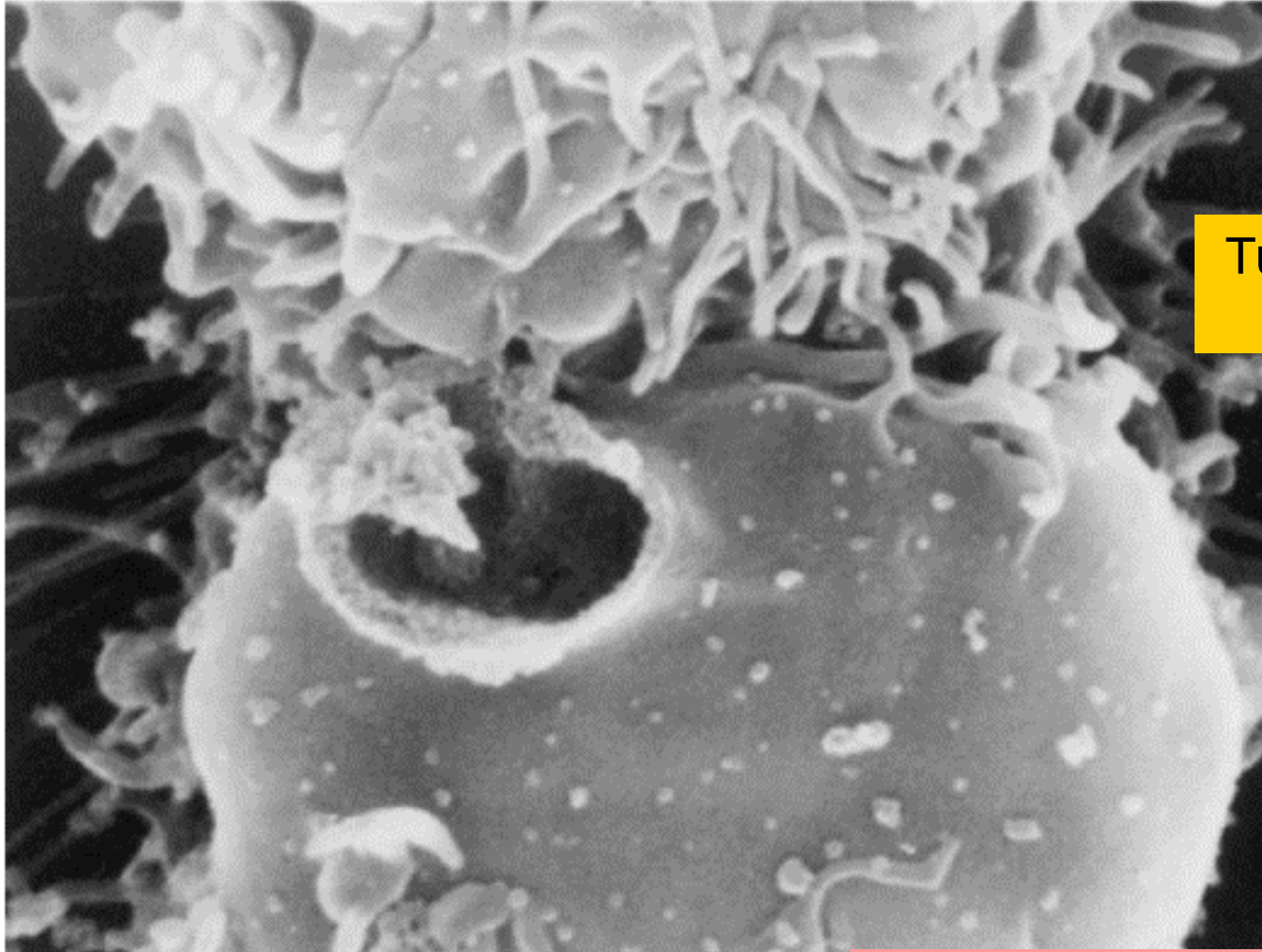


Immunology applied to computer security

A useful source of inspiration or a distraction?

Immunology is about *death* and *destruction* ...

(b)



Tumor cell destruction
by a CTL

...But it is attractive

What makes the Immune System attractive?

- It has the ability to *detect*, *identify*, and *eliminate* completely autonomously and with *great selectivity* a very large variety of immune challenges.
- It has a very low probability of false positive or negative
- It memorizes the previous challenges (It learns)
- Adjust to new threats



Can that be a dangerous attraction?

