Cyber From First Principles

CPT Roy Ragsdale

roy@home:~/talk$ git blame -s me

^4349ead 1) Enthusiast

0347d596 2) [EECS] CS @ USMA

7d0887ba 3) [Army] MI -> 17A

323609fc 4) [780th] CO/Operator

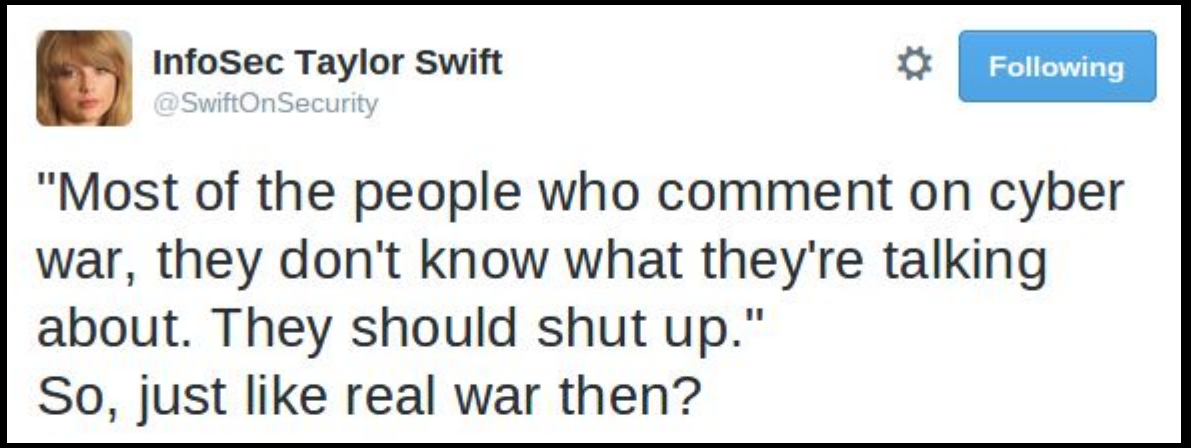
The views expressed in this talk are those of the speaker and do not reflect the official policy or position of the 780th MI BDE, the Department of the Army, the Department of Defense or the United States Government.

if you like them feel free to make them yours too

Cyber According to:

“There was an electronic device involved. By definition, that’s cyber.”
- Special Agent Avery Ryan

@SwiftOnSecurity



JP 3-12: Cyberspace Operations

CYBERSPACE OPERATIONS:

Cyberspace Operations are the employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace. Cyberspace Operations are composed of the military, intelligence, and ordinary business operations of DOD in and through cyberspace. The military component of Cyberspace Operations, which is the only one guided by joint doctrine, is the focus of this publication. Combatant commanders (CCDRs) use Cyberspace Operations in and through cyberspace in support of military objectives.

