Referentia Systems Incorporated

referentia

Maturing Cyber Security Using BioThreat Experiences and Resources

Norman Lee Johnson

Tim Williams

15 Jun 2009

njohnson@referentia.com

twilliams@referentia.com

Goal: Provide a new viewpoint for maturing cybersecurity

What was it like to live in London 200 years ago?

- How common was disease?
- Life expectancy? What changed?

Background

- Related work: Adaptive Immunity

Maturity of Cyber and Bio

Similarities

- Function-Process
- System

Maturing Cyber with Bio

Specific Guidelines

Specific Examples

White House’s 60-day Review of National CyberSecurity

From Pres. Obama’s introduction of the report:

- “…cyberthreat is one of the most serious economic and national security challenges we face as a nation."
- ”…not as prepared as we should be, as a government, or as a country.”
- ”… from a few keystrokes on a computer -- a weapon of mass disruption."

Lead by Melissa Hathaway, Senior Advisor to the Director of National Intelligence (DNI) and Cyber Coordination Executive

- Reviewed more than 250 executive orders, policies and advisory reports
- Held 40 meetings with stakeholders
- Reviewed more than 100 papers submitted to it
- “Dealing with security piecemeal by different sectors and stakeholders, and dealing with security as a stand-alone issue, has not provided a secure infrastructure.”

A commentary made the observation:

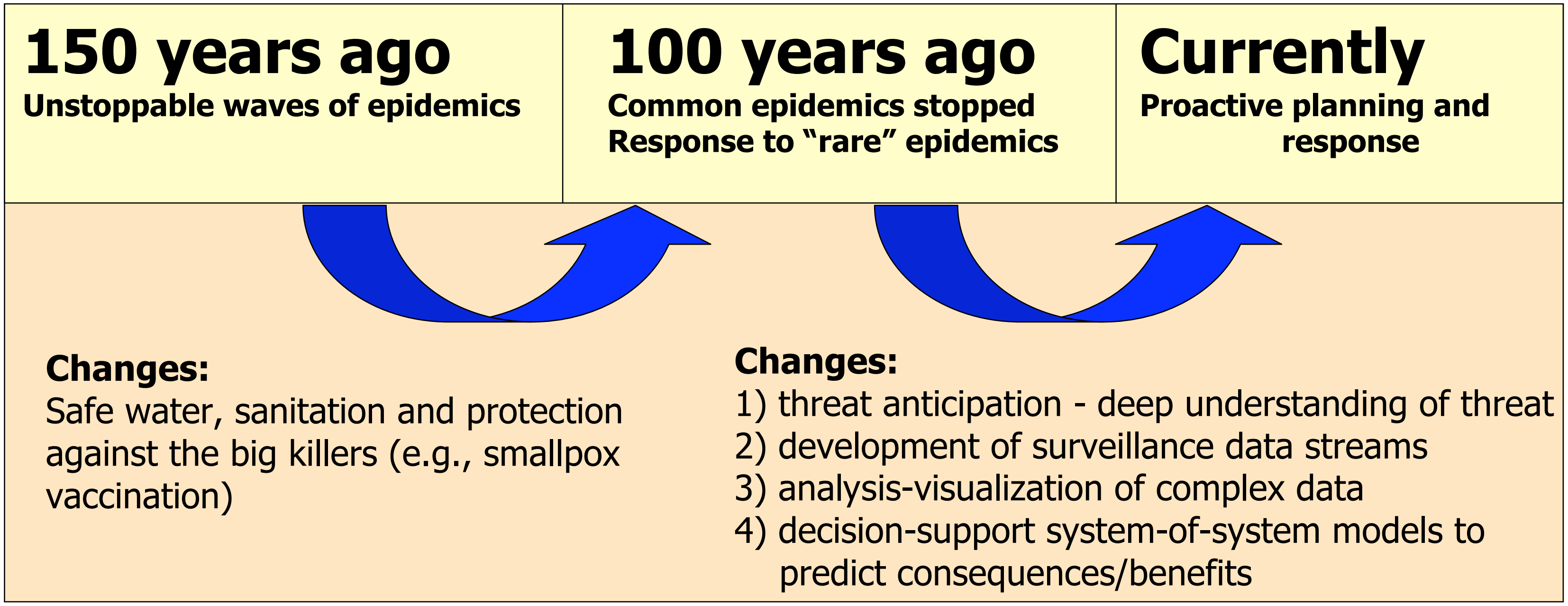
- ”…It’s like we’re playing football and our adversaries are playing soccer”

Difference in Maturation of Bio and Cyber systems

Frequency and types of events

Depth and breadth of response to events

How Public Health was changed over 150 years….



150 years ago

Unstoppable waves of epidemics

100 years ago

Common epidemics stopped
Response to "rare" epidemics

Currently

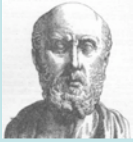
Proactive planning and response

Changes:
Safe water, sanitation and protection against the big killers (e.g., smallpox vaccination)

Changes:
1) threat anticipation - deep understanding of threat
2) development of surveillance data streams
3) analysis-visualization of complex data
4) decision-support system-of-system models to predict consequences/benefits

The Maturation of Public Health

460 BCE
Birth of Hippocrates the *Father of Medicine*



Rhazes suggests blood is the cause of disease
910

1300's
Plague in Europe (rats/fleas)

Introduction of antisepsis in prevention of cross-infection
1796

1832
Cholera in London and Paris (water)

Humans began to investigate how disease spreads

Edward Jenner develops first vaccination for smallpox
1860's

1870's
Louis Pasteur and Robert Koch establish the germ theory of disease

Scottish bacteriologist Sir Alexander Fleming discovers penicillin
1928

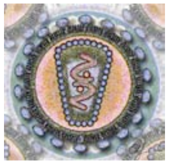
1940's-present
Emergence of antibiotic resistance and multi-drug resistance

James Watson and Francis Crick describe the structure of DNA
1953

1970's-80's
Emergence of new viral diseases (Lassa, Ebola, Marburg)

1980
W.H.O. (World Health Organization) announces smallpox is eradicated.

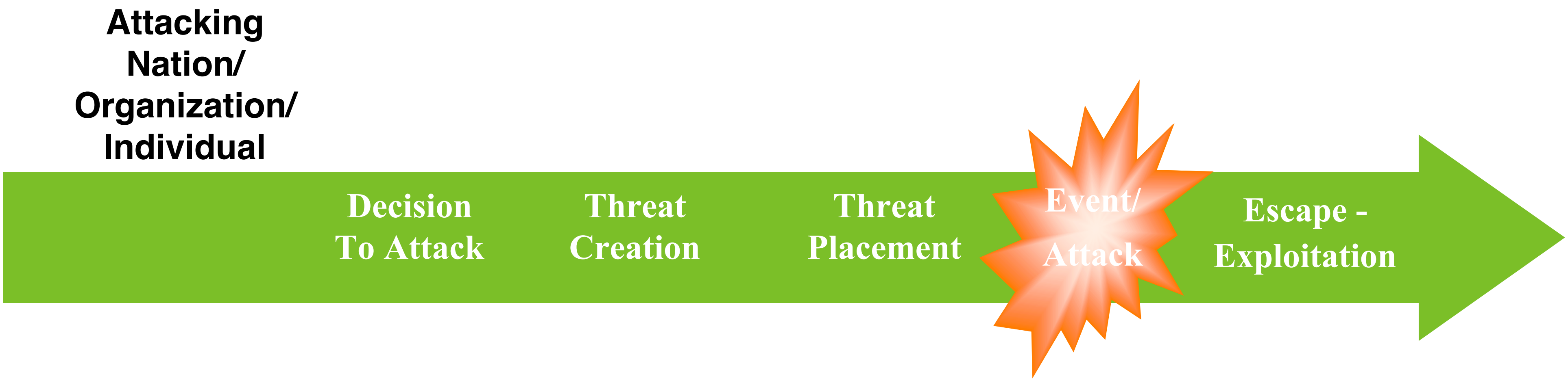
HIV, the virus that causes AIDS, is identified
1983



