RSAConference2016

San Francisco | February 29 – March 4 | Moscone Center

Connect to Protect

SESSION ID: MASH-F03

Five InfoSec Lessons from the Great Generals of the Ancient World

Spencer Wolfe

Head Security Research Writer
ZeroFOX
@wolfesp18

Kenneth Geers

Ambassador
NATO Cooperative Cyber Defence Centre of Excellence
@kennethgeers

#RSAC

Introduction

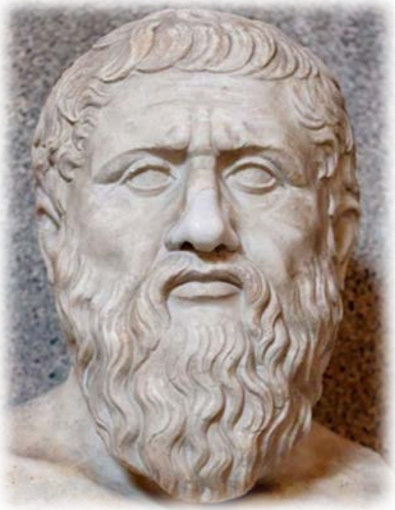
“The bravest among us are surely those who have the clearest vision of what is before them, danger and glory alike, and yet notwithstanding, go out to meet it.”

-Thucydides, *The History of the Peloponnesian War*

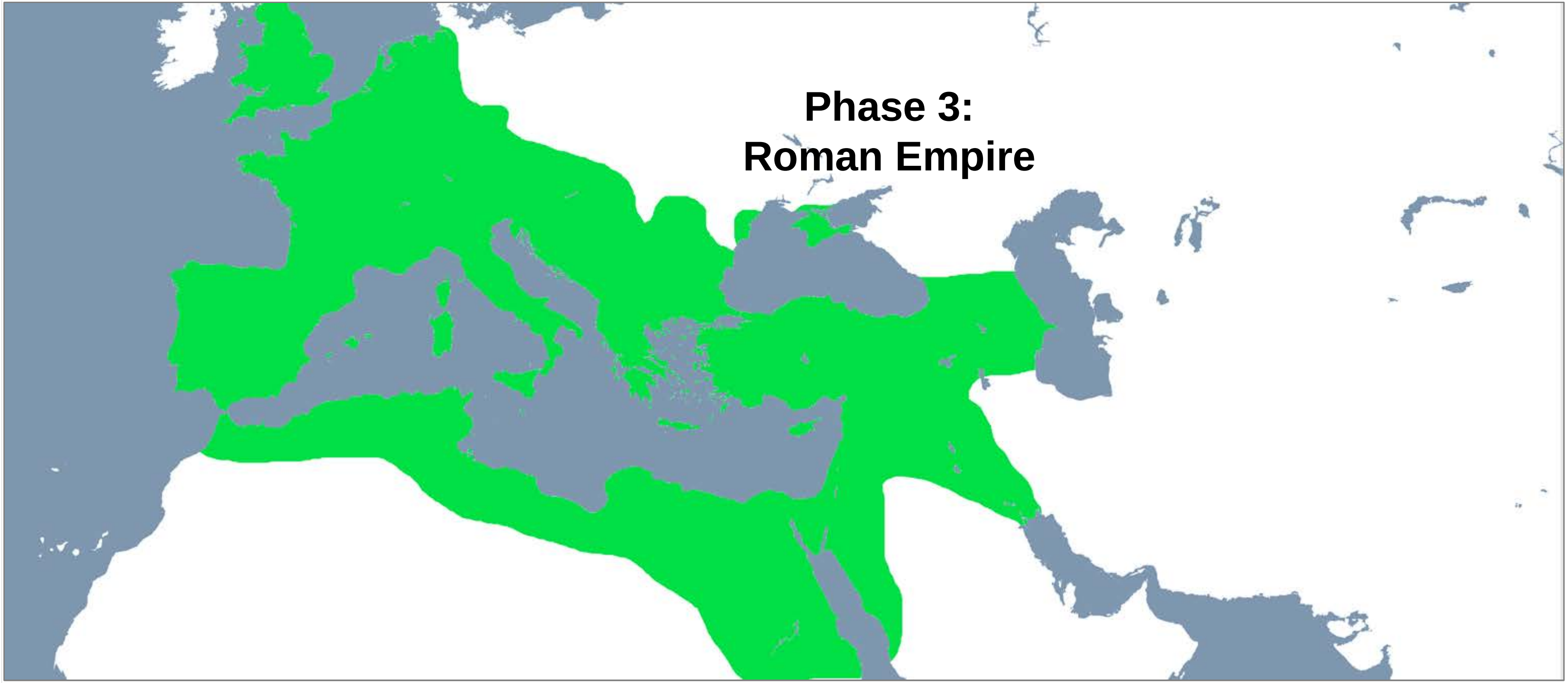
What’s This Talk About, Again?

“Come then and let us pass a leisure hour in storytelling, and our stories shall become the education of our heroes.”