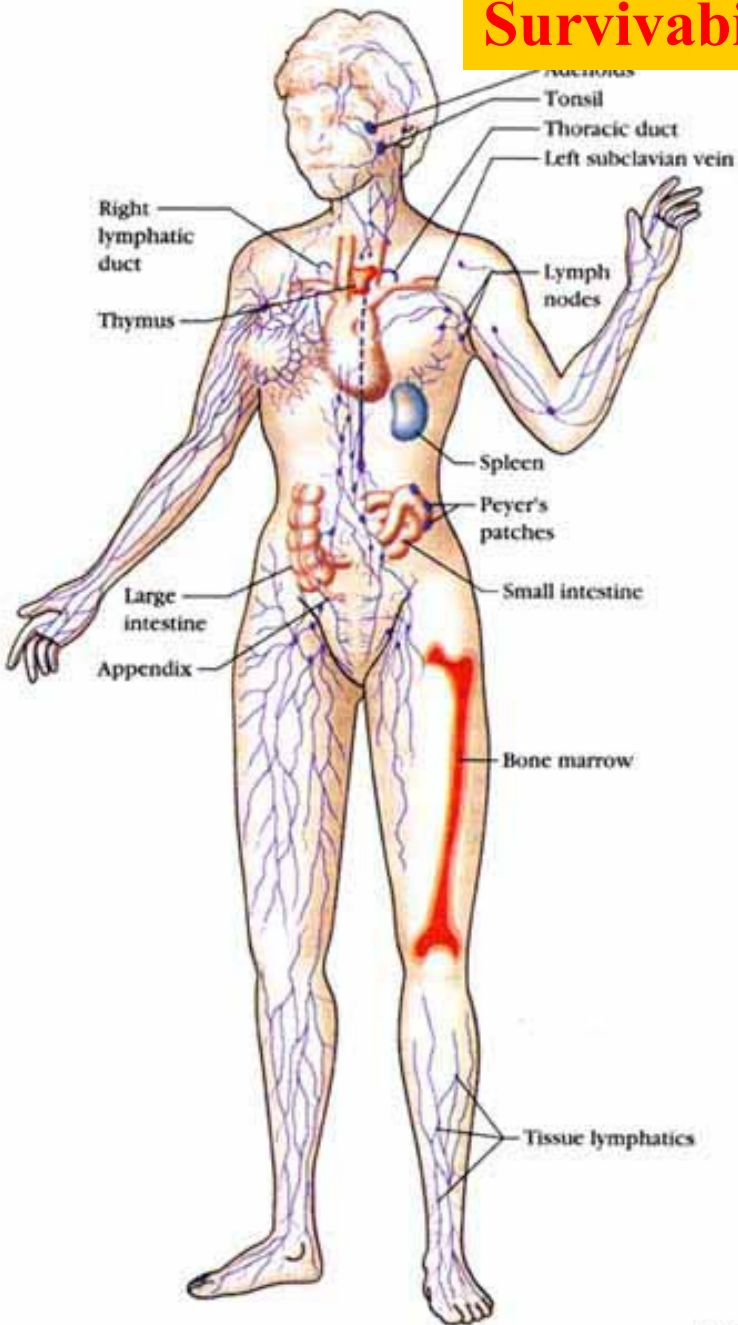
The immune system projects an impression of almost perfection: the result of millions of years of a co-evolution which seems to have a lot in common with the way cyber defense is evolving.

We should not forget the trail of deaths and extinctions which litter the history of this co-evolution.

The hope is that we can learn from the result and avoid the trail



Survivability of the human critical infrastructures



Through the obvious differences between the immune system and cyberdefense of critical infrastructures, architecture is a potential point of convergence.

The human “critical infrastructure” is made of different “organs” (The intestine, nervous system, eyes, motor system, heart are different tissues with very different immunological properties. Different inoculations of the same antigen elicits completely different responses.)

They are coupled but in such a way that the degradation of one sector does not propagate to others.

Innate/Adaptive responses are fundamental **building blocks** in the **architecture** of the immune system

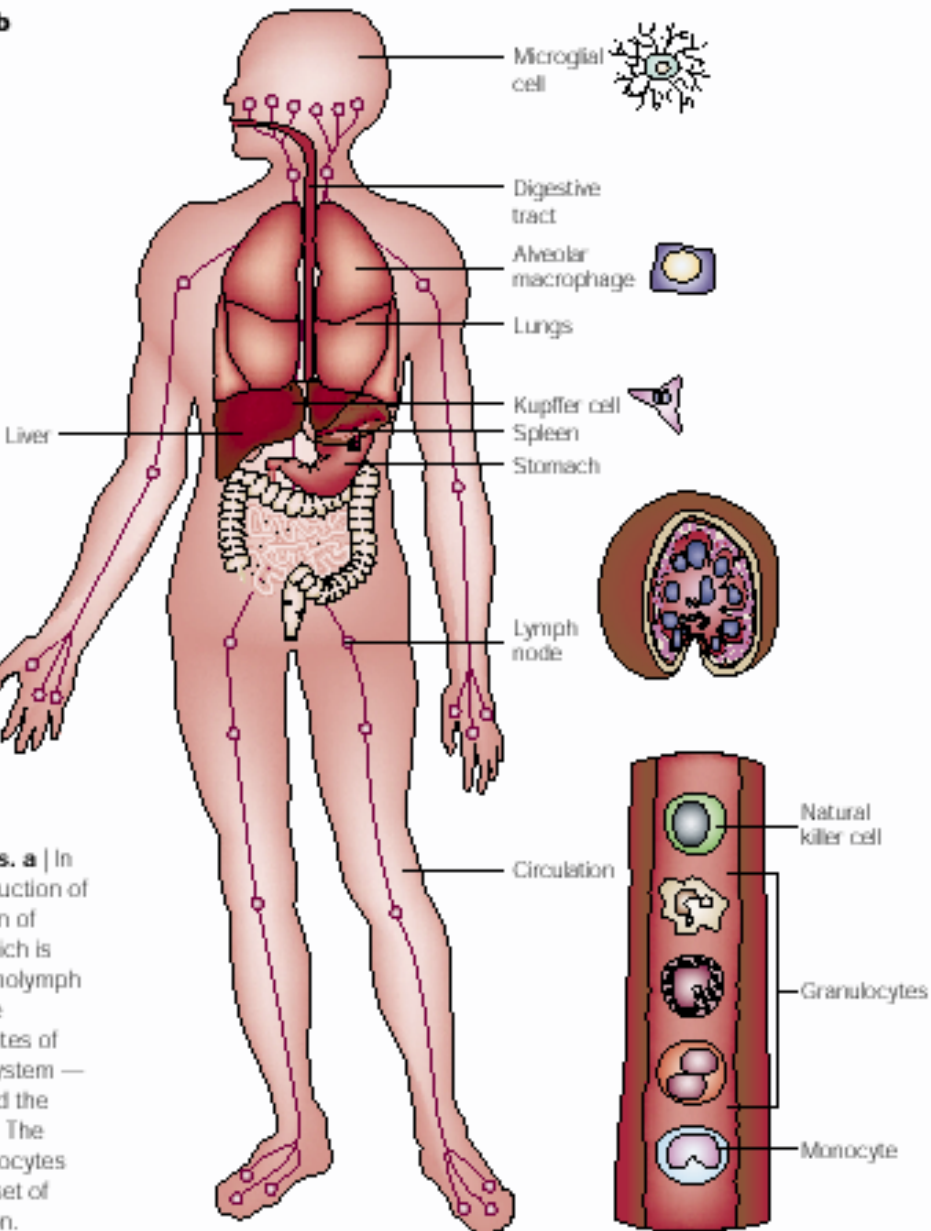
Two phases in the immune response (of the vertebrates):

1. The first is detection: it is made by the **innate system**, (The innate response is also the first line of defense and contributes later to the elimination of the antigen)
2. The **adaptive response** deals with elimination of intruder after detection and the immunological memory.

