Low-cost Active Cyber Defence

Kārlis Podiņš*
University of Latvia
Iveta Skujiņa, Varis Teivāns
CERT.LV

Cycon 2014, June 6, Tallinn, Estonia

Me and Cycon

Me and Cycon

- 2009 track moderator

Me and Cycon

- 2009 track moderator

Me and Cycon

- 2009 track moderator
- 2010 proceedings editor

Me and Cycon

- 2009 track moderator
- 2010 proceedings editor
- 2011-12 ?

Me and Cycon

- 2009 track moderator
- 2010 proceedings editor
- 2011-12 ?
- 2013 VIP driver

Me and Cycon

- 2009 track moderator
- 2010 proceedings editor
- 2011-12 ?
- 2013 VIP driver
- 2014

Me and Cycon

- 2009 track moderator
- 2010 proceedings editor
- 2011-12 ?
- 2013 VIP driver
- 2014
- ∞ exclusive rights to wear yellow pants at CyCon [CyCon phrasebook]

Outline

- Active Cyber Defence
- Why Low-cost Active Cyber Defence?
- Low-cost solutions
  - Spam
  - Advanced Fee Fraud
  - Phishing
  - Practical implementation and experiments

Cyber

≠

Physical

Intuition

- Evolved over millions of years
- Fine tuned for dealing with other *homo sapiens* in physical world

eMail

- Digital mail, right?

