„Something, that is allegedly secure
is not necessarily secure,
Something, that is allegedly known
might turn out to be unknown.
Appearance can be deceptive,
our senses can deceive us.
Even though experience and knowledge
can limit errors,
reality also limits those.“

Inspired by Berthold Brecht

Author: unknown

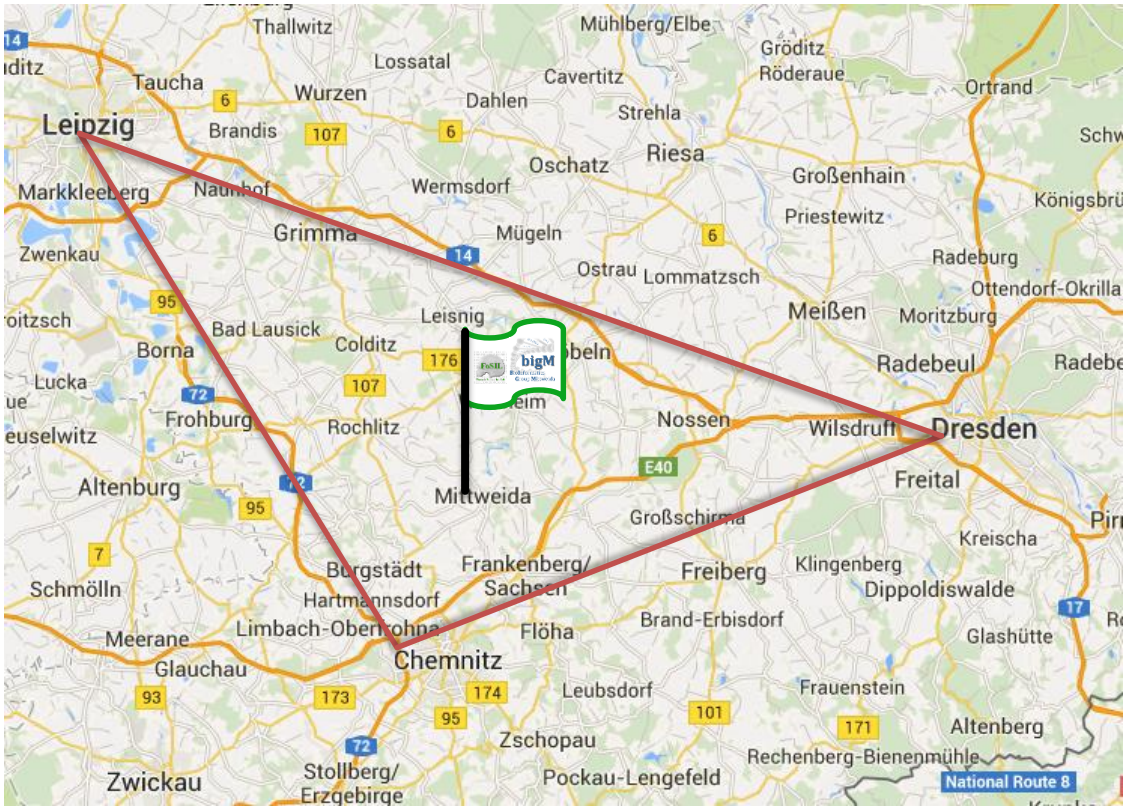
Learning from the Human Immune System: Artificial T-cells as a Response to Cyber Attacks

Michael Spranger and Dirk Labudde

Sonntag, 9. Juli 2017

Mittweida

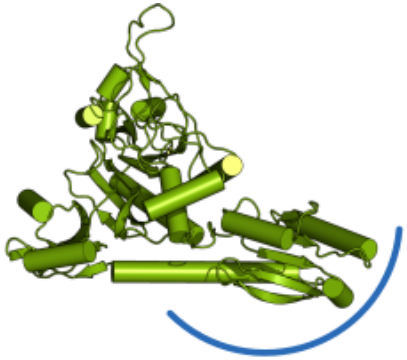

Schleswig Holstein
Mecklenburg Vorpommern
Hamburg
Bremen
Niedersachsen
Brandenburg Berlin
Sachsen Anhalt
Nordrhein-Westfalen
Hessen
Thüringen
Sachsen
Rheinland Pfalz
Saarland
Baden-Württemberg
Bayern

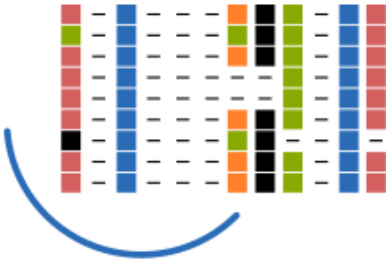

Leipzig
Chemnitz
Dresden
Zwickau
Mittweida
Altenburg
Meißen
Radebeul
Freital
Pirna
Wilsdruff
Nossen
Freiberg
Oschatz
Riesa
Grimma
Borna
Frohburg
Rochlitz
Colditz
Leisnig
Mügeln
Wermsdorf
Markkleeberg
Taucha
Wurzen
Brandis
Dahlen
Strehla
Lossatal
Cavertitz
Thallwitz
Mühlberg/Elbe
Gröditz
Röderaue
Ortrand
Großenhain
Priestewitz
Radeburg
Ottendorf-Okrilla
Moritzburg
Lommatzsch
Ostrau
Zwenkau
Bad Lausick
Lucka
Schmölln
Burgstädt
Hartmannsdorf
Limbach-Oberfrohna
Frankenberg/Sachsen
Flöha
Brand-Erbisdorf
Klingenberg
Dippoldiswalde
Glashütte
Kreischa
Großschirma
Meerane
Glauchau
Leubsdorf
Frauenstein
Zschopau
Altenberg
Rechenberg-Bienenmühle
Pockau-Lengefeld
Stollberg/Erzgebirge
Nossen
bigM
National Route 8
E40


HOCHSCHULE MITTWEIDA
UNIVERSITY OF APPLIED SCIENCES

bigM - Bioinformatics

FoSIL



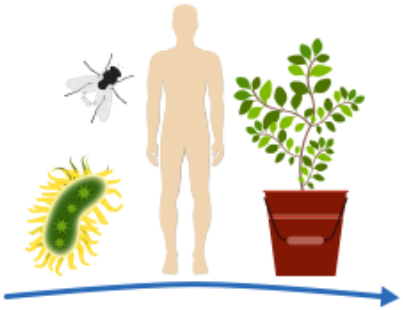


Protein Structure Analysis

...

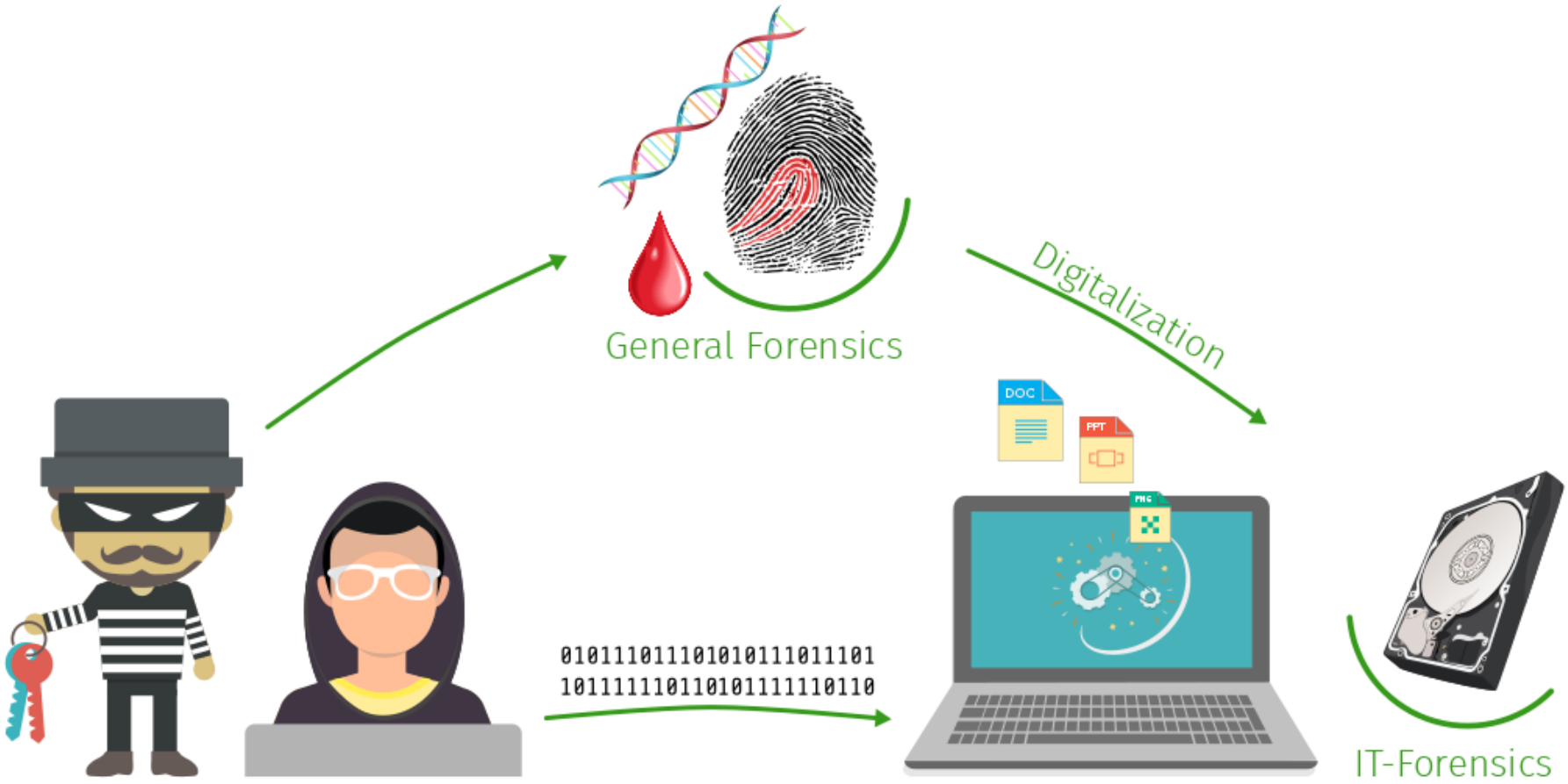
DNA Sequence Analysis

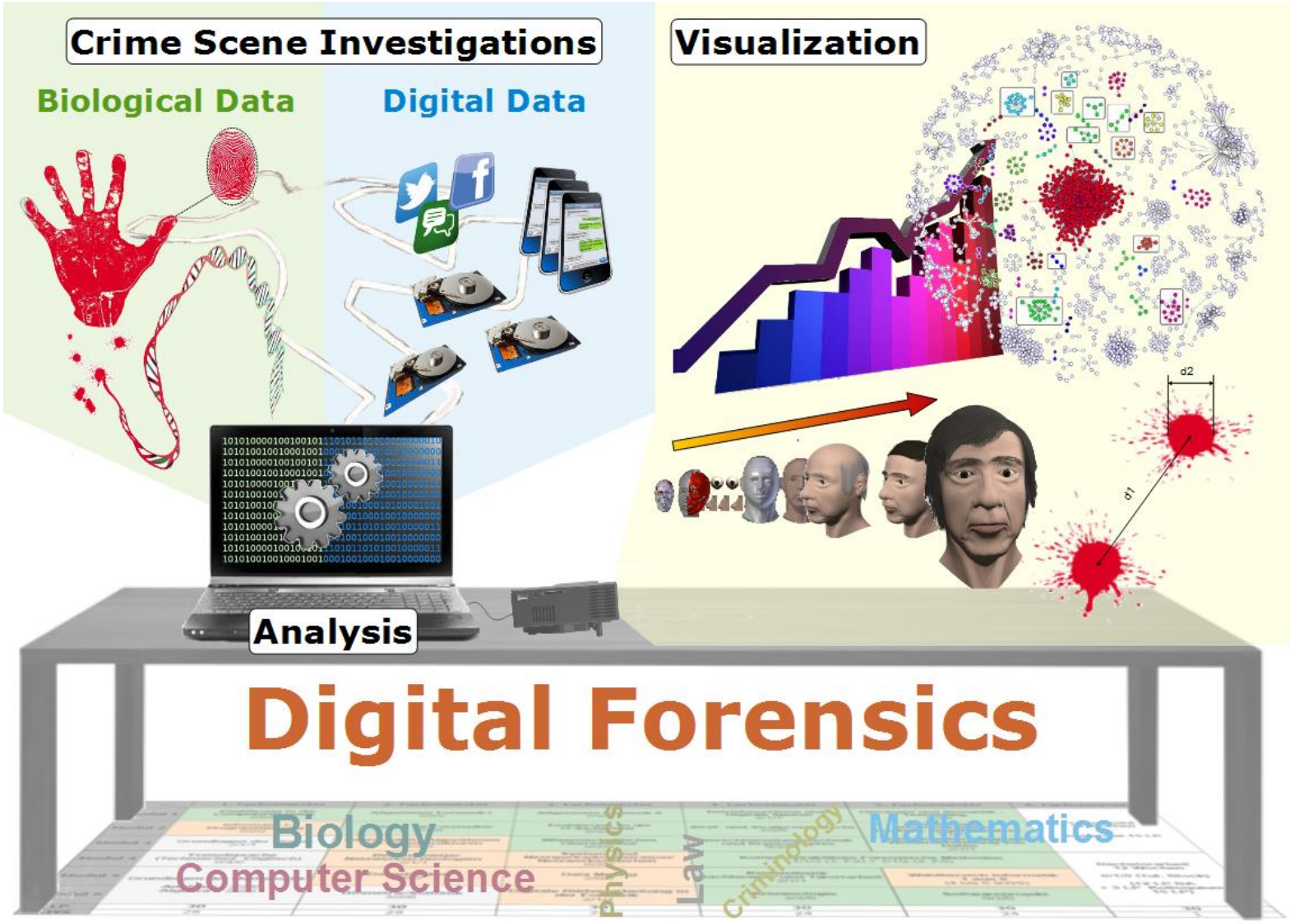
Experimental Data



Computational Analysis &
Gain of Knowledge

FoSIL – Forensic Sciences

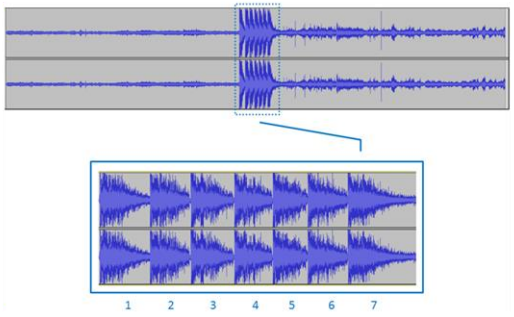



Crime Scene Investigations
Biological Data
Digital Data
Visualization
d2
d1
Analysis
Digital Forensics
Biology
Computer Science
Physics
Law
Criminology
Mathematics
© by Grustentier