1980's-90's
Multi-drug resistant pathogens re-emerge (TB, Staph)

Cyber protection: Policy scale

This is what attackers do:



Attacking Nation/ Organization/ Individual

Decision To Attack

Threat Creation

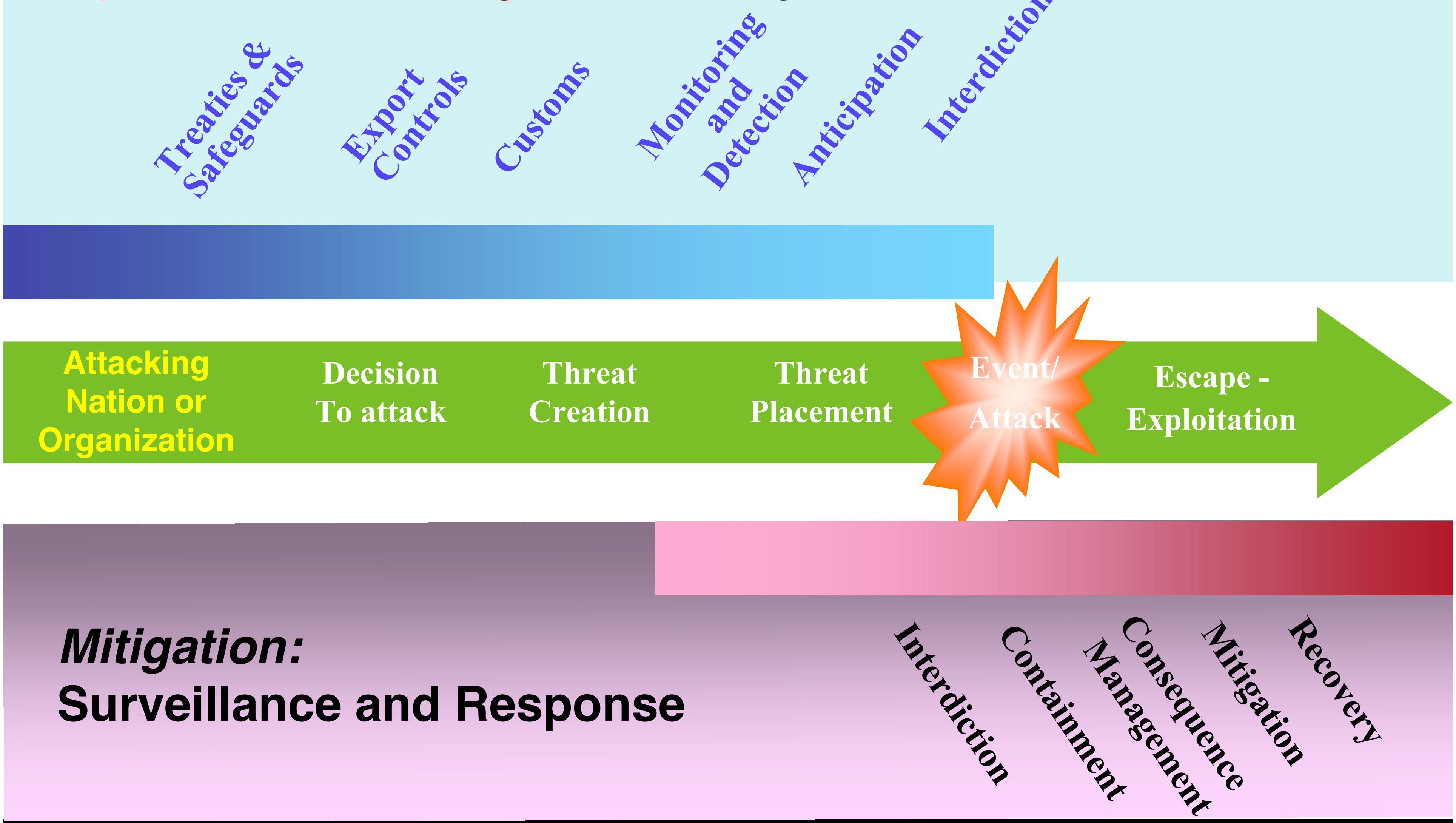
Threat Placement

Event/ Attack

Escape - Exploitation

How do we operationally respond?