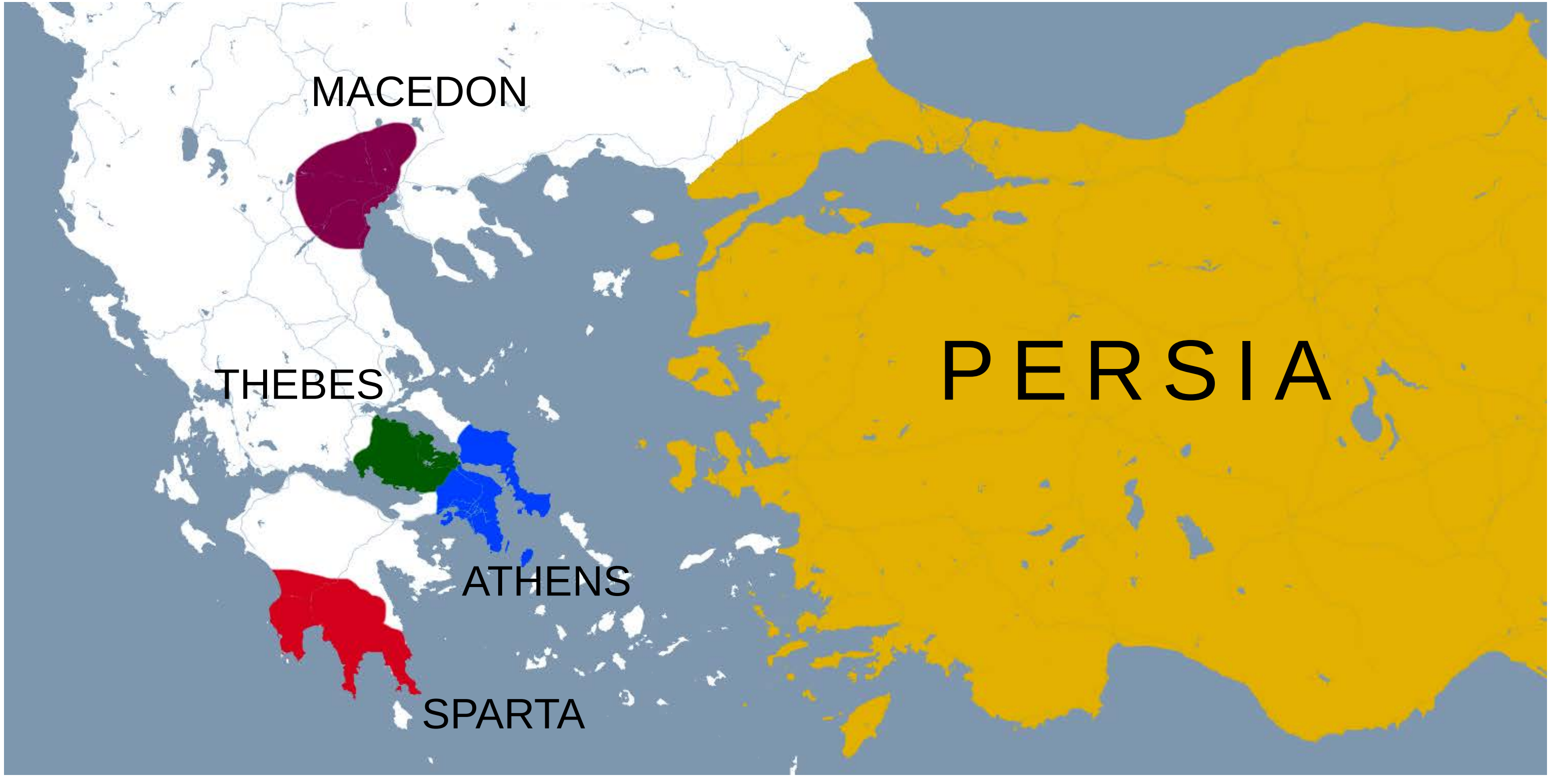
--Plato, *The Republic*



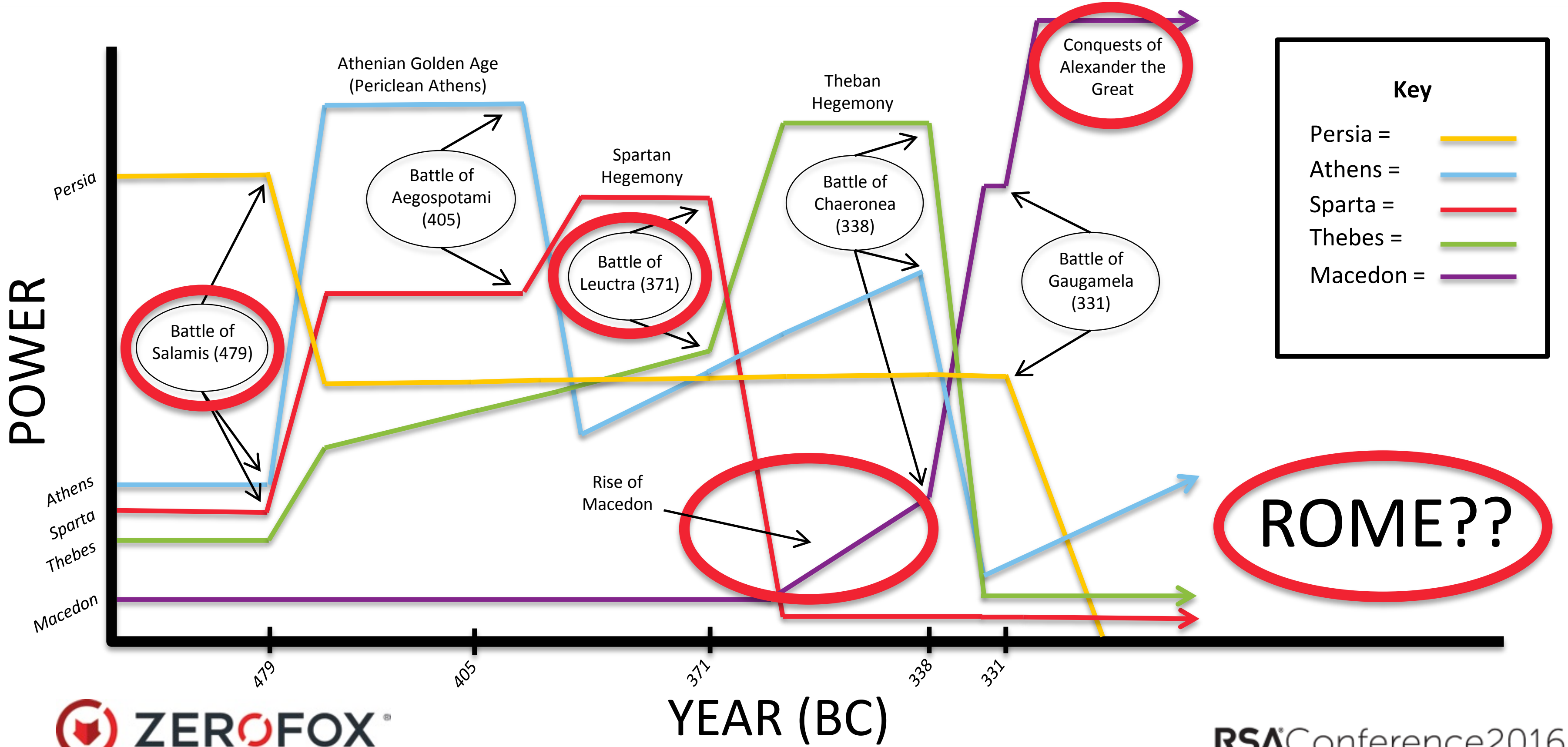
Mappetizer



Close Up: Greece



The History of Greece in a Single Slide



Lesson 1: Choose Your Battlefield

Thermopylae, Salamis and the Greeks Fighting on Their Own Turf

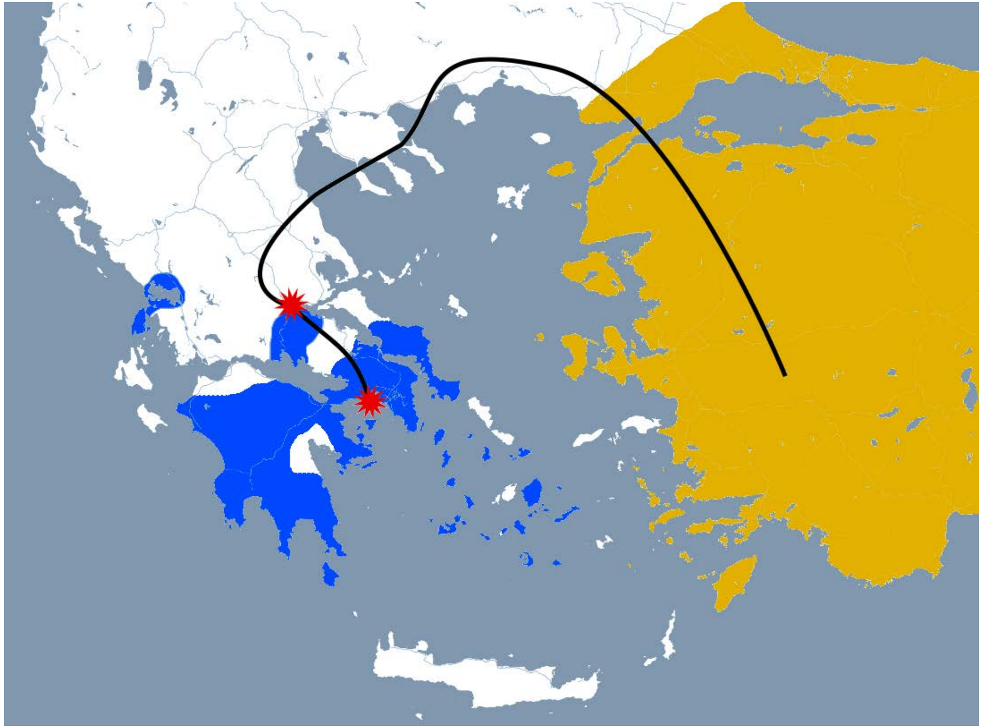
Leonidas & Themistocles

Warner Brothers Pictures, 2006

© c.Everett Collection/REX

Warner Brothers Pictures, 2014

The Greco-Persian Wars: 480-479



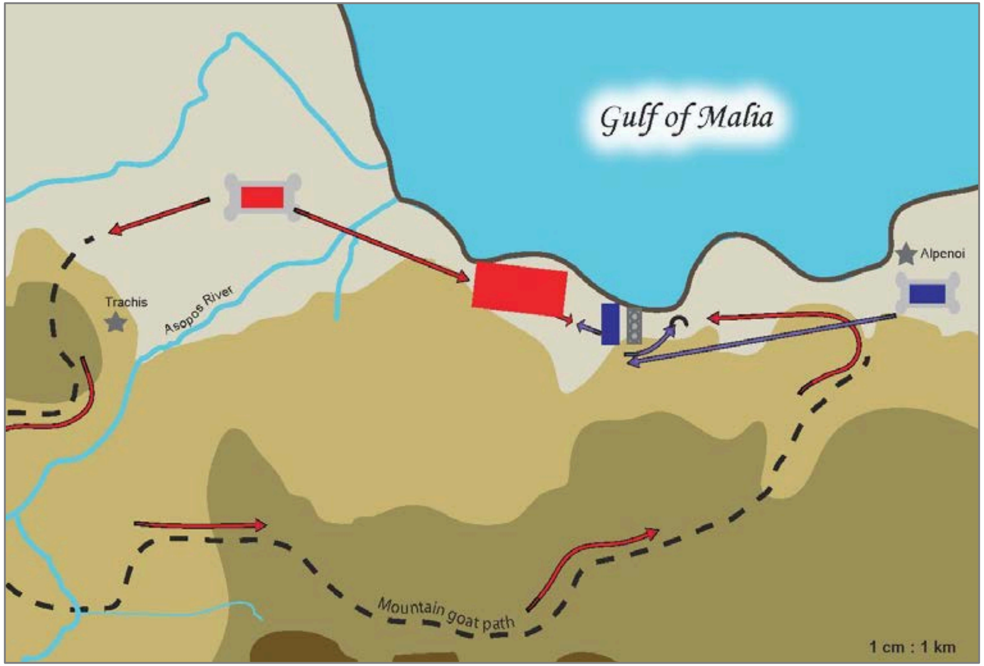
mapbox.com

- Persia, under Xerxes, invades in Greece in 480
- Leonidas & the Spartans defend Thermopylae to the last man
- In 479, the Persian navy is decisively defeated at Salamis by a Greek fleet led by Themistocles
- Xerxes leaves, the rest of his army is destroyed at Plataea

Thermopylae: The Bottleneck

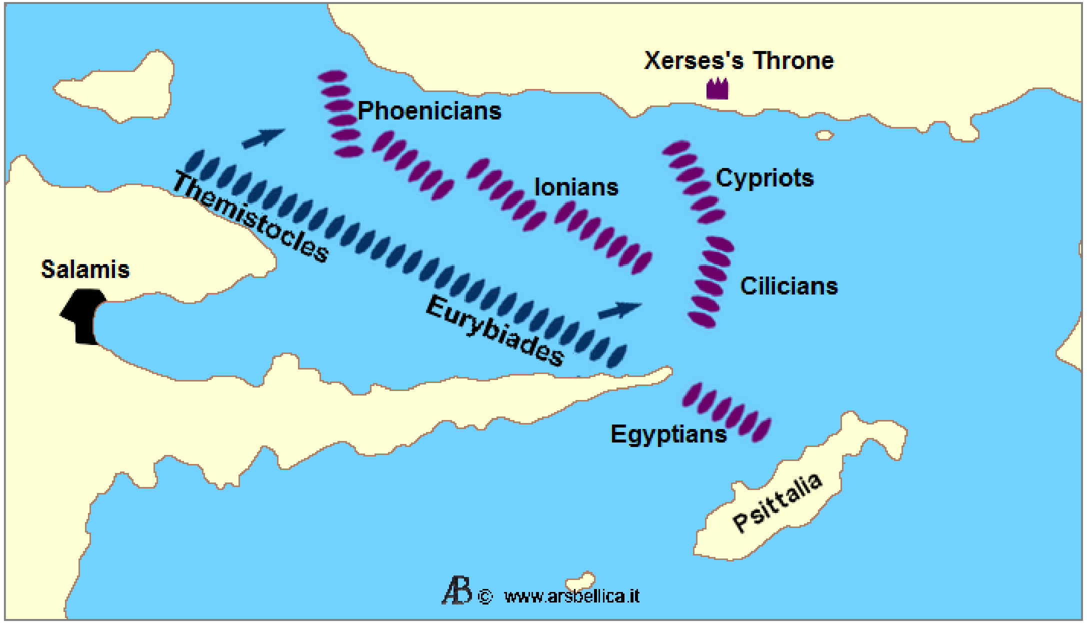
“The Persians were roughly handled by the Spartans, since they used shorter spears than the Greeks and **could not use their numbers fighting in a narrow space.** The Spartans fought memorably, showing themselves skilled fighters amidst unskilled.”