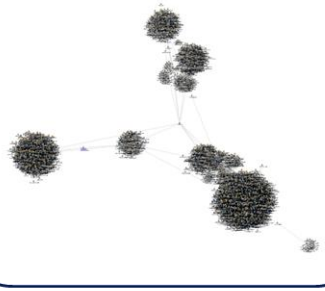
FoSIL – Expert Opinions

FoSIL

Audio Analysis



Social Engineering

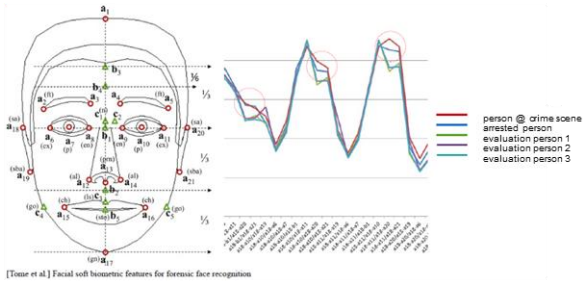


Scientific-Technical Report

Video Analysis

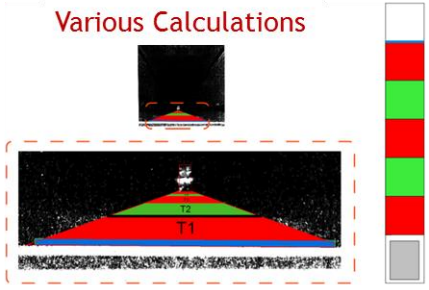
other

Person Identification



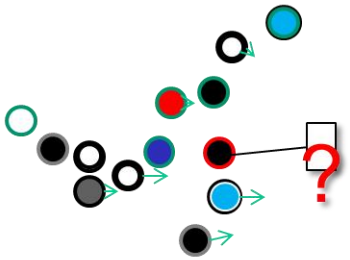
Customized Examinations

Various Calculations



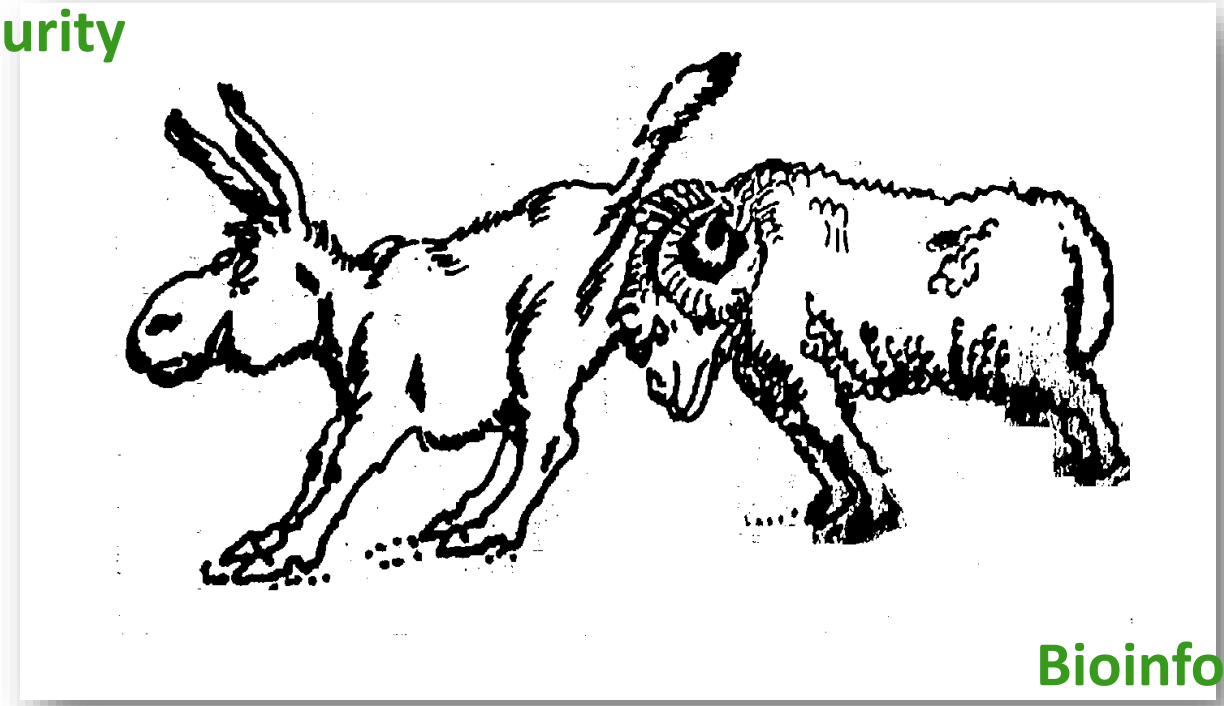
...

Movement Profiles



Bioinformatics and Forensics - How today's Life Science Technologies can shape the Crime Sciences of tomorrow