Cyber by analogy

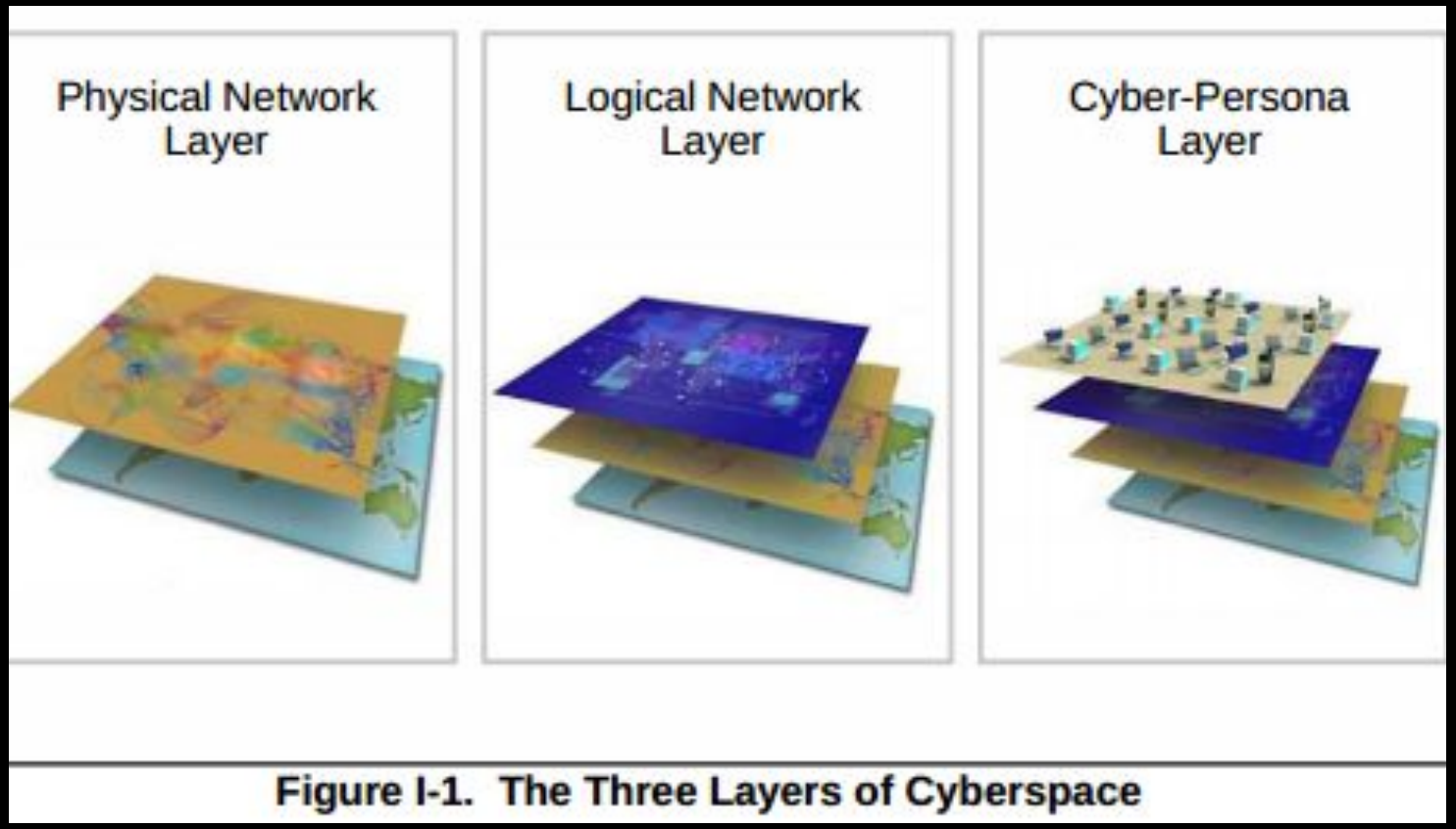


Figure I-1. The Three Layers of Cyberspace

Cyber by analogy

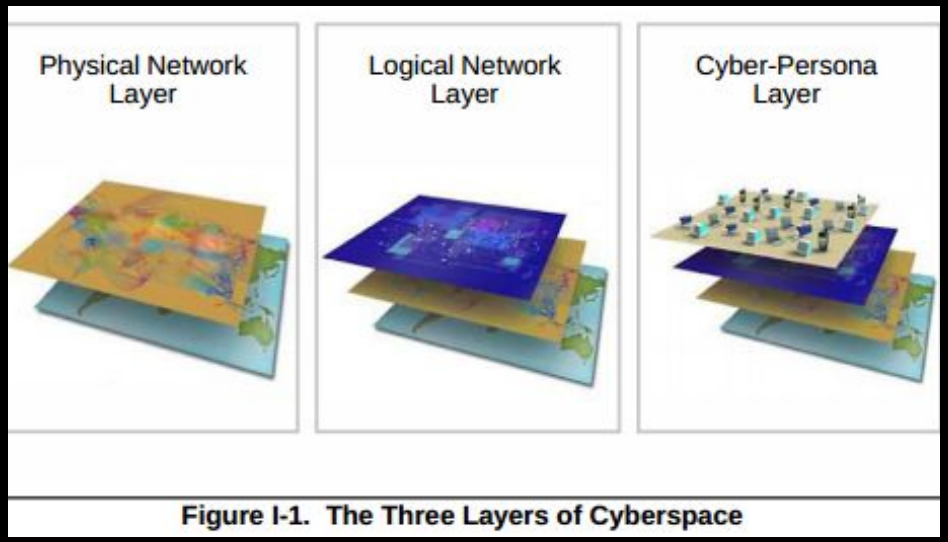
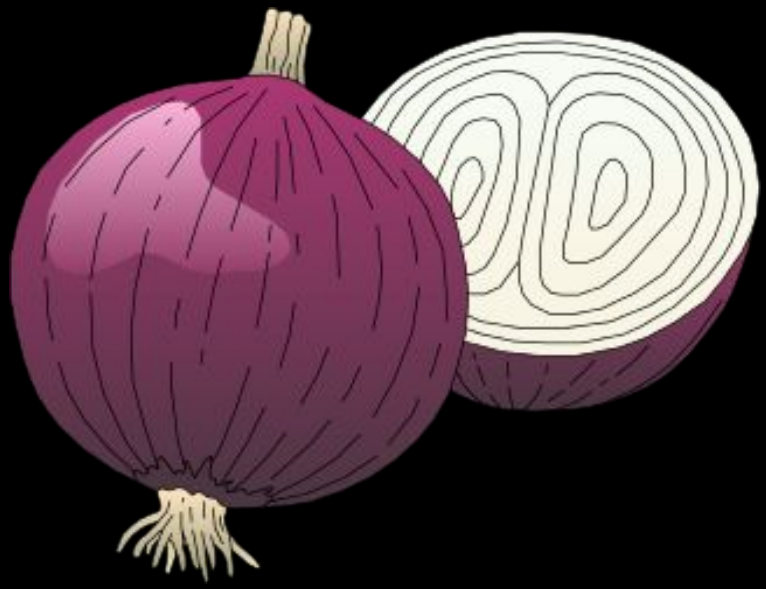
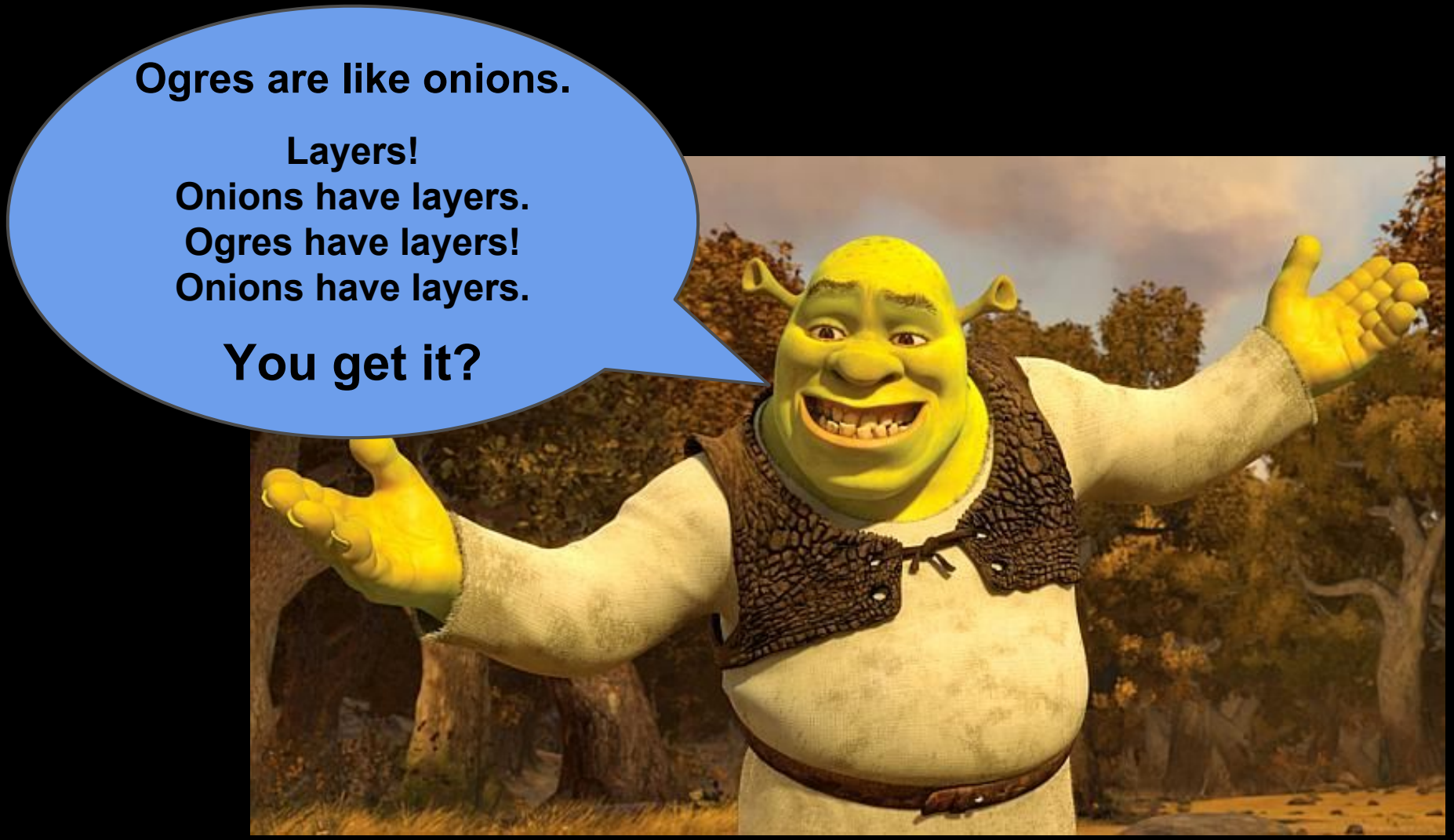