-Herodotus, *Histories* (VII, 211)



Brian Martens – 11/8/2012
livius.org

Salamis: Same Tactic, Different Element

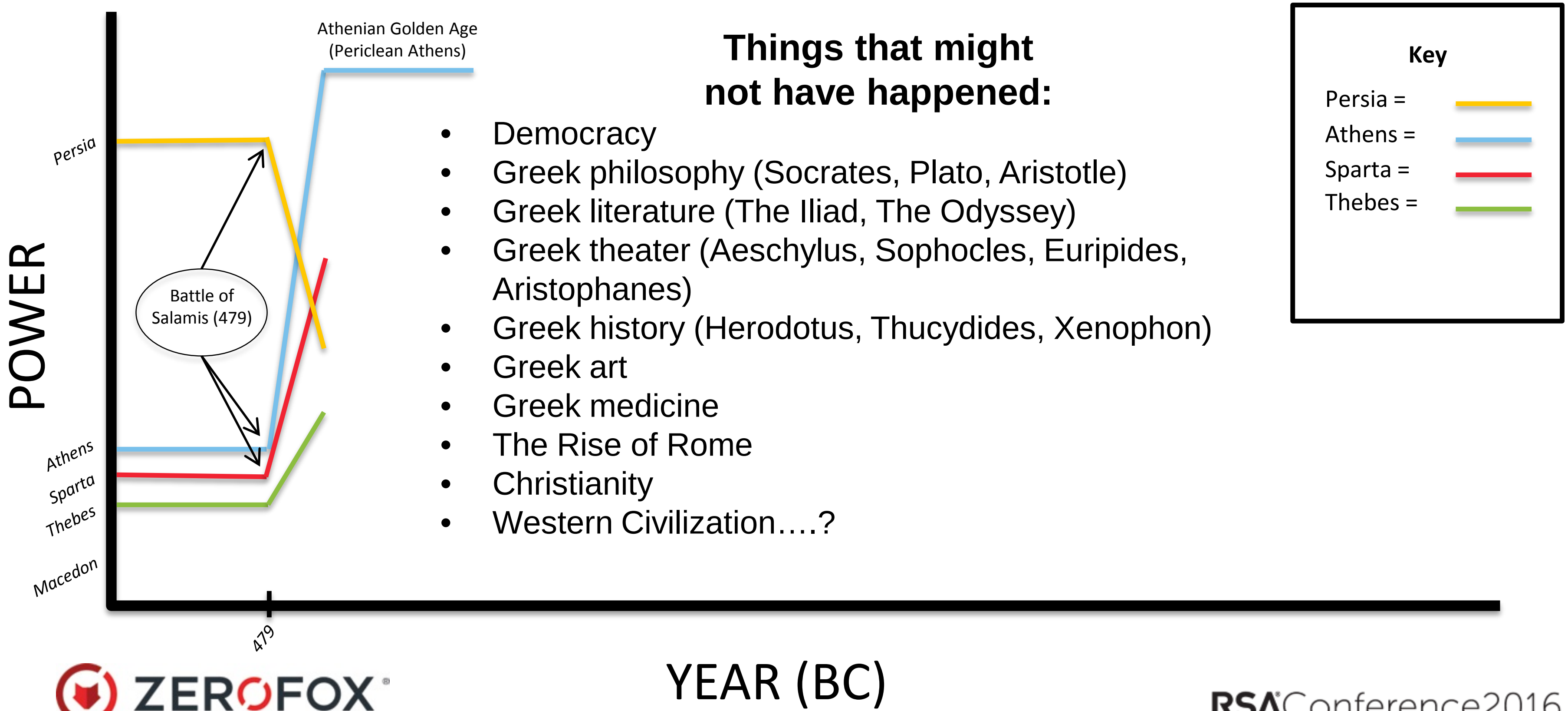


www.arsbellica.it

"By engaging many ships with our few ships in the strait, we shall win a great victory. If the war turns out reasonably, **it is to our advantage to fight in the strait** and to their advantage to fight in the open ocean."

- Themistocles, from: Herodotus, *Histories* (VII, 60)

Who cares? You do.



Things that might not have happened:

- Democracy
- Greek philosophy (Socrates, Plato, Aristotle)
- Greek literature (The Iliad, The Odyssey)
- Greek theater (Aeschylus, Sophocles, Euripides, Aristophanes)
- Greek history (Herodotus, Thucydides, Xenophon)
- Greek art
- Greek medicine
- The Rise of Rome
- Christianity
- Western Civilization….?

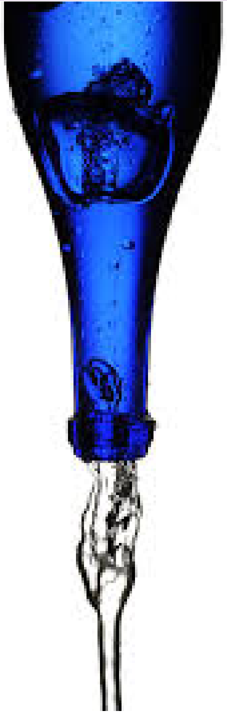
What this means for you

You know your system better than anyone, so…

Where is your Thermopylae?

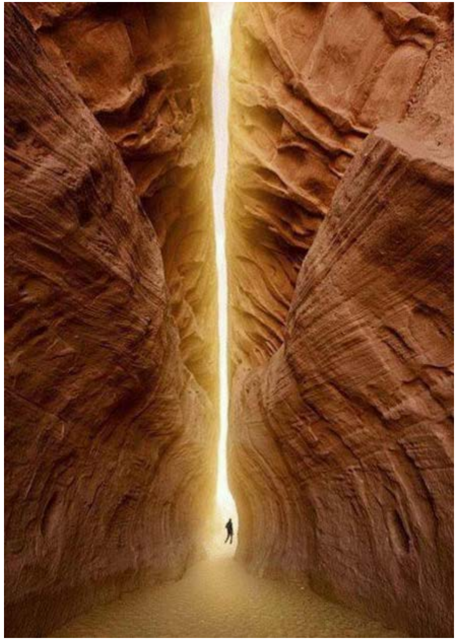
Where is your Salamis?

Where do you choose to fight?



Lesson #1: Choose your battlefield

- Cyber terrain
  - USG: decrease # of nets, homogenize
  - Risk: all eggs in one basket
- Utopia vs. Big Brother
  - Elections and surveillance
  - Belarus, China, Russia, Zimbabwe
- Creativity on cyber defense
  - Code Red worm vs. MS IIS web server (2001)
  - Bot army: 359,000 infected servers
  - DoS Target: White House website
  - Techies “blackholed” the attack



Lesson #1: Choose your battlefield

- Strategy before tactics
  - Crown jewels
- Traffic analysis
  - Alice, Bob, Charlie
- Old paradigm
  - Defined perimeter
- New paradigm
  - Undefined perimeter, social media
- Compartmentalization
  - Assume insider / penetration

Lesson 2: Be Original

Epaminondas Beats the “Unbeatable” Spartans

Greece divided (again)

Greece after 479

- 479-431: Athenian Golden Age
- 431-405: Peloponnesian War, fought between Athens and Sparta
  - Sparta defeats Athens
- 405-371: Spartan Hegemony
- 371: Thebes defeats Sparta at the Battle of Leuctra

The Greek Phalanx

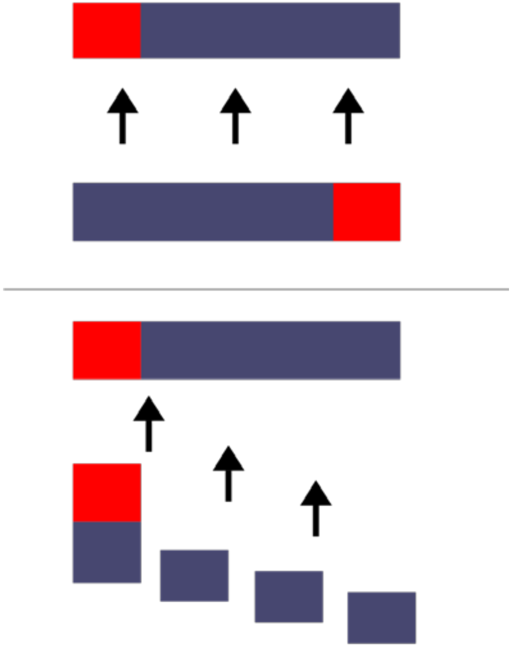
- Rounds shields called *hoplons*
- Overhand spear
- Short sword called a *xiphos*
- Shields overlap one another, forming a solid block
- Opposing forces clash and try to push one another off the field
- 8-12 men deep

Ancientgreekbattles.net

Oblique Formation: Leuctra, 371BC

“The Spartans led each half-company three files abreast, and this resulted in the phalanx being not more than twelve men deep. **The Thebans, however, were massed not less than fifty shields deep**, calling that if they conquered that part of the army around the king, all the rest of it would be easy to overcome.”

- Xenophon, *Hellenica*



Wikimedia commons

What this means for you

Pitched battles and cybersecurity are games of wit.

Originality is your ace in the hole.