The coupling between the two phases is through the cognate interaction: a very information intensive phase of the immune response of the vertebrates.

The invertebrates do not have an adaptive response

The emphasis on the distinction between adaptive and innate responses is relevant for cybersecurity, because:



1. Most of the immunological concepts used in cybersecurity are borrowed from the adaptive response, and at the same time,
2. most of what today's IDS want to accomplish is what the innate system does.

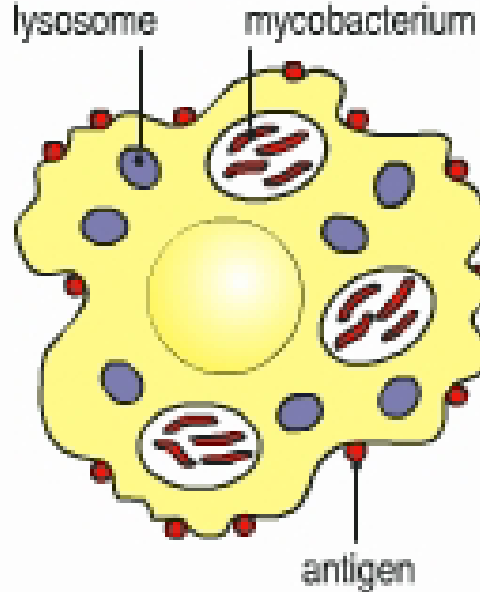
•It is in the Innate response that the explanation for the low false positive and negative in detection lies.

•It is not centrally based on self-non-self and statistical recognition

Some common misconceptions in the cyber-community about the immune system

- Self/non-self is not in general the trigger of an immune response, it is an important component of the *adaptive response*
- Clonal expansion and affinity maturation are parts only of the *adaptive response*, a prelude to the elimination of the pathogen
- The challenges of IDS's today have far more in common with the *innate response* than with the *adaptive response*

Infected macrophage



The macrophages:

They are typical representatives of the innate response.

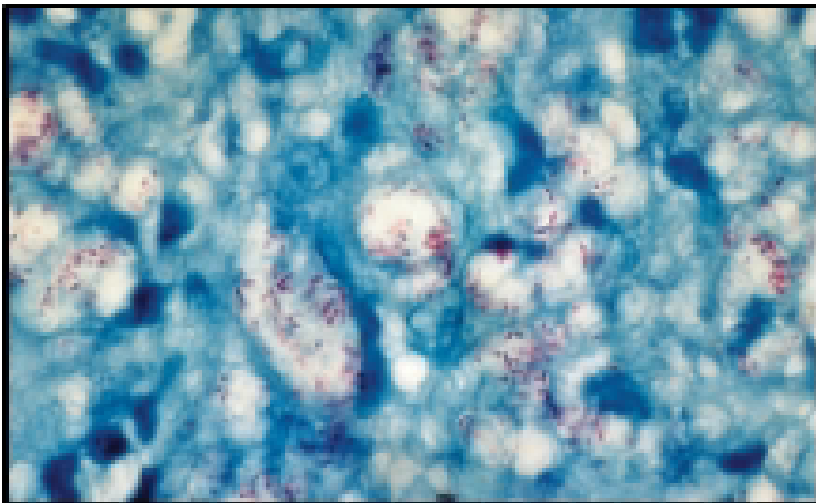
They play a central role in the early warning, but also in tissue maintenance

It is involved in the first detection of presence of attack

Macrophages are scavengers.

They make the difference between apoptosis and necrosis

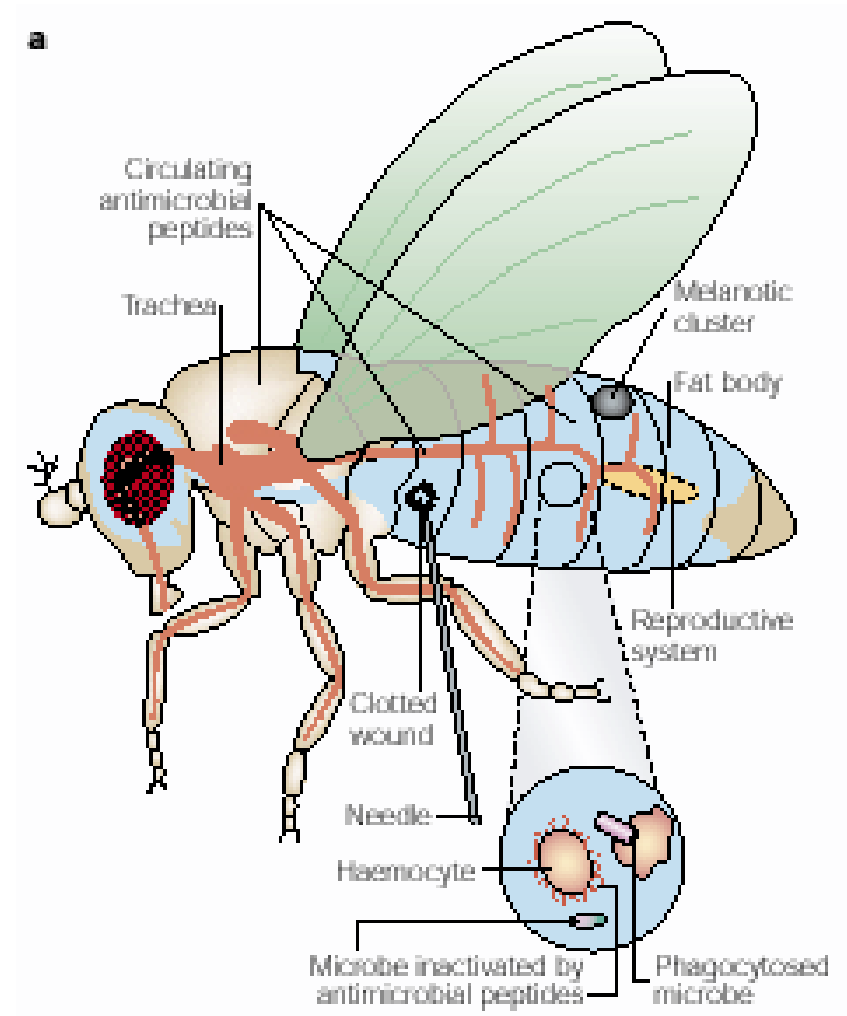
(anomaly detection)



