

RSAC[®]Conference2015

San Francisco | April 20-24 | Moscone Center

SESSION ID: MASH-R01

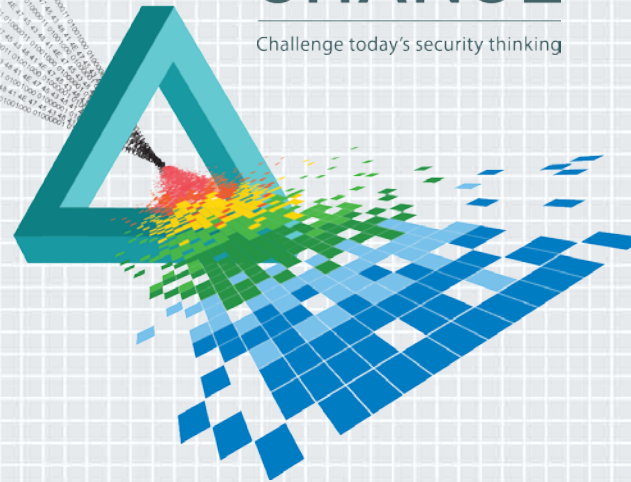
More Books You Should Have Read By Now: The Cybersecurity Canon Project

Rick Howard

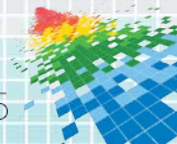
Chief Security Officer
Palo Alto Networks

CHANGE

Challenge today's security thinking



plus.google.com/+BrunoOliveira

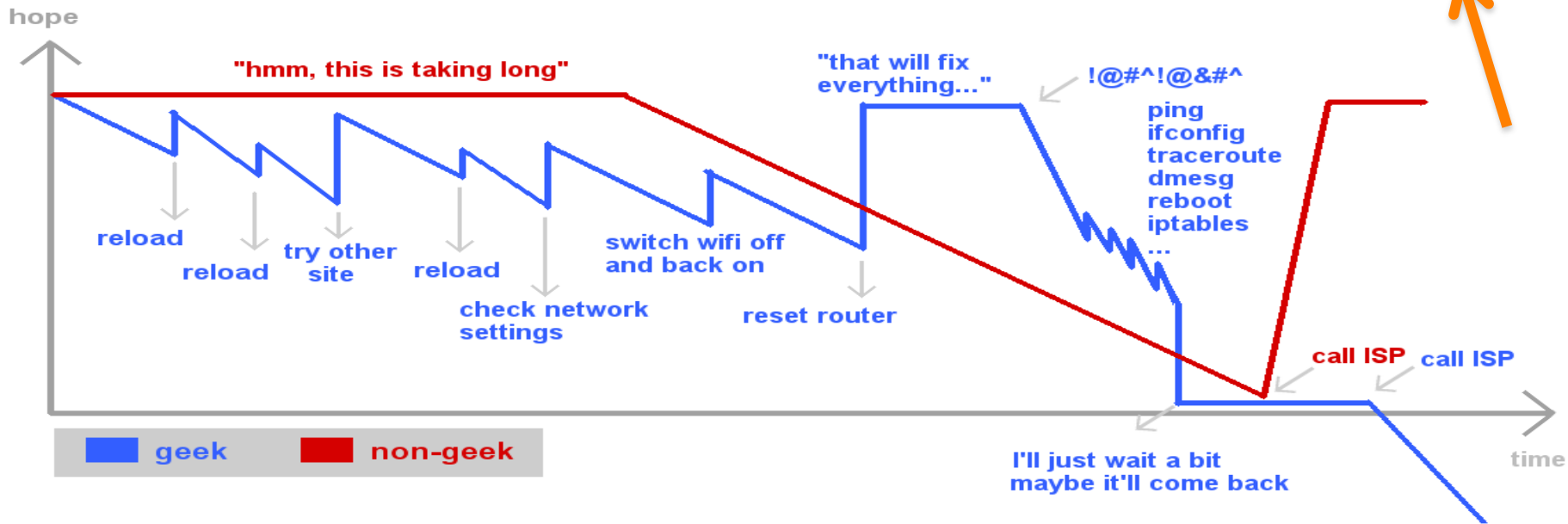


How technical are you?