Lesson #2: Be original

- ZeroDay philosophy
  - Element of surprise
- Home field advantage
  - Unique defense
- SEC vs. Pac-12
  - Best players on defense
- *Art of War* chapter 13
  - Collect evidence
- The “Moscow Rules”
  - Muhammed Ali

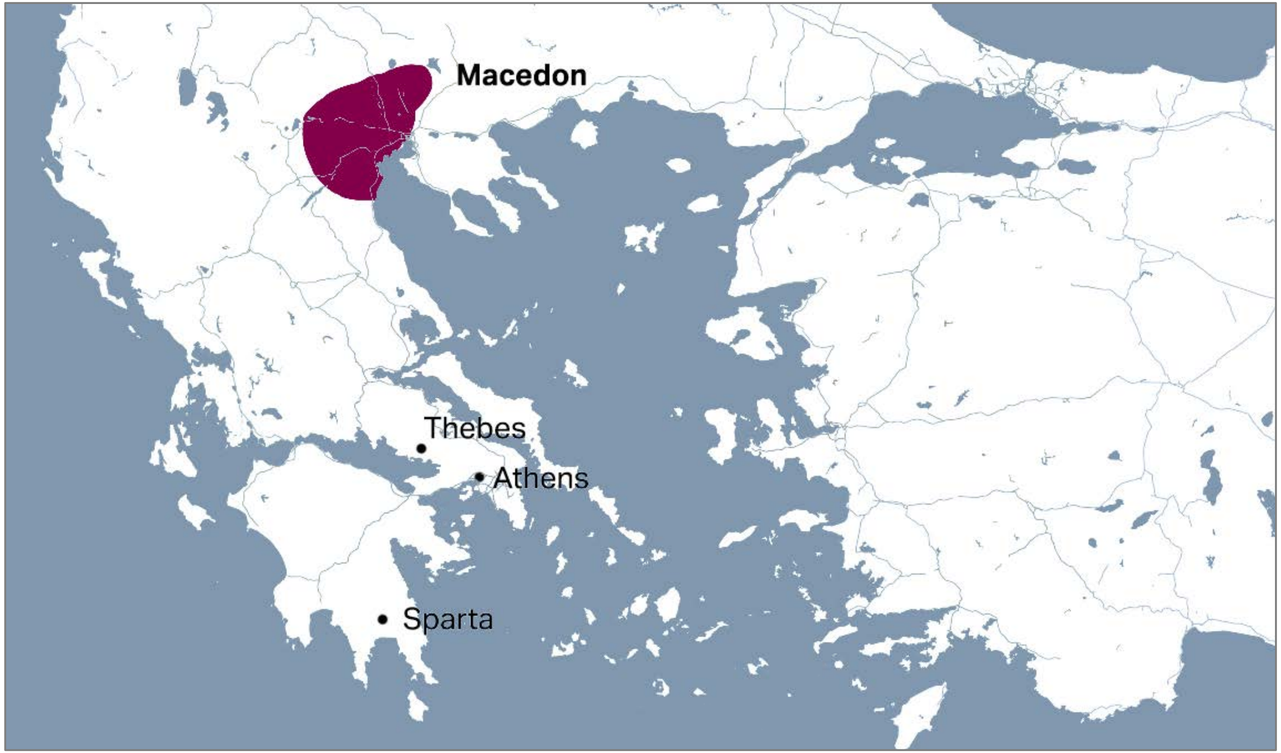
Lesson #2: Be original

- What is malware?
  - Characteristics, signatures, behavior
  - Known vs. novel
- Analysis
  - AV, sandboxing, white/blacklisting
  - OK to reject safe programs
- Limitations
  - Complexity, obfuscation, time
  - Simplistic: malicious / non-malicious
- Education
  - Awareness, policy, enforcement