forensics/
it-security

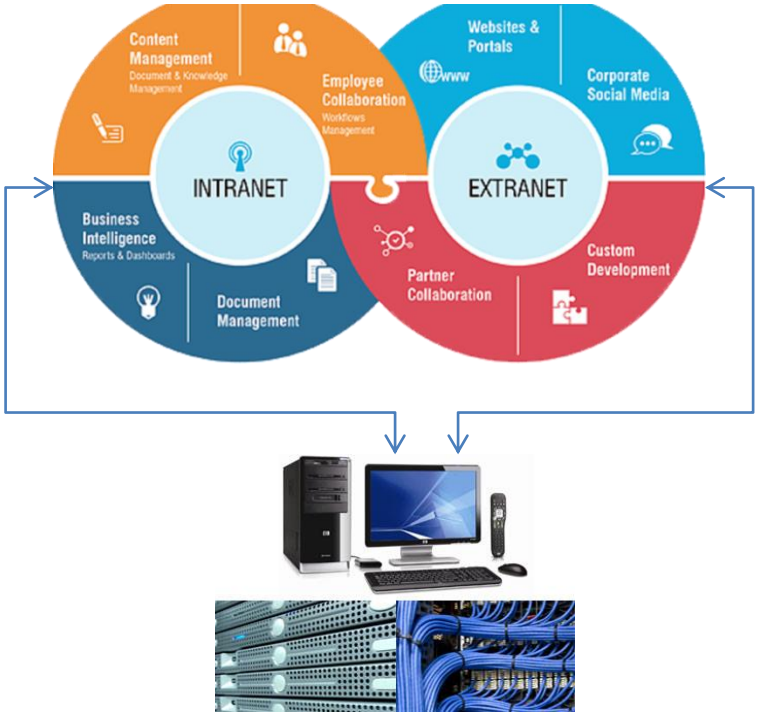


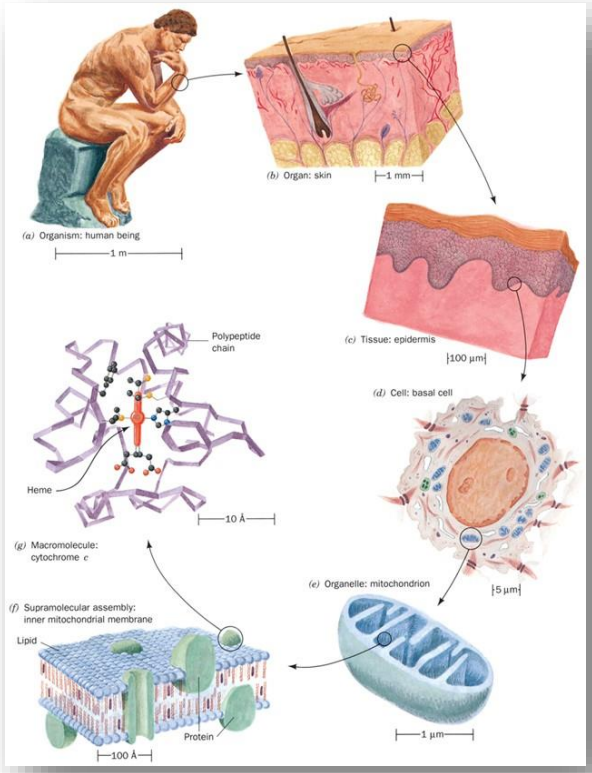
Bioinformatics/
Life Science

The lift in the human body

www

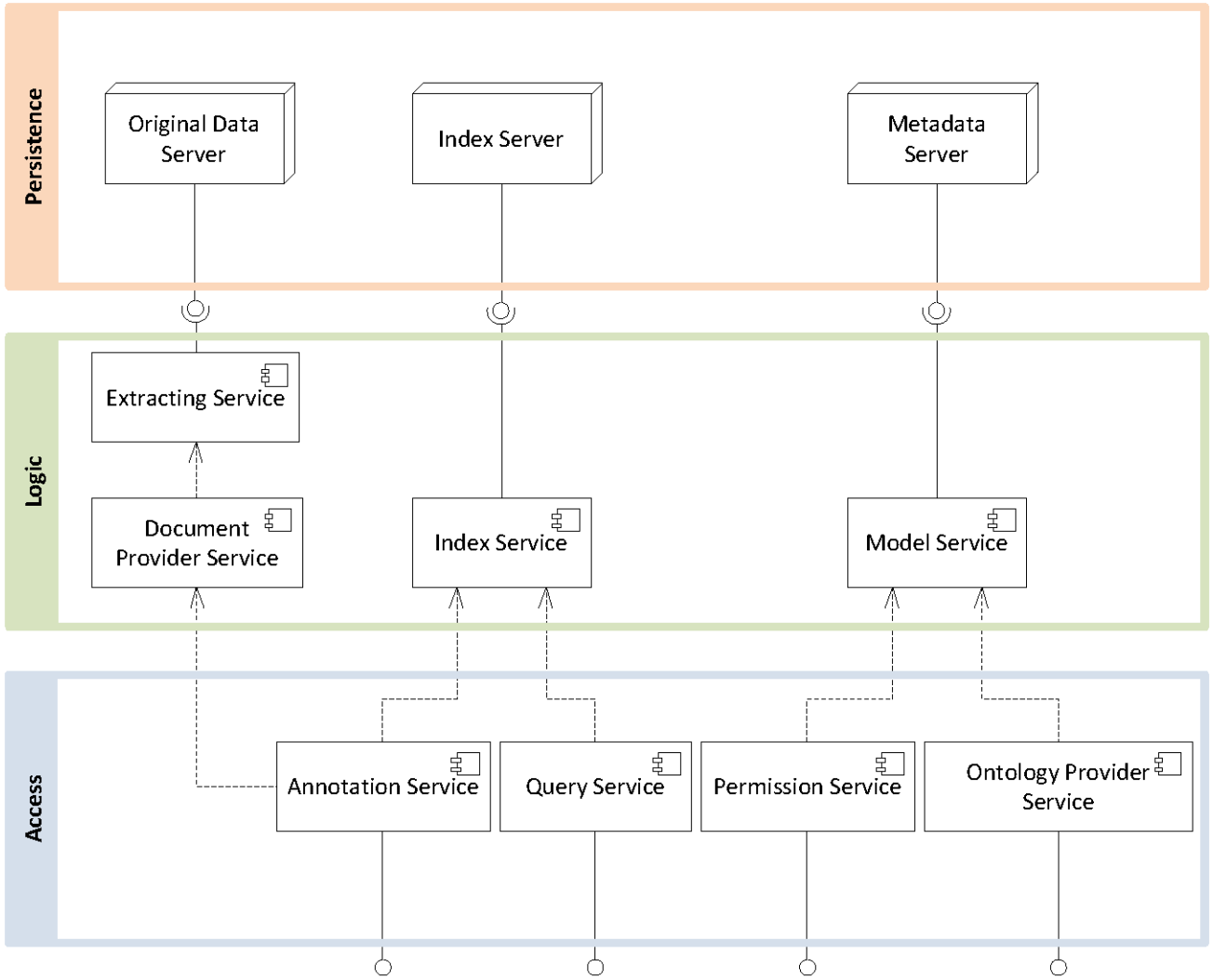
intranet



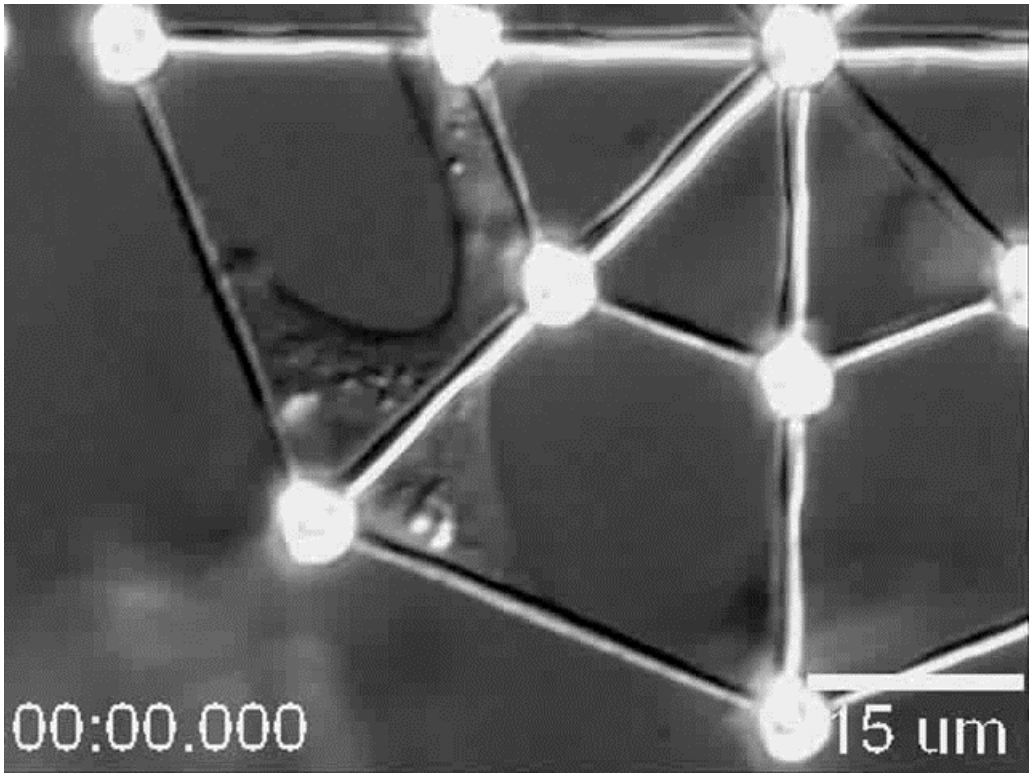


- organism
- organ
- tissue
- cell
- organelle

Technical Perspective - SOA



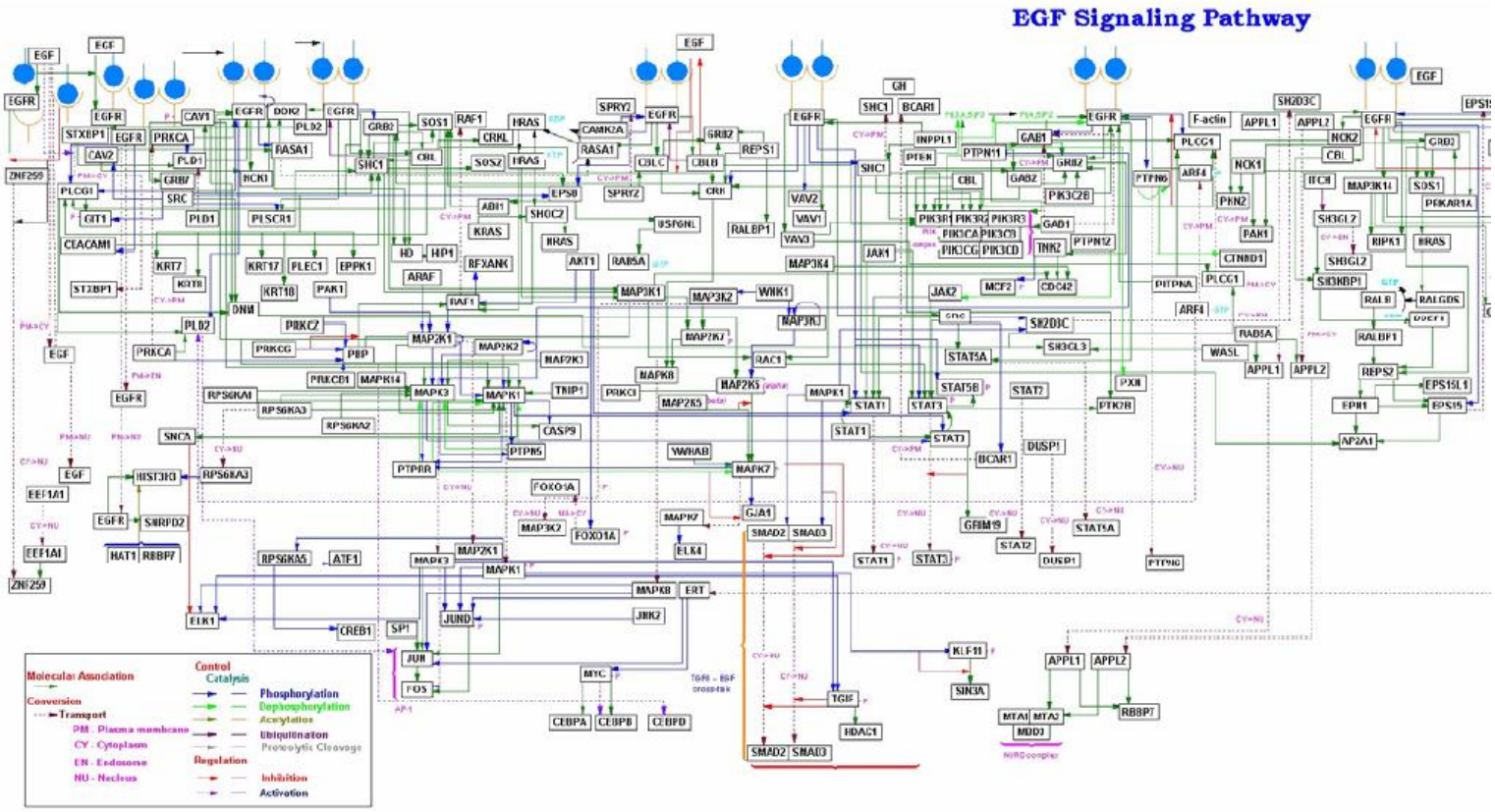
The living cell



functional and structural unit

The cell and the surrounding

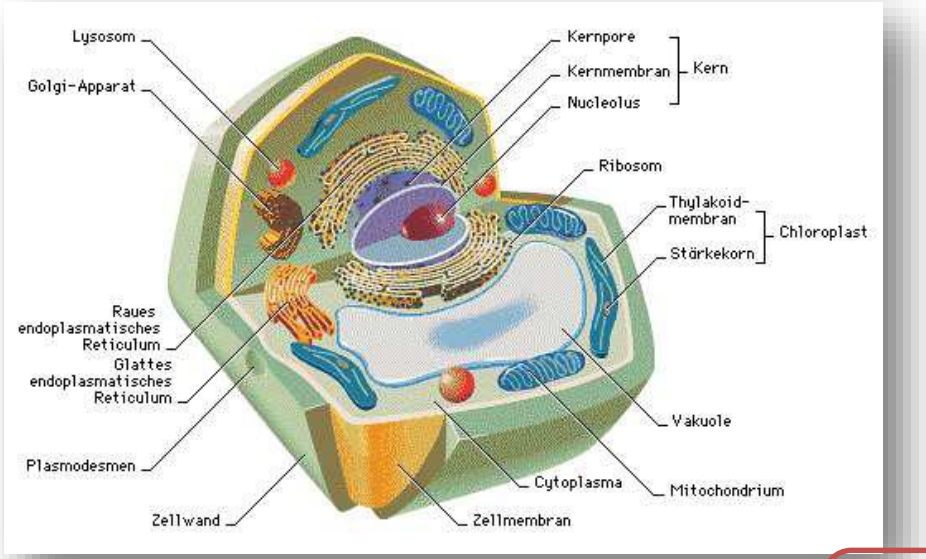
signaling pathway of EGF



Human Protein Reference database http://www.hprd.org

A human cell and the surrounding

omnis celula e celula



signal transduction

metabolic pathways

gen regulation

Protein-protein-interaction

infections

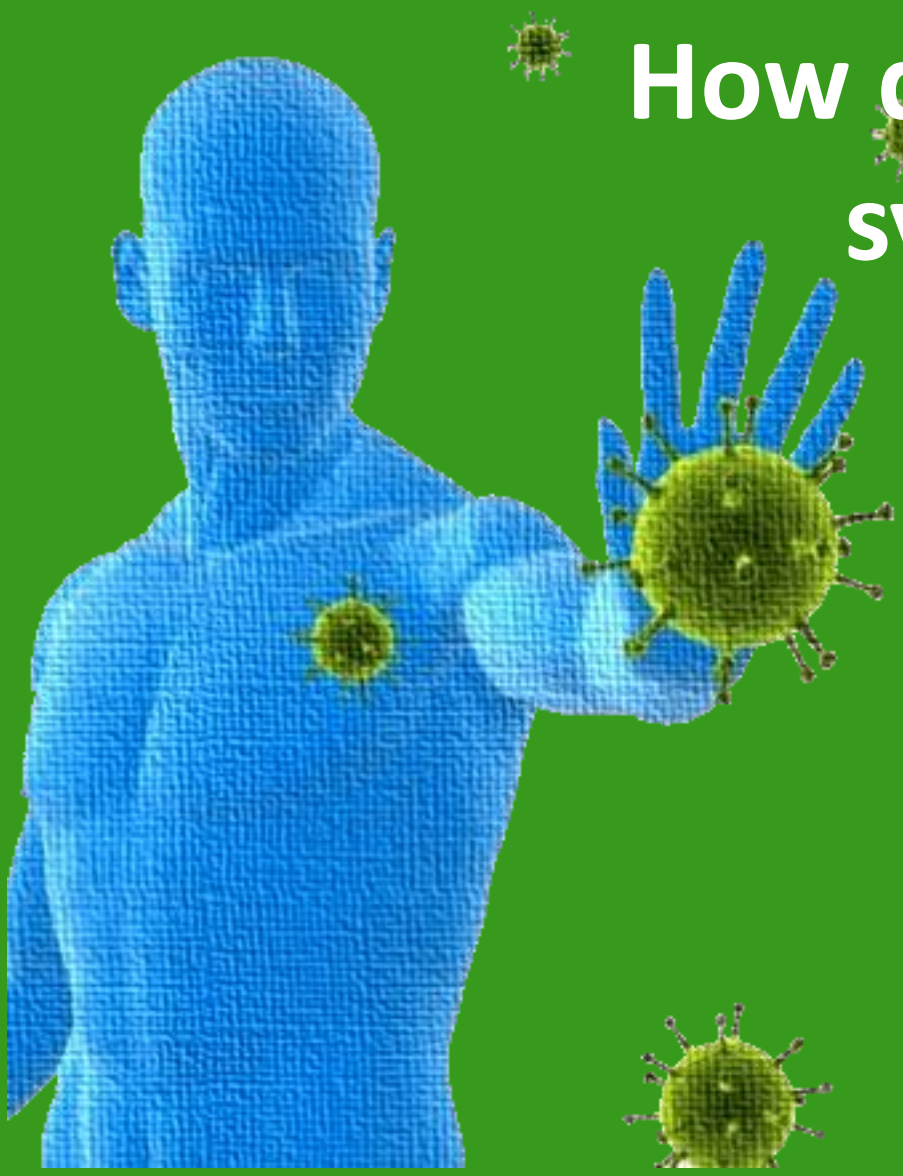
specific reactions

immune reaction

Why does this work in a cell?

Why can we not implement this in a technical manner?

How does the immune system work?