Preparation: Planning, Monitoring and Prevention



Treaties & Safeguards

Export Controls

Customs

Monitoring and Detection

Anticipation

Interdiction

Attacking Nation or Organization

Decision To attack

Threat Creation

Threat Placement

Event/ Attack

Escape - Exploitation

Mitigation: Surveillance and Response

Interdiction

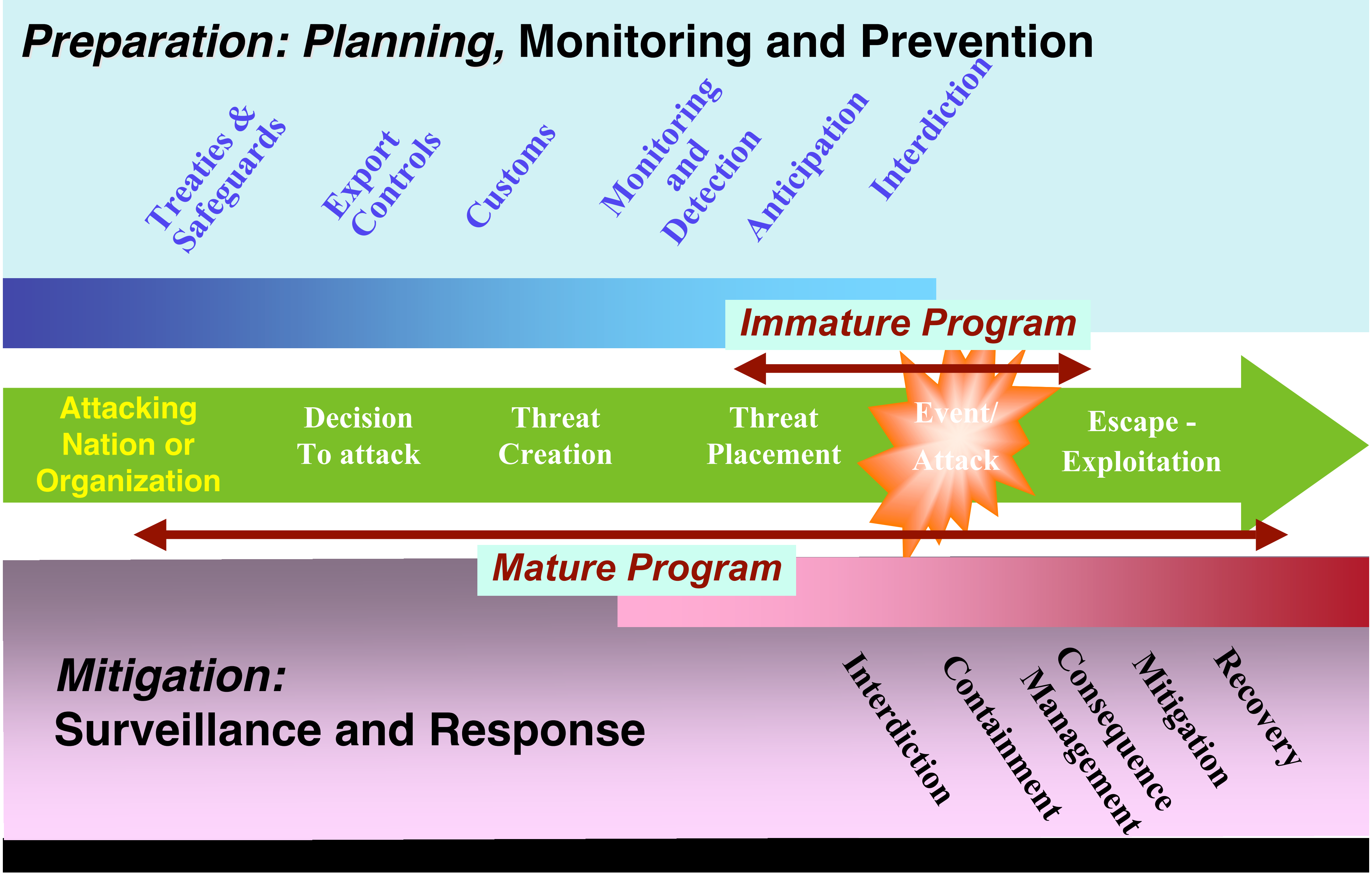
Containment

Consequence Management

Mitigation

Recovery

Maturity of Program = Pushing out from the event



Preparation: Planning, **Monitoring and Prevention**

Treaties & Safeguards

Export Controls

Customs

Monitoring and Detection

Anticipation

Interdiction

Immature Program

Attacking Nation or Organization

Decision To attack

Threat Creation

Threat Placement

Event/ Attack

Escape - Exploitation

Mature Program

Mitigation:

Surveillance and Response

Interdiction

Containment

Consequence Management

Mitigation

Recovery

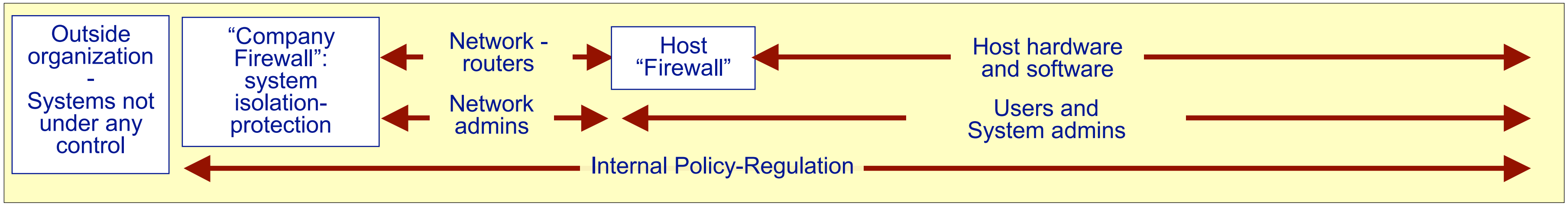
Similarities - Why Bio is relevant to Cyber

Function-Process Similarities

- The threat-host lifecycle (the infection process)

The Lifecycle of a Threat in a Host System

Threats require a host or host systems - within which they attack, enter, exist, manipulate, steal resources, and evade. The life of a threat is a “threat lifecycle”



Outside organization - Systems not under any control

“Company Firewall”: system isolation-protection

Network - routers

Network admins

Host “Firewall”

Host hardware and software

Users and System admins

Internal Policy-Regulation

Threat Life-Cycle	Enter network	Evade detection	Move to host	Attack or Collect data	Replicate	Spread to other hosts	Exit or communicate outside	Repeat Cycle
Defender Actions	Protect from entry	Detect entry	Detect - Stop move	Detect - stop attack	Detect - stop replication	Detect - stop spread	Detect and/or deter communication	Assess damage, locate source, etc …

Examples of threat lifecycles:

Viral threat:

Denial of service:

DNS/BGP spoofing:

Similarities - Why Bio is relevant to Cyber

Function-Process Similarities

- The host system immune response options
  - Host immune state determines susceptibility
  - Host defense options are very similar - Layered defense systems :
    - Cell wall - firewall, with preferential transport
    - Innate immune response - always active
    - Adaptive immune response - takes time to work the first time
    - System isolation
    - Death of host

