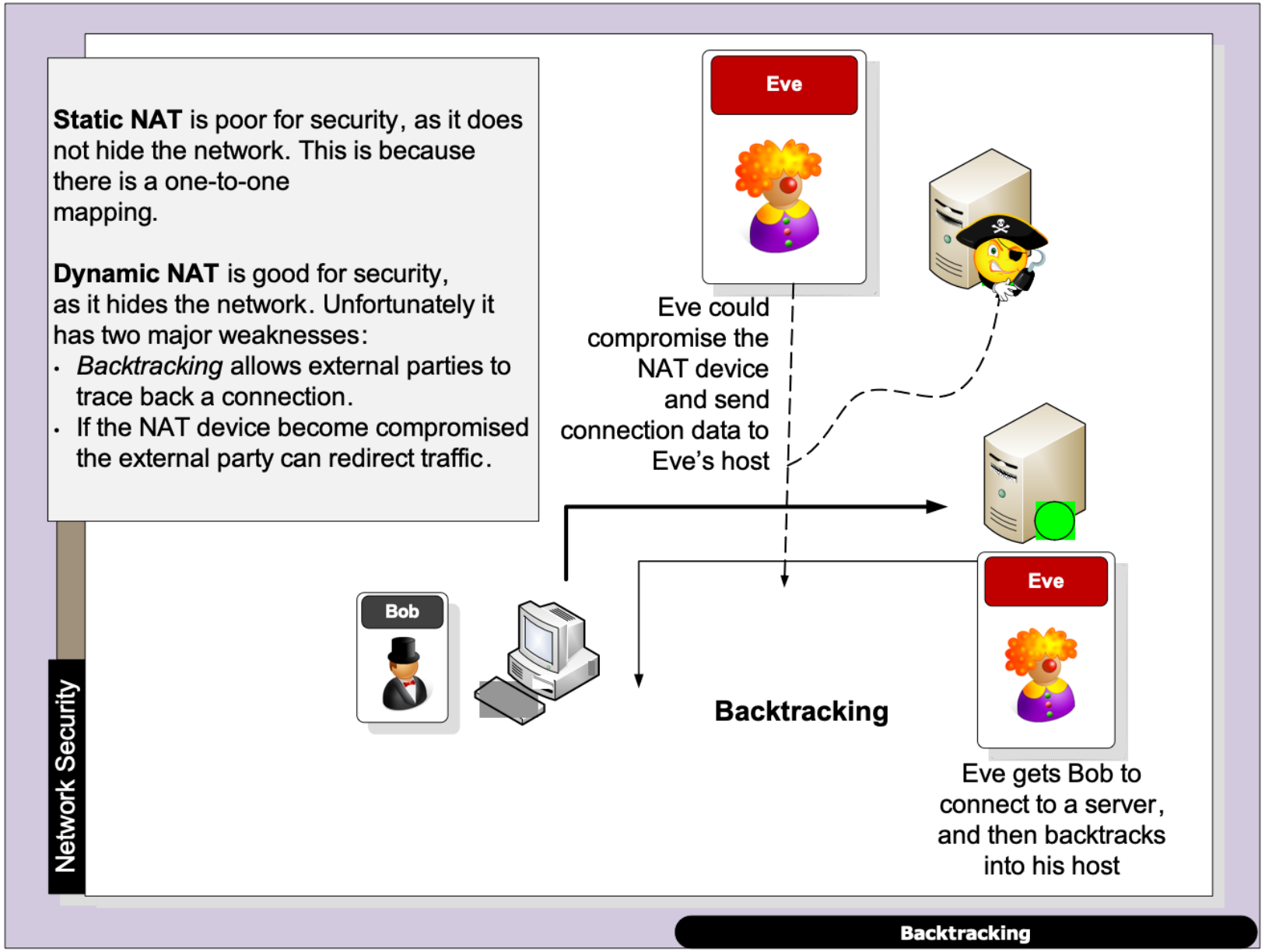
&cyber data

Layered Model



&cyber data

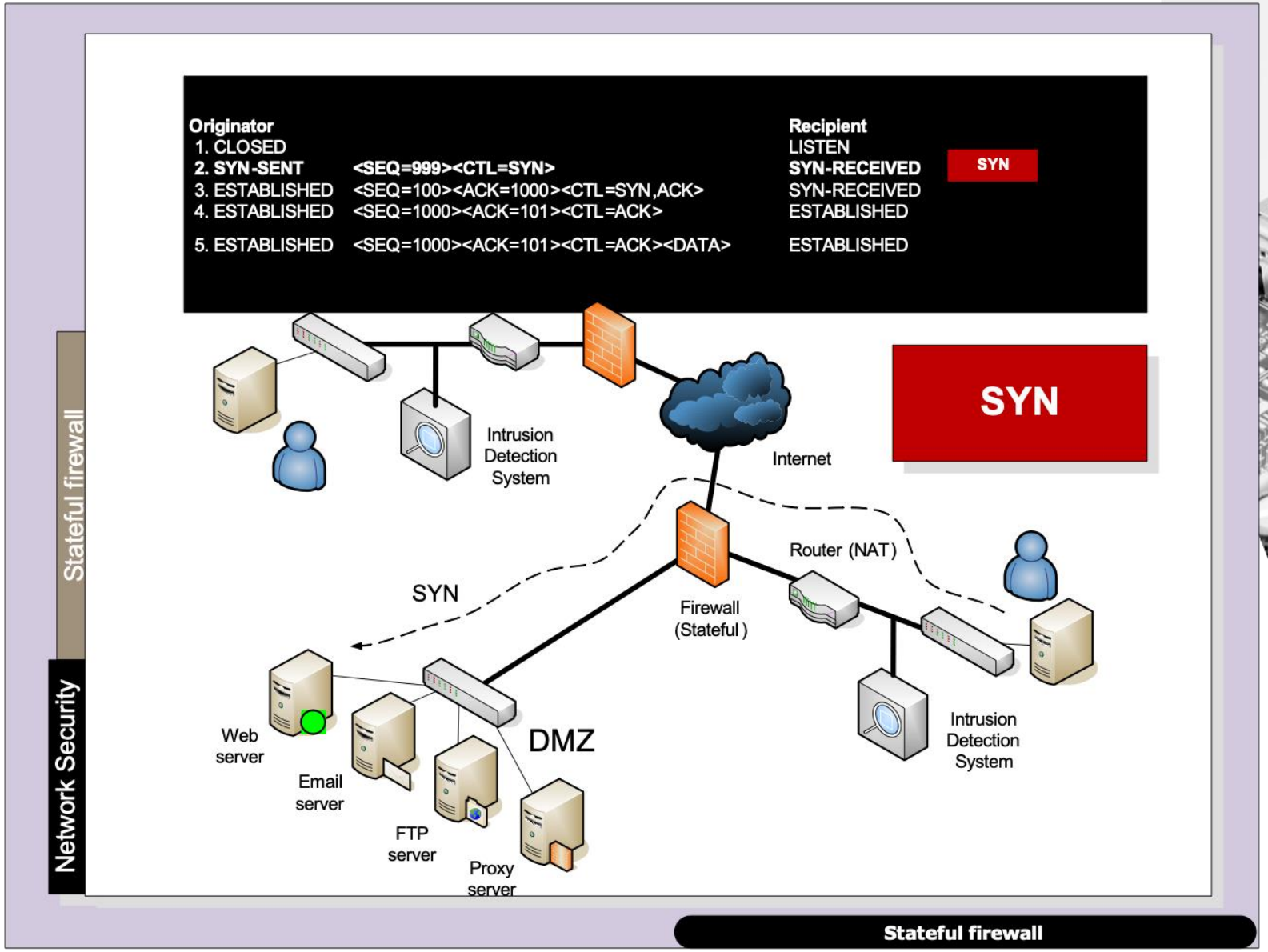