eMail

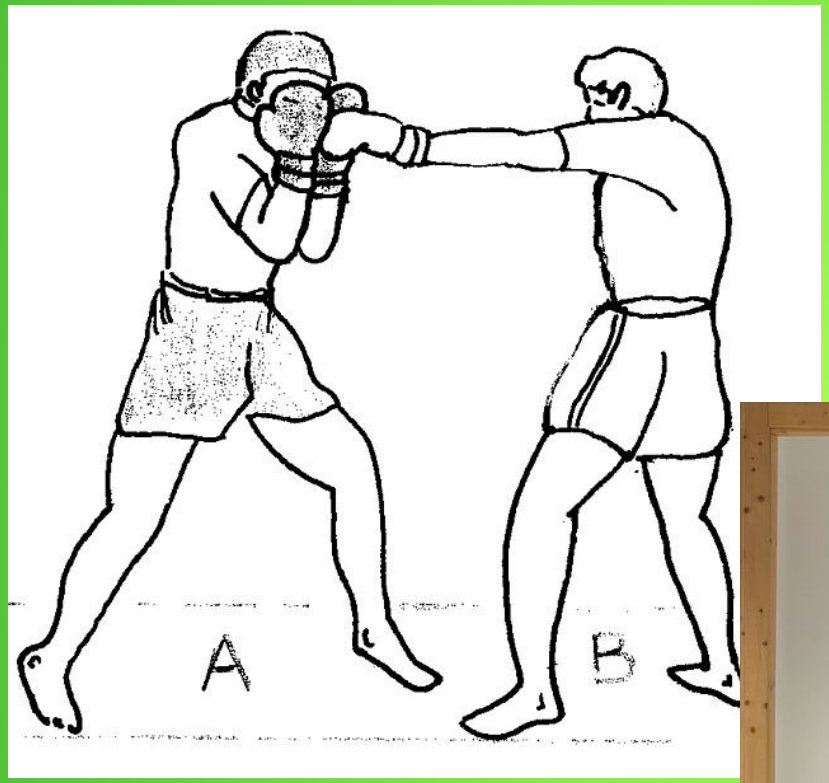
Counter-intuitiveness

- Most effective means to extinguish wildfires

Counter-intuitiveness

- Most effective means to extinguish wildfires

Active-passive spectrum



Picture by Alain Delmas Magyar Balázs

Active Cyber Defence

- 2000 Wood et. al.
- Sexy
- Unclear

ACD - Timing

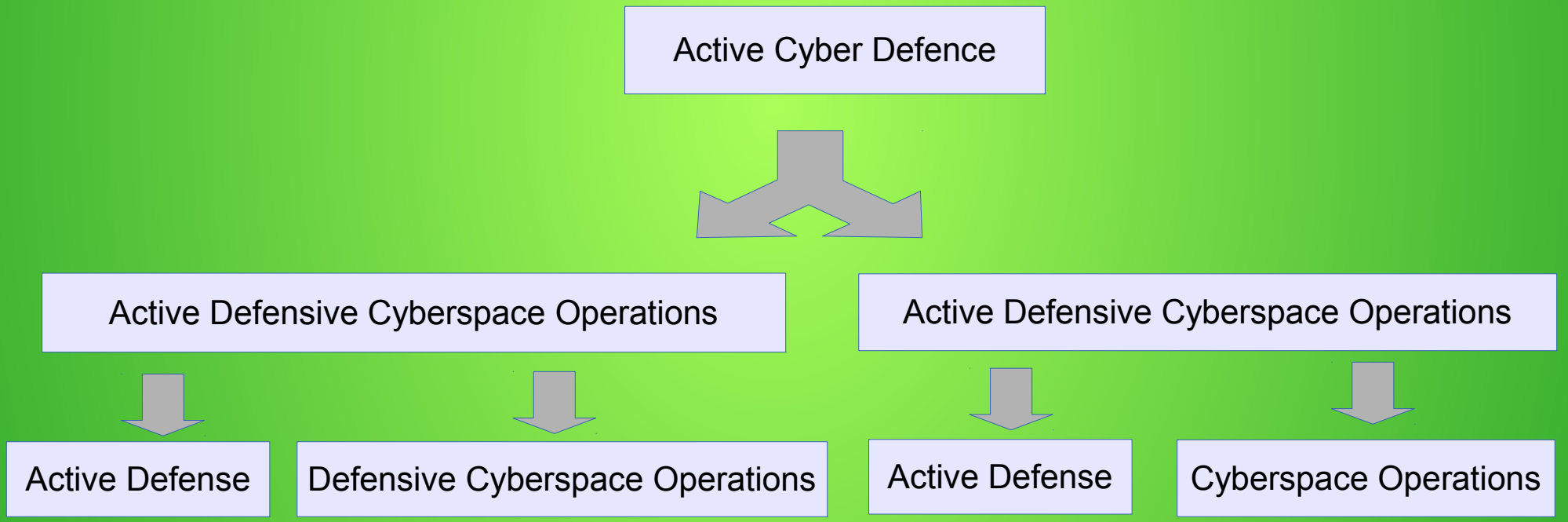
- 2011 US DoD Strategy for Operations in Cyberspace:
  - “synchronized, real-time capability...”
- 2013 Lachow:
  - “range of proactive actions ... before and during the incident”

ACD – the O word

- 2012 US DARPA Active Cyber Defense program:
  - “Capabilities would be solely defensive in nature, the ACD program specifically excludes research into cyber offense capabilities.”“
- 2010 US DoD Dictionary of Military Terms:
  - Active defense - “employment of limited offensive action and counterattacks”