Similarities - Why Bio is relevant to Cyber

System Similarities

- Direct Consequences
- Secondary and indirect consequences

Maturing the Cyber domain from bio resources

Develop programs that extend out from the event

Similar challenges require similar solutions

- Inherent chaotic nature of systems require a data-driven approach

From a Analysis of Cyber Gaps and Bio Opportunities

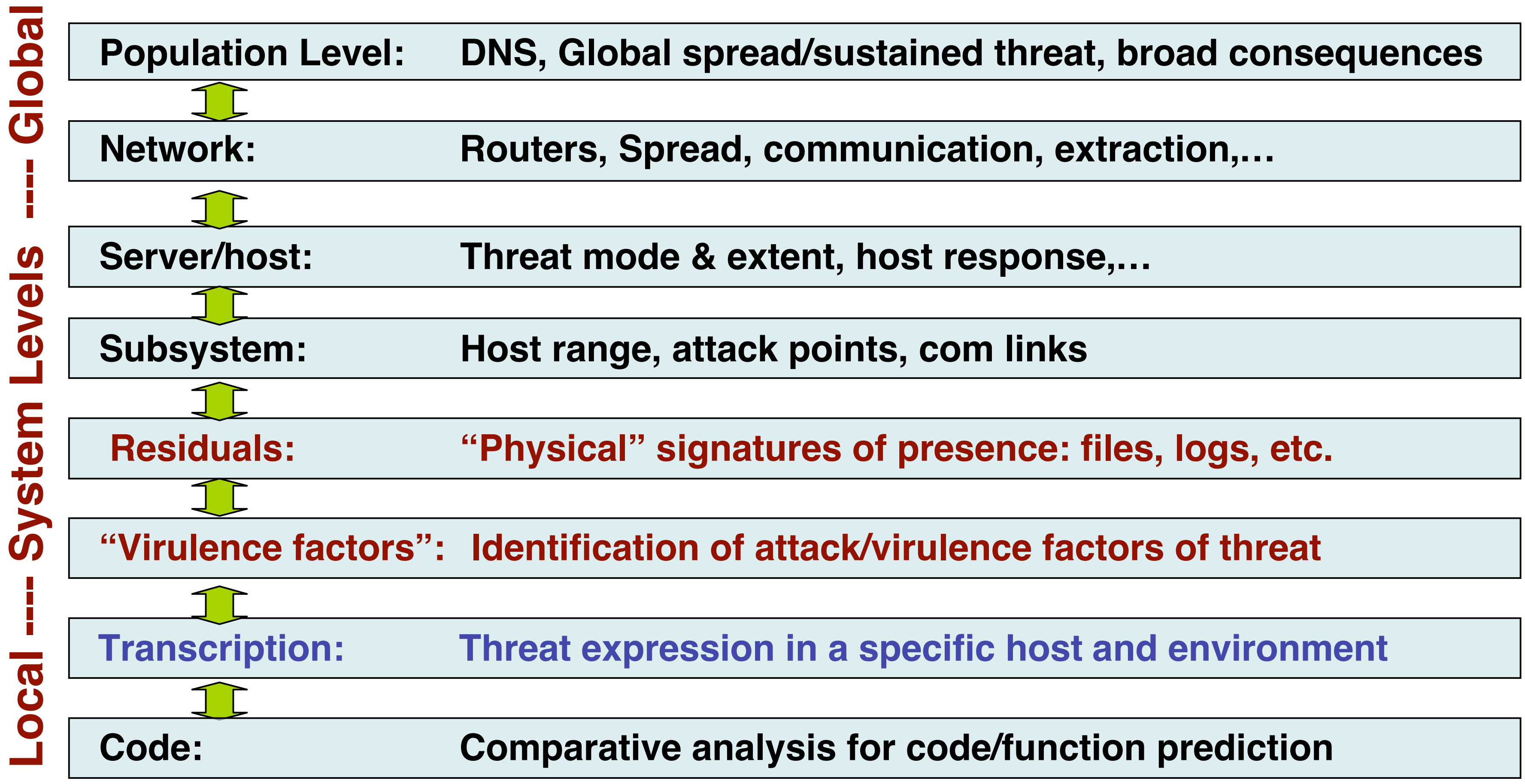
- Data stream development
- Surveillance and situational awareness
- Analysis and visualization
- Decision support resources
  - Predictive/forecasting simulations
  - Consequence-benefit analysis resources
  - Resources to integrate all of the above

Analysis of Requirements, Gaps and Resources

Cyber Resources Required	Existing Cyber Resources	Cyber Gaps: Needed Resources	Enabling Bio-Resources
Diverse cyber data: providing historical and real-time data of current network topology and traffic; enclave, component and user activity, access, status	**Rich and more in development** - Network flow traffic types/volume; component types & programs used	Status of components: susceptibility, symptoms of attack, readiness, activity, threat level	Genome” threat data bases, “virulence” databases, current threats, current news
Analysis and visualization of complex data streams: past and situational health, attacks, losses; global-to-local drill down, weak-signal precursors, threat ID and attribution, intuitive analysis of large data sets	**In development** - Large data set analysis identifying trends and precursors, anomalous behavior, ideally automated	Health of network and components, direct and inferred attack status, syndromic precursors to attack ID, forensics, threat attribution, …	Threat phylogeny, syndromic surveillance, health metrics, virulence change ID, forensic tools, responsiveness status, visualization resources
Predictive models of future state/losses from an attack given historical and current state, with transparency of outcome-to-cause and uncertainty quantification	**Scarce** - mostly academic simulations of network activity for limited threats; no exhaustive studies of tipping points	Databases of threats, standard threat models, emerging threat theory, effectiveness of response options	Epidemiological simulation resources, studies of mitigation options, coupled infrastructure sims, cost estimates,
Consequence - benefit resources including risk assessment, management and communication, expert-stakeholder conflict resolution, mission continuity	**Very limited for real-time response; limited for planning; limited fundamental understanding**	Metrics for mission readiness, threat-vulnerability mapping, integration of simulations	Standard threat scenarios for uniform preparedness, advanced risk assessment, adversary models,
Decision-support integration of above for planning and response: quantitative and transparent assessment of options, local-to-global cost-readiness tradeoffs, acquisition guidance, etc.	**Very limited** - currently wet-ware (human) based, no policy-level guidance on infrastructure acquisition, no operations support tools	Cost-benefit analysis of “what if” scenarios and response options; Risk management and communication	Threat anticipation-prediction, risk-based training, multi-stakeholder net-assessment studies, acquisition tools

A Multi-Level Threat View of Cyber Security/Defense

View the system as **signatures/activities/processes at different levels** - from small & localized to large & system-wide.