PAMPs

(Pathogens Associated Motif Patterns)

- Toll receptors: a link between different species
- Comparisons across phyla and classes does not only give an idea of the history of the immune system but, by distinguishing what has been conserved from what has varied, they tell more about what is essential and what is accessory in the human immune system.
- “the implications of an ancient regulatory cascade uniting insects, mammals and plants are far reaching, especially considering that the last common ancestor of these diverse groups was probably unicellular.”



Signature-based detection (?)

- C' : Complement
- C1, C2, V Ig domain types
- Dlg : Ig superfamily members involved in defense
- E : Effector cells of mesodermic origin
- H : Histoincompatibility reaction under genetic control
- IL : Interleukin homologues or analogues
- M : Specific memory in graft rejection
- MHC I, II, III : Major histocompatibility complex components of the class I, II or III types
- NK : Natural killer cell activity
- Reg. : Conservation of lymphocyte signal transduction pathways

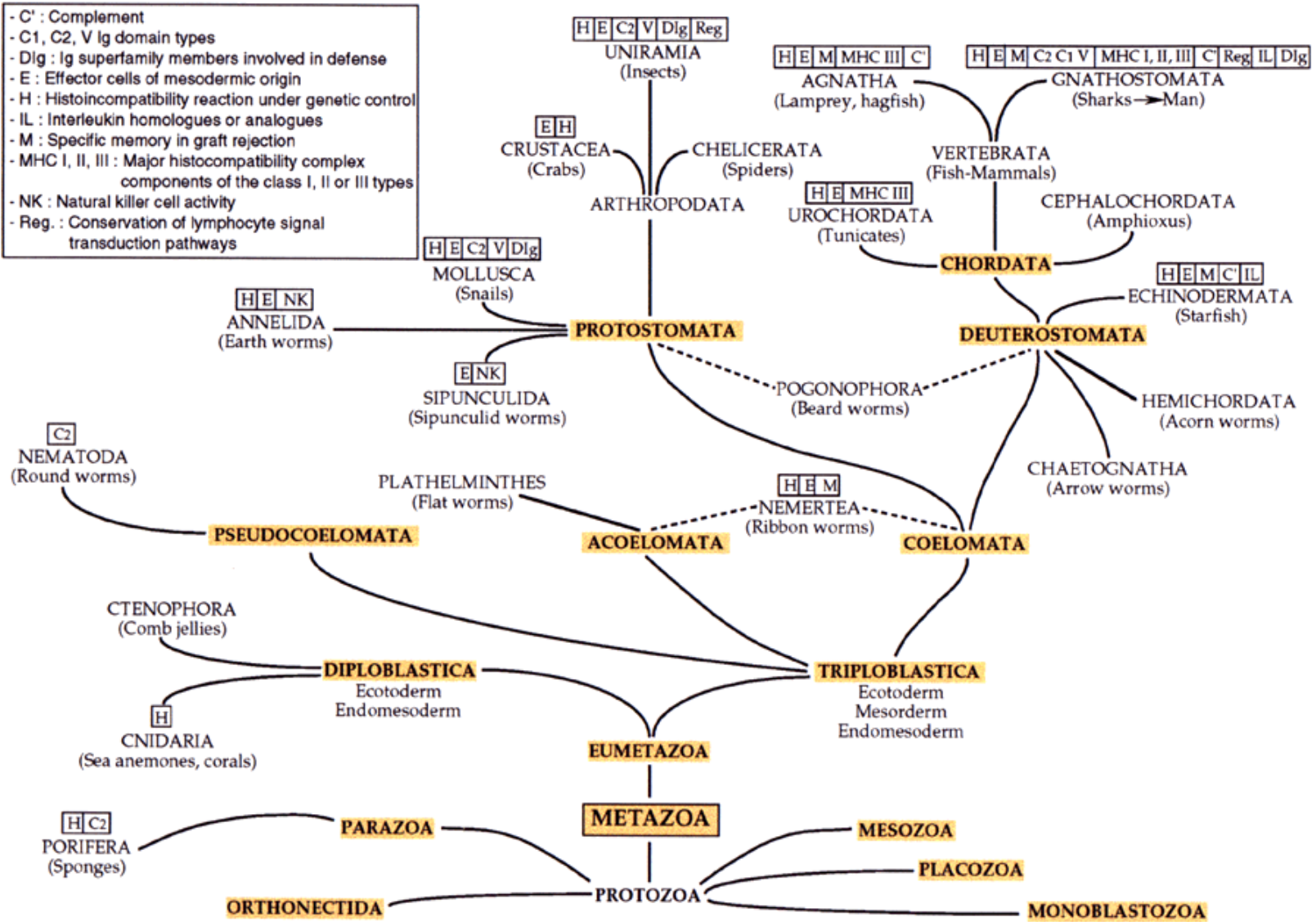
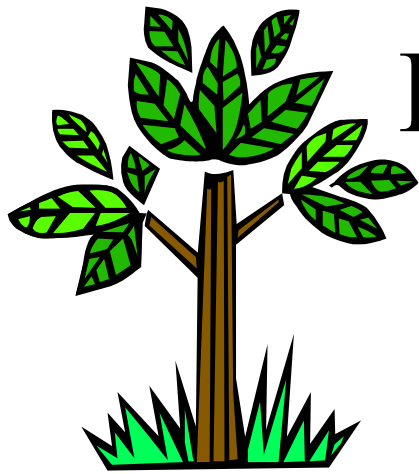