ACD by DoD

2010 US DoD Dictionary of Military Terms



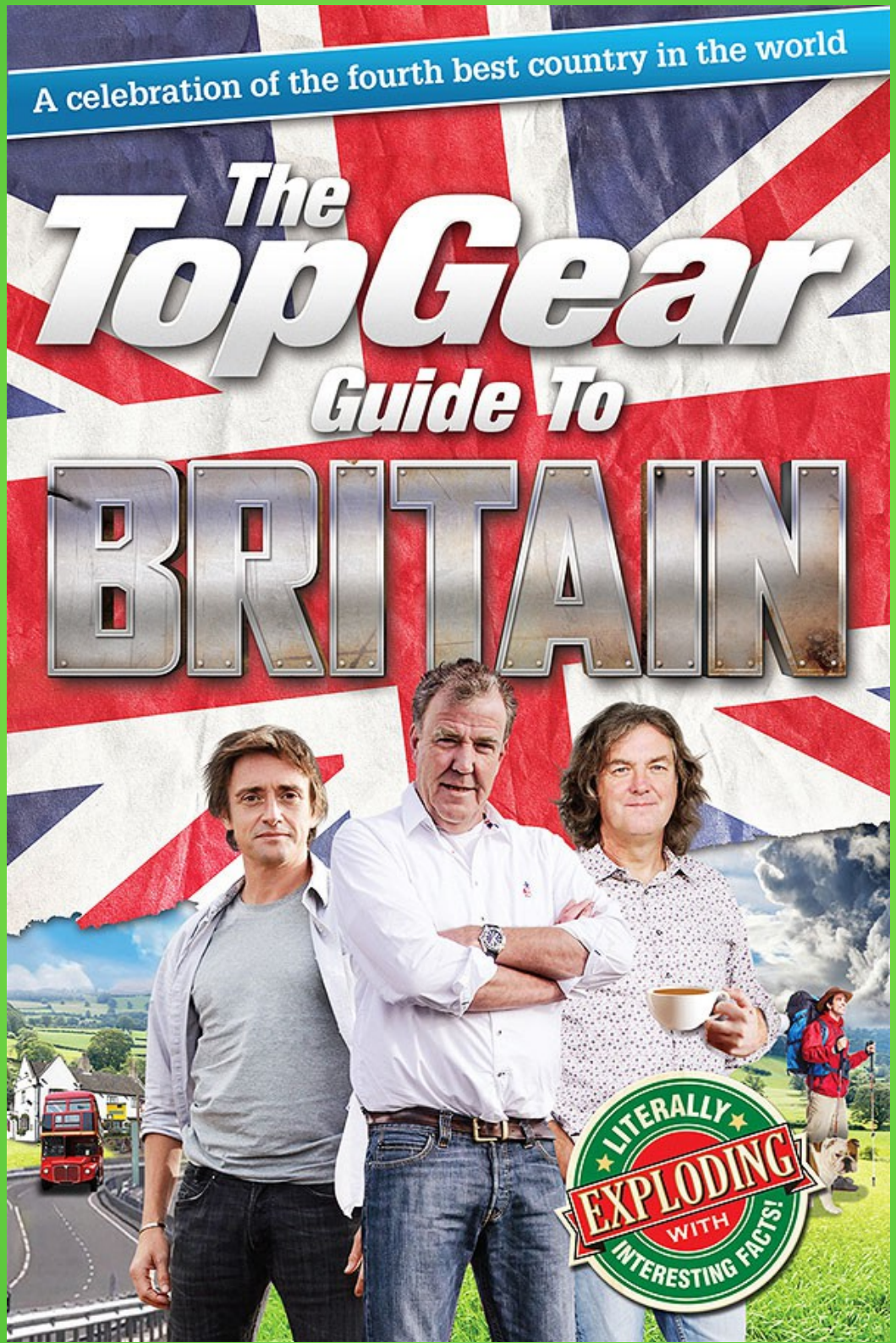
ACD by DoD

- Employment of limited offensive cyberspace capabilities and counterattacks to deny a contested area or position to the enemy**,** in or through cyberspace
- Employment of limited offensive cyberspace operations to deny a contested area or position to the enemy, intended to preserve the ability to utilize friendly cyberspace capabilities and protect data, networks, net-centric capabilities, and other designated systems

Low-cost ACD

- Popular cyber crime - spam, phishing, advance fee fraud etc.
- Well described and understood
- Inefficient passive countermeasures
- Abundant data
- Findings widely applicable
- Principle – find ~~attack~~ active defence vectors that are the most effective from economic perspective
- Goal - increase the costs to exceed income
- Attribution is not necessary
- Stay within budget