Figure I-1. The Three Layers of Cyberspace

≈



Cyber by analogy



Cyber by analogy

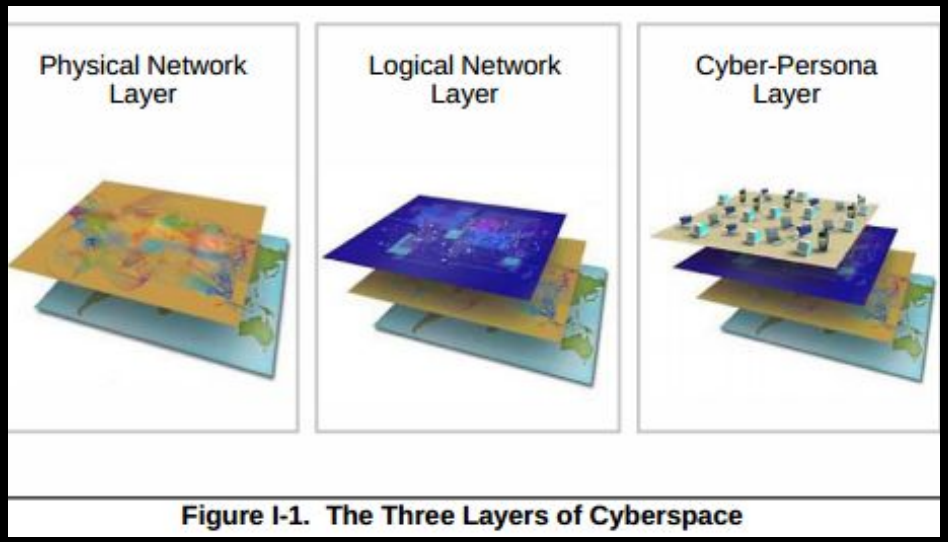
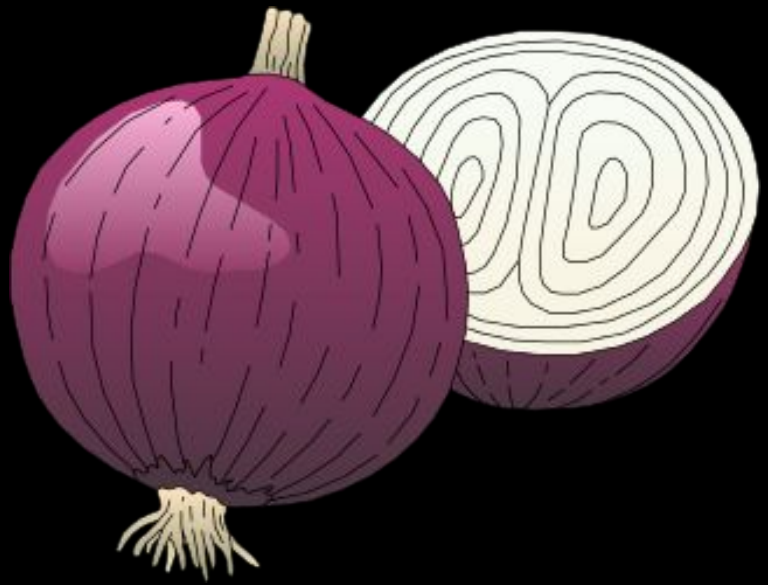