FIG. 1. Elemen

Where would cyberdefense be in this chart, today??
 Where should it be?

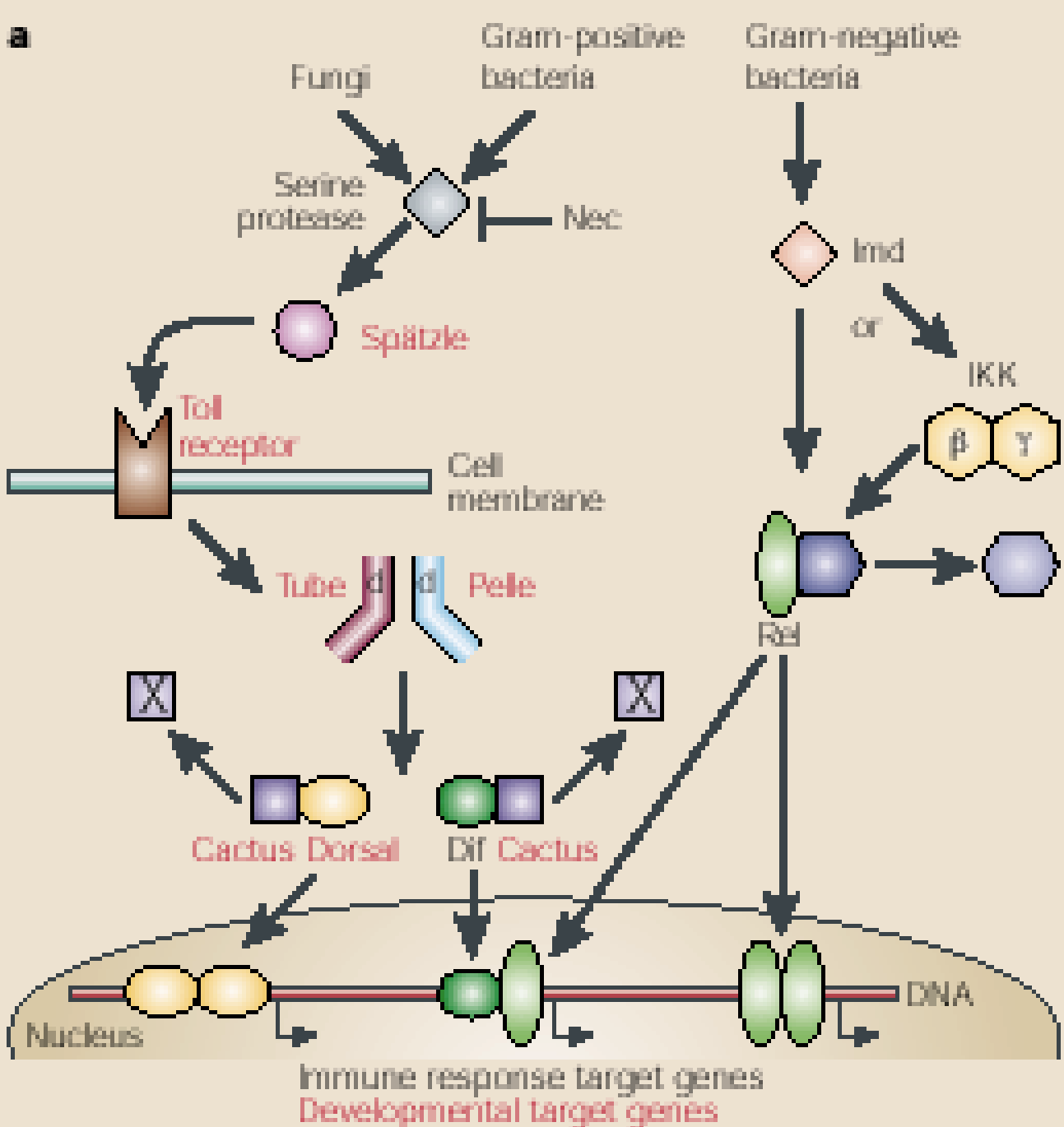


Repertoire and plants' immunity



- No moving parts.
- LRRs (Leucine Rich Receptors) are intra-cellular recognizers There are only 175 LRRs
- Too small number to constitute a repertoire against existing antigens... Two possibilities:
 - either they are promiscuous or
 - the “ligand universe” is limited (and, possible explanation: *is sensitive to a limited number of factors characterizing the good functioning of the plant*)

An example of anomaly-based detection based on a limited repertoire!?



Toll receptors

Part of a complex
Pattern
Recognition
system

Involved many
cofactors.