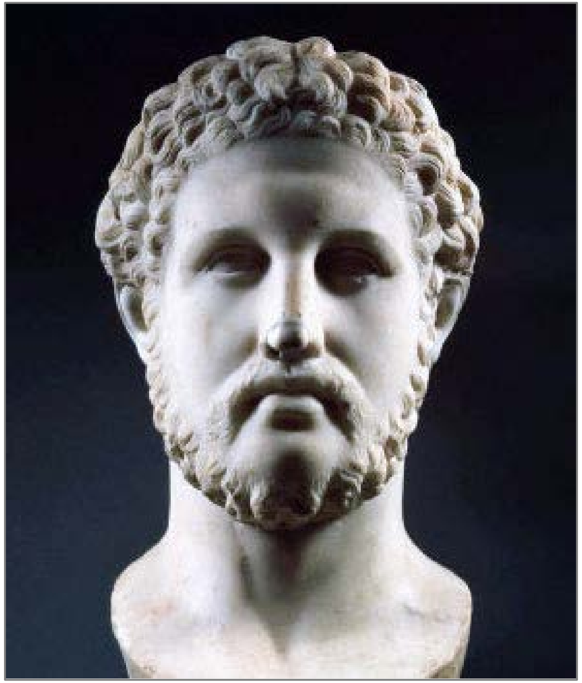
Lesson 3: Know Thy Enemy

The Brilliant Statesmanship of Phillip II

Humble Beginnings, 359BC



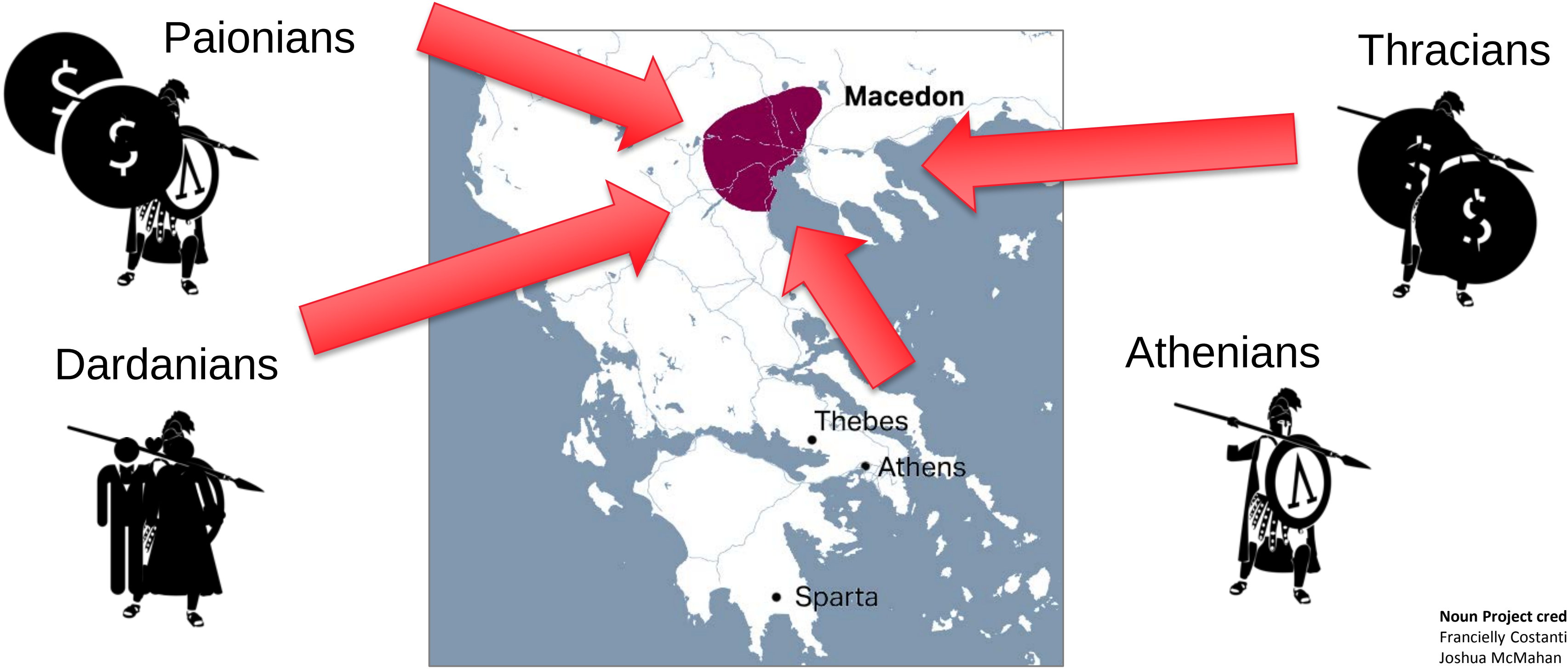
Philip of Macedon



Historyofmacedonia.org

Warner Brothers Pictures, 2004

Quadruple Threat



Paionians

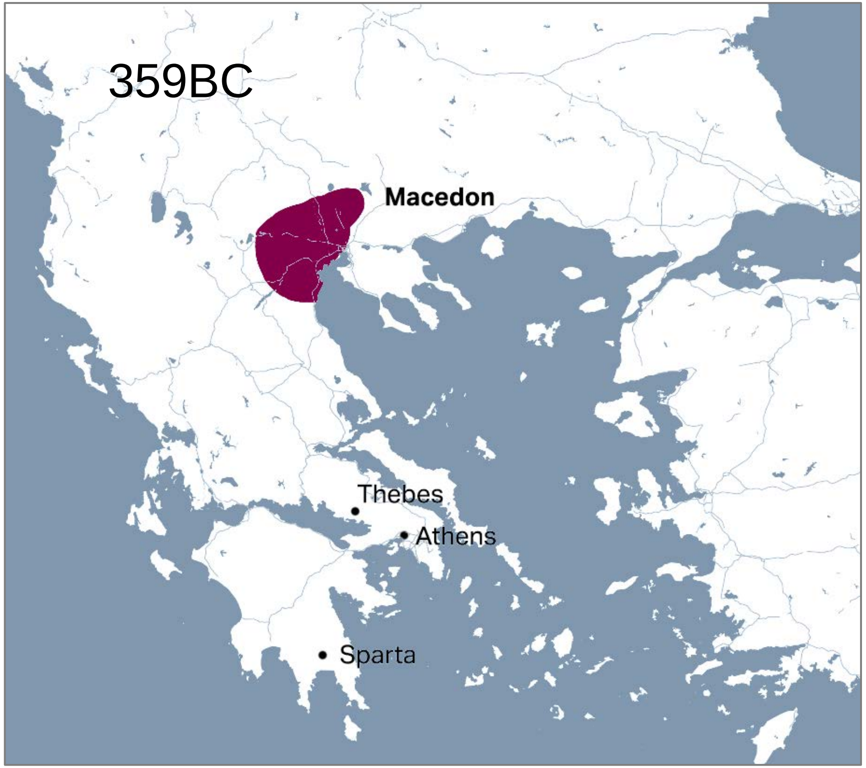
Thracians

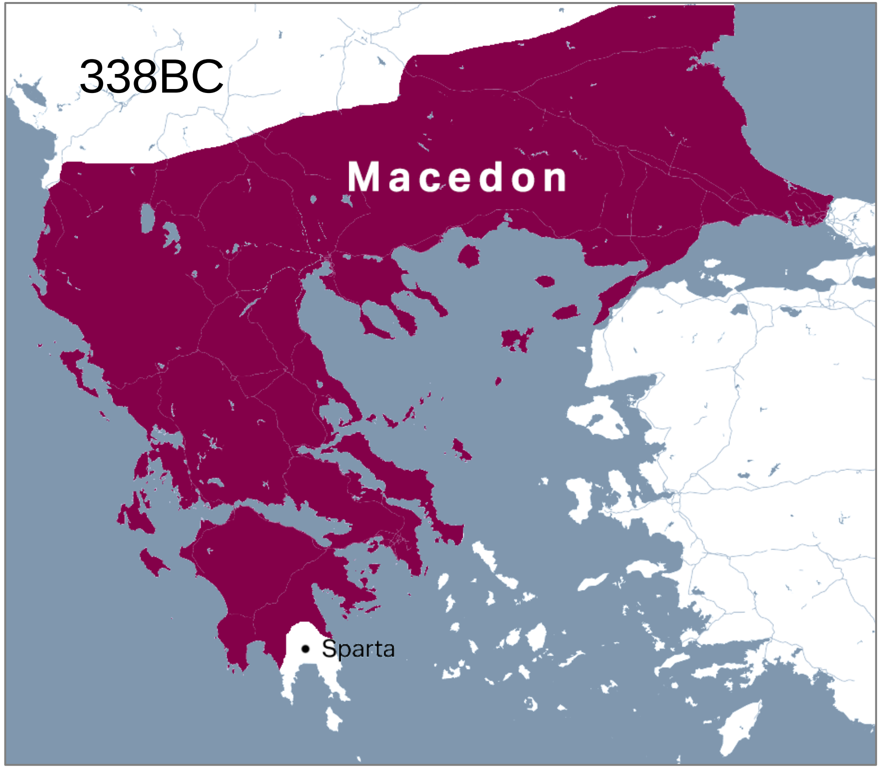
Dardanians

Athenians

Noun Project credits:
Francielly Costantin Senra
Joshua McMahan
Creative Stall
Divya Kulshreshtha

Macedon from 359-338 BC





Lesson: know thy enemy

"If you know your enemies and yourself, you will not be imperiled in a hundred battles ... if you neither know your enemies nor yourself, you will be imperiled in every single battle."

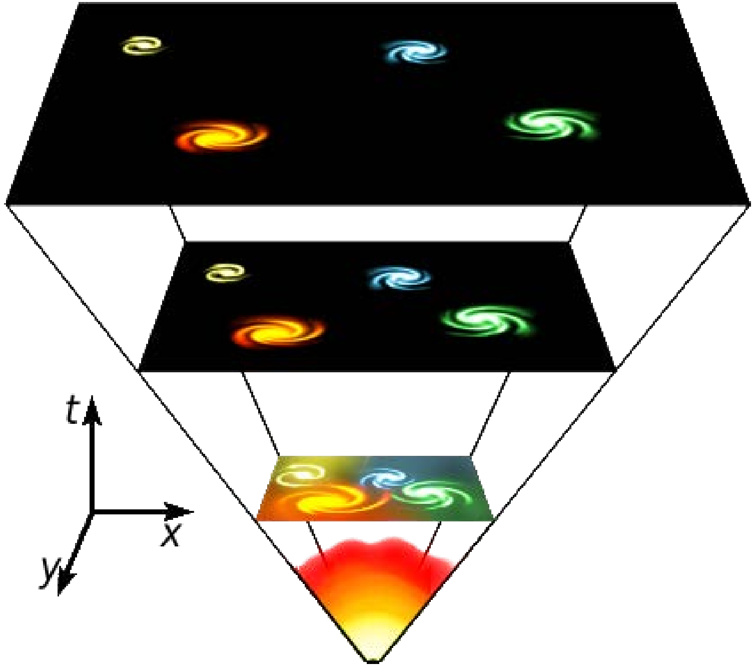
- Sun Tzu, *The Art of War*

Lesson #3: Know Thy Enemy

- 1980s: Cuckoo's Egg
- 1990s: Moonlight Maze
- 1990s: Chechnya
- 1999: Kosovo
- 2007: Estonia
- 2008: Georgia
- 2009: Kyrgyzstan
- 2010: Microsoft
- 2011: Azerbaijan
- 2012: Red October
- 2013: Lithuania
- 2014: Ukraine
- 2015: Turkey

Lesson #3: Know Thy Enemy

- Analysis
  - Data -> information -> intelligence
- Geopolitical insight
  - Technical + non-technical
- Modelling
  - Physics, analogies, napkins
- The “attribution” problem
  - APT vs. APT
- Logic
  - Think horses, then zebras



Lesson 4: Lead from the Front

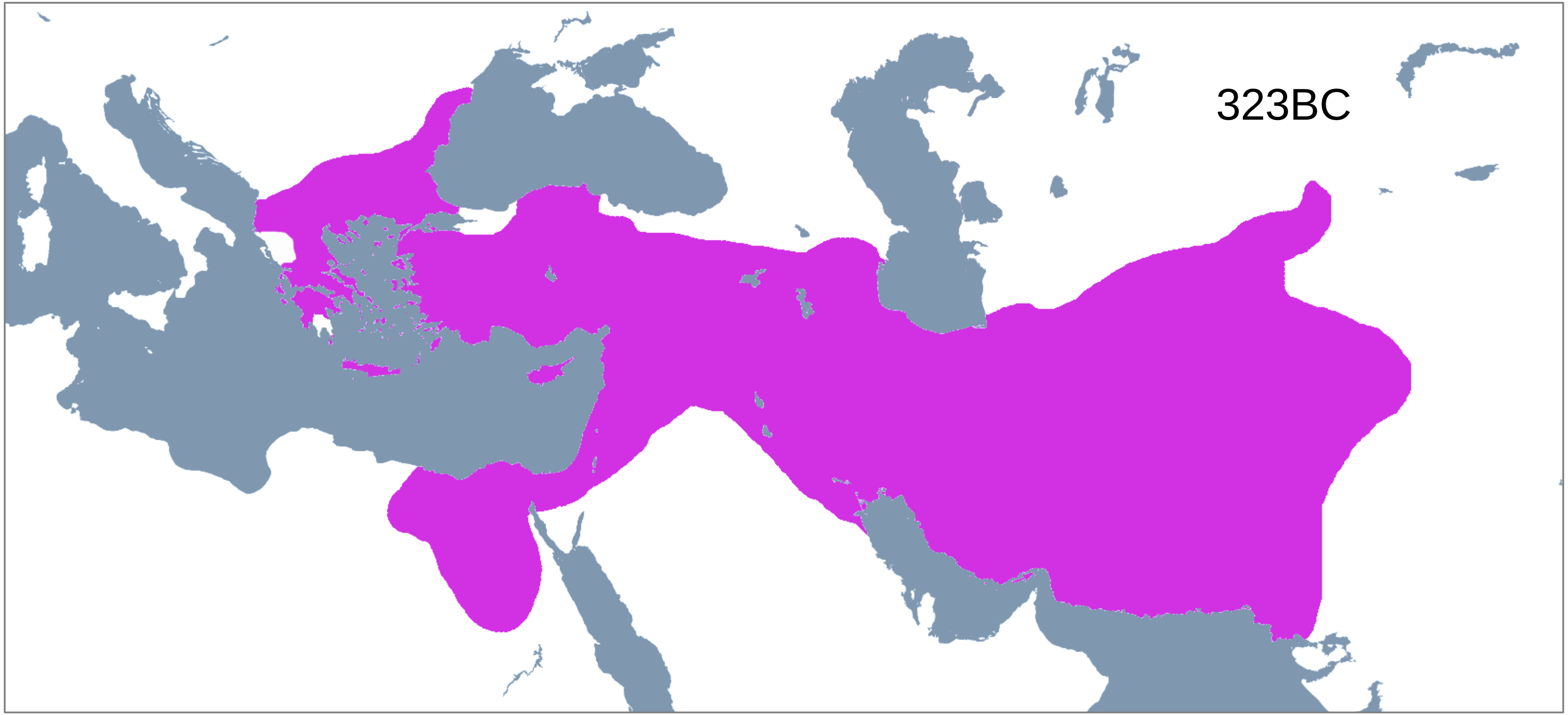
The Conquests of Alexander the Great

Alexander the Great

Artcreationforver.com

Warner Brothers Pictures, 2004

The Conquests of Alexander



Follow the Leader

- 334: Alexander crosses into Asia
- 334-332: Wins a streak of major victories
- Founds Alexandria in Egypt
- 331: Defeats Darius, king of the Persians at the Battle of Gaugamela
- Enters Babylon
- Travels as far east as the Hindu Kush and the Indus River
- 326: Troops beg Alexander to turn back
- Returns to Babylon via the Persian Gulf
- 323: Dies at age 32