Figure I-1. The Three Layers of Cyberspace

≈



∴

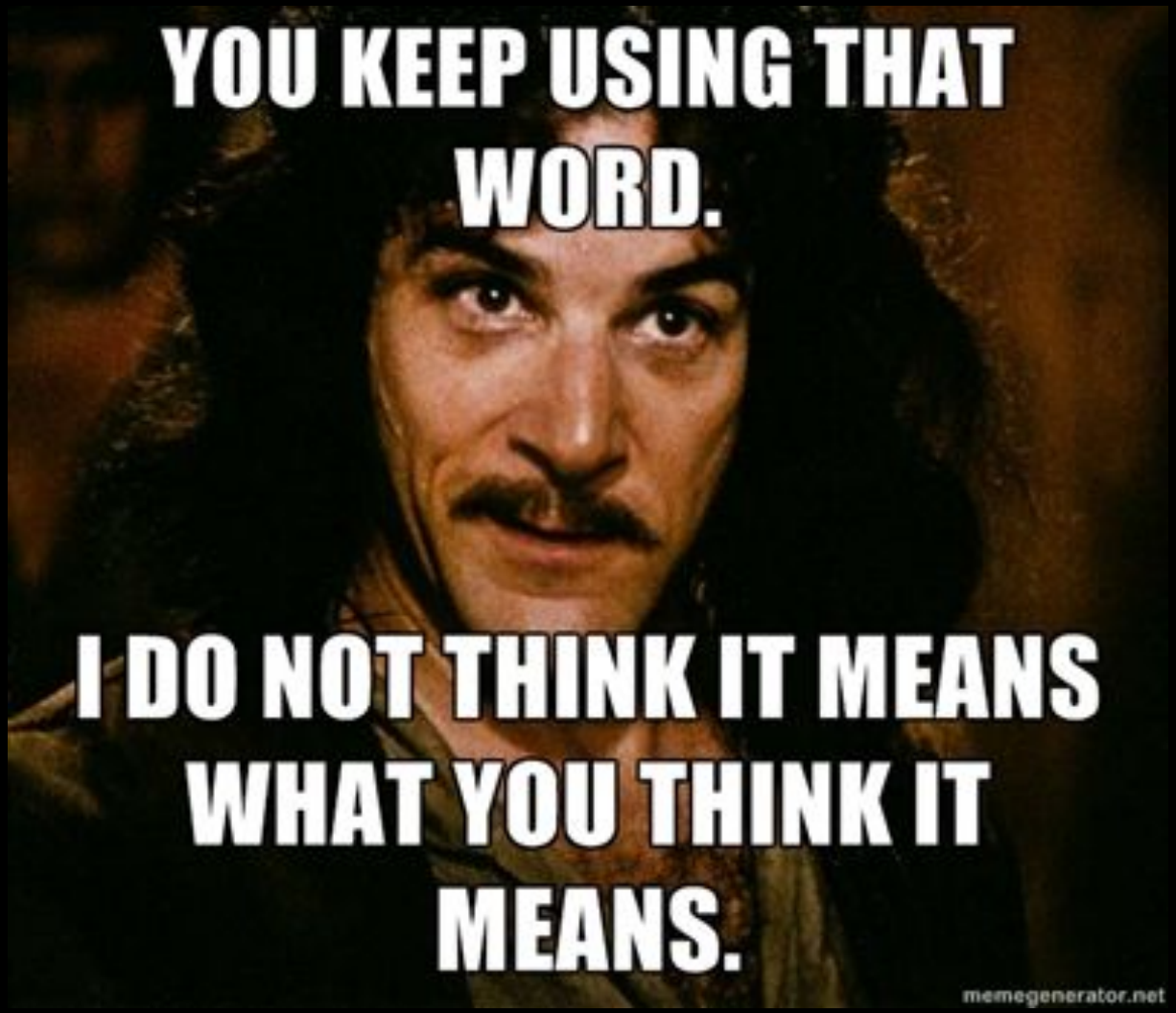
Cyber ≈


@SecureSamurai
Everybody knows you never go full cyber

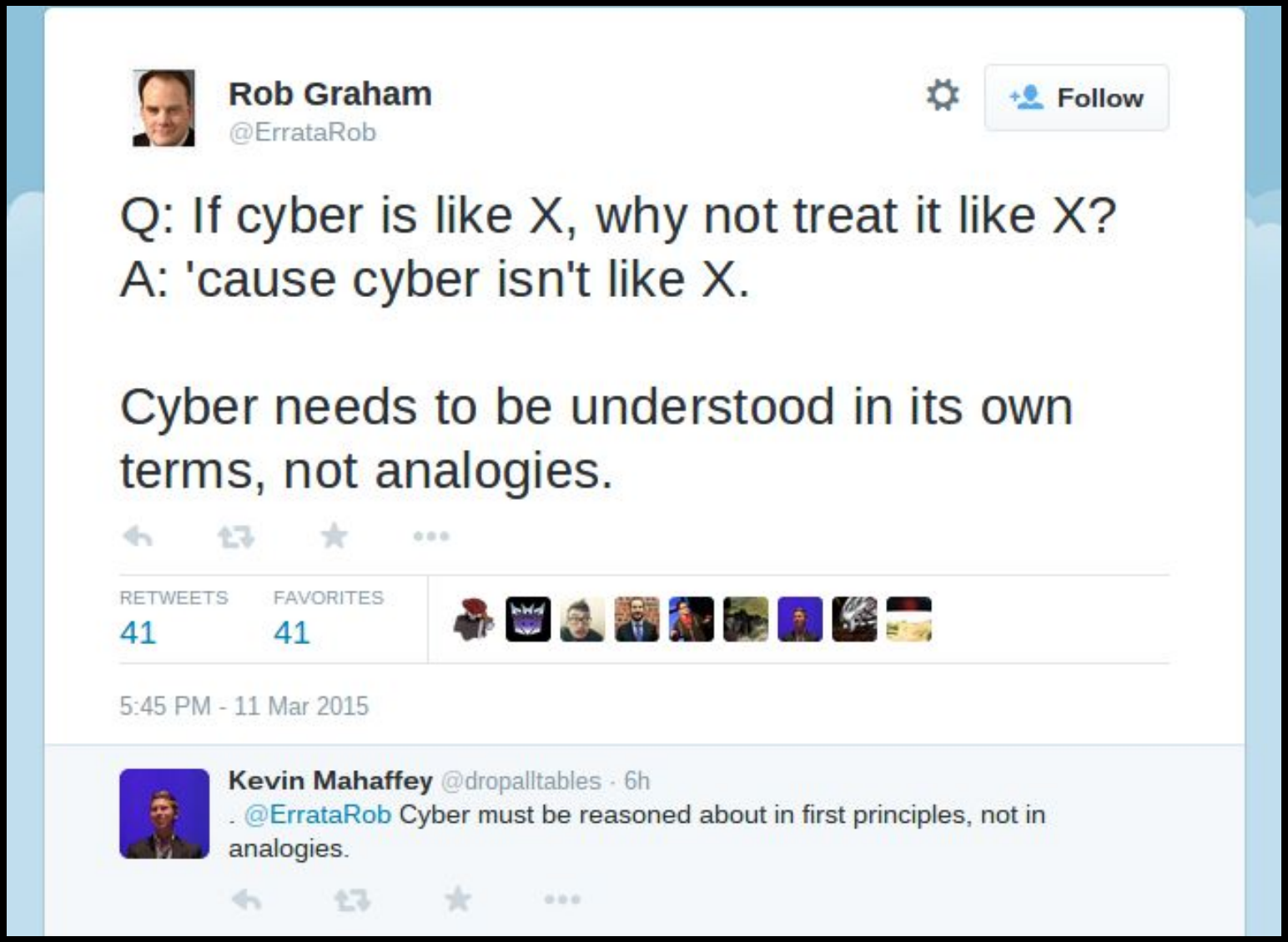

1
@
#
3
Q
W
E
A
S
Z
X


CYBER WAR
CYBER WAR

Cyber…


YOU KEEP USING THAT WORD.
I DO NOT THINK IT MEANS WHAT YOU THINK IT MEANS.
memegenerator.net

Twitter Says...



Rob Graham
@ErrataRob

Follow

Q: If cyber is like X, why not treat it like X?
A: 'cause cyber isn't like X.

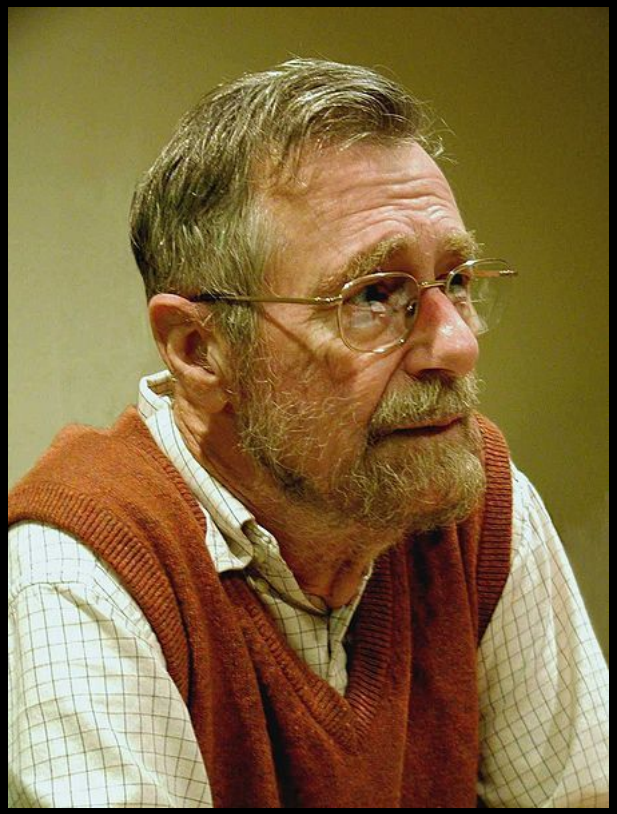
Cyber needs to be understood in its own terms, not analogies.

RETWEETS 41 FAVORITES 41

5:45 PM - 11 Mar 2015

Kevin Mahaffey @dropalltables · 6h
. @ErrataRob Cyber must be reasoned about in first principles, not in analogies.

Dijkstra says...

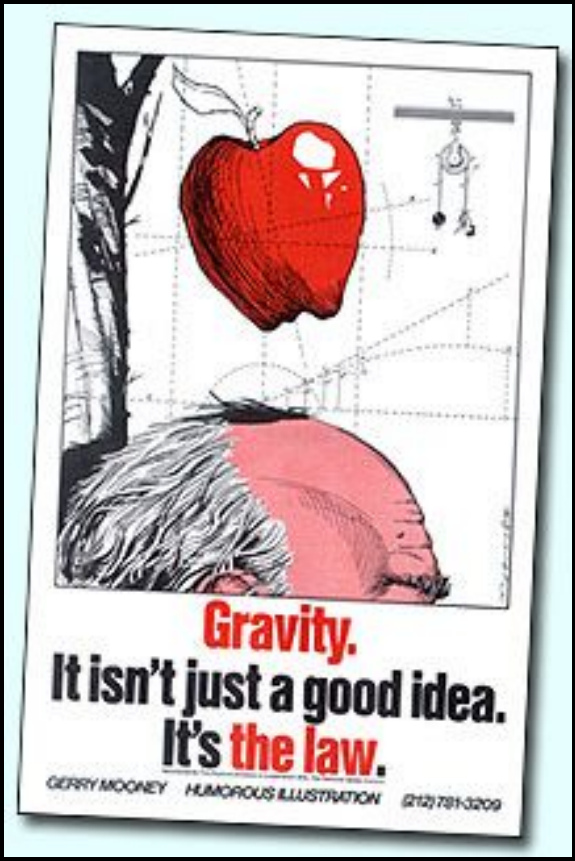


"the most common way of trying to cope with novelty [is] by means of metaphors and analogies [...] in the case of a sharp discontinuity, however, the method breaks down: though we may glorify it with the name 'common sense', our past experience is no longer relevant"

Musk says...