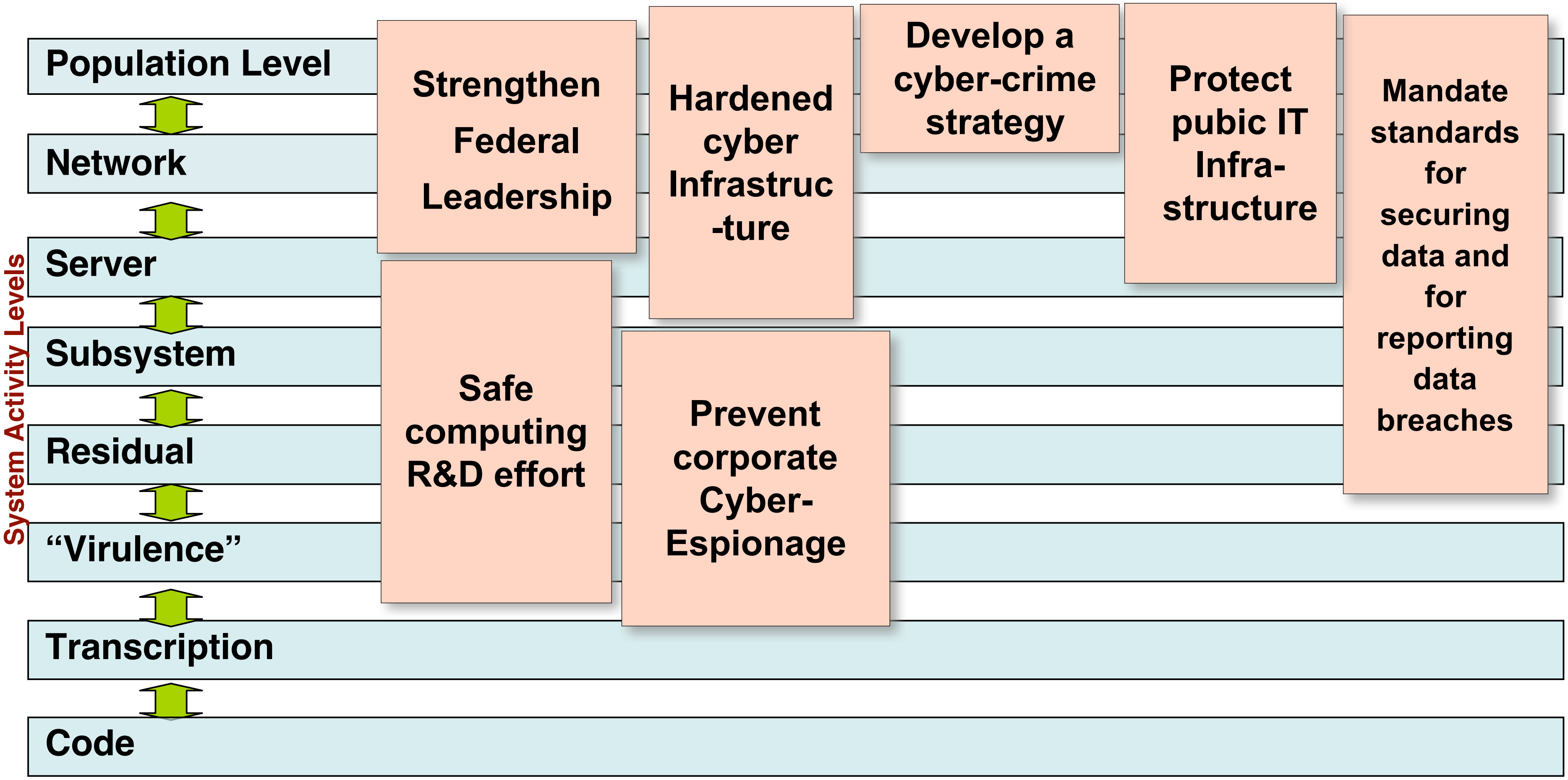


Local ---- System Levels ---- Global

Population Level:	DNS, Global spread/sustained threat, broad consequences
Network:	Routers, Spread, communication, extraction,…
Server/host:	Threat mode & extent, host response,…
Subsystem:	Host range, attack points, com links
Residuals:	"Physical" signatures of presence: files, logs, etc.
"Virulence factors":	Identification of attack/virulence factors of threat
Transcription:	Threat expression in a specific host and environment
Code:	Comparative analysis for code/function prediction

Example using this Landscape to understand Programs:

White House program in cyber security
Policy Initiatives tend to populate the top levels



System Activity Levels

Population Level

Network

Server

Subsystem

Residual

“Virulence”

Transcription

Code

Strengthen Federal Leadership

Hardened cyber Infrastructure

Develop a cyber-crime strategy

Protect pubic IT Infrastructure

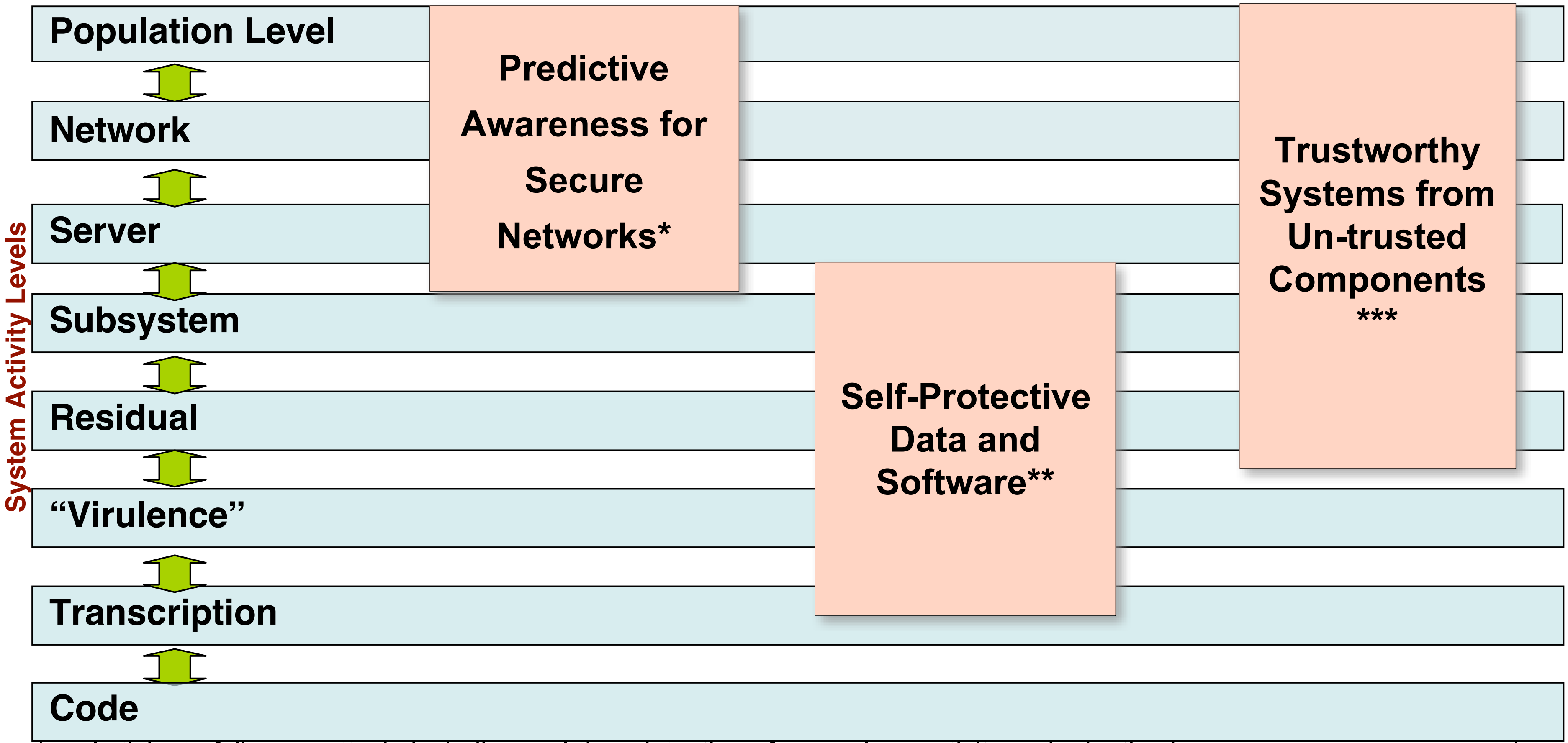
Mandate standards for securing data and for reporting data breaches

Safe computing R&D effort

Prevent corporate Cyber-Espionage

Example using this Landscape to understand Programs:

DOE's Report on Scientific R&D for CyberSecurity Dec 2008



System Activity Levels

Population Level

Network

Server

Subsystem

Residual

"Virulence"

Transcription

Code

Predictive Awareness for Secure Networks*

Self-Protective Data and Software**

Trustworthy Systems from Un-trusted Components ***

* Anticipate failure or attack, including real-time detection of anomalous activity and adaptive immune-system response using data-driven modeling and evaluation of optimal responses,