Pbase.com

Follow the Leader

Wikipedia commons

Lesson #4: Lead from the Front

- Alexander the GEEK
  - DIRNSA / CYBERCOM 2005-2014
- Education
  - 4 Masters: EW, physics, strategy, business
  - USMA ‘74: Petraeus (CIA), Dempsey (JCS)
- Dominant personality
  - Like Hoover
- 10th Fleet, 24th Air Force, 2nd Army
  - 40,000+ geek soldiers
- SIGINT today
  - Proactive deterrence
- Massive mission expansion
  - Cyber “fire support”

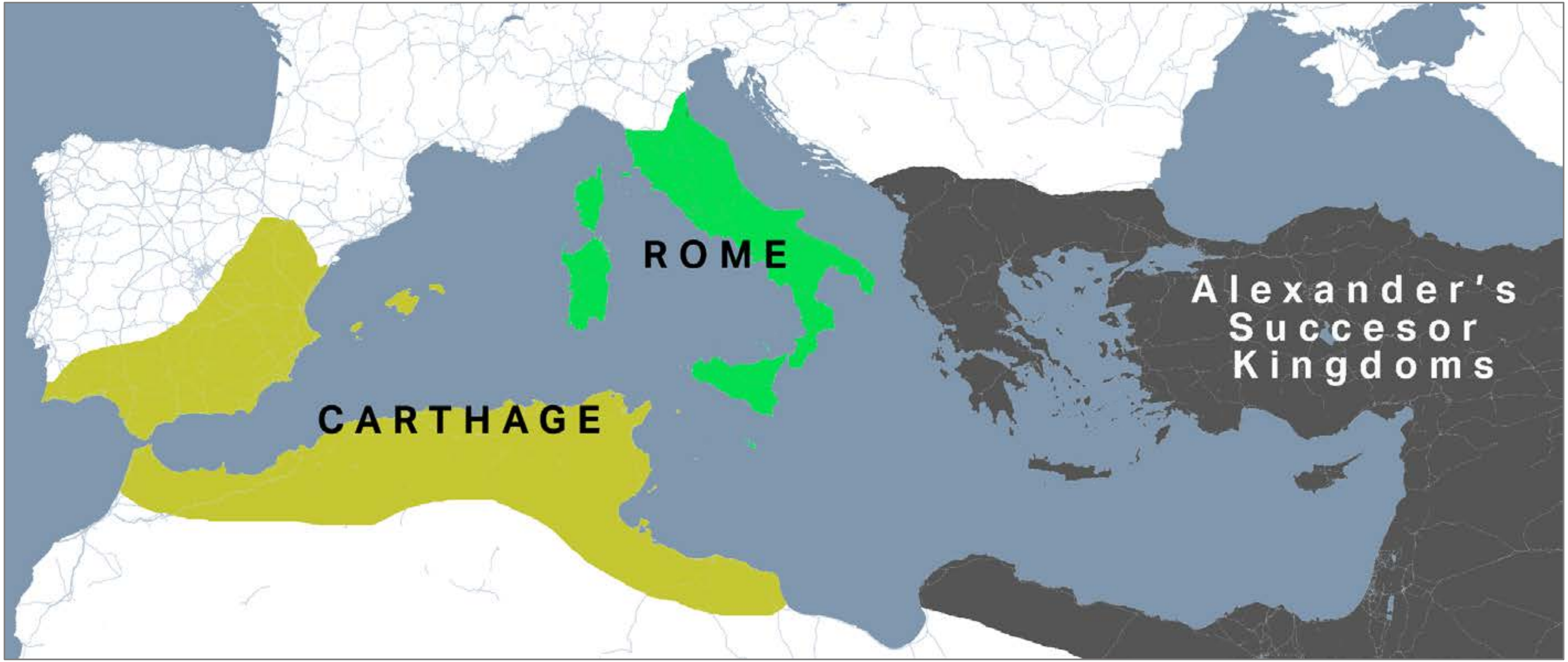
Lesson #4: Lead from the Front

- Cyber weapons
  - Nukes of 21st century?
  - Rated ahead of terrorism
- NSA / CYBERCOM
  - Line blurring between traditional, digital
  - Defend private sector?
- Alexander controversy
  - Collection on US citizens
  - US Congressman: “mockery of oversight”
  - Militant on secrecy, leaks
- Iran counterattack post-Stuxnet
  - Saudi Aramco, RasGas, Wall Street
  - DHS: US energy should be on alert

Lesson 5: Fight Fire With Fire

Rome Reverse Engineers Carthage’s Tactics

Fast forward 100 years



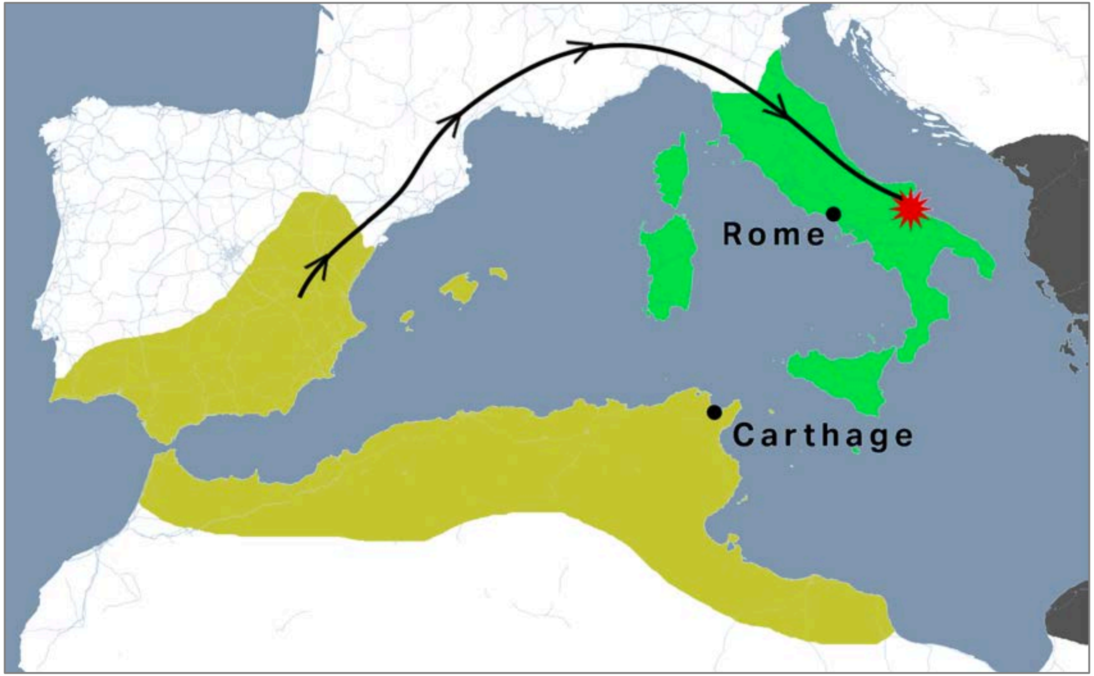
Hannibal Barca

Ancienthistorylist.com

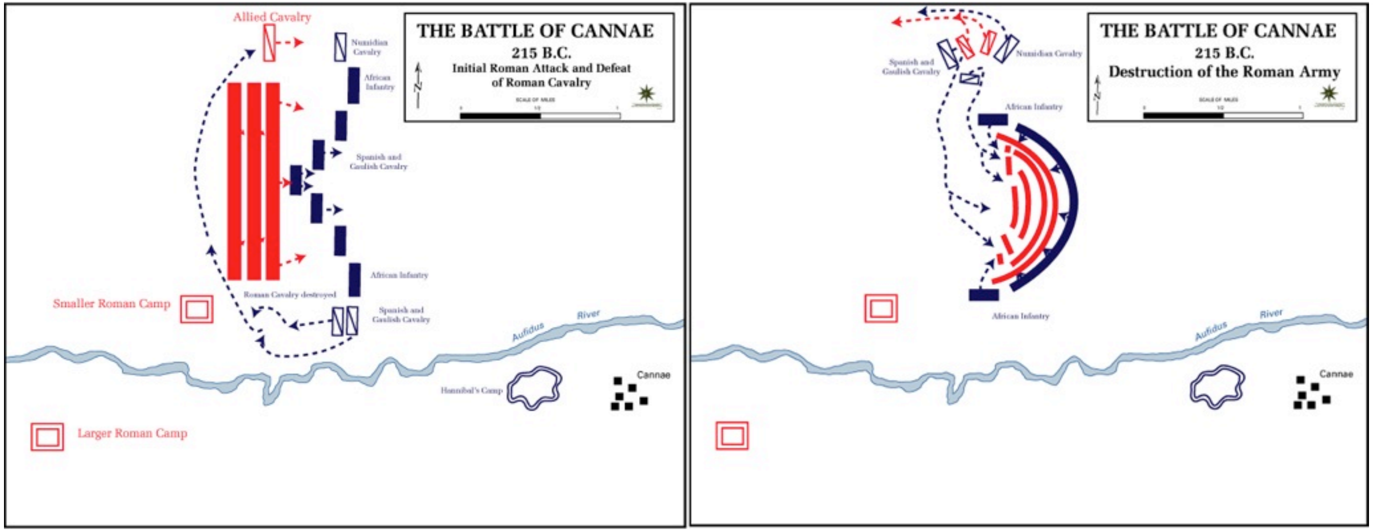
Act I: Elephants don’t belong in snow

The Punic Wars

- Carthage enters Spain, Rome declares war under false pretenses
- 218: Hannibal takes his army, with elephants, over the Alps & invades Italy
- 216: Rome and Carthage fight the Battle of Cannae