"physics teaches you to reason from first principles rather than by analogy"

What can we learn from Physics?



- Gerry Mooney

"If it disagrees with experiment, it is wrong"

-Richard Feynman

A First Principle for Cyber

CODE

A First Principle for Cyber

CONFLICT in

CODE

for CONTROL

A First Principle for Cyber

CONFLICT in **CODE** for CONTROL

Hacker Ethic

"get [technology] to do things it was never intended to do."

- Mudge (1997)

Corollaries

Abstraction

Asymmetry

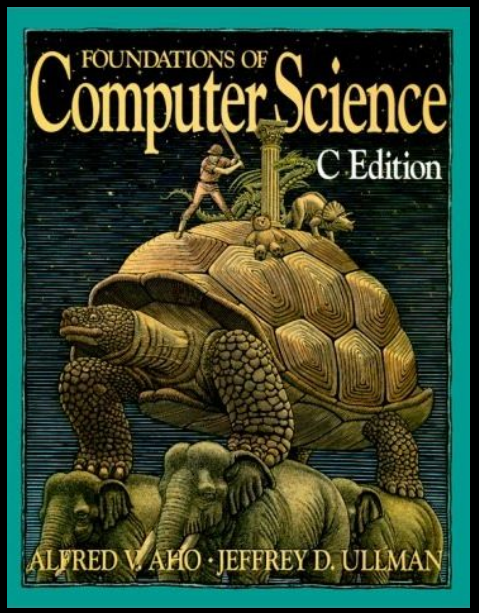
Expertise

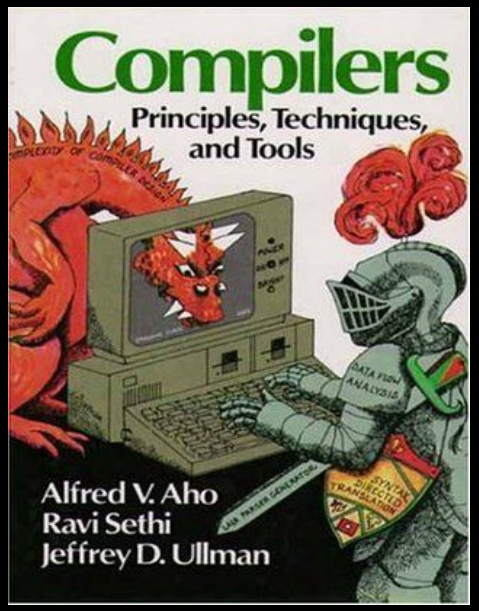
Tools

Abstraction

"Computer Science is a science of abstraction - creating the right model for a problem and devising the appropriate mechanizable techniques to solve it."