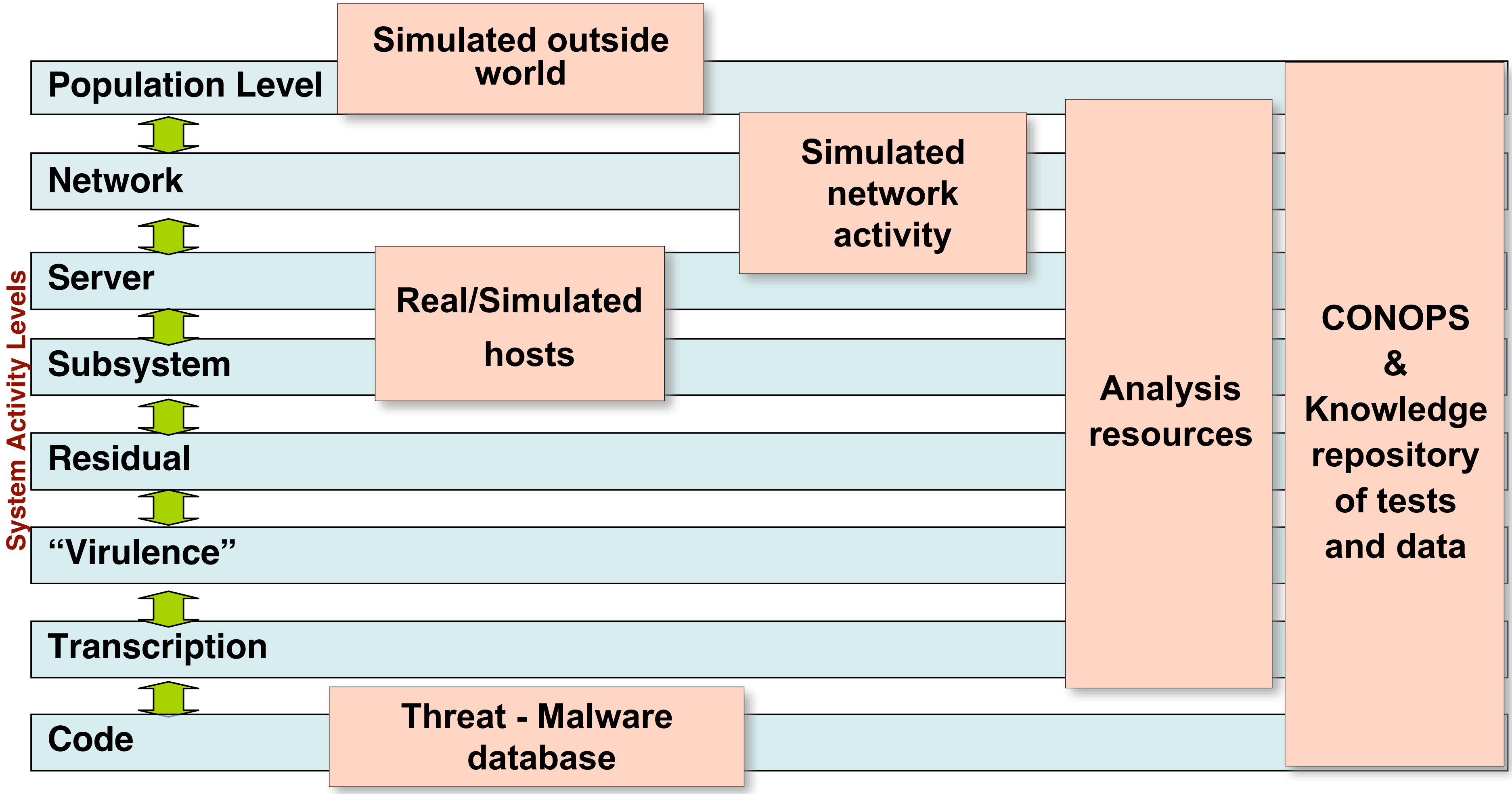
** Enable self-protective, self-advocating, and self-healing digital objects using policy-enabled technologies

*** Techniques for specifying and maintaining overall trust properties for operating environments and platforms using ?

http://www.er.doe.gov/ascr/ProgramDocuments/Docs/CyberSecurityScienceDec2008.pdf

Example using this Landscape to understand Programs:

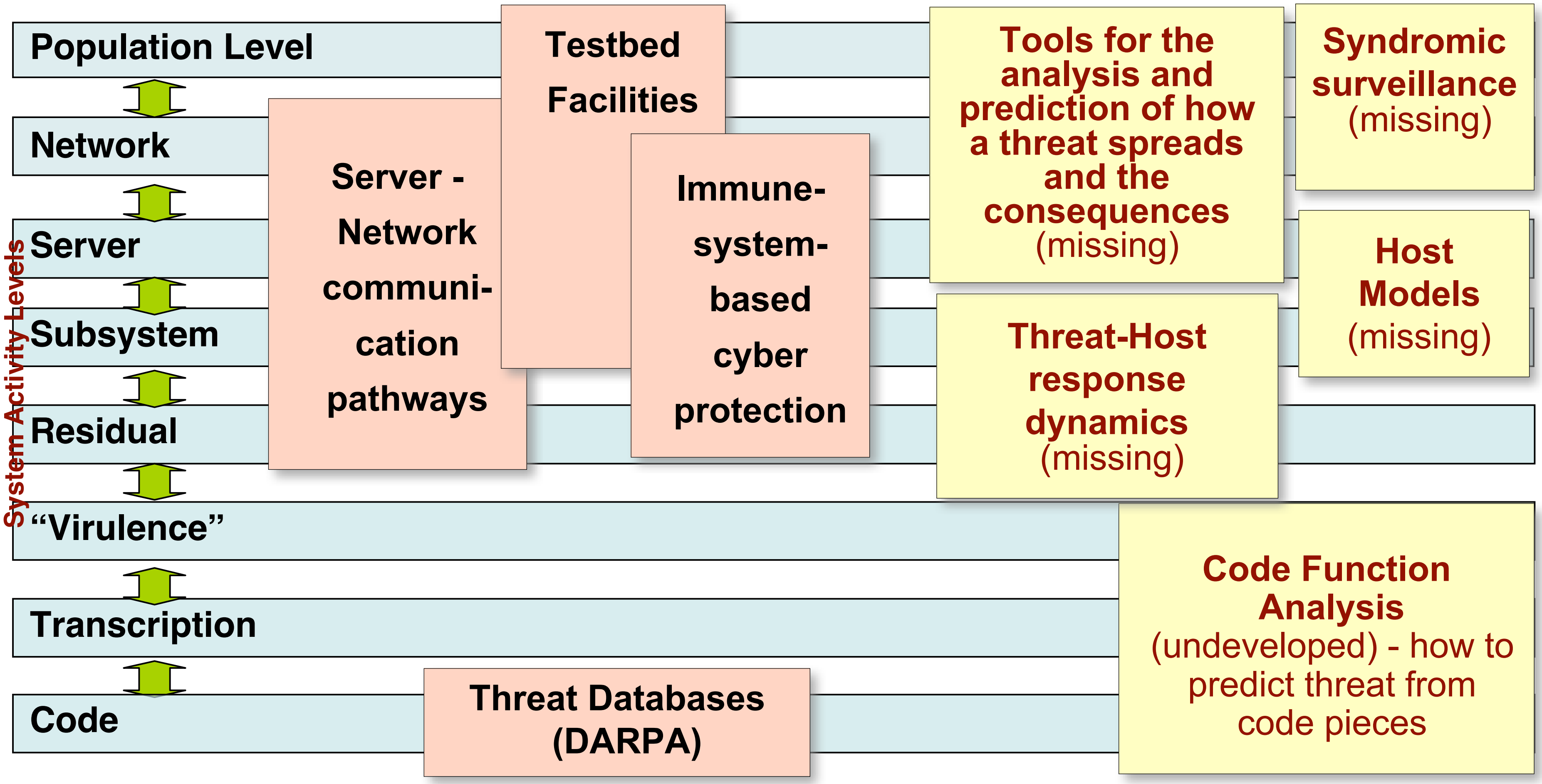
DARPA’s program in *National Cyber Range (NCR) Testbed*