Layered Model

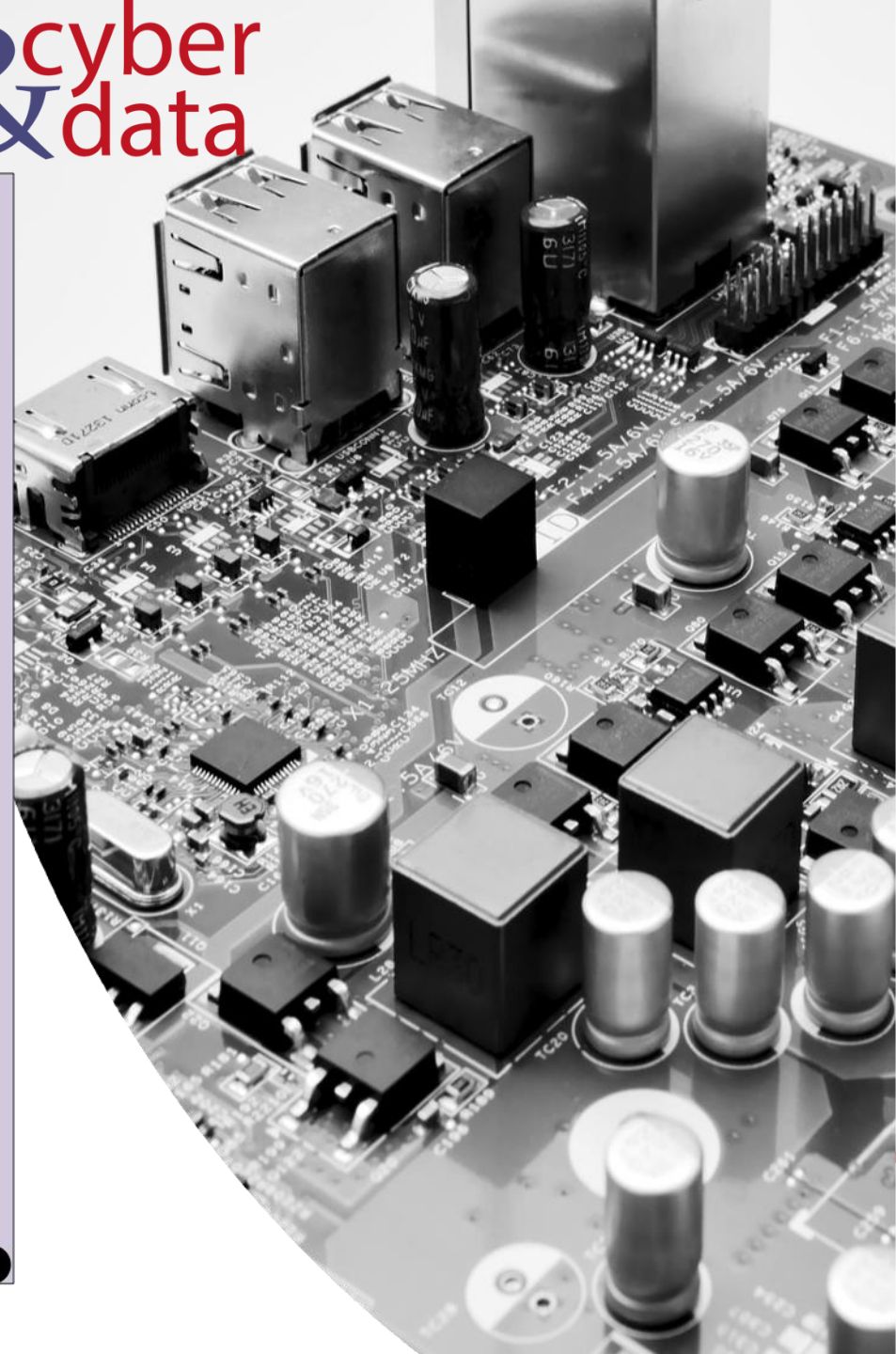


"From bits to information"