Transfer pathogens to people

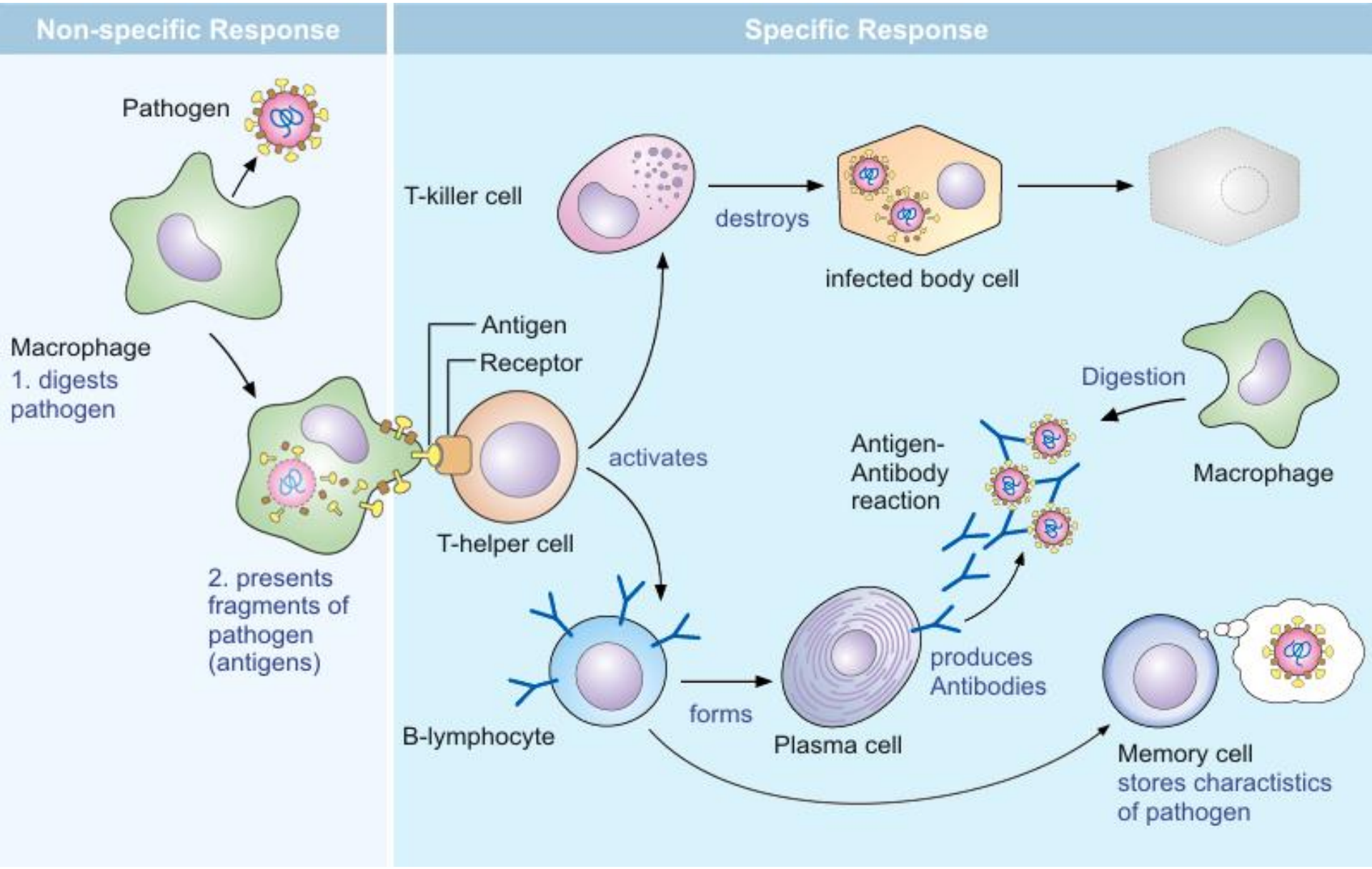
droplet

water

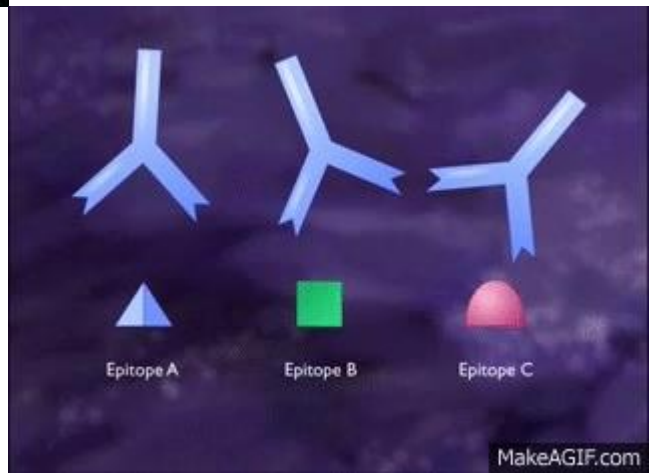
Contact

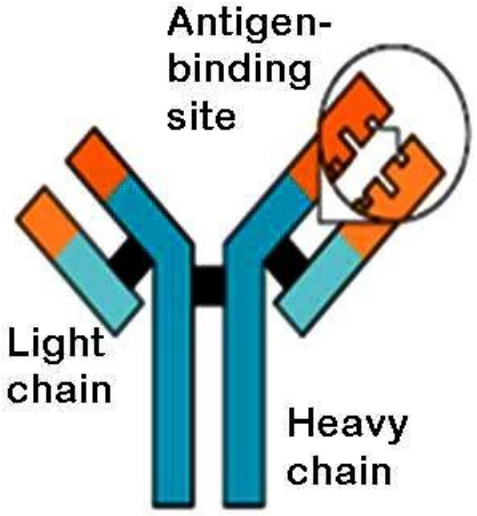
Blood and tissue

Human Immune Response System



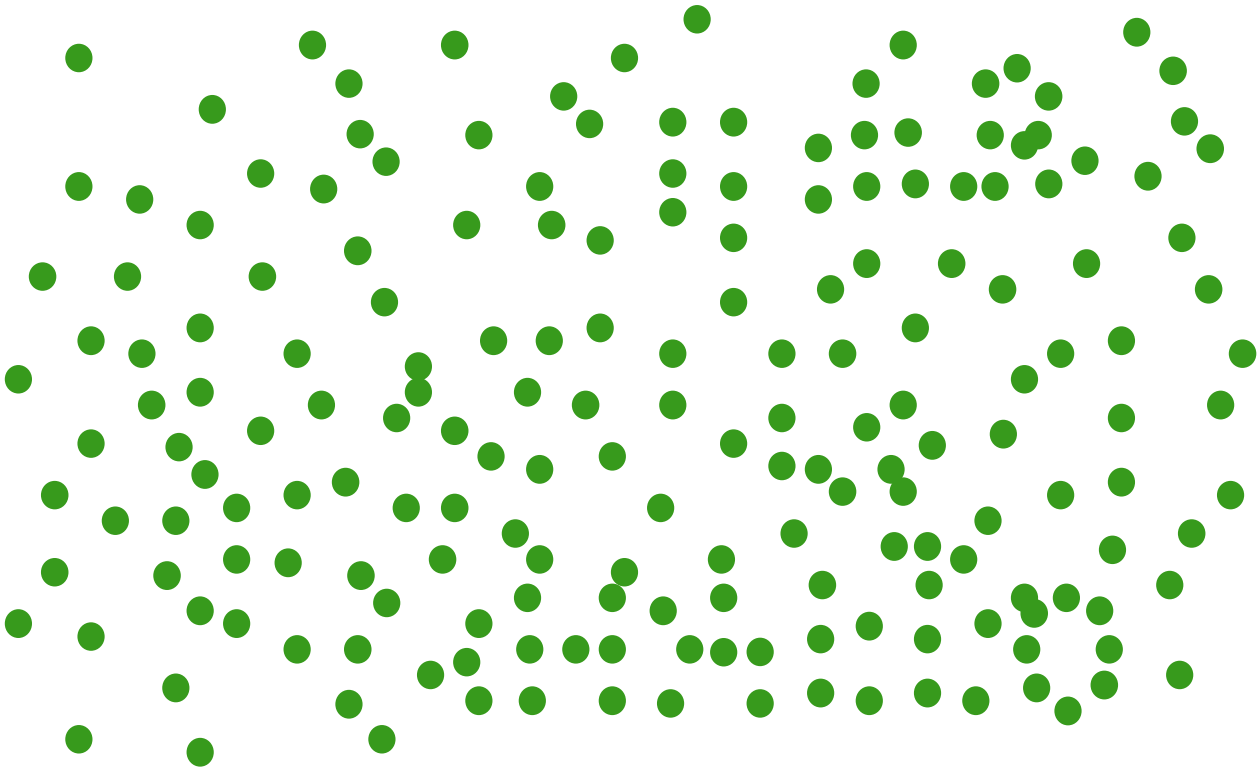
The Antigen (Virus) and Anti-body





Pattern/signatures for recognition and binding

Pattern recognition

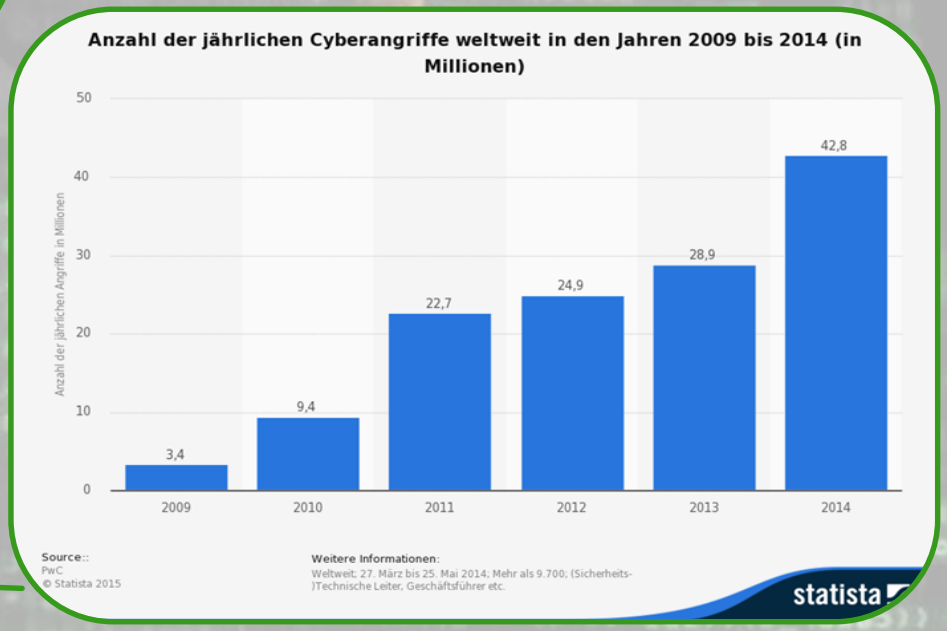


Methods for information extraction

What does this mean for cyber attacks?

Infection of „computer-networks“

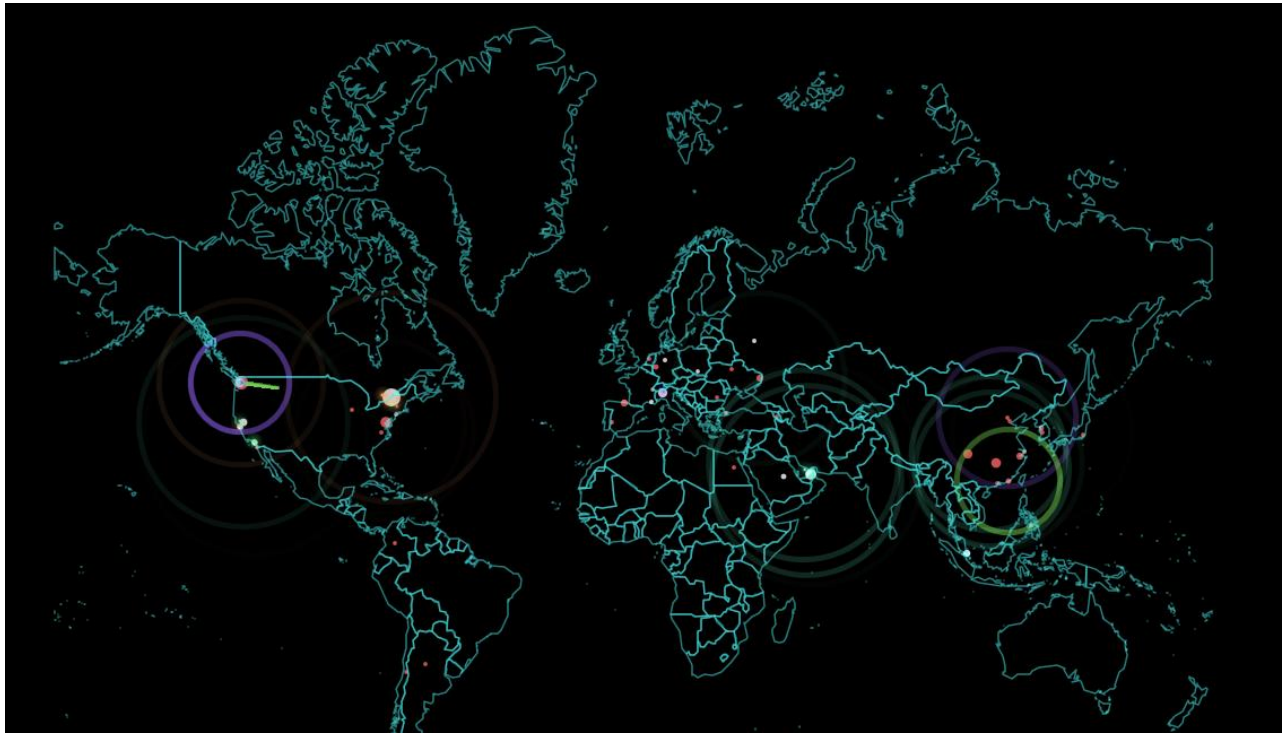
Hacker hits on U.S. power and nuclear targets spiked in 2012



Number of annual cyber attacks in the years 2009 to 2014 (in millions)

Targets for critical infrastructure

Cyber attack



ATTACK ORIGINS

	COUNTRY
64	China
51	United States
8	Ukraine
0	Netherlands
	South Korea
	Spain
	Turkey
	Romania
	Colombia

ATTACK TYPES

#	PORT	SERVICE TYPE
119	25	smtp
82	8080	http-alt
76	23	telnet
30	3389	ms-wbt-server
20	5900	rfb
10	50864	xsan-filesystem
15	3306	mysql
6	445	microsoft-ds
4	22	ssh

ATTACK TARGETS

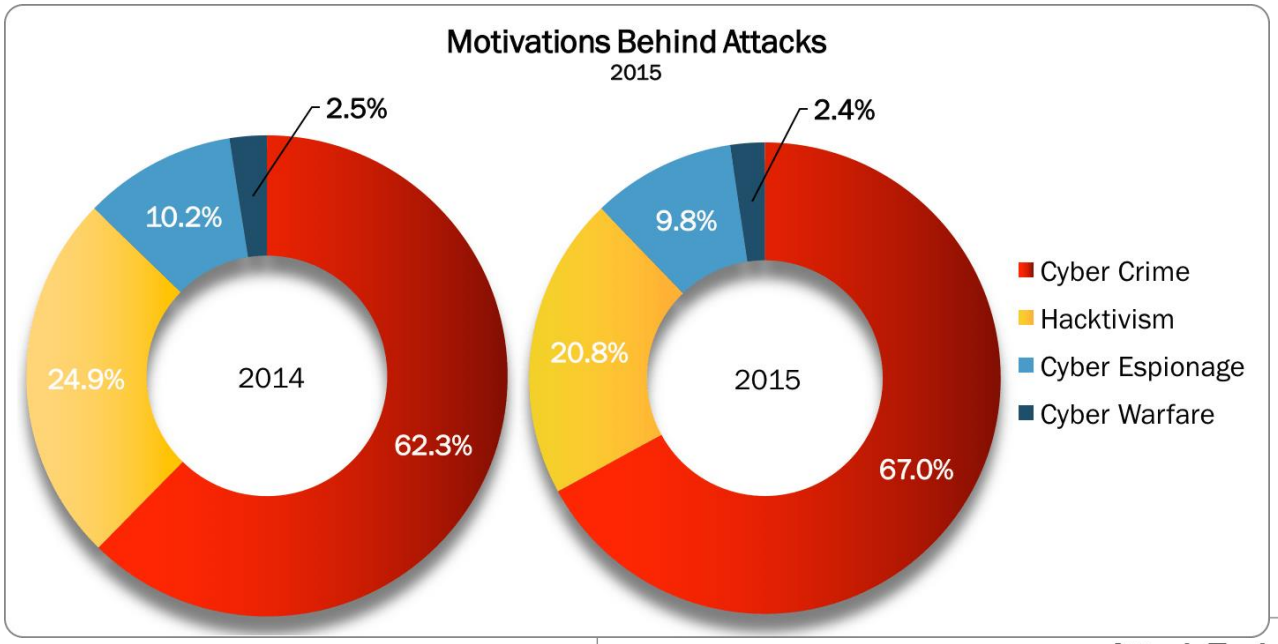
#	COUNTRY
214	United States
96	United Arab Emirates
36	Spain
21	Italy
15	Singapore
4	Saudi Arabia
3	Belgium
2	Hong Kong
2	France