2009 DARAP funding about $30 mil for 8 months for Phase 1 (studies only).

General Guidelines for Cyber Development

Bio-Inspired Resources: Existing and Missing



System Activity Levels
Population Level
Network
Server
Subsystem
Residual
"Virulence"
Transcription
Code
Testbed Facilities
Server - Network communication pathways
Immune-system-based cyber protection
Threat Databases (DARPA)
Tools for the analysis and prediction of how a threat spreads and the consequences (missing)
Syndromic surveillance (missing)
Host Models (missing)
Threat-Host response dynamics (missing)
Code Function Analysis (undeveloped) - how to predict threat from code pieces

Maturing the Cyber domain from bio resources

Similar dynamic challenges require similar solutions

- Inherent chaotic nature of systems require a data-driven approach

Develop programs that extend out from the event

From a Cyber Gap Analysis

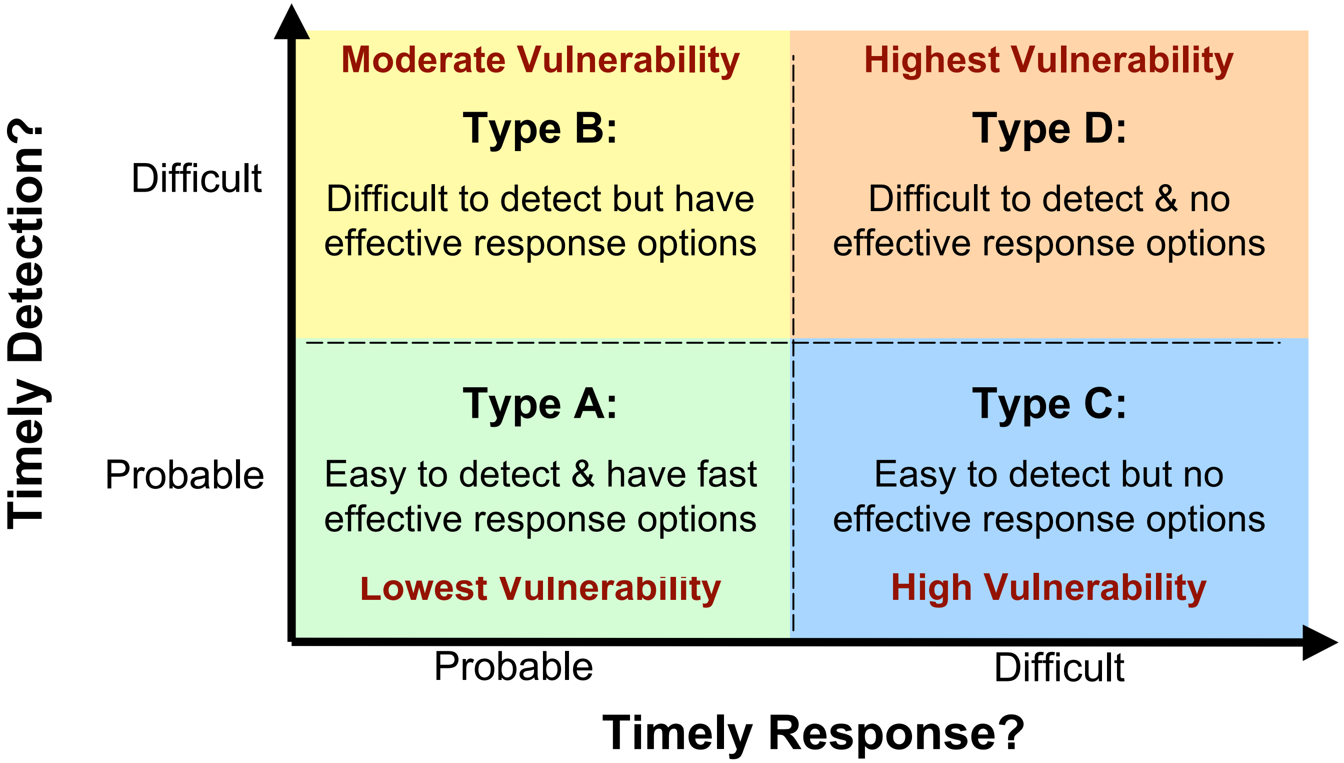
- Threat anticipation
- Surveillance and situational awareness
- Analysis and visualization
- Decision support systems-of-systems resources

Two Specific Examples

- Addressing the complexity of threat categorization
- Graded response to limit "regret" or degrade system performance

Cyber Threat Types Are Complex

This Threat Chart is a way to simplify the complex landscape of threats



Moderate Vulnerability

Type B:

Difficult to detect but have effective response options

Highest Vulnerability

Type D:

Difficult to detect & no effective response options

Type A:

Easy to detect & have fast effective response options

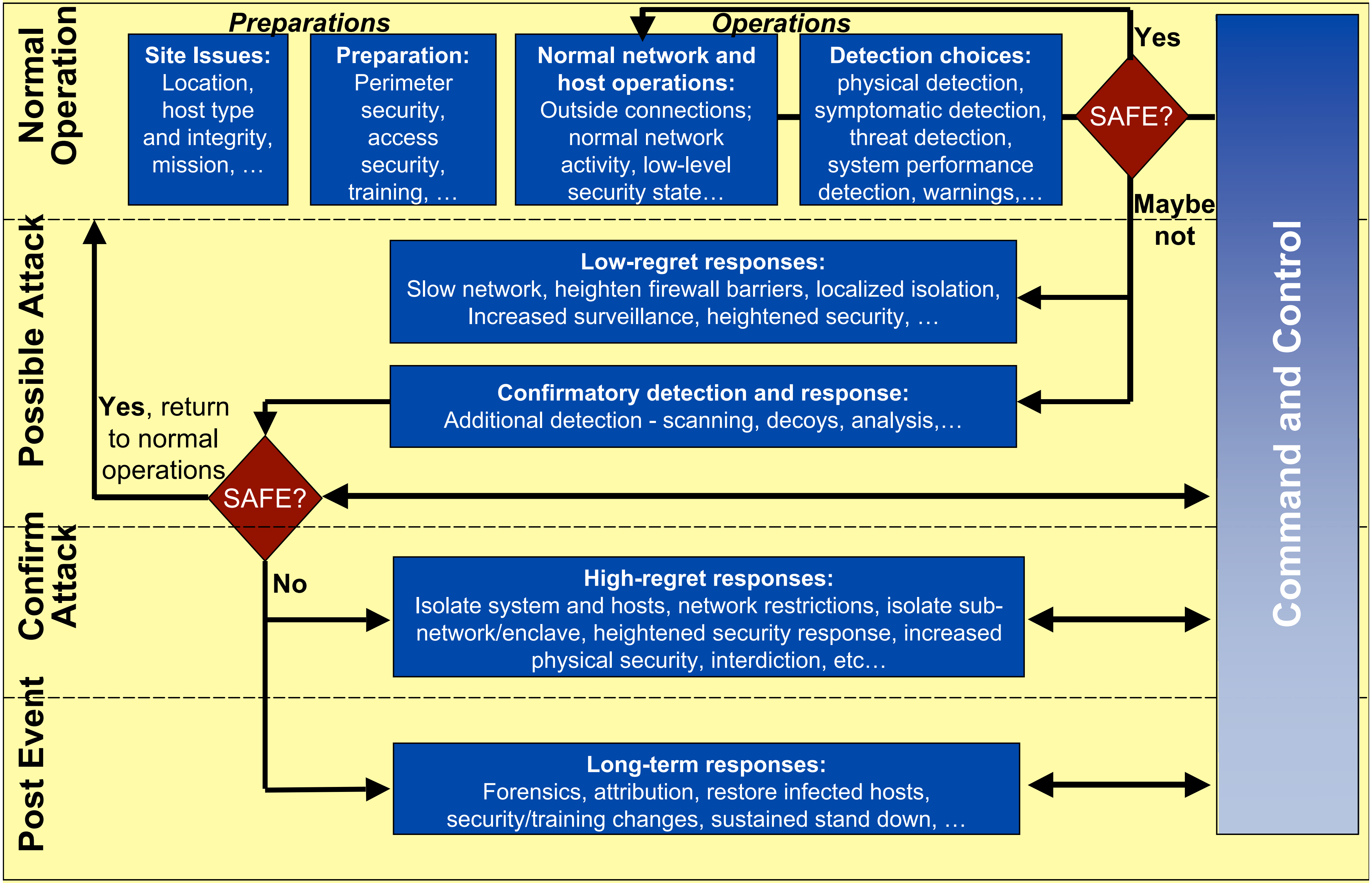
Lowest Vulnerability

Type C:

Easy to detect but no effective response options

High Vulnerability

Graded Cyber Response - Operational View



Normal Operation

Preparations

Site Issues: Location, host type and integrity, mission, …

Preparation: Perimeter security, access security, training, …

Operations

Normal network and host operations: Outside connections; normal network activity, low-level security state…

Detection choices: physical detection, symptomatic detection, threat detection, system performance detection, warnings,…

SAFE?

Yes

Maybe not

Possible Attack

Low-regret responses: Slow network, heighten firewall barriers, localized isolation, Increased surveillance, heightened security, …

Confirmatory detection and response: Additional detection - scanning, decoys, analysis,…

Yes, return to normal operations

SAFE?

No

Confirm Attack

High-regret responses: Isolate system and hosts, network restrictions, isolate sub-network/enclave, heightened security response, increased physical security, interdiction, etc…

Post Event

Long-term responses: Forensics, attribution, restore infected hosts, security/training changes, sustained stand down, …

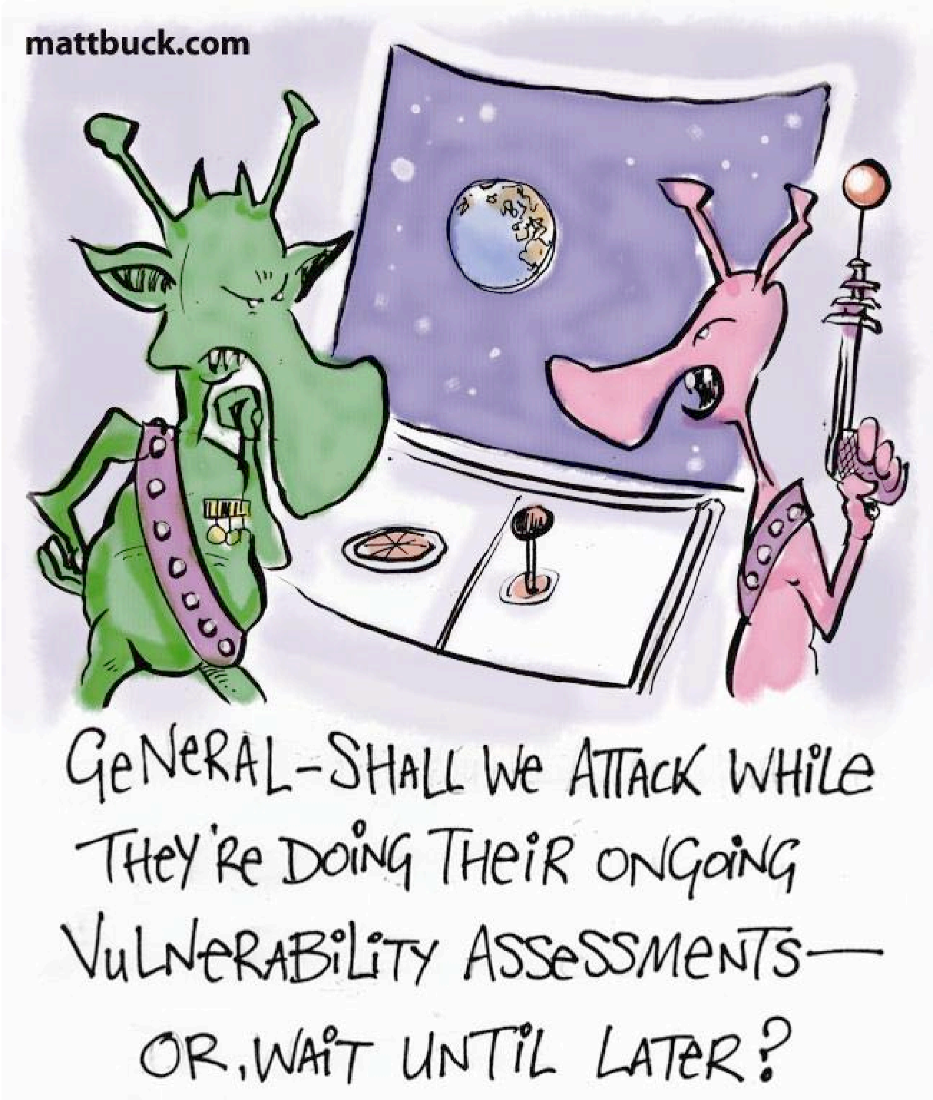
Command and Control

Conclusions: Many systems involved; Graded response is essential due to impacts of responses; Response options vary by stage and severity

Summary of Using Bio to Mature Cyber

- **Current policy and resource development are aligned with immediate needs, but policy lacks over-the-horizon thinking**
- **Use the bio-threat programs as template and justification for the growth of federal programs and international engagement**
- **Use the analysis herein to transfer specific technologies from bio domain**
- **Define research areas from bio-domain lessons**
- **What is a common unmet challenge to both?**
  - Characterization and prediction of the response of users/attacker/defenders accounting for behavioral, social and cultural differences.

Are we planning too much?


mattbuck.com
GENERAL-SHALL WE ATTACK WHILE THEY'RE DOING THEIR ONGOING VULNERABILITY ASSESSMENTS— OR, WAIT UNTIL LATER?

Are we too little - too late?