Stateful Firewalls

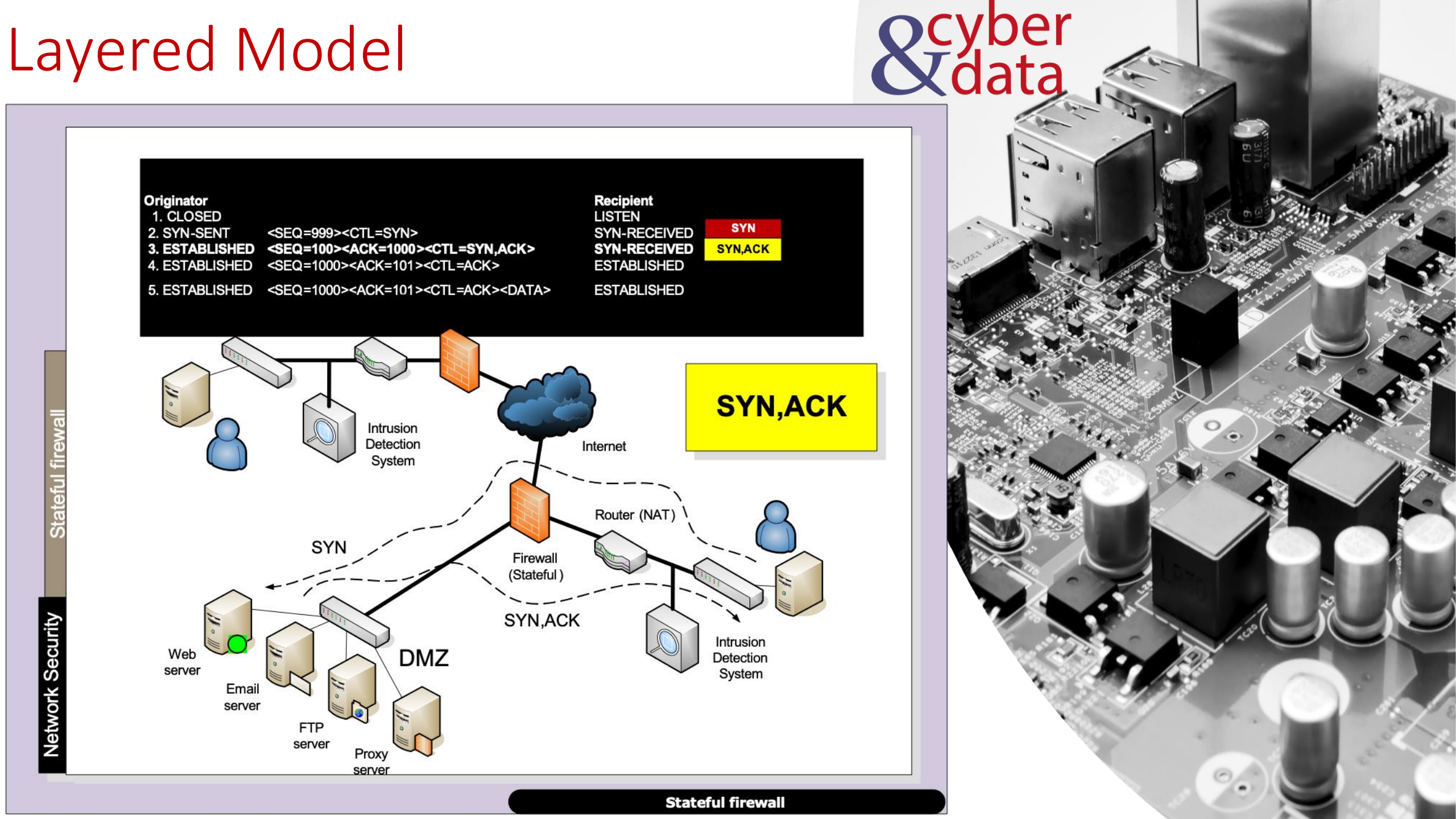
Layered Model