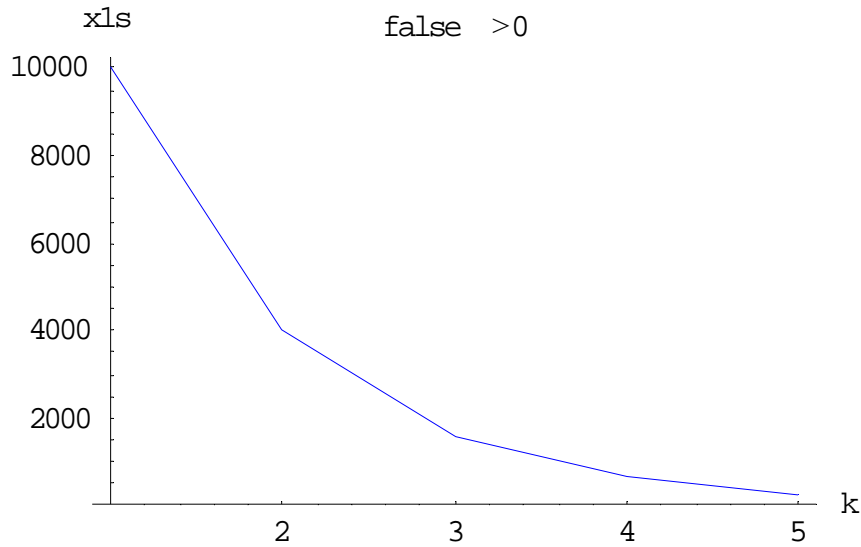
Cascade of events

A form of
sequential
signature based
detection?



Origin of low false negative and low false positive in immune identification: a mathematical characterization

- Architecture of immune detection: two possibilities: $\square = 0$, or $\square = 1$.
- Let's assume that if:
 - the measurement yields $X = 1$, the probability that $\square = 1$ is p_1 .
 - Or the probability that it is wrong to infer that $\square = 1$ is $(1-p_1)$ and
 - if the measurement yields $X=0$, $\square = 0$ with probability p_0
 - and $\square = 1$ with probability $1-p_0$.
- The question is what is the probability of false positive and false negative after a sequence of measurements, as a function of p_0 and p_1 ?



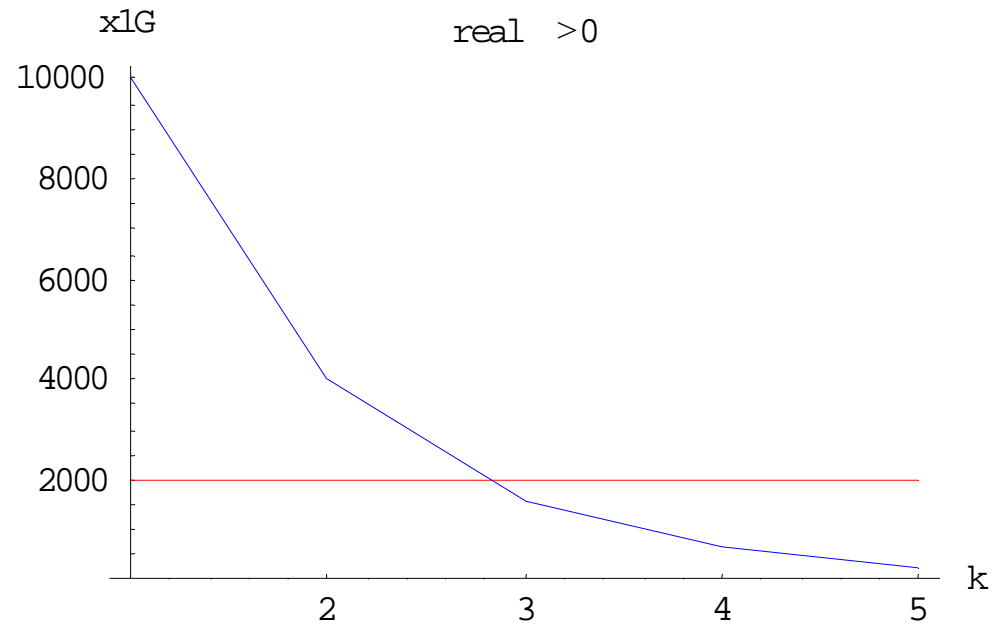
$P1=1$

$P2=0.6$

$N0= 10,000$

$N1= 2000$

The performance of the system is **very sensitive to 1-p1 (false negatives)** but **less to 1-p0 (false positives)** because of the **number of steps**, even when $N0 \gg N1$.