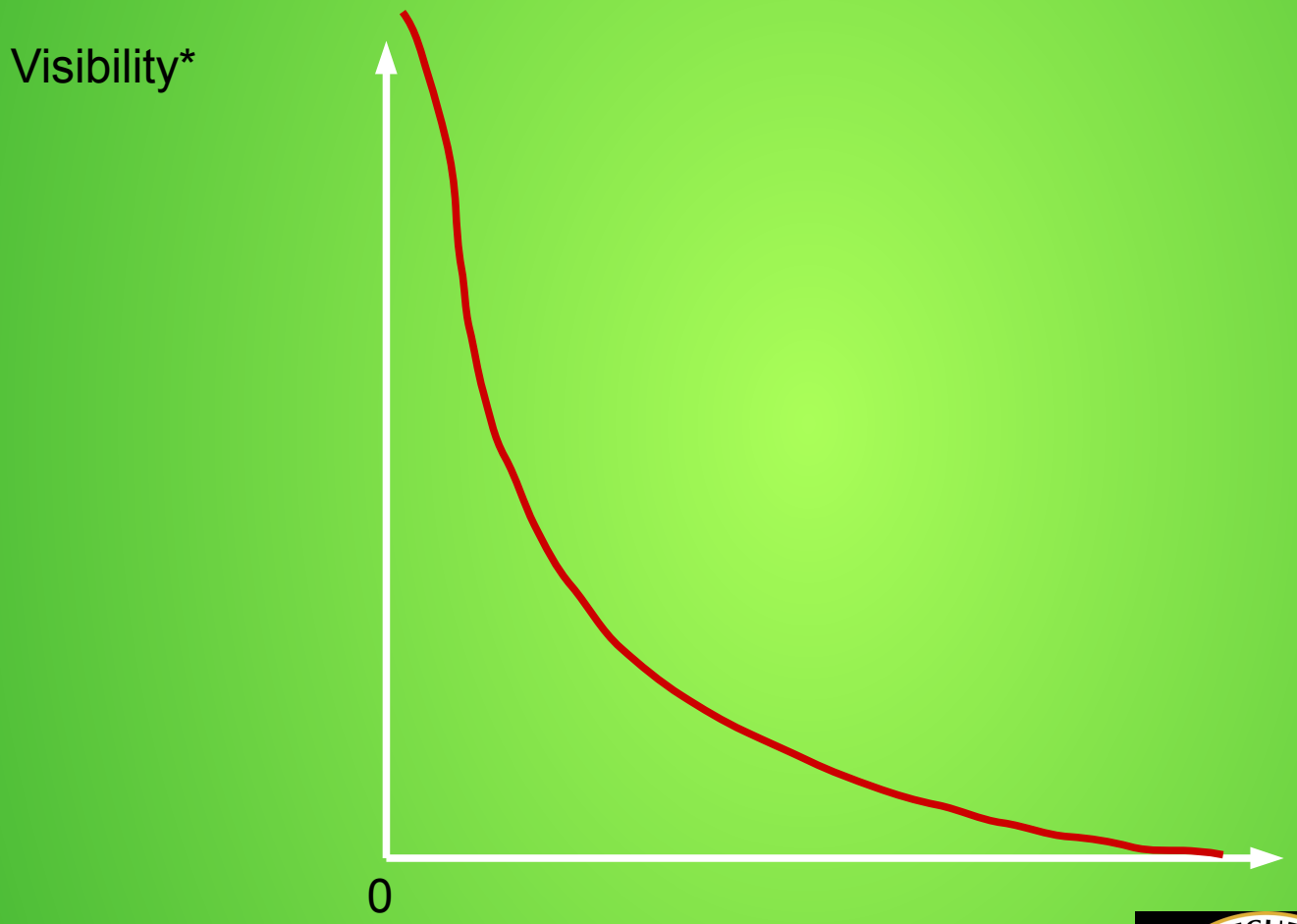
Source of inspiration


A celebration of the fourth best country in the world
The TopGear Guide To
BRITAIN
LITERALLY
EXPLODING
WITH
INTERESTING FACTS!

The Art of War

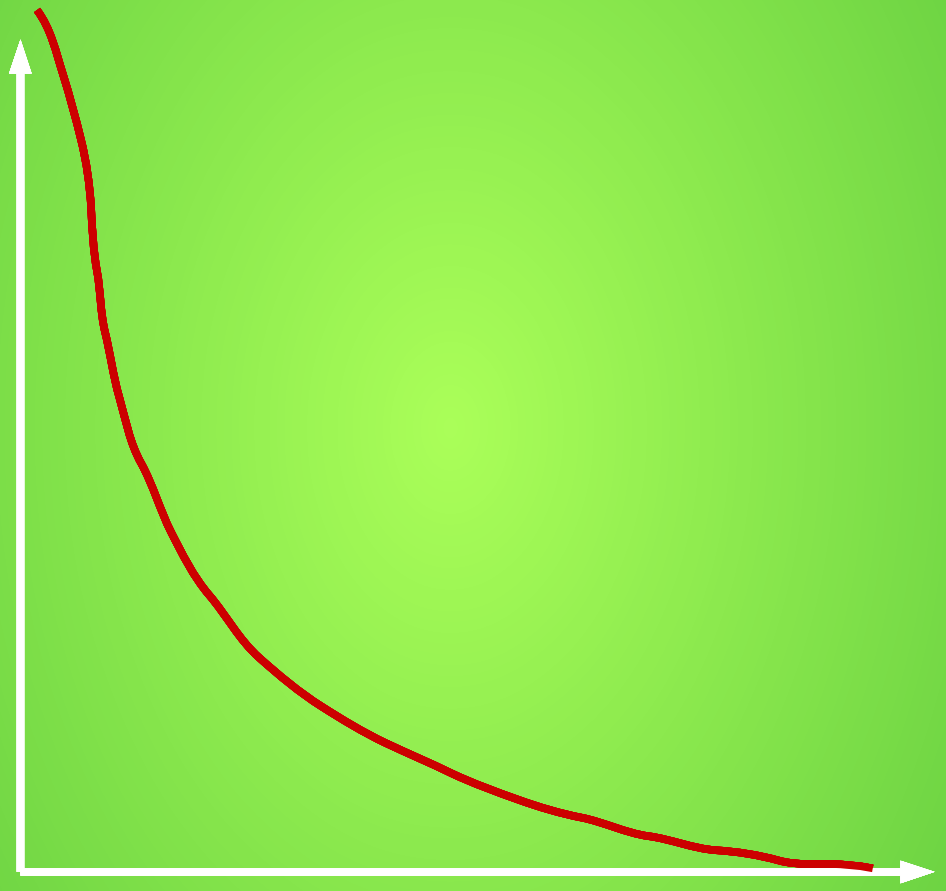
- “Thus the highest form of generalship is to balk the enemy's plans; … the worst policy of all is to besiege walled cities”