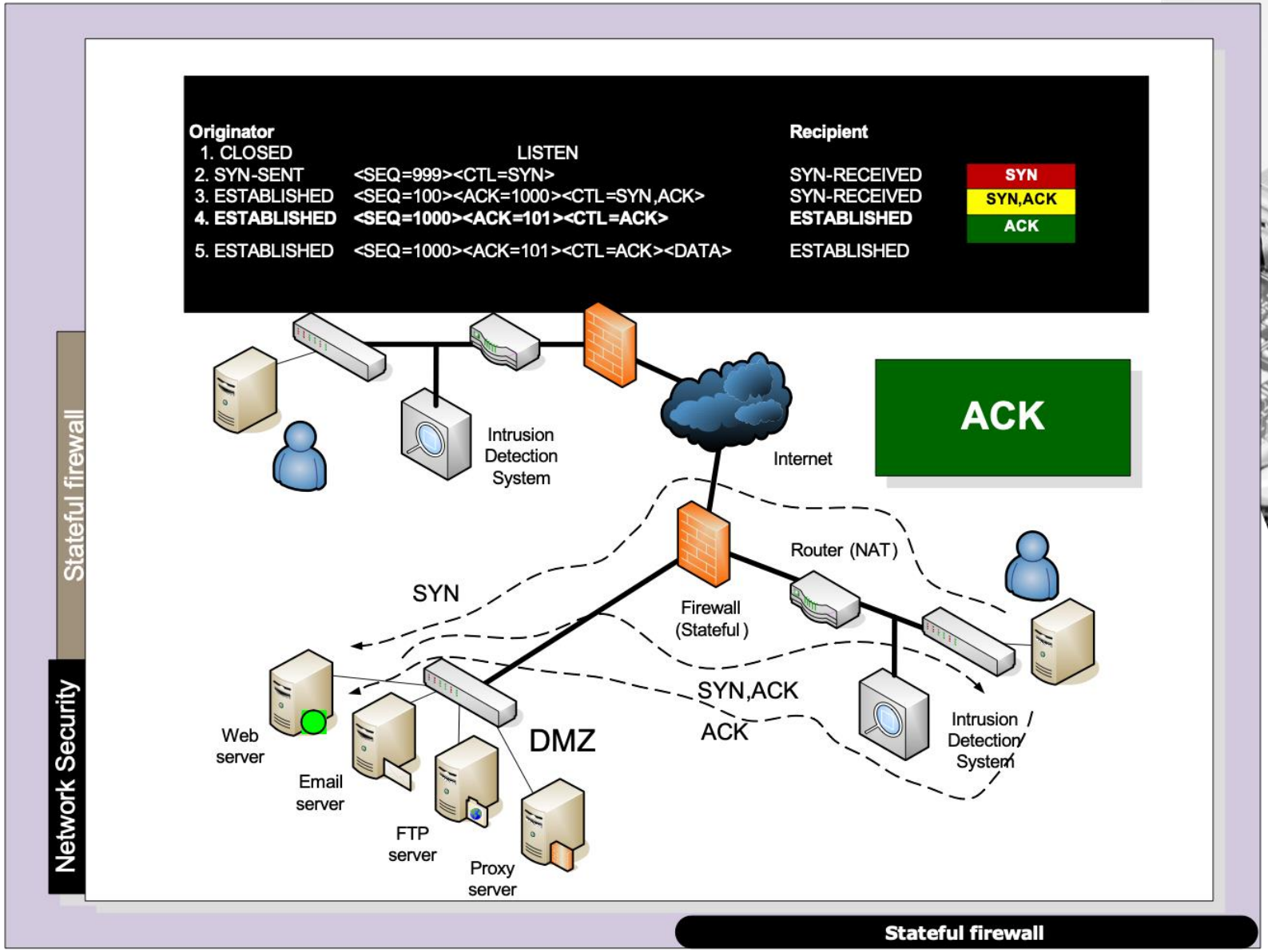


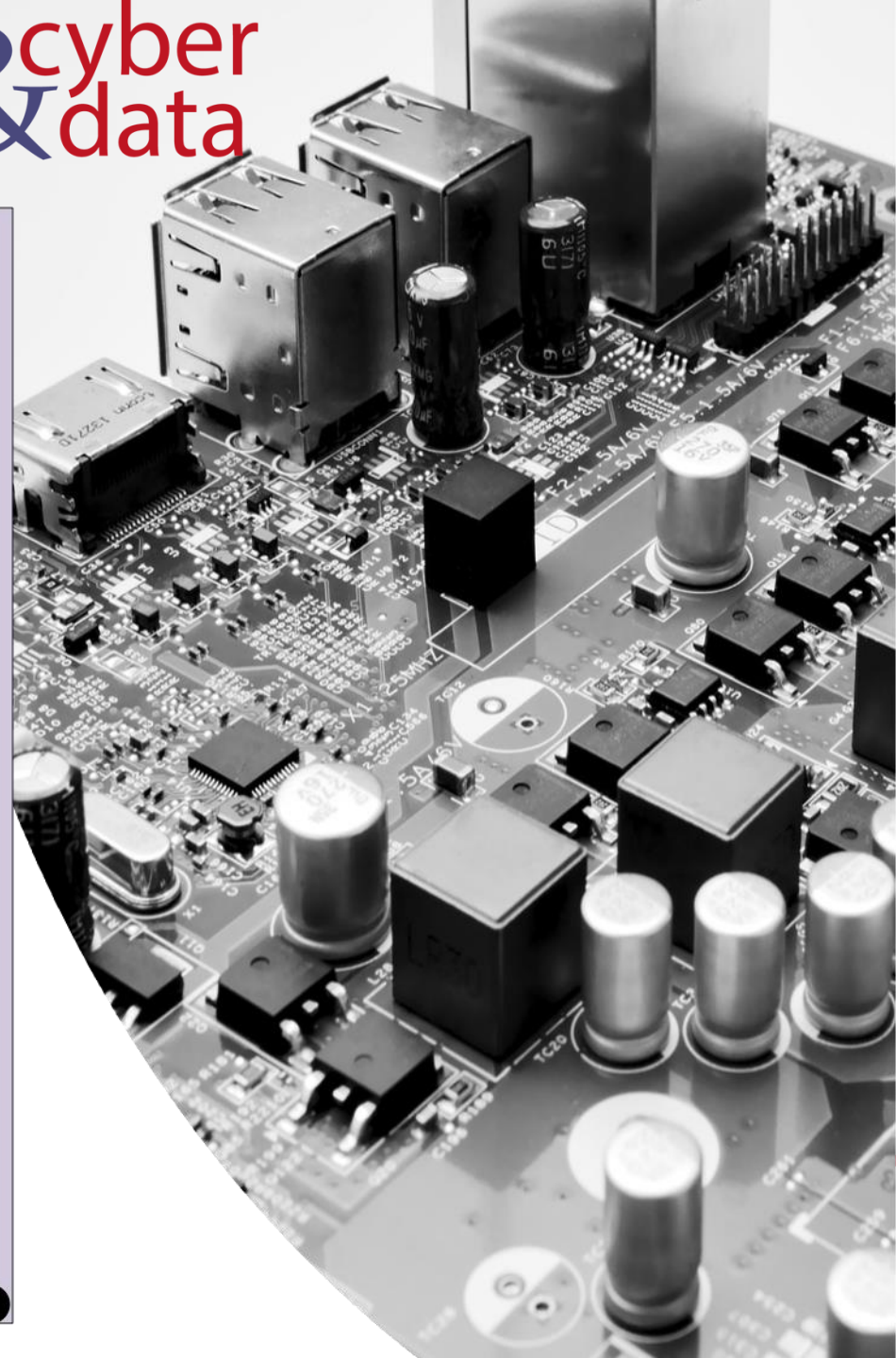