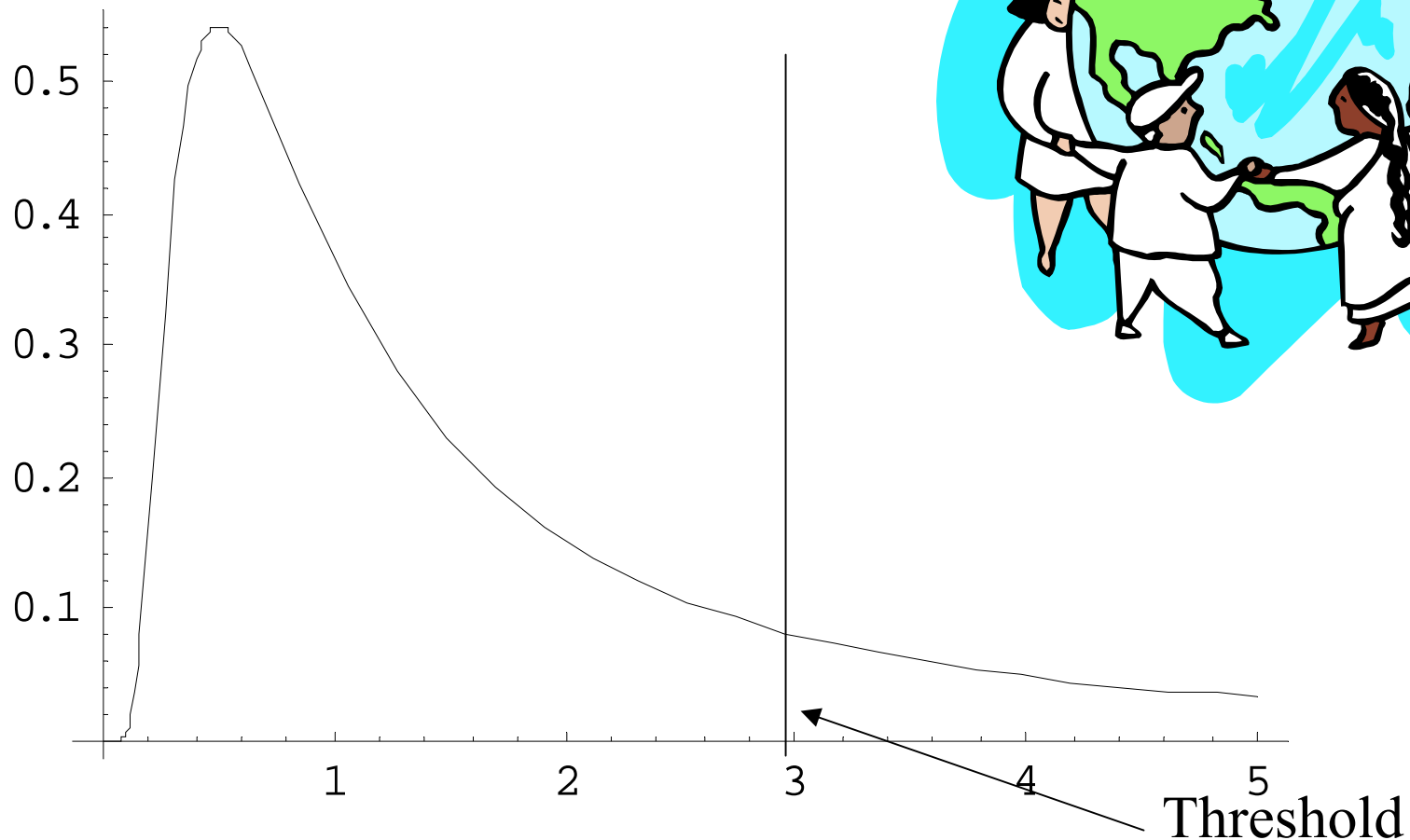
Large numbers, variability, thresholds

Interactions between lots of different kinds of
molecules (complements, Toll receptors,
protein cascades, cytokines, chemokines), and
cells (Macrophages, Neutrophils, NK cells,
Dendritic Cells, epithelial cells),

Each involves a high degree of variability
(lognormal distributions)

System of thresholds

Combined effect of variability and large number

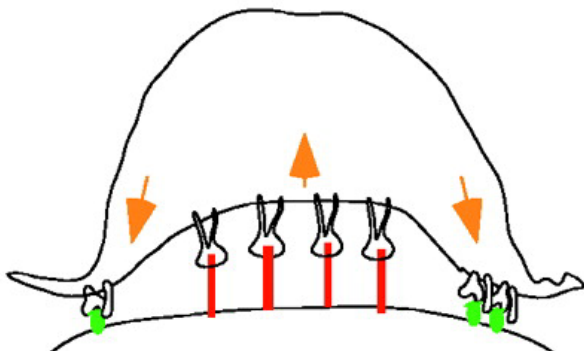


From the innate to the adaptive response: the cognate interaction

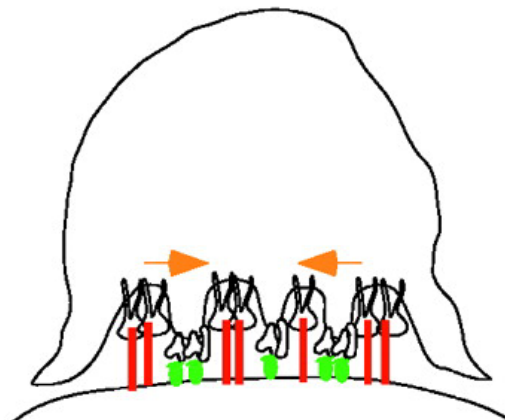
A very information intensive phase (what information)

It uses the “Immunological synapse”:

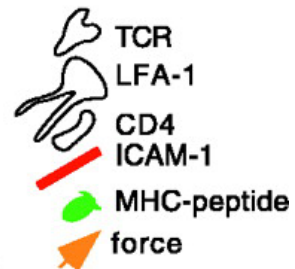
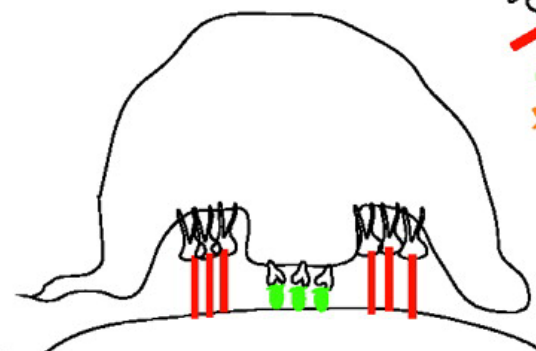
Stage 1- Junction formation