Setting the scene



Setting the scene

Visibility*



0

Technical Complexity

Spam


Festive! Fun to make!
SPAM® UPSIDE DOWN PIE
SPAM® UPSIDE DOWN PIE
SPAM
HORMEL
GOOD FOODS
COLD OR HOT... SPAM HITS THE SPOT!

Spam

- Industrial-grade spamming – for more than 15 years
- 69% of email traffic
- Annual spam costs 20B$ (US only)
- Black market price 10$ per 1M emails
- Business model

Spam (2)

- Email with commercial content that is sent to a recipient who has not requested it
- Phases:

1. Bulk email sent out
2. Spam delivered to inbox
3. User action

A) Delete/mark as spam
B) OMG cheap Viagra Click click click <0.00001%

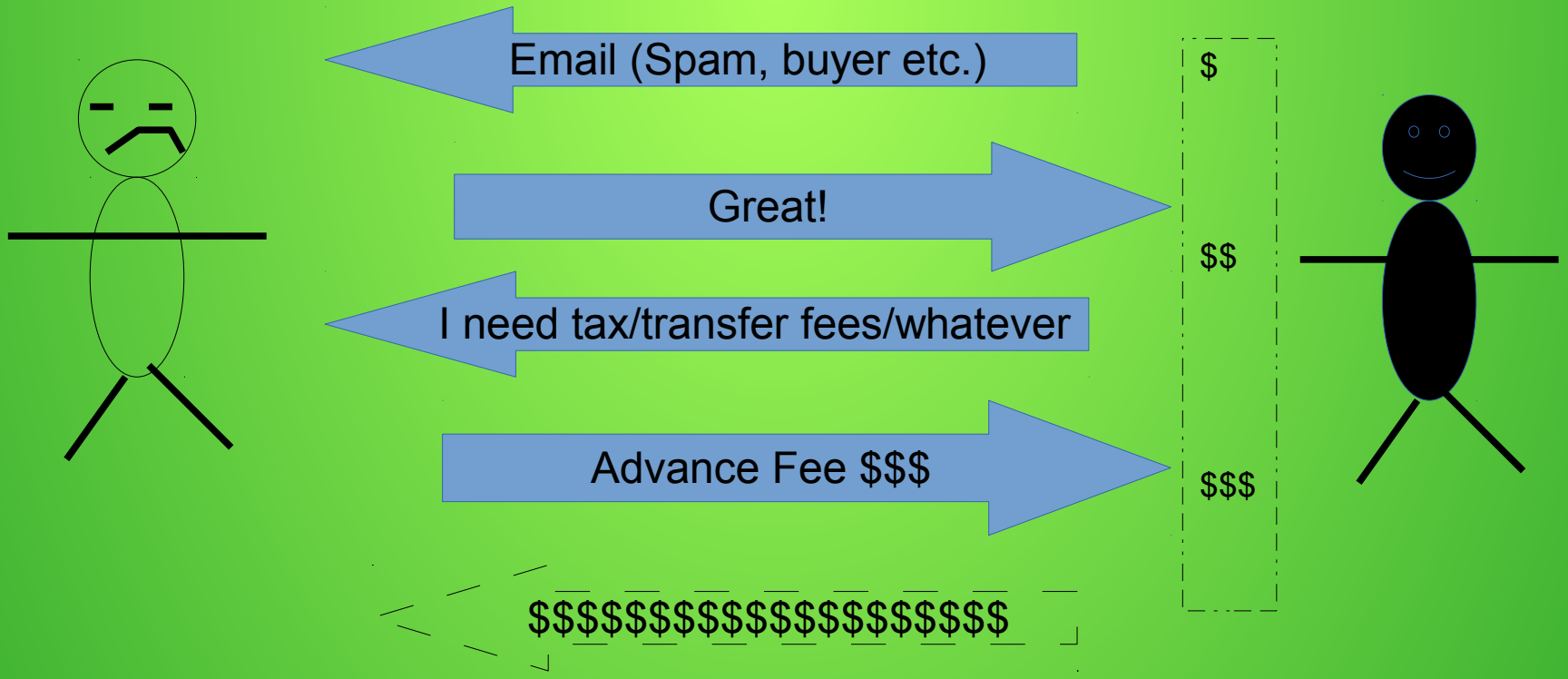
Fighting Spam

- Blacklists
- Filtering
- Last phase - manual filtering by user
  - Penalty for success
  - Advanced spam button - generate traffic for advertised website
  - Production grade product by Blue Security in 2005, discontinued
  - Difficulties if intermediaries involved (facebook, ebay etc.)
- No customers → no spam

Advance Fee Fraud

Advance Fee Fraud

- AKA Nigerian letters and “419 scam”
- Existed well before cyber
- Annual costs 150 M GBP (UK only)



Advance Fee Fraud

- Stop spam – unrealistic
- Complicate email discussion – AI email bot
  - Not to pass Turing test
  - If #bots>>#victims then a few rounds of emails necessary
  - Proof of concept in scambaiting forums
  - Increase conversation costs above income
  - Scammers likely to come up with 2nd communication channel – e.g. phone
    - Hey, Siri!
  - Fairly efficient as it attacks medium cost resource
  - Fairly easy to implement

Advance Fee Fraud

- Stop spam – unrealistic
- Complicate email discussion – AI email bot
- Complicate money transfer/cash-out
  - tainted transfer IDs
  - cooperation with money transfer services necessary
  - Works with Western Union, doesn't work with Bitcoins, web payment systems
  - Difficult to implement, many parties involved
  - Would be effective because high cost resource attacked

Phishing

TrustedBank™

Dear valued customer of TrustedBank,

We have recieved notice that you have recently attempted to withdraw the following amount from your checking account while in another country: $135.25.