The Battle of Cannae, 218BC



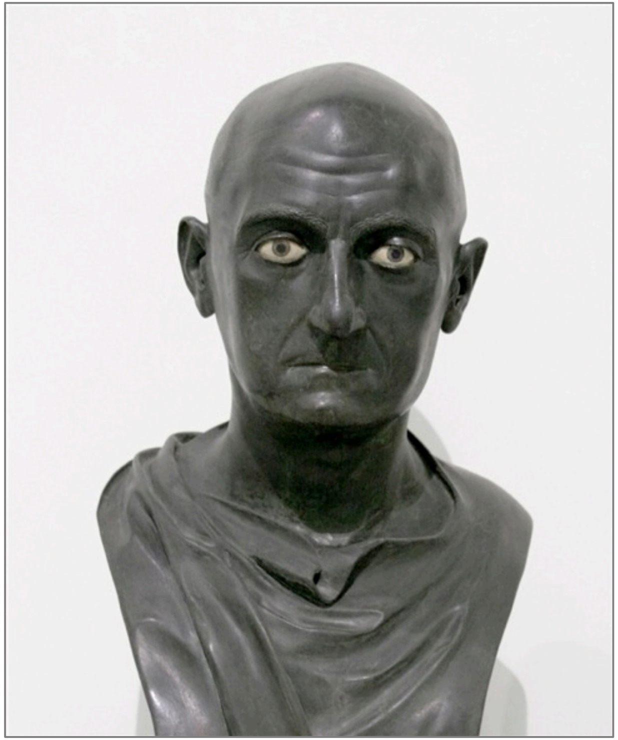
dcc.dickinson.edu

“As the outer ranks fell, and the rest were gradually huddled in and surrounded, they were all killed where they stood. While this murderous combat was going on, the Carthaginians killed most of the cavalry and unseated others. **Some 70,000 died bravely**.”

- Polybius, *The Histories*

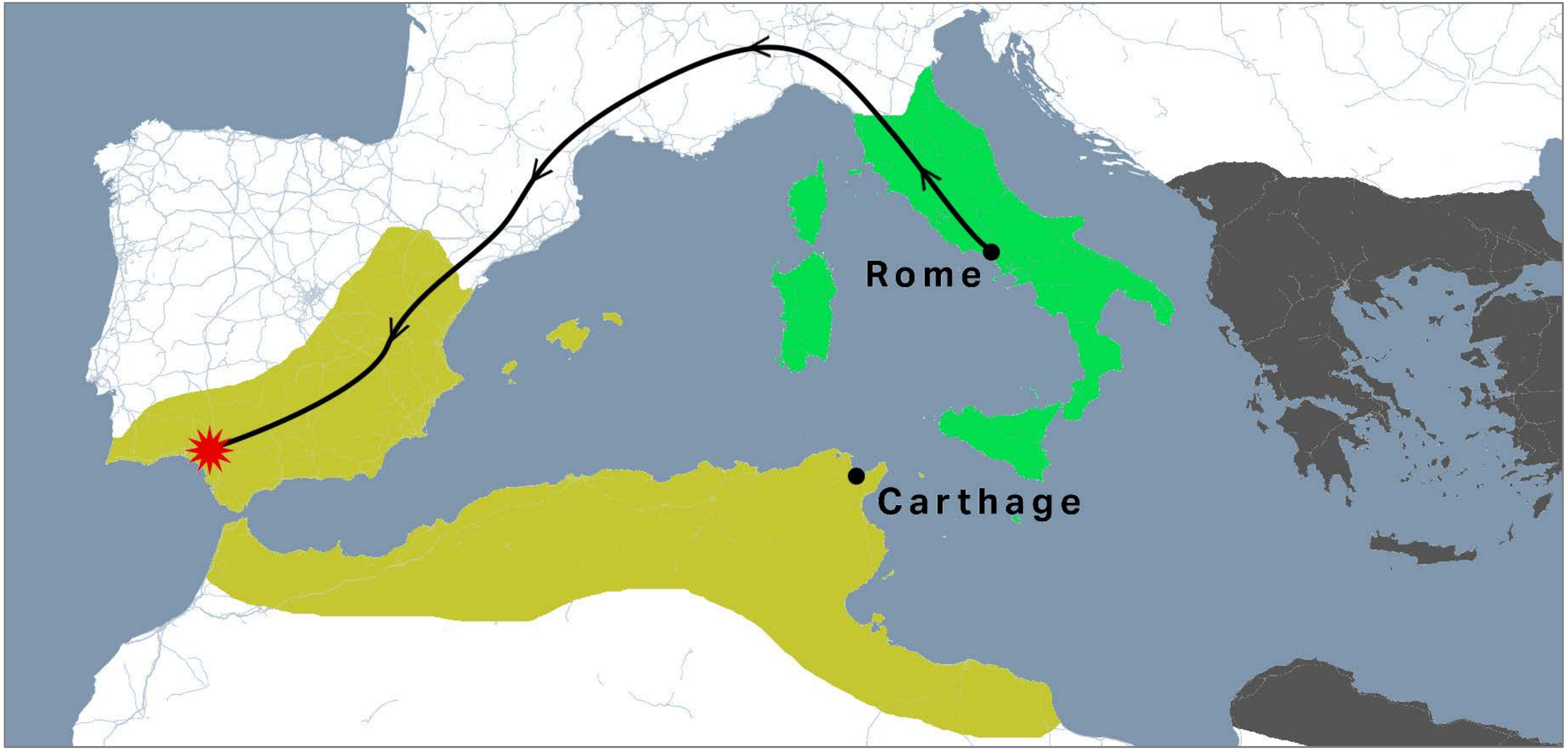
Scipio Africanus

Leopard.booklikes.com

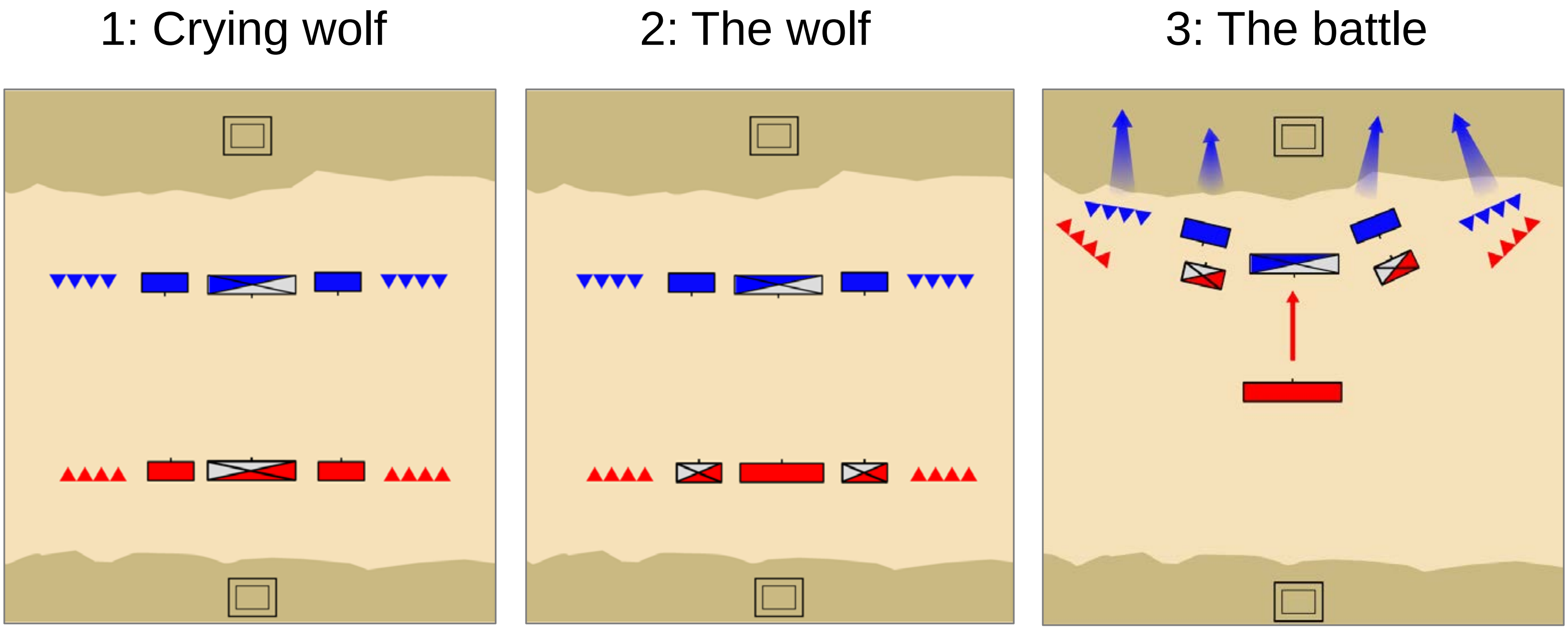


Peoplecheck.de

Act II: Return of the Romans



The Battle of Ilipa, 206BC



1: Crying wolf

2: The wolf

3: The battle

Wikipedia commons

What this means for you

Don’t just know thy enemy.

Act like them.