Bruno Oliveira

plus.google.com/+BrunoOliveira

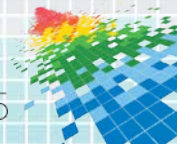
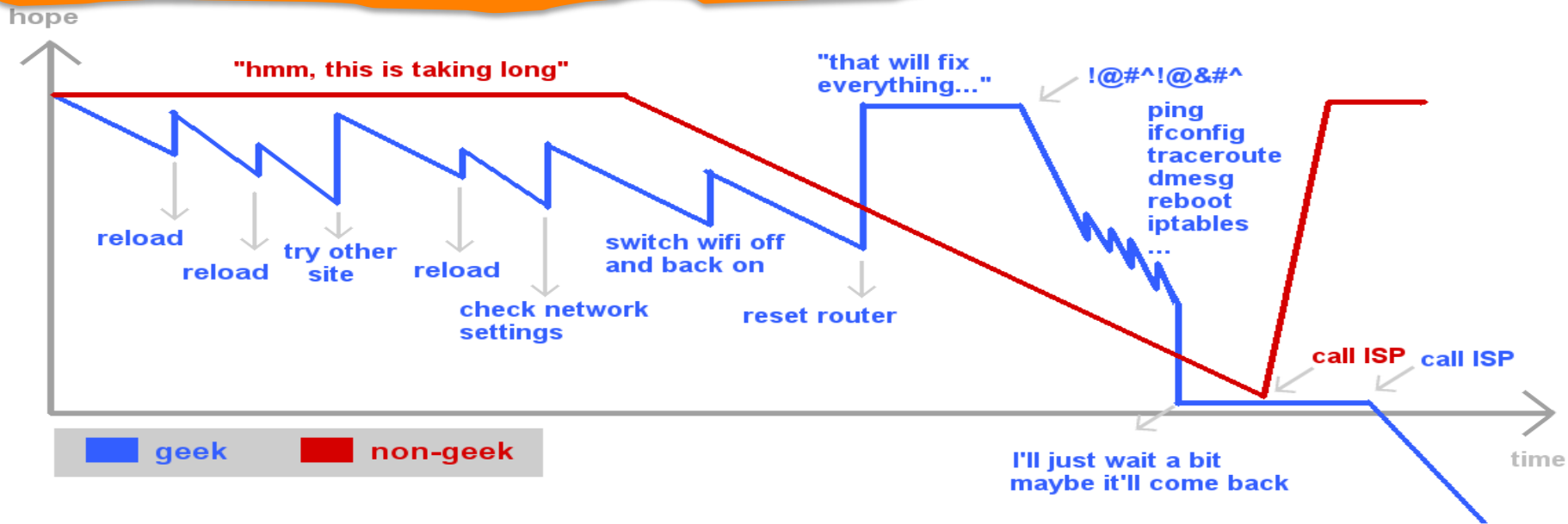
geek vs. non-geek reaction to flaky internet connection



How technical are you?

geek vs. non-geek reaction to flaky internet connection

plus.google.com/+BrunoOliveira

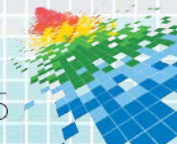
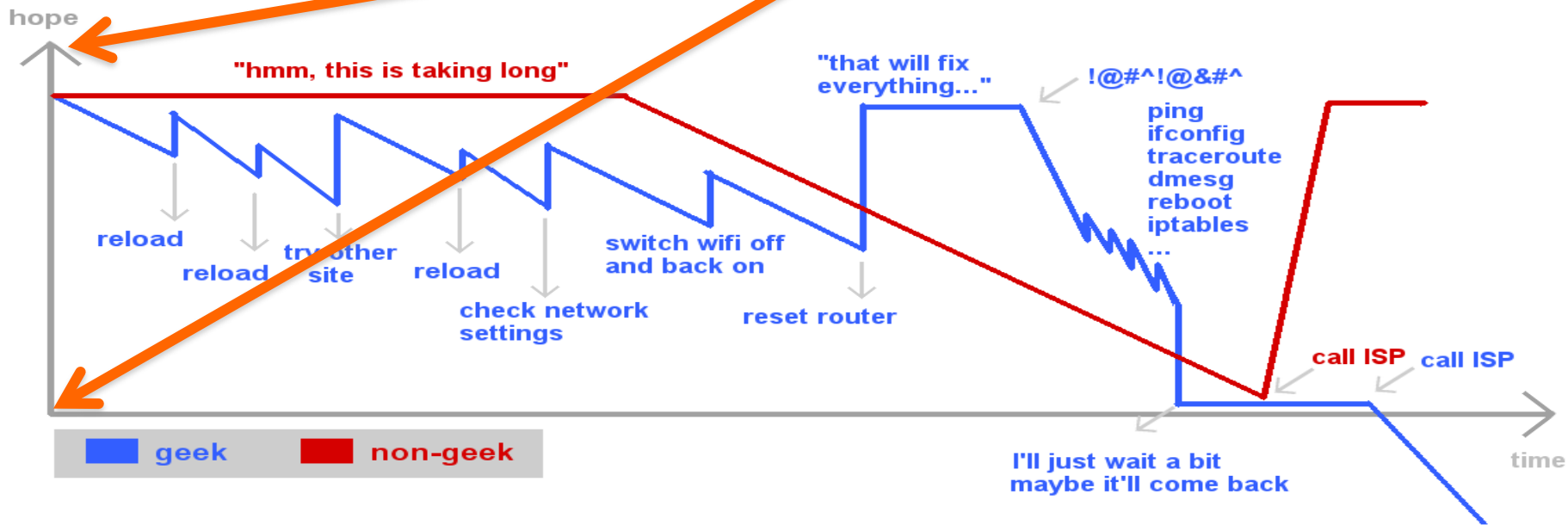


How technical are you?

Y-Axis: Hope

geek vs. non-geek reaction to flaky internet connection