If this information is not correct, someone unknown may have access to your account. As a safety measure, please visit our website via the link below to verify your personal information:

http://www.trustedbank.com/general/custverifyinfo.asp

Once you have done this, our fraud department will work to resolve this discrepency. We are happy you have chosen us to do business with.

Thank you,
TrustedBank

Member FDIC © 2005 TrustedBank, Inc.

Phishing

- Phishing email received and clicked
  - No email in typo-squatting
- Credentials entered in fake web page
- Fake website = walled city
- Poison the well
- Feed phising site with fake data
  - Phished credentials usually of high quality
  - Low quality data needs to be validated – costs possible
  - Proof of concept successfully tested, 2 sites down

Phishing

- Phishing email received and clicked
  - No email in typo-squatting
- Credentials entered in fake web page
- Fake website = walled city
- Feed phising site with fake data
- Submit tainted credentials for monitored accounts
  - Extract info on intermediaries, money mules etc. - expensive resources
  - Done by industry

Phishing

- Phishing email received and clicked
  - No email in typo-squatting
- Credentials entered in fake web page
- Fake website = walled city
- Fleed phising site with fake data
- Submit tainted credentials for monitored accounts
- Applicable to information stealing botnets

Pheeding teh Phishing Sites

- Practical experiments

Pheeding teh Phishing Sites

- Proof of concept
- Tested on 2 phishing sites, both closed quickly
- Content
  - Authentic, not random
  - Modified leaked credentials can be used
  - Most popular password lists
  - Target specific/localized

Pheeding teh Phishing Sites

- Proof of concept
- Tested on 2 phishing sites, both closed quickly
- Content
- Meta-data
  - Useragent
  - Time, timezone
  - Counters in protocol fields

Pheeding teh Phishing Sites

- Proof of concept
- Tested on 2 phishing sites, both closed quickly
- Content
- Meta-data
- Infrastructure
  - Legitimate-looking IP space
  - Randomized in time

Conclusions

- Low-cost active strategies do exist
- Active strategies – possible solution for long-term problems
- Lots of open ground to research and experimentation
- If you see something, do something


STORE
THE PALACE
FEED S
LICENSED GAMBLING

[name].[surname]@gmail.com