Layered Model

&cyber data

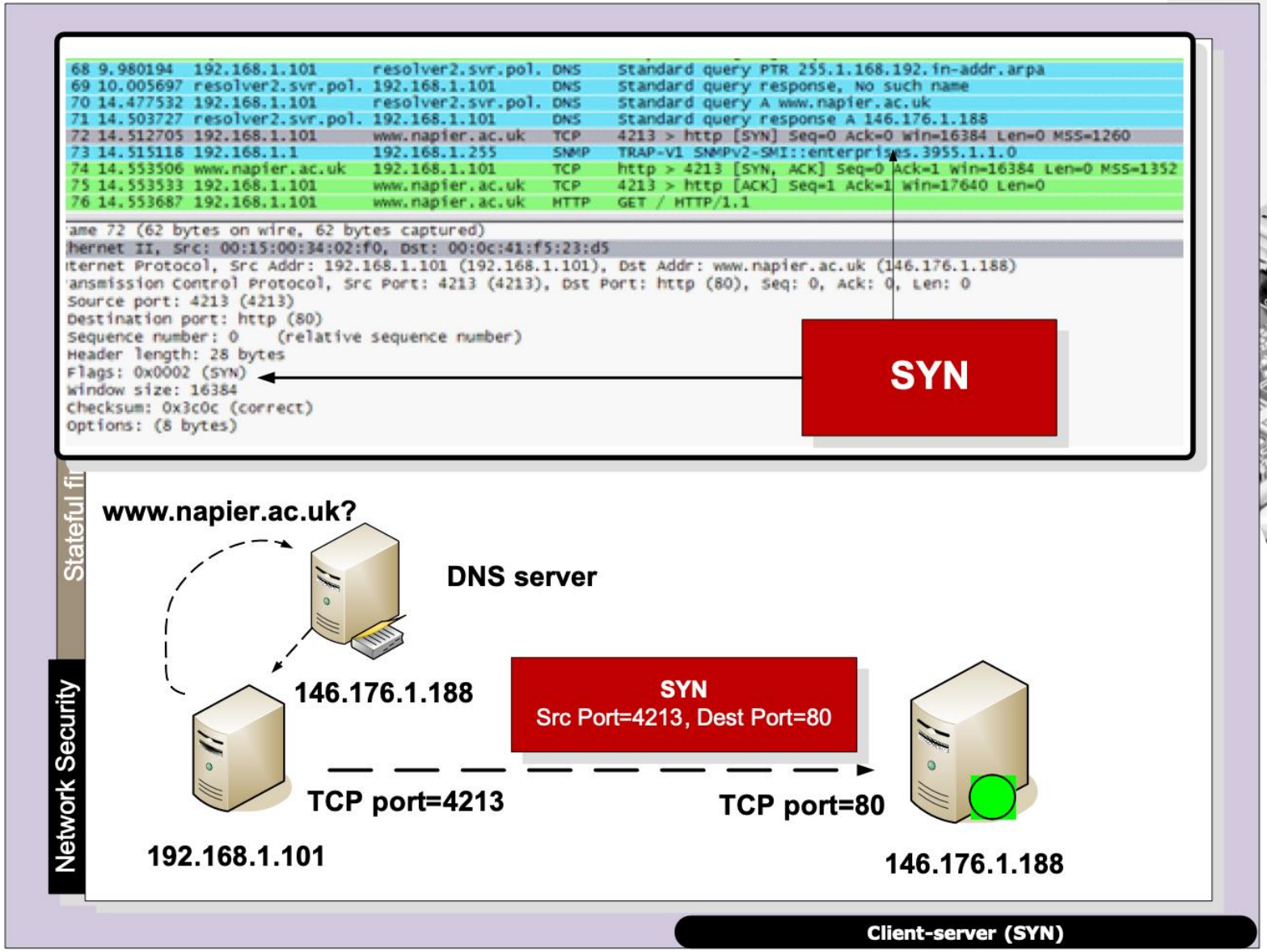