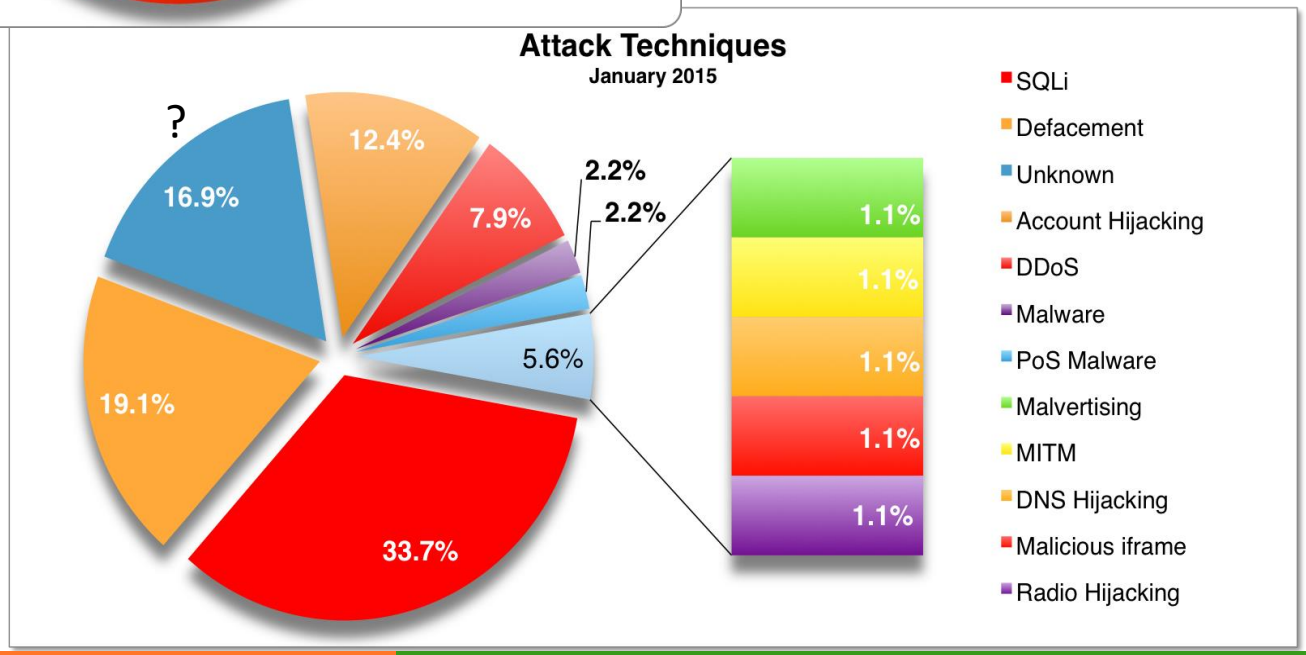
LIVE ATTACKS

TIMESTAMP	ATTACKER	ATTACKER IP	ATTACKER GEO	TARGET GEO	ATTACK TYPE	PORT
20:54:05.759	Chinanet Hubei Province Network	116.211.0.90	Wuhan, CN	Dubai, AE	http-alt	8080
20:54:05.758	Chinanet Hubei Province Network	116.211.0.90	Wuhan, CN	Dubai, AE	http-alt	8080
20:54:05.480	Net For Ankas	46.161.40.120	Luhansk, UA	Roseville, US	ms-wbt-server	3389
20:54:05.370	Chinanet Hubei Province Network	116.211.0.90	Wuhan, CN	Dubai, AE	http-alt	8080
20:54:04.915	As29073 Ecatel Ltd	80.82.65.120	The Hague, NL	Brussels, BE	nnsp	433
20:54:04.369	Microsoft Corporation	157.56.110.248	Redmond, US	De Kalb Junctio...	smtp	25
20:54:04.142	Chinanet Hubei Province Network	116.211.0.90	Wuhan, CN	Dubai, AE	http-alt	8080
20:54:03.811	Microsoft Corporation	207.46.100.252	Redmond, US	De Kalb Junctio...	smtp	25
20:54:03.351	Cox Communications	70.183.54.227	Tulsa, US	De Kalb Junctio...	telnet	23

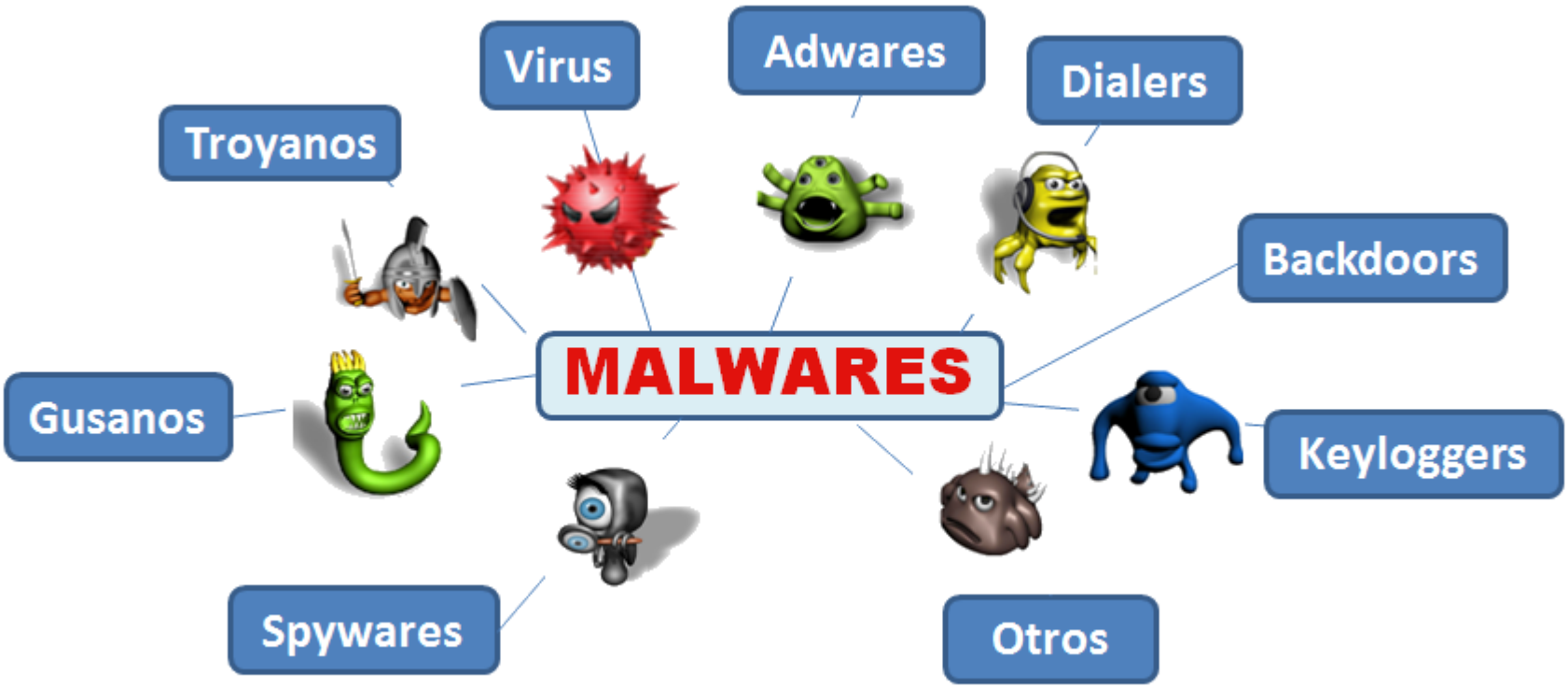
http://map.norsecorp.com/#/

Statistics

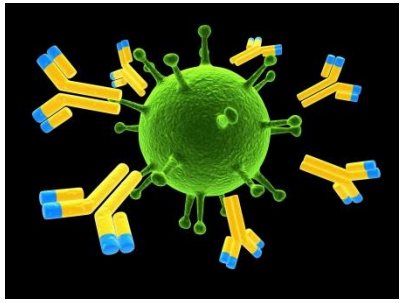

Motivations Behind Attacks
2015
2.5%
10.2%
24.9%
2014
62.3%
2.4%
9.8%
20.8%
2015
67.0%
Cyber Crime
Hacktivism
Cyber Espionage
Cyber Warfare


Attack Techniques
January 2015
?
16.9%
12.4%
7.9%
2.2%
2.2%
5.6%
19.1%
33.7%
1.1%
1.1%
1.1%
1.1%
1.1%
SQLi
Defacement
Unknown
Account Hijacking
DDoS
Malware
PoS Malware
Malvertising
MITM
DNS Hijacking
Malicious iframe
Radio Hijacking

Types of Malware



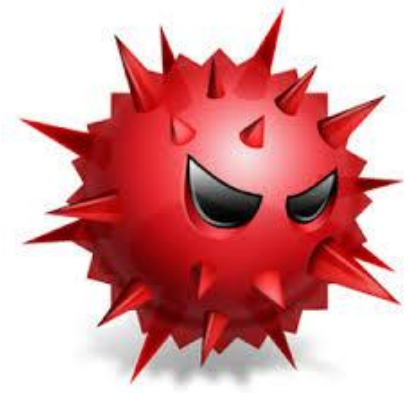
Common characteristics



Malware is similar to a software:
it consists of a program code that can perform various actions **when it is activated or started**.

In contrast to serious software, however, the unwanted code usually tries to spread **unintentionally**. This can be done independently or with the help of other programs / functions.

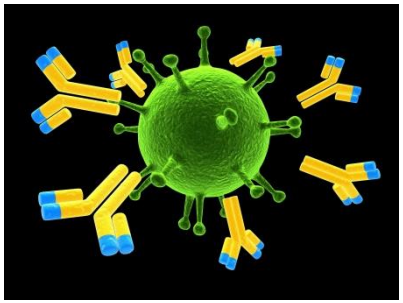
After **infection**, the malware continues **to hide** (to download program codes from the Internet, to send SPAM or to spy on personal data), or to identify itself by trying to blackmail the user, delete files, or encrypt and unwanted ones Web pages.

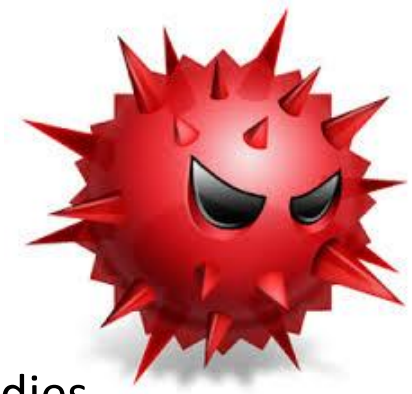


A computer virus regularly consists of three parts.

- **replication unit**
- **trigger**
- **Payload**

Malware





- time-independent detection
- Specific and adaptive antibodies
- isolation

Current security systems:

- Virus Scanner
- Real-time protection
- firewall management
- mail protection

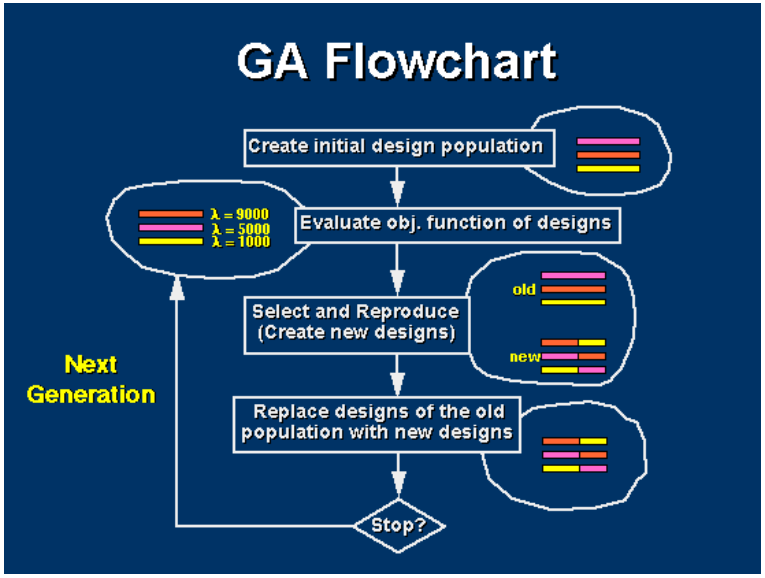
Problems: signatures too old, Adaption to slow (there is no really adaption), heuristics not good enough (minimal true positives)

Virus Scanner – new/old ideas

Real time scanning (continuously)