- A. Aho and J. Ullman



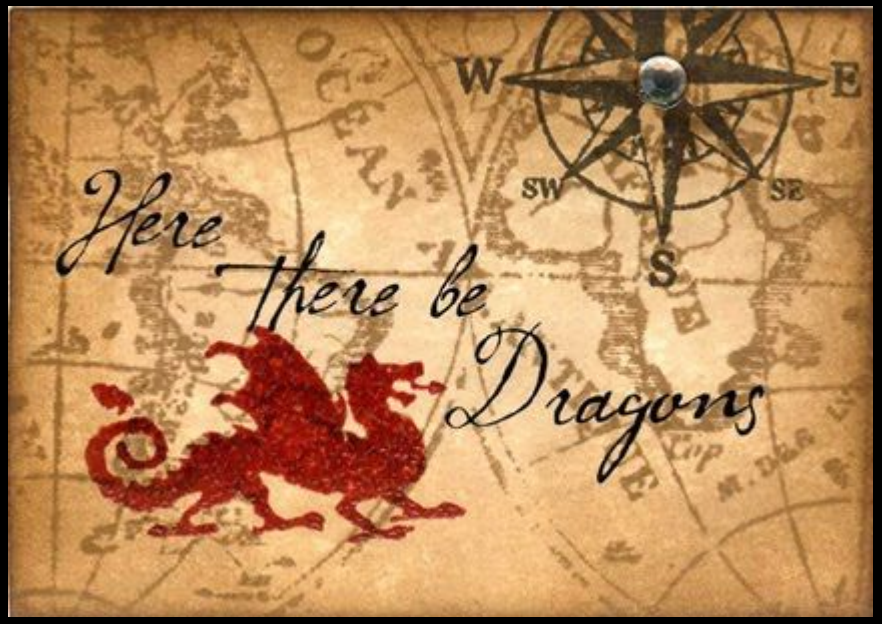


Abstraction

Manifest in **code**

Slays complexity

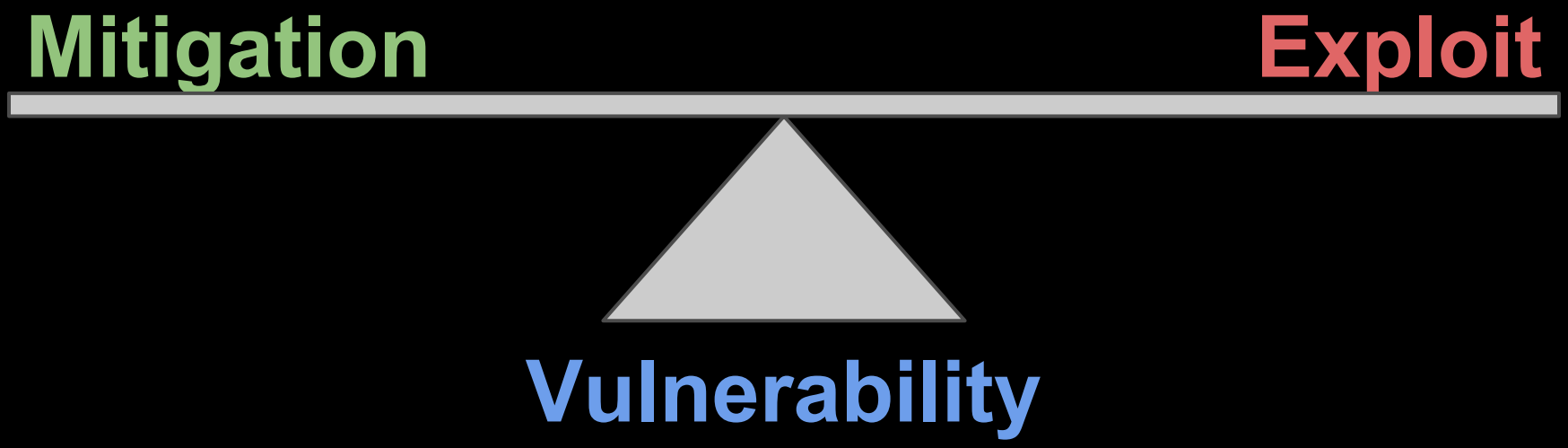
But... mind the gap



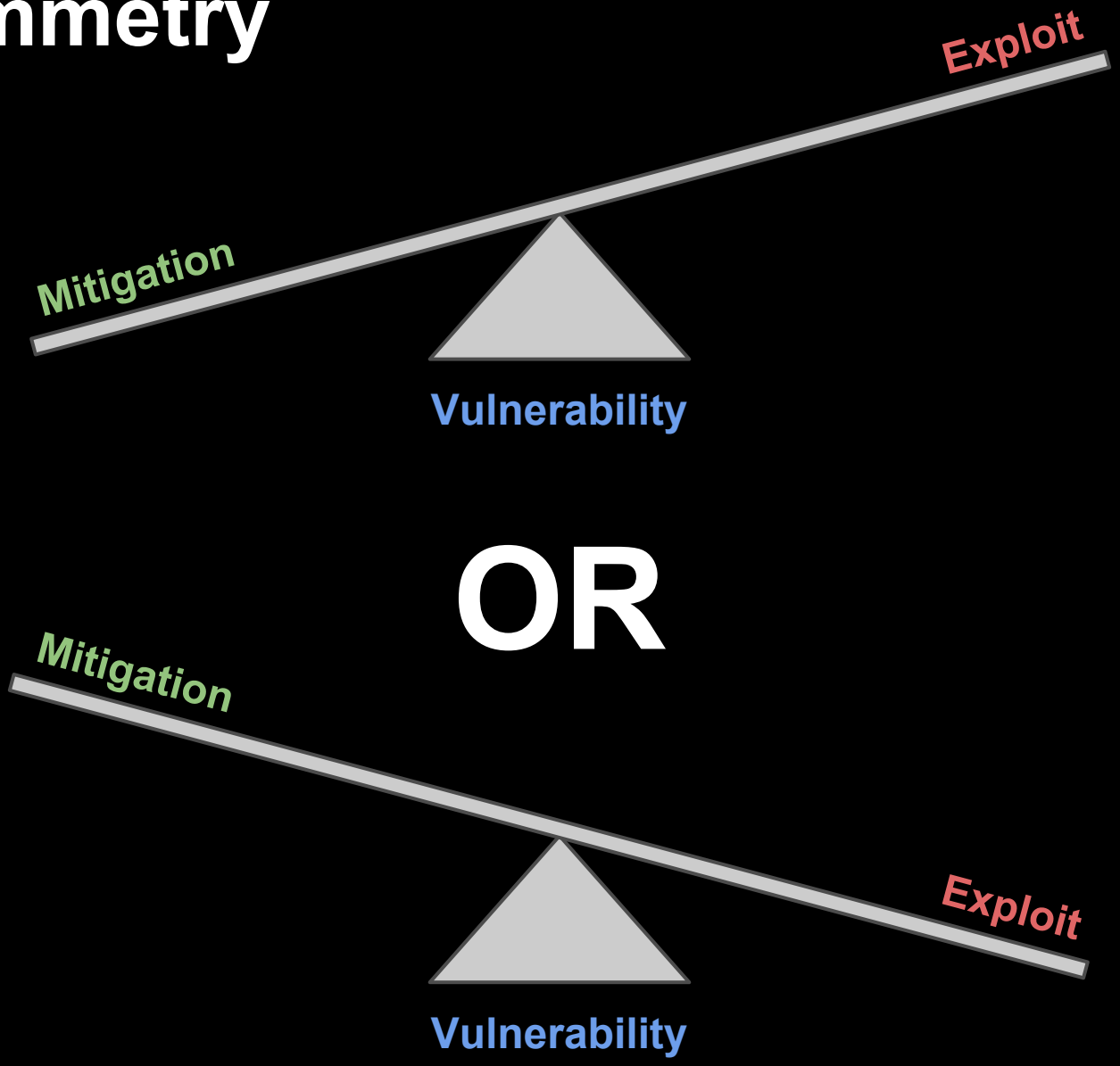
Asymmetry

"to circumvent or negate an opponent's strengths while exploiting his weaknesses"