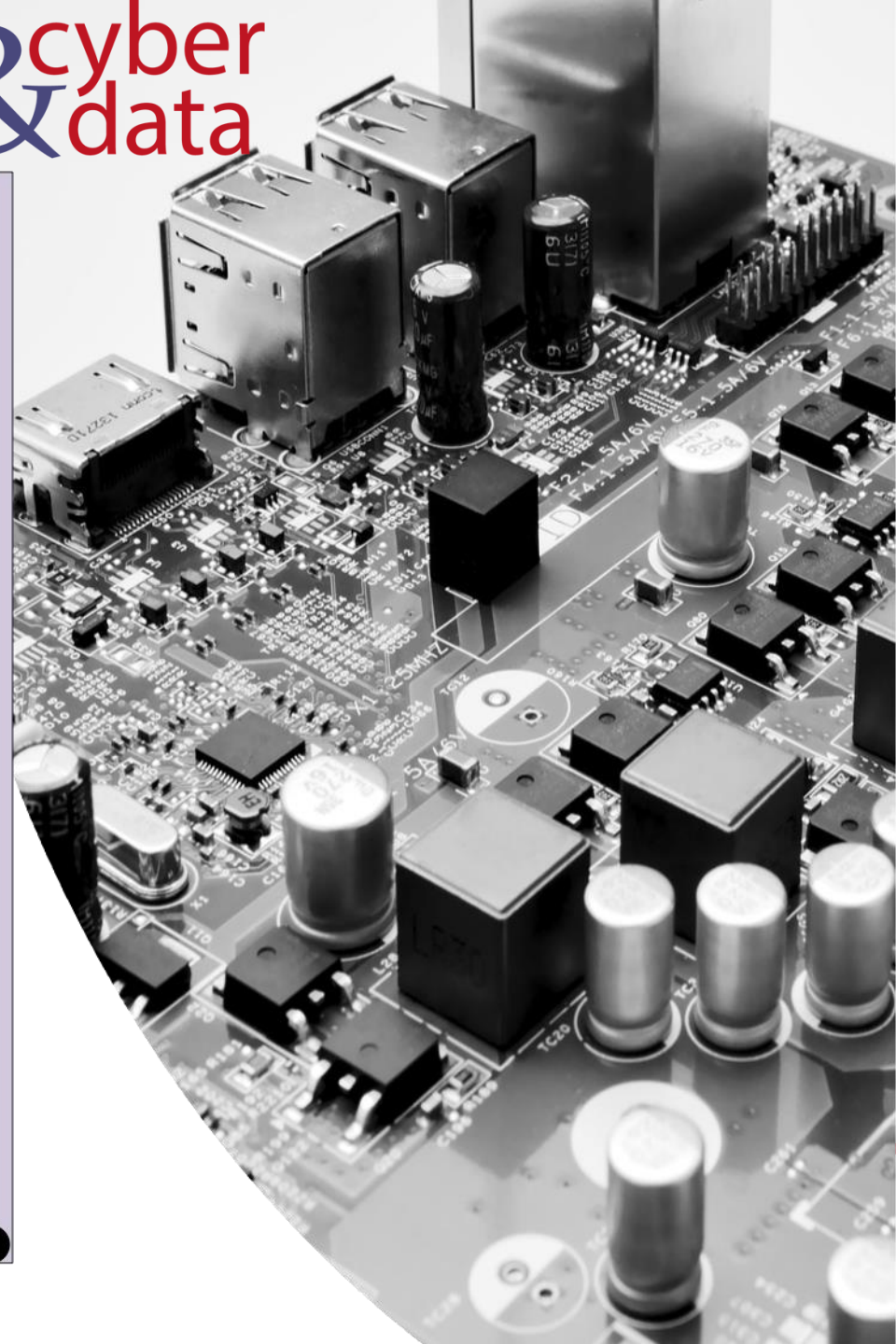
Layered Model



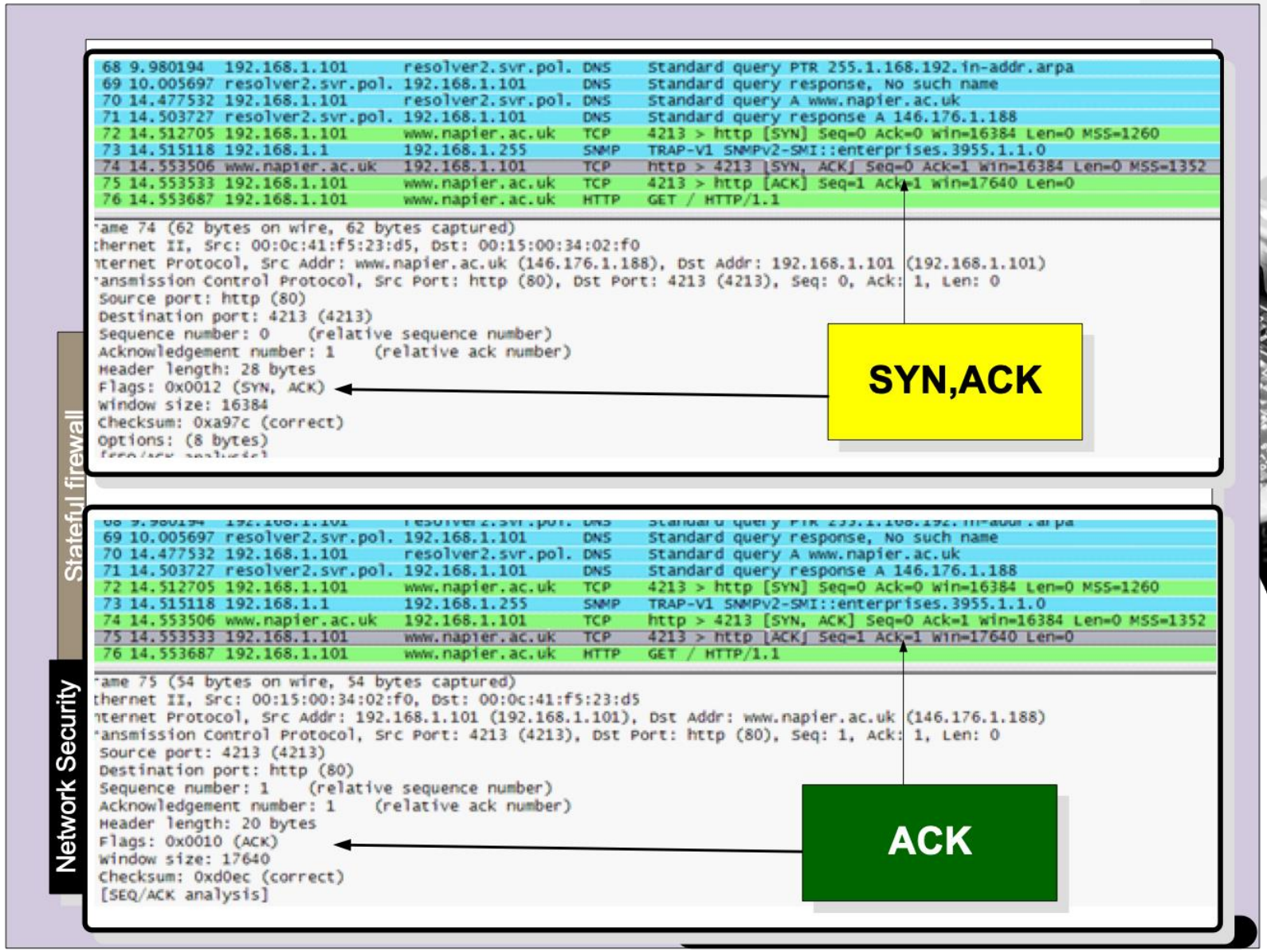