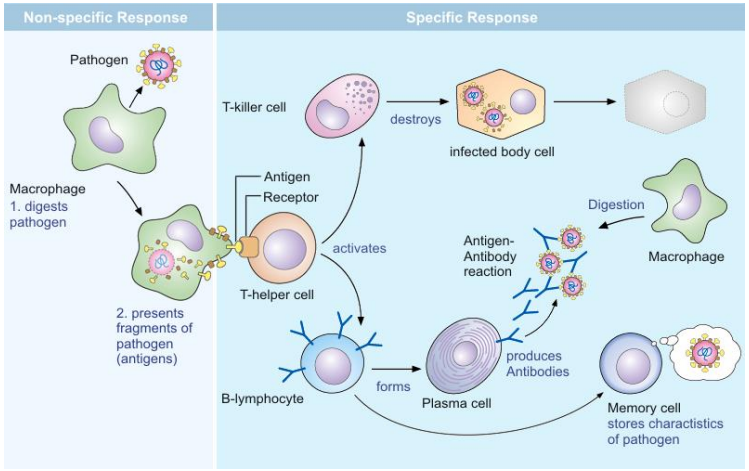
- all components
- random access memory
- Known signatures
- Algorithms for the prediction of unknown signatures (Genetic algorithms)
- code scanner (emails, documents) – new software fragments (quarantine)
- Automatic (semi-automatic) penetration tests

New independent components

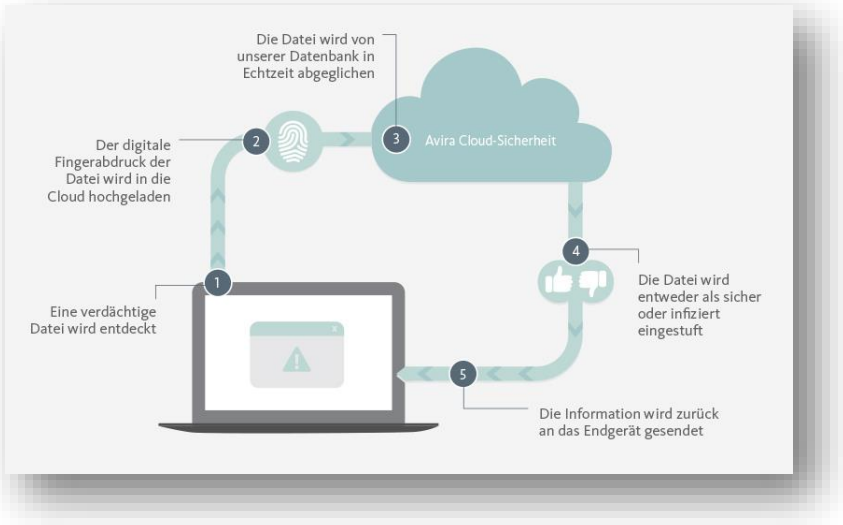


- Information units for the whole network
- Scanning of trigger units - Logical network

Virus Scanner – new/old ideas

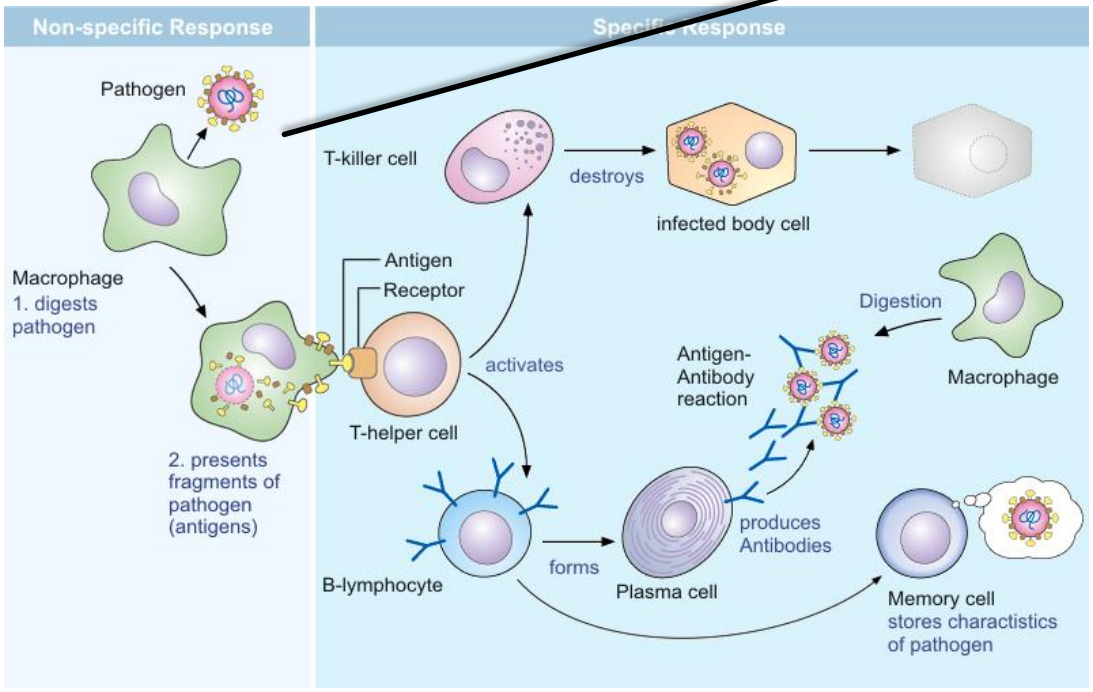


Adaption of the biological process



New independent component

Virus Scanner – new/old ideas



Classical Virus Scanner

Signature modulation

Σ modulations

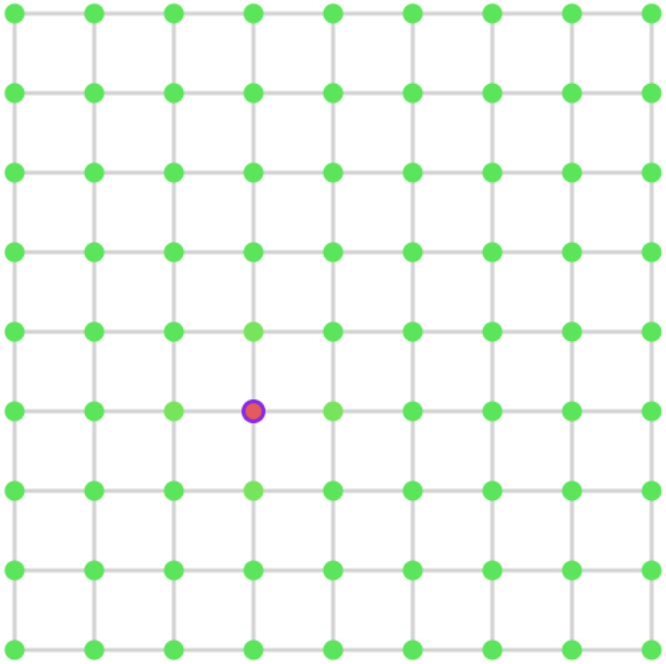
activation

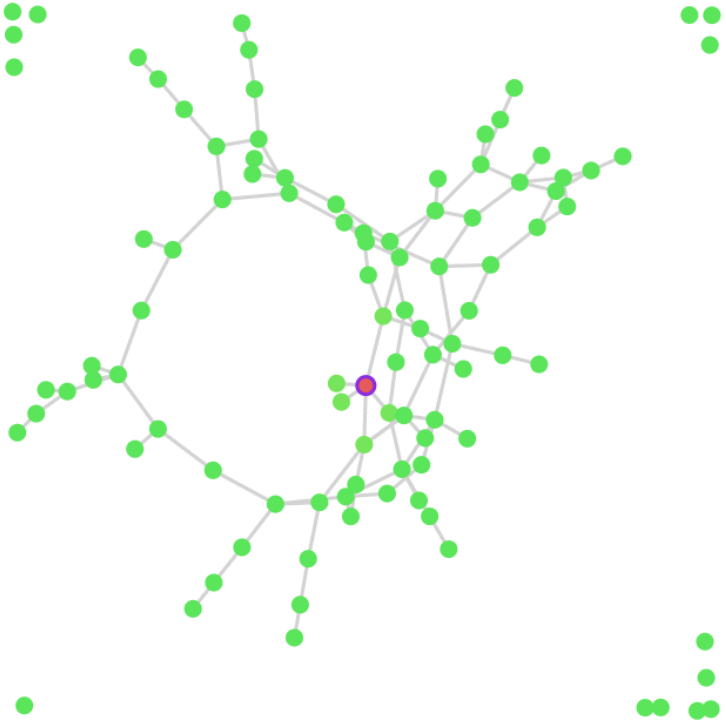
elimination

New independent component

isolation

Simulation Grid --- Topology - spread





Topology encapsulates

FoSIL

The Infiltration Game

Artificial Immune System for the Exploitation of Crime Relevant Information in Social Networks

Securing the **signal transduction** of the socio-technical environment: Social network (Facebook)

Introduction

FoSIL

“Most massive attack in Leipzig since the Pogrom Night in November 1938”

[LVZ 12th January 2016]

Are we able to predict such incidents?

Yes, by monitoring of social networks?

Rage announced and stoked by Social Networks

FoSIL

"Area-wide terrorists attack blonde German women by Muslim asylum seekers."

Storm on Leipzig!

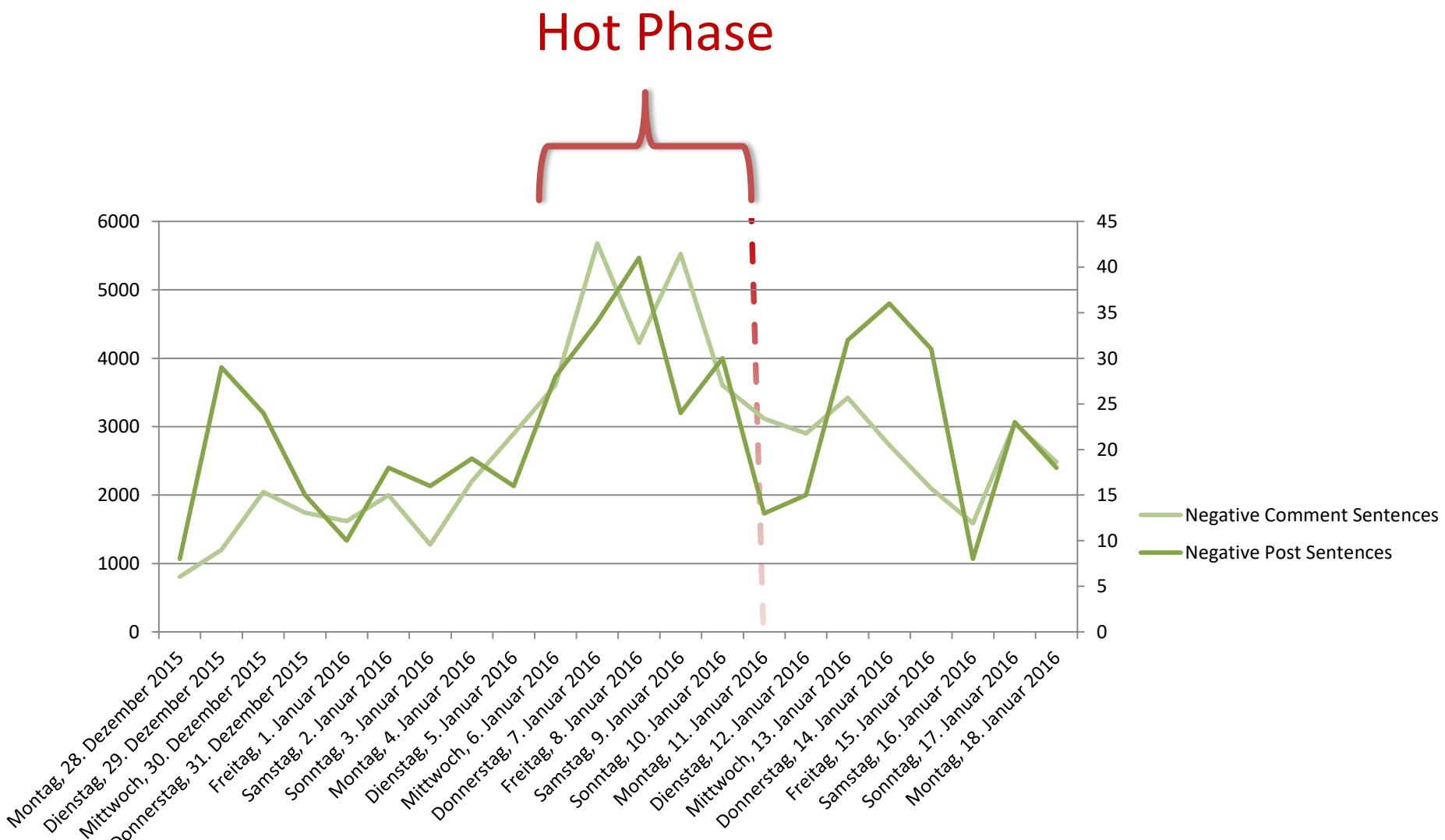
29 24

BHS_KHS @khs_bhs 14 h
Sturm auf Leipzig!!!
m.facebook.com/story.php?st...
#halle #leipzig #Dresden #Magdeburg
#Deutschland