JP 1-02



Asymmetry


Exploit
Mitigation
Vulnerability
OR
Mitigation
Exploit
Vulnerability

Asymmetry

The nature of the conflict in code

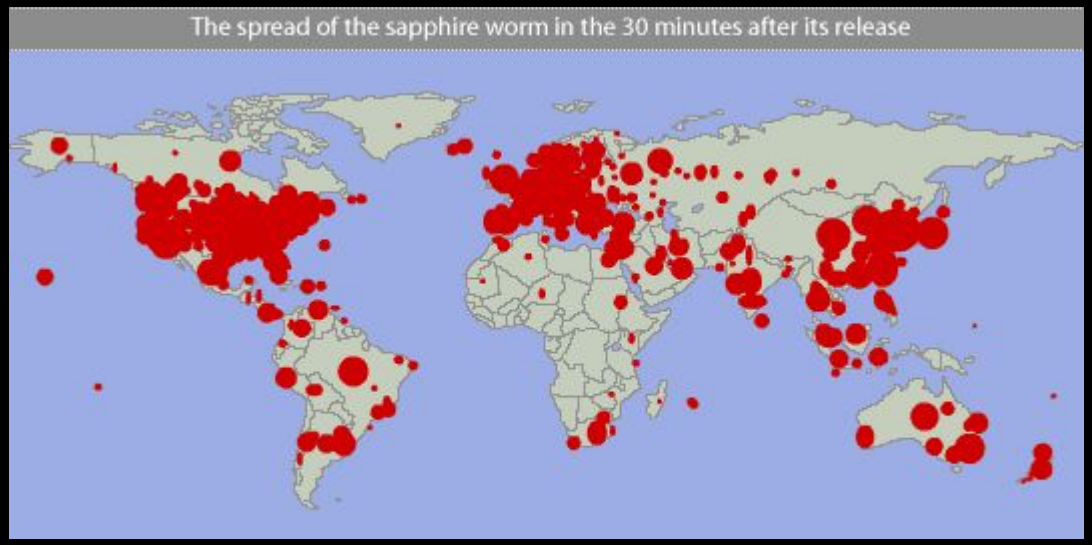
SQL Slammer

1 packet

376 bytes

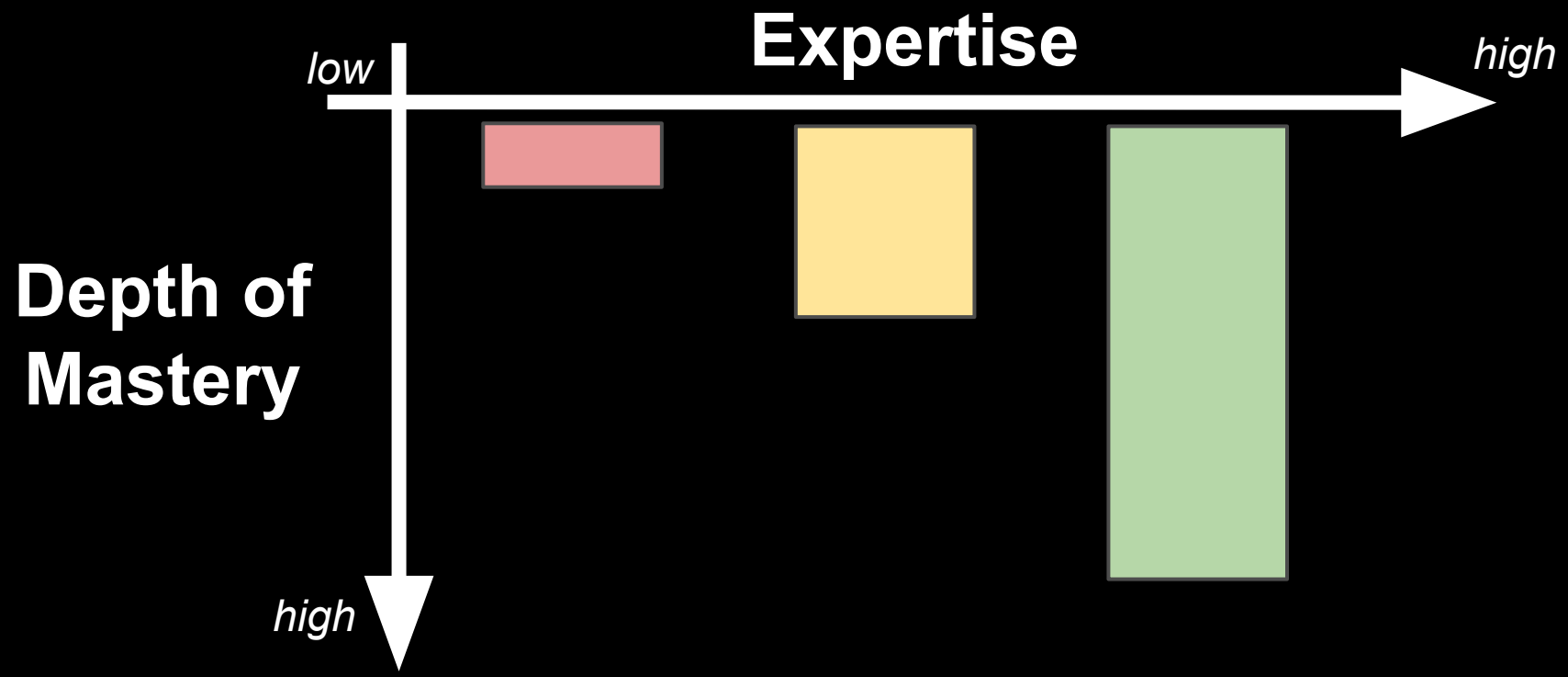
10 minutes

75,000 victims

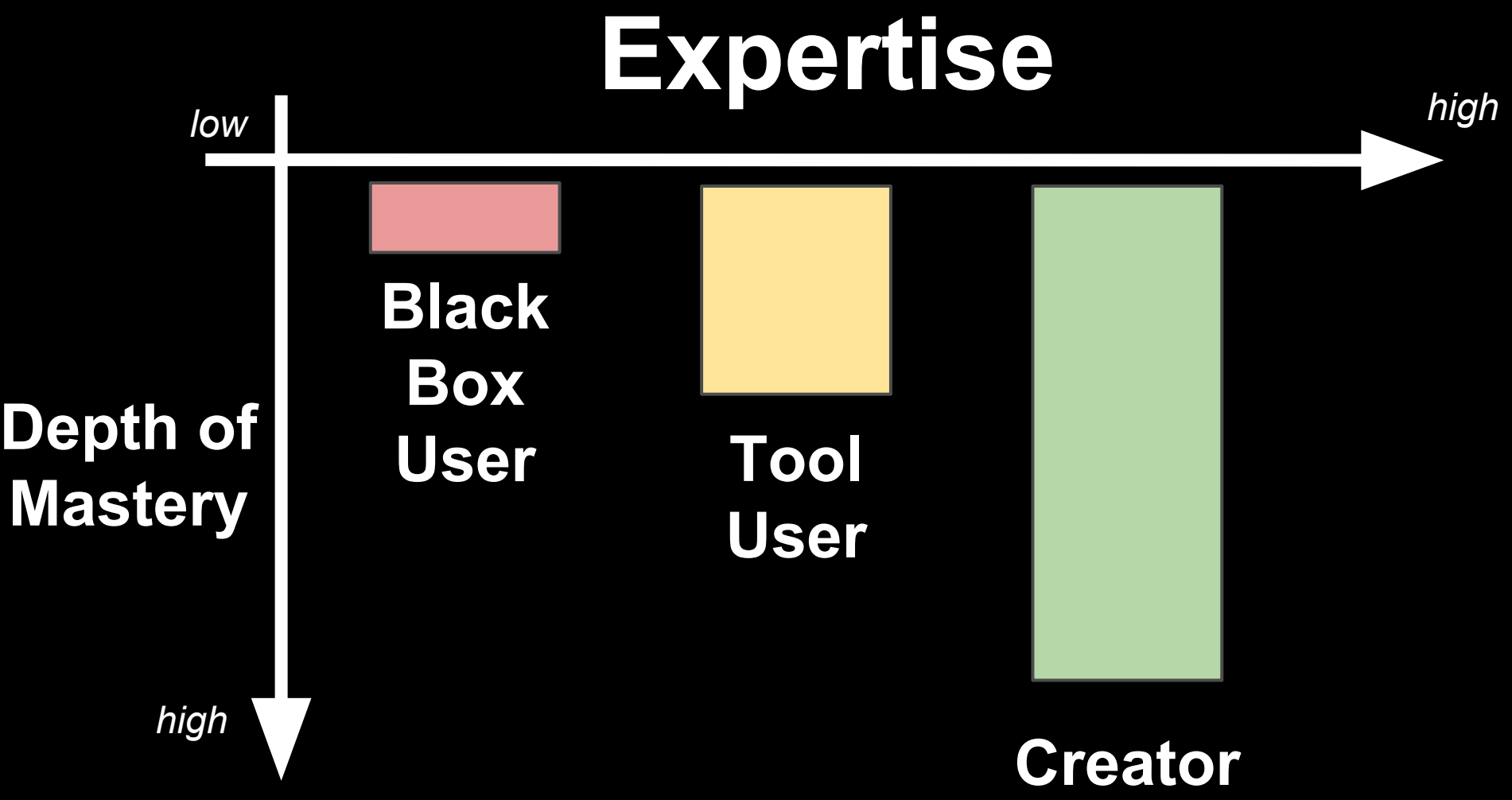


Expertise

The depth of abstraction one has mastered



Attitude / Aptitude / Ability



in the context of conflict in code for control

Tools

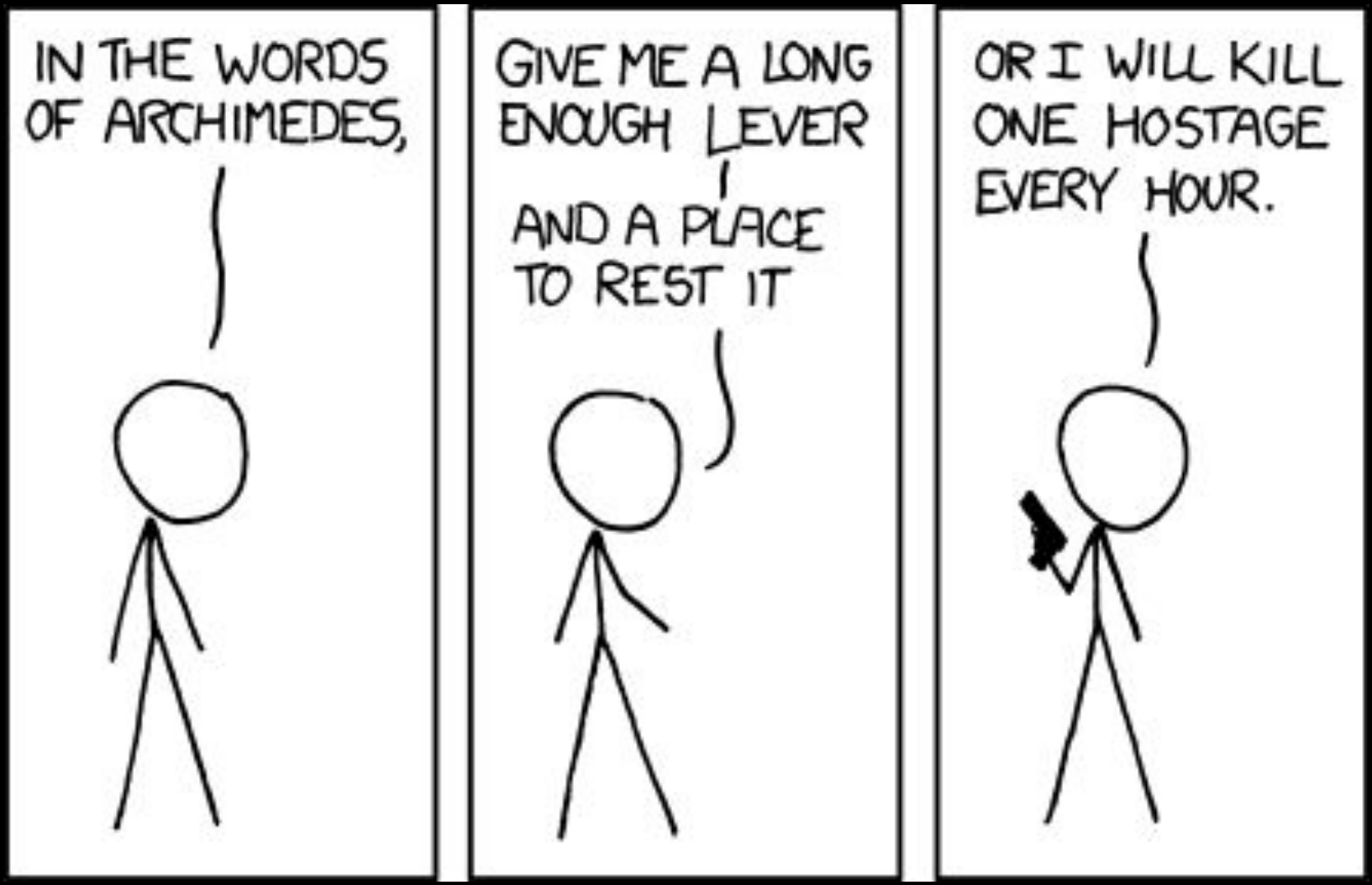
"Give me a long enough lever and a place to rest it, and I will move the Earth"

- Archimedes

Intermediary between intent and action

CODE

Tools


IN THE WORDS OF ARCHIMEDES,
GIVE ME A LONG ENOUGH LEVER
AND A PLACE TO REST IT
OR I WILL KILL ONE HOSTAGE EVERY HOUR.

Tools

HDMoore's Law

"Casual Attacker power grows at the rate of Metasploit"

- Joshua Corman

Tools

HDMoore's Law

"Casual Attacker power grows at the rate of Metasploit"

- Joshua Corman

Generalized Law of Tools

All actors capacity for control grows at the rate of their tools

A First Principle for Cyber

CONFLICT in **CODE** for CONTROL

Corollaries

Dual Edged Sword of **Abstraction**

Winner takes all **Asymmetry**

Compounding returns of **Expertise**

Intent actioned by **Tools**

Principle Applied to the Force

What type of a resource is the Cyber Mission Force?

What is possible at the Brigade level?

How do we maximize the effectiveness of our expertise?

A First Principle for Cyber

CONFLICT in **CODE** for CONTROL

Corollaries

Dual Edged Sword of **Abstraction**

Winner takes all **Asymmetry**

Compounding returns of **Expertise**

Intent actioned by **Tools**

References (0)

http://threatpost.com/csi-cyber-we-watched-so-you-didnt-have-to/111440

http://en.wikipedia.org/wiki/File:CSI-Cyber-Logo.jpg