KEEP

CALM

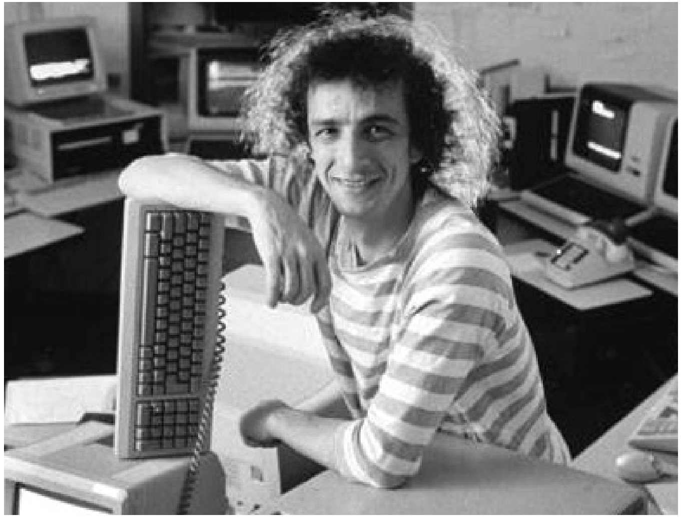
AND

FIGHT FIRE

WITH FIRE

Lesson #5: Think like a hacker

- Cliff Stoll, SysAdmin vs. KGB (1986)
  - Astronomer, inventor, physics teacher
  - Followed $0.75 around the world
- Stoll gaffes
  - Doubted e-commerce, e-media
- Pioneer in digital forensics
  - Honeypot: “SDInet”
  - Teleprinter recorded everything
  - GNU Emacs vuln gave root access
- Capture of hacker Markus Hess
  - Breached US military



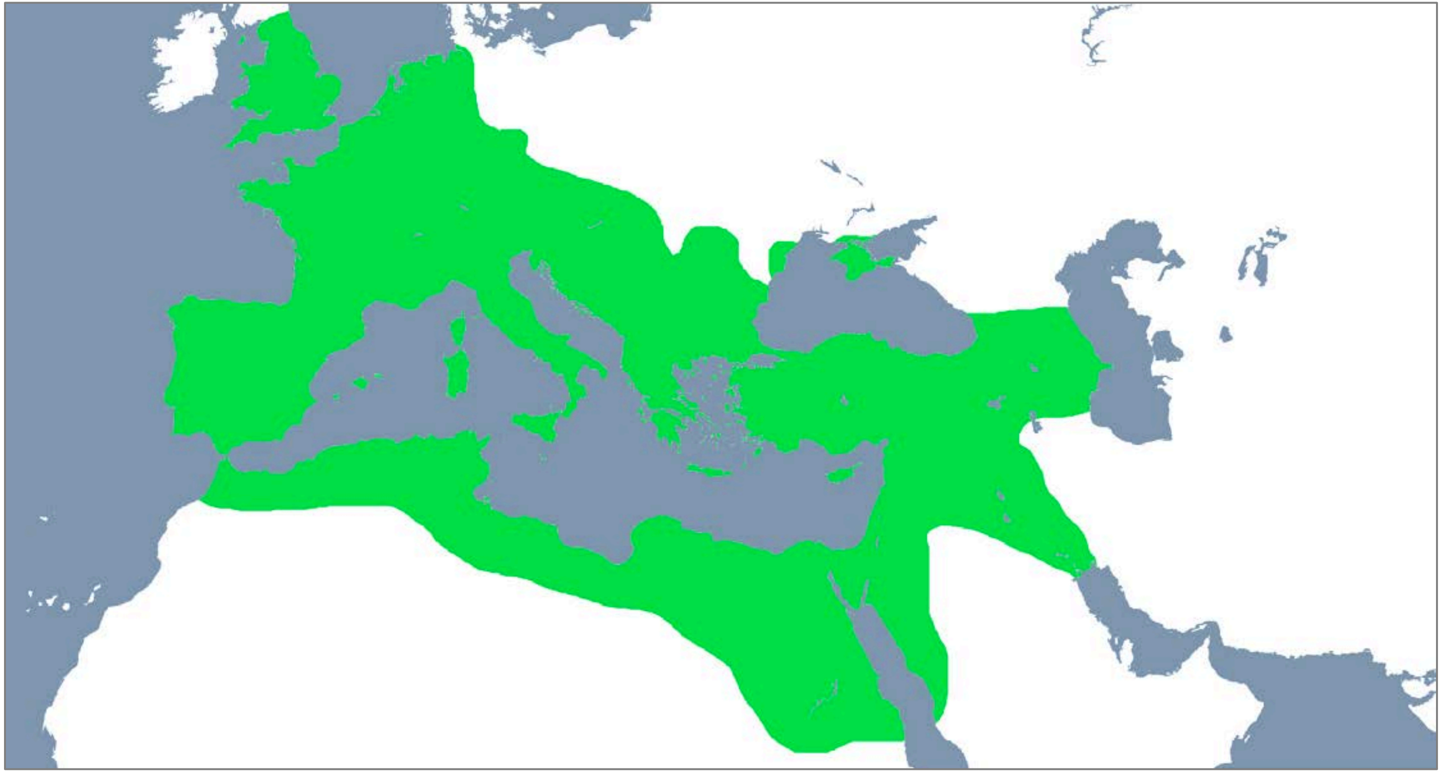
Lesson #5: Think like a hacker

- What is this thing?
- How does it work?
- What else does it do?
- Is it secure?
- Can I break it?
- Can I improve it?
- Can I own it?

Conclusion: The Modern Perimeter

The Fall of the Roman Empire

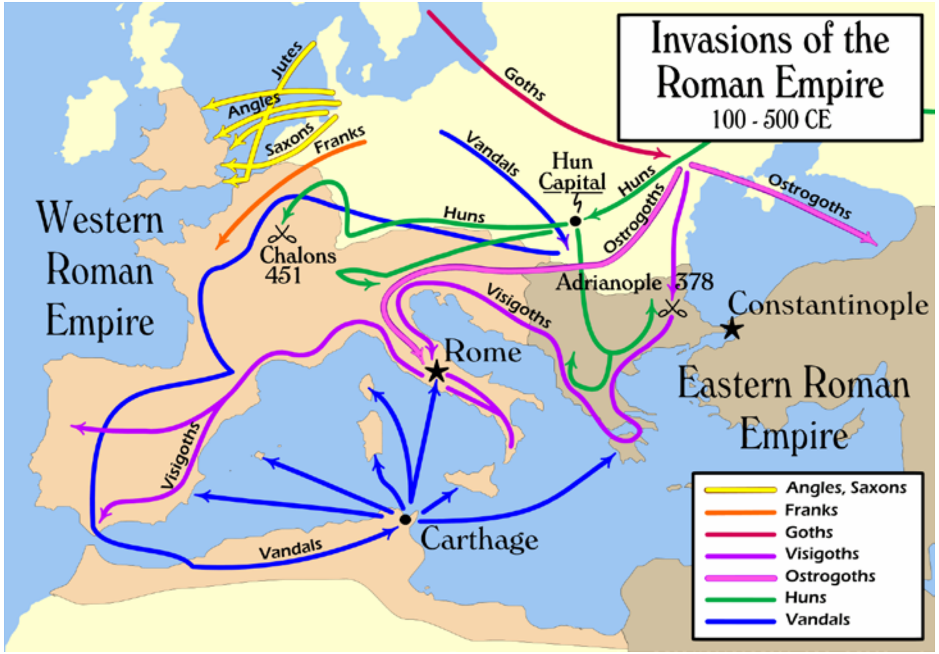
Height of the Roman Empire: 200AD



Advance Persistent Threat: Barbarians

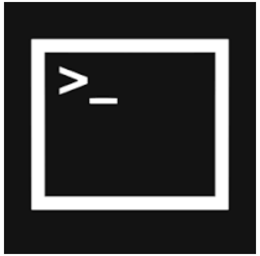
The Fall of Rome

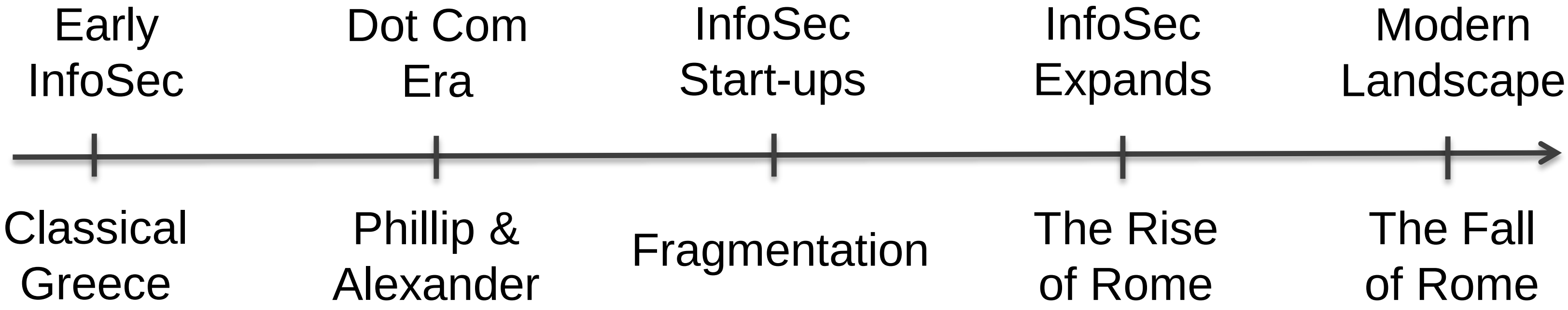
- The borders are immense and incredibly difficult to police
- Threats from the East & North
- When one army is in trouble, others can't come to their aid
- Political infighting divides the empire – split in two
- Rome sacked twice
- Last Roman emperor killed in 476



Wikipedia commons

Parallel Lives





Early InfoSec

Dot Com Era

InfoSec Start-ups

InfoSec Expands

Modern Landscape

Classical Greece

Phillip & Alexander

Fragmentation

The Rise of Rome

The Fall of Rome

Drop us a line

ZEROFOX®

#

SOCIAL MEDIA SECURITY

zerofox.com
@zerofox

Spencer Wolfe
@wolfesp18
spencer@zerofox.com

Dr. Kenneth Geers
@kgeers
kgeers@zerofox.com