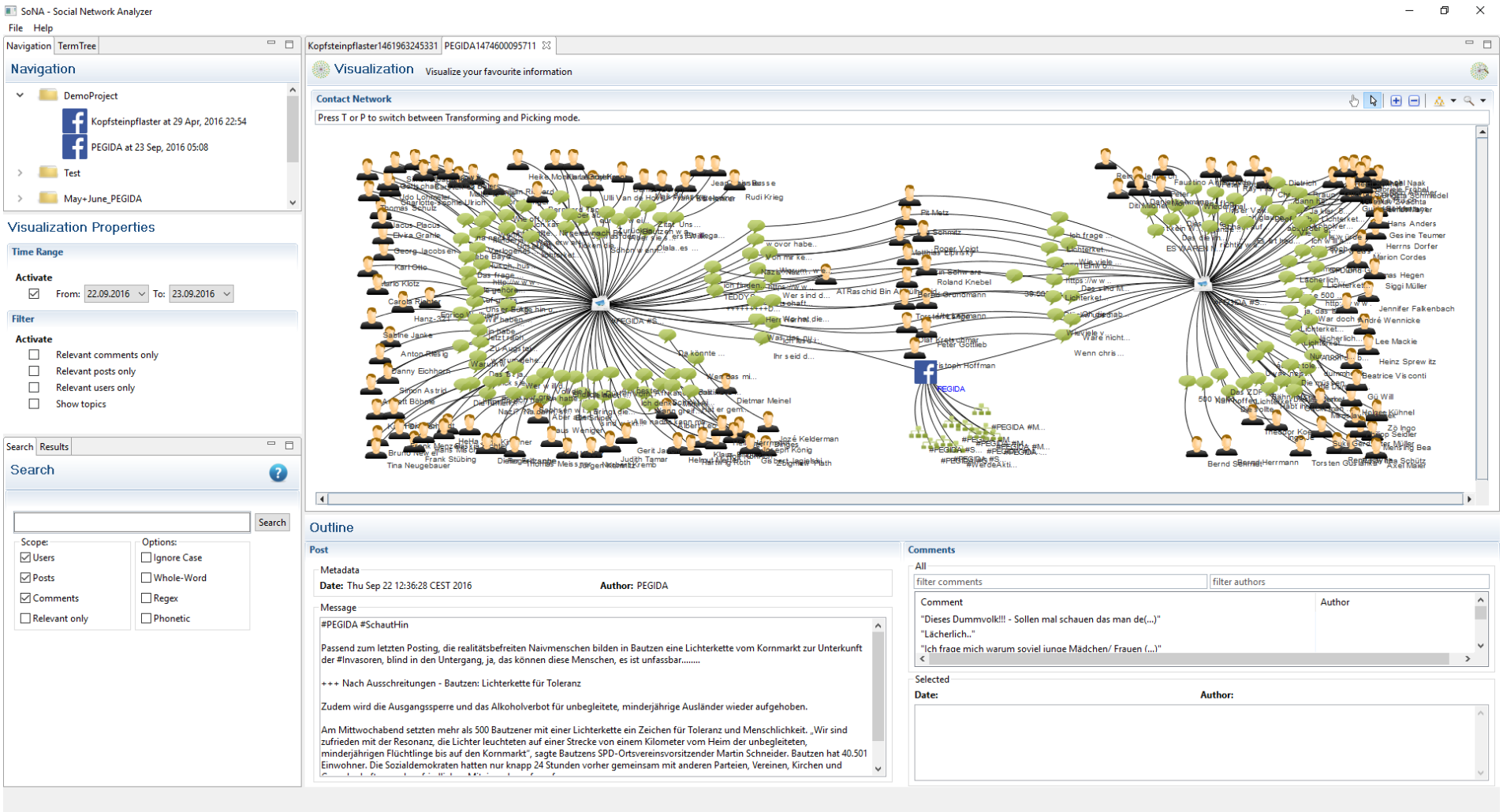
2 1

"Rapefugees not welcome!"