https://twitter.com/SwiftOnSecurity/status/555927006421213184

http://www.dtic.mil/doctrine/new_pubs/jp3_12R.pdf

http://www.clipartlord.com/wp-content/uploads/2012/11/onion.png

http://www.straitstimes.com/sites/straitstimes.com/files/20140225/SHHREJDK2502e.jpg

http://www.imsdb.com/scripts/Shrek.html

https://twitter.com/SecureSamurai/status/573500244614344704

http://www.evolvement.net/images/grenade.png

http://www.iamit.org/blog/wp-content/uploads/2012/02/cyber-weapon.jpg

http://www.ginnytonkin.com/wp-content/uploads/2012/07/Do-not-think-it-means.jpeg

https://twitter.com/ErrataRob/status/575774491269197824

https://www.cs.utexas.edu/~EWD/transcriptions/EWD10xx/EWD1036.html

http://commons.wikimedia.org/wiki/File:Edsger_Wybe_Dijkstra.jpg

http://www.wired.com/2012/10/ff-elon-musk-qa/all/

http://commons.wikimedia.org/wiki/File:Elon_Musk_-_The_Summit_2013.jpg

http://www.thegravityposter.com/historyof_04.html

http://servv89pn0aj.sn.sourcedns.com/~gbpprorg/l0pht/L0phTV.html

https://www.cs.cmu.edu/~pattis/quotations.html

References (1)

http://www.goodreads.com/book/show/703102.Compilers

http://www.goodreads.com/book/show/112268.Foundations_of_Computer_Science

http://blogs.pinkelephant.com/images/uploads/troy_dumoulin/HTBD.jpg

http://mwsu.info/annemarie-williamson/wp-content/uploads/2014/04/Mind-the-Gap.png

http://en.wikipedia.org/wiki/SQL_Slammer

http://www.pbs.org/wgbh/pages/frontline/shows/cyberwar/warnings/slammermapnoflash.html

http://www.explainxkcd.com/wiki/index.php/857:_Archimedes

http://xkcd.com/857/

http://blog.cognitivedissidents.com/2011/11/01/intro-to-hdmoores-law/

https://community.rapid7.com/community/metasploit/blog/2011/11/21/hd-moores-law

http://www.safcioa6.af.mil/shared/media/document/AFD-140512-039.pdf