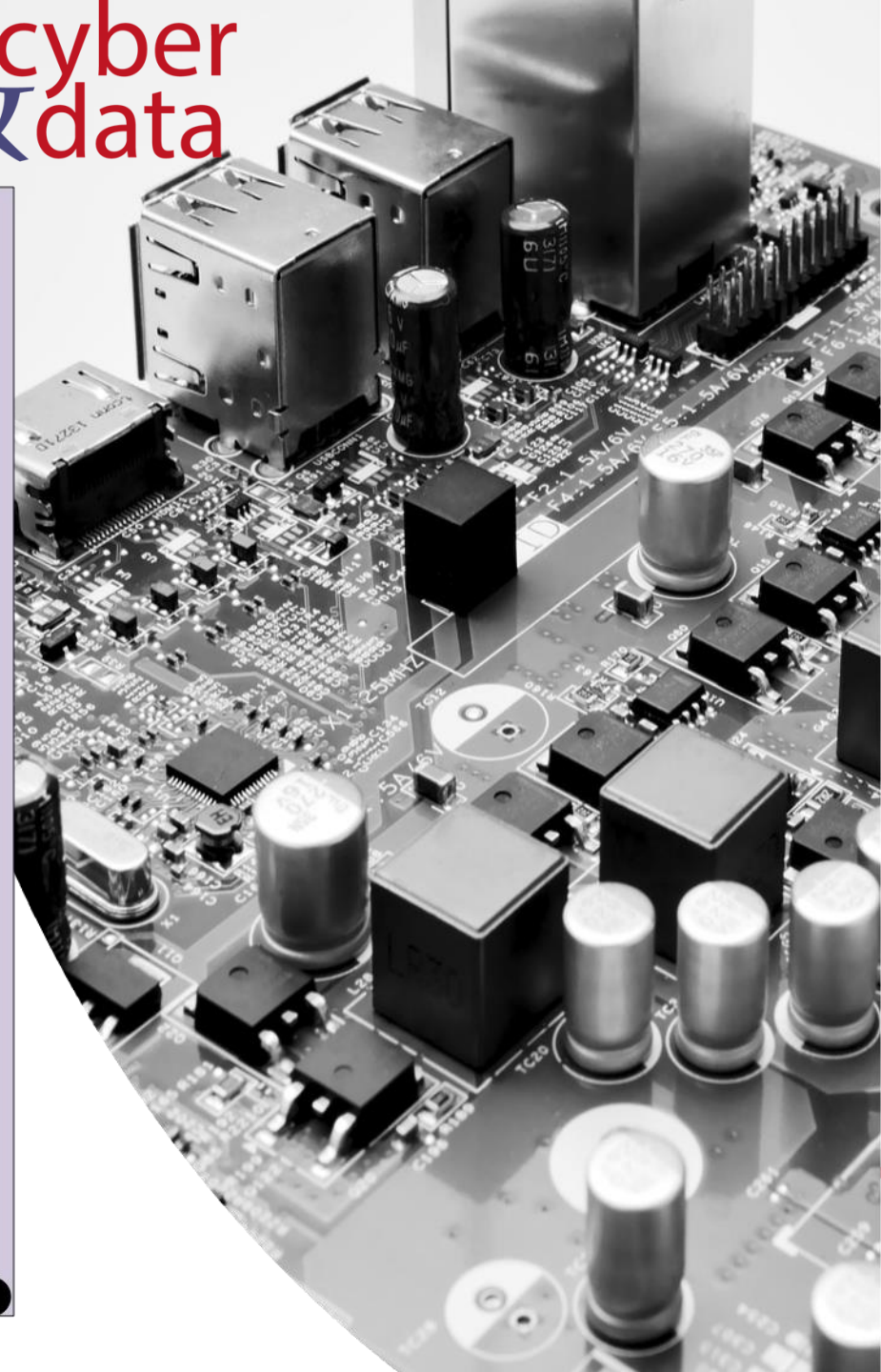
Layered Model





Layered Model





cyber & data

"From bits to information"

Defence Systems, Policies and Risks