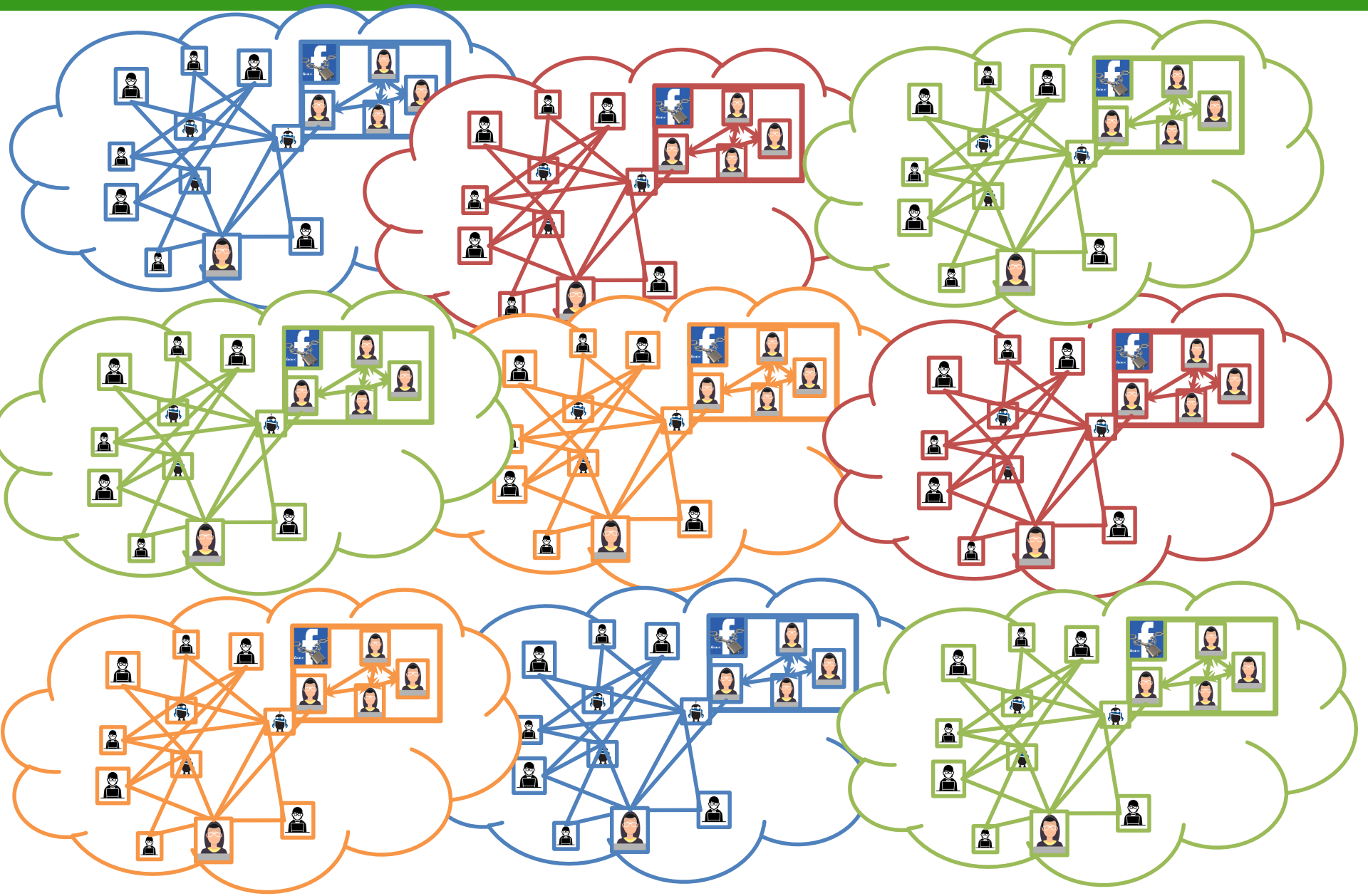
Incident Detection



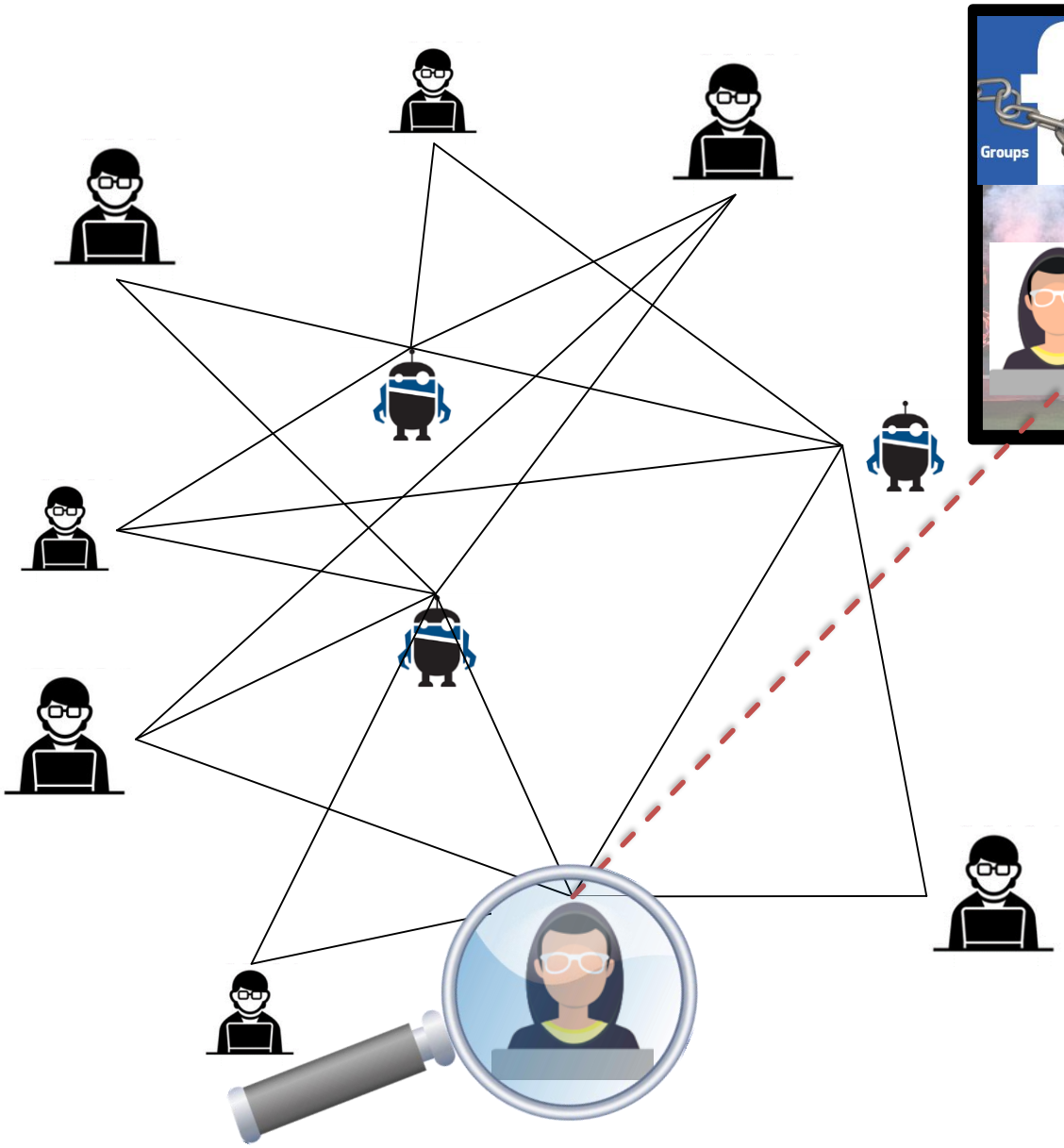
SoNA: A Prototype

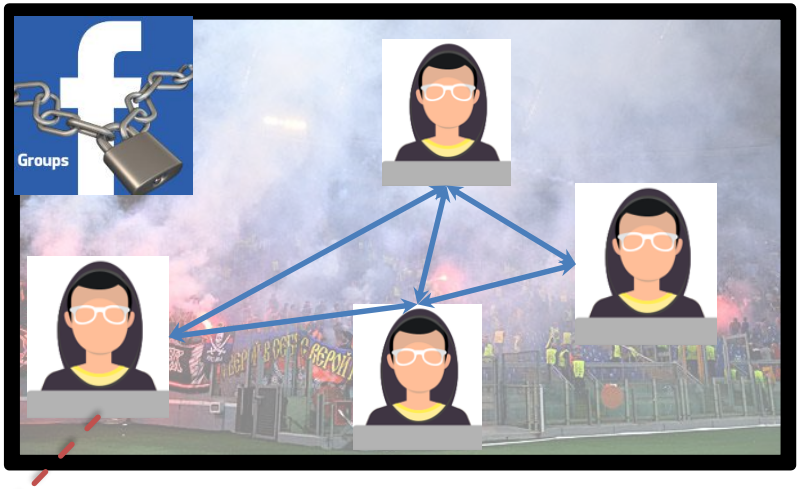


Challenge – vast amount of profiles



Challenges – closed/secret groups



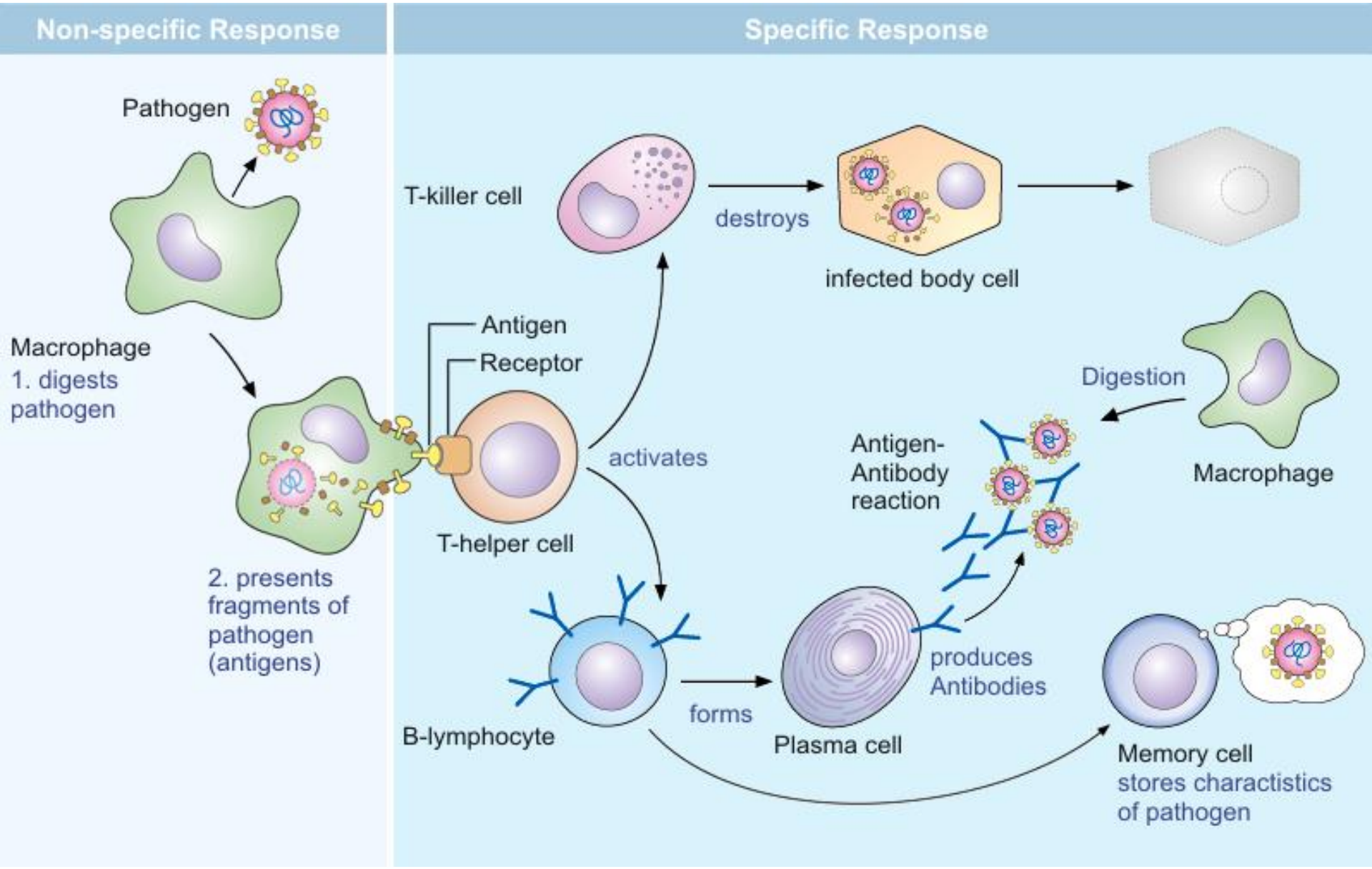


This is just like pathogens, isn‘t it?

Remember, what does the human body do?

Human Immune Response System

FoSIL

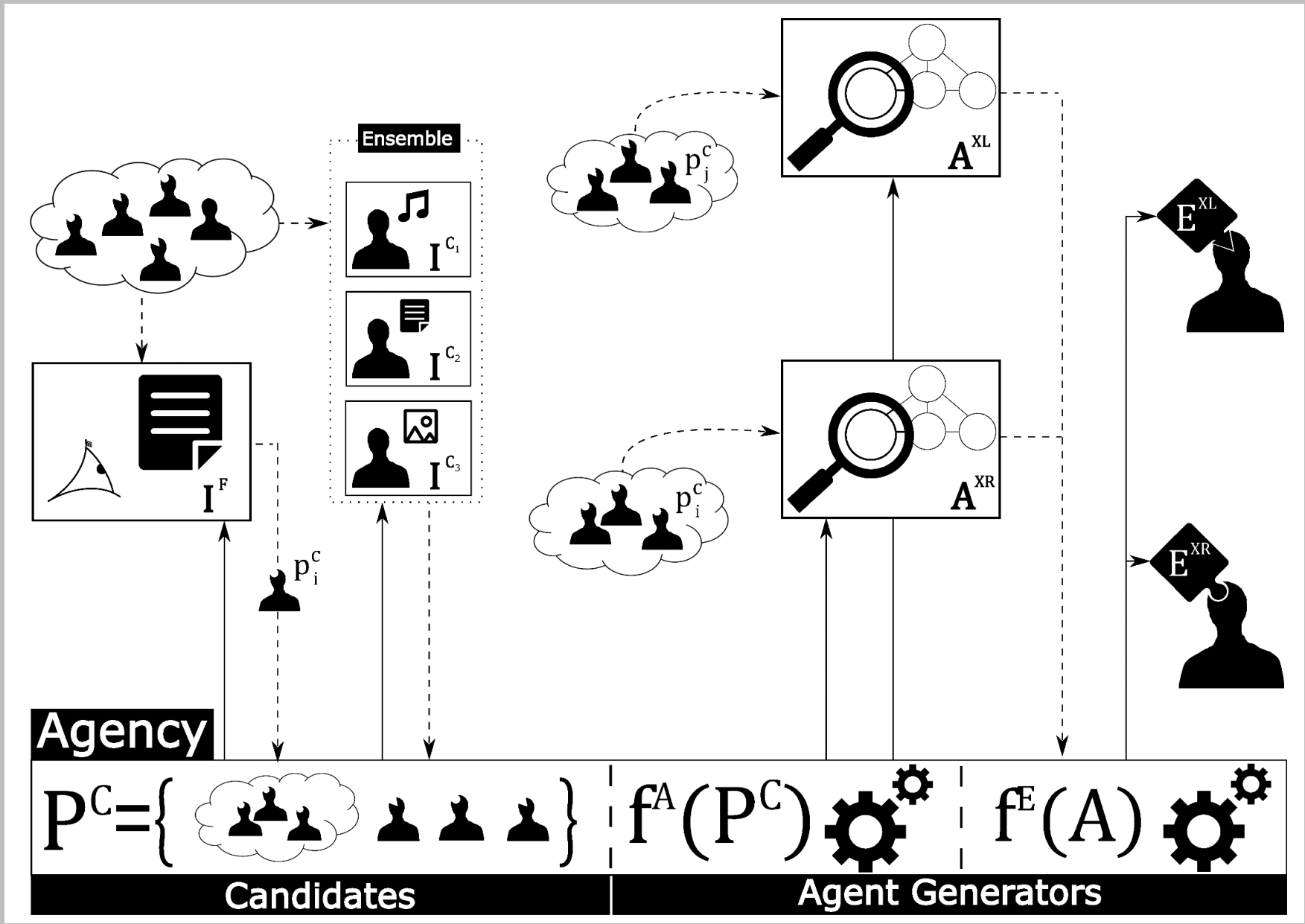


Can we do this for social networks in the same way?

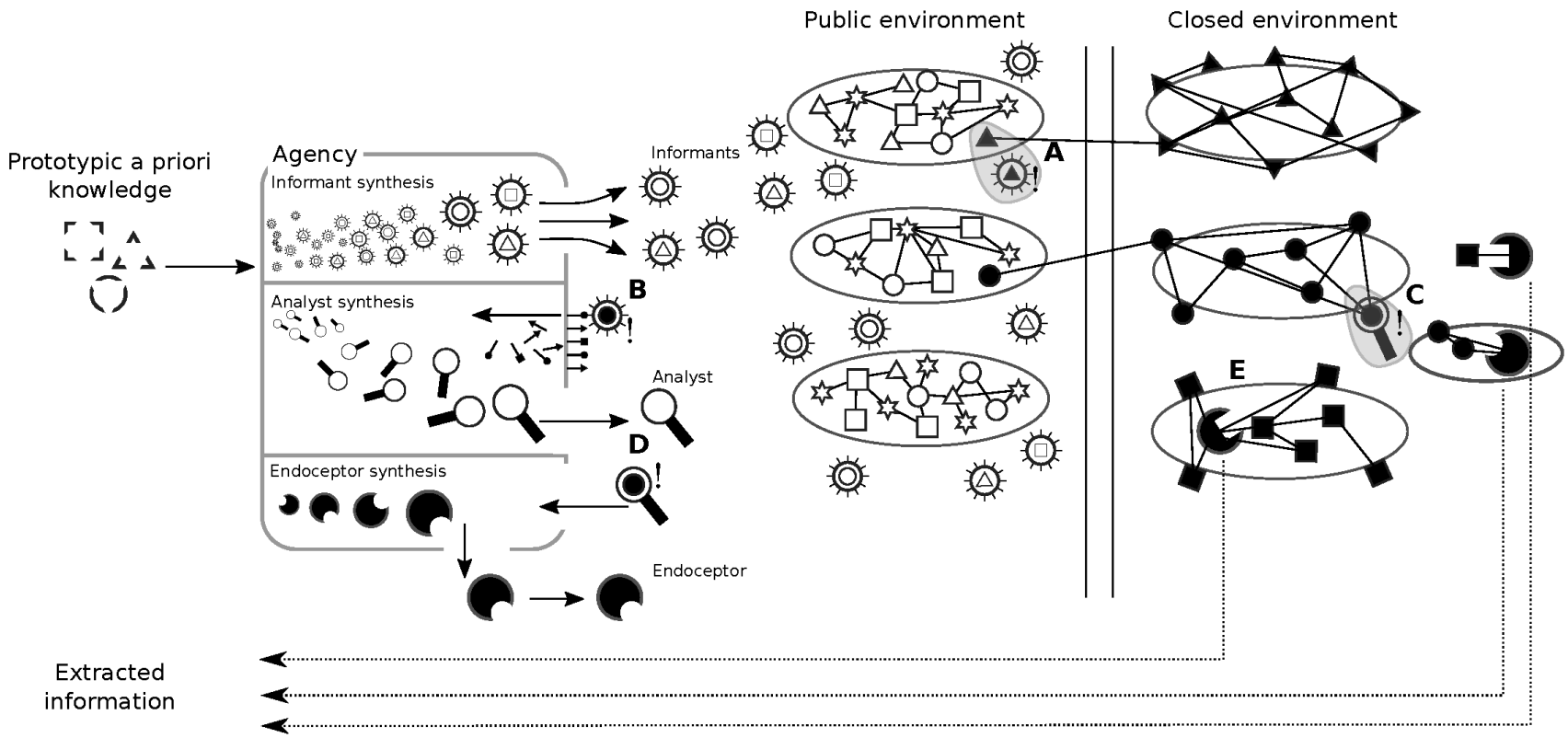
Are we able to construct an artificial immune system?

Agent-based Social Network Analysis

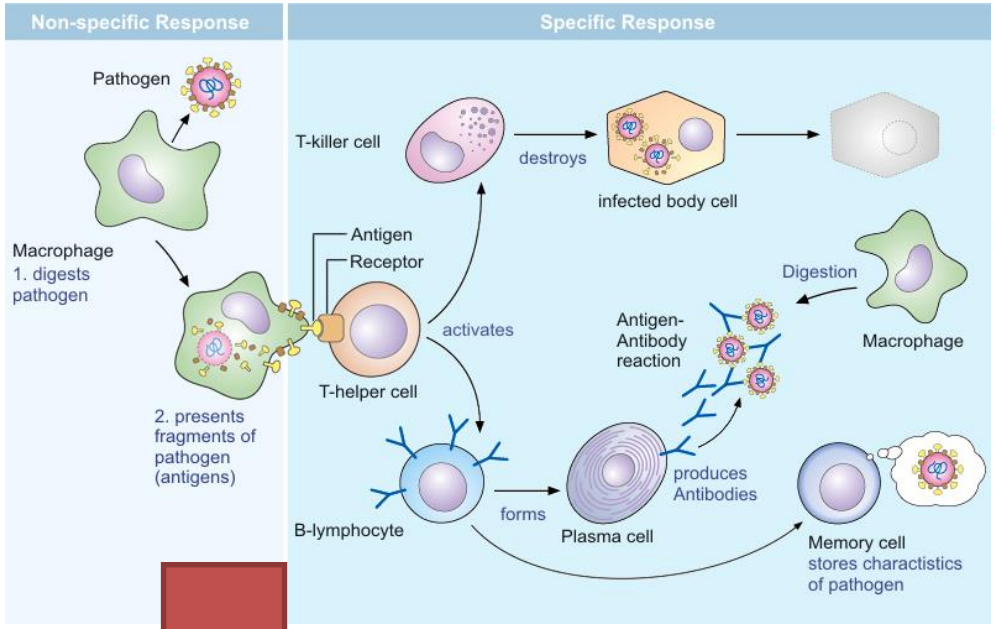
FoSIL

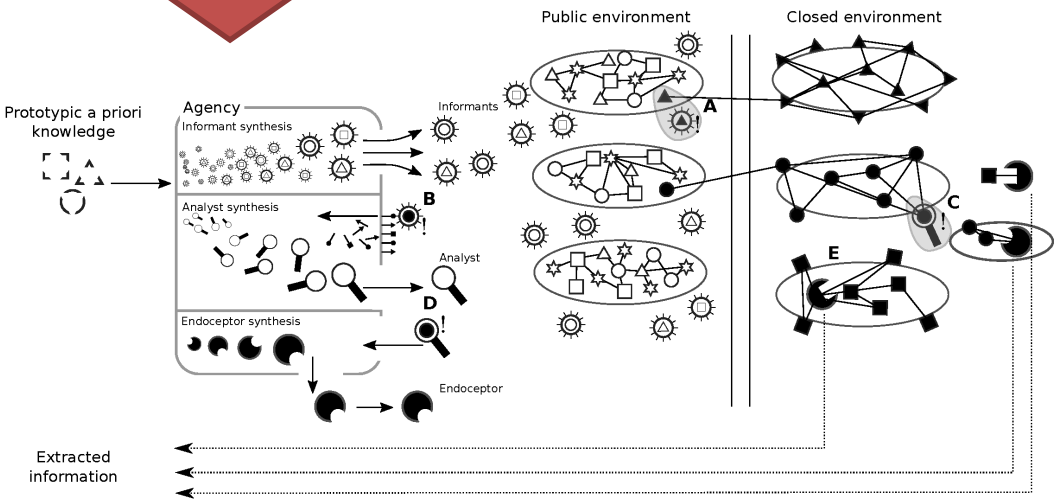


Artificial Immune System - Workflow



Conclusion





- Classical Virus Scanner
- Signature modulation
- Σ modulations
- activation
- elimination

FEEL FREE TO ASK QUESTIONS

VISIT US AT: www.bioforscher.de/FoSIL