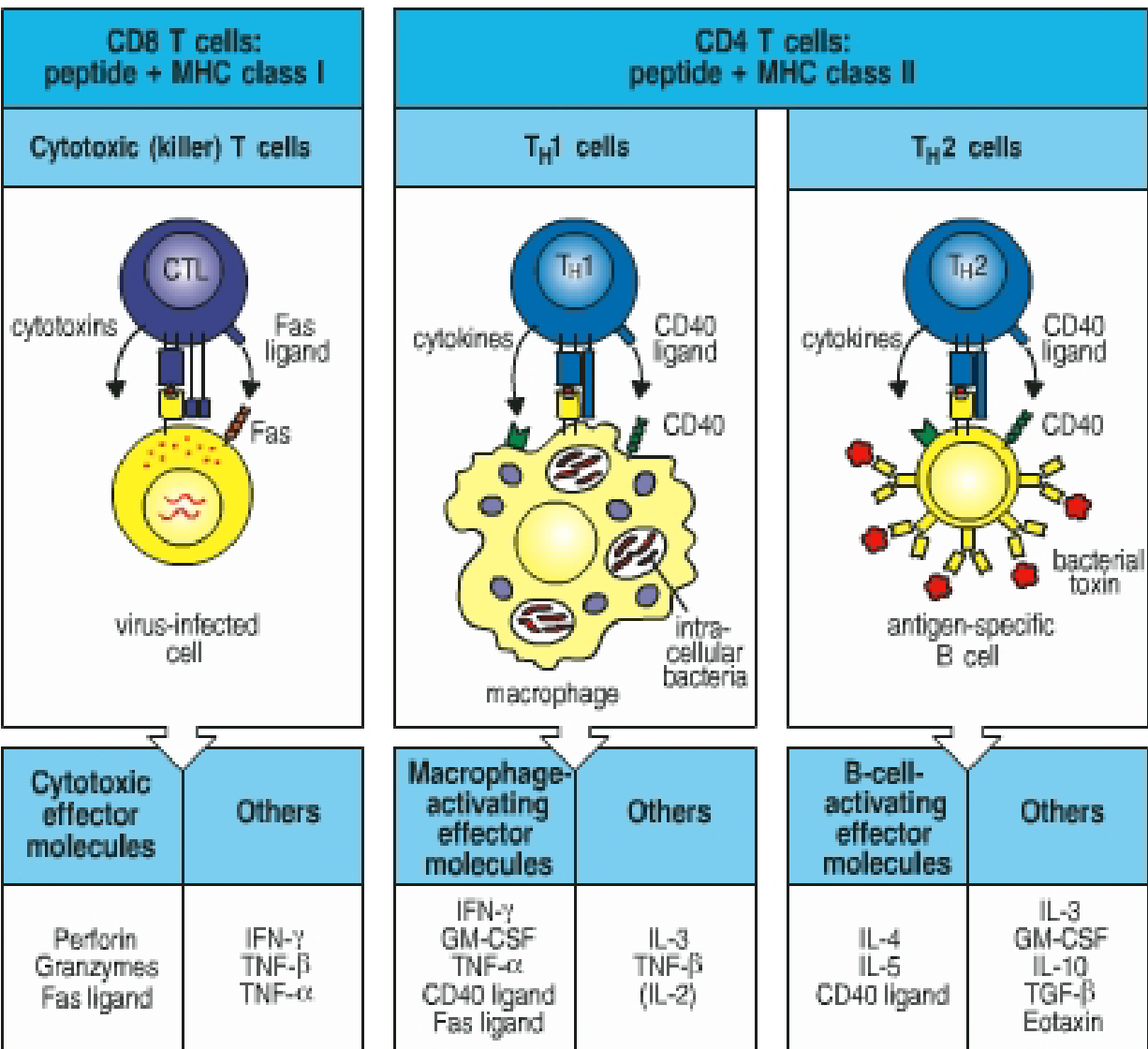
Stage 2- MHC-peptide transport



Stage 3- Stabilization

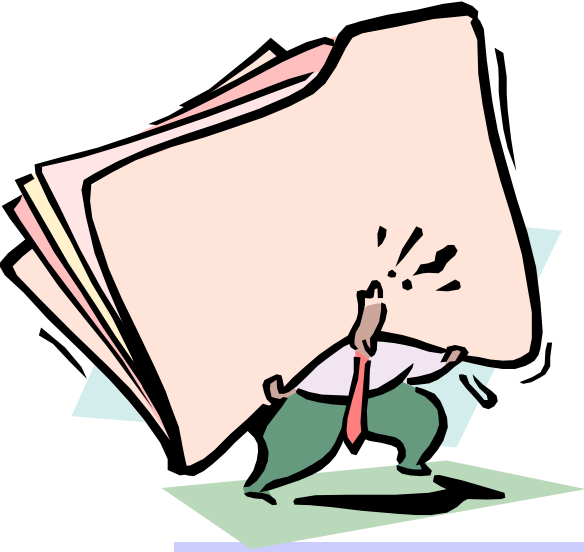


Activation of naïve CD8/CD4 T cells



Activated effector CD8 T cell (CTL), ready to kill

CD4 cells use MHC class II. They do not kill, they are processors and distributors of information.



Cytokines: the immunological information highway

- Hundreds different kinds of molecules secreted by activated cells which affect the nature of activation of other cells in a variety of ways.
- Cells are complex objects. Cytokines is a favorite way to change their state.

Is there a cyber-equivalent of cytokines, or can they exist only in a biochemical environment?

An apparent mega-difference between cybersecurity and Immunology: the biochemistry of the interaction

Biochemical properties of proteins not related to sequencing: It is an emergent property

The immune system detects the presence of an intruder, in general through clues which are **not related** with its virulence (PAMPS/ACAMPS)...

An unsolved mystery in immunology: PAMPs are carried by “good” bacteria. How does the body make the difference between good and bad bacteria



As other forms of beauty, survivability may have its cost...

IDS's are designed to introduce as small an overhead and disturbance as possible, whereas...

... the immune system is a large “organ”: It has 10^{12} cells, roughly the same number as the nervous system and is omnipresent in the body..

Most if not all the components of the immune system are multi-tasking:

Many physiological functions are ensured by the immune system.

Its role is NOT limited to protect the organism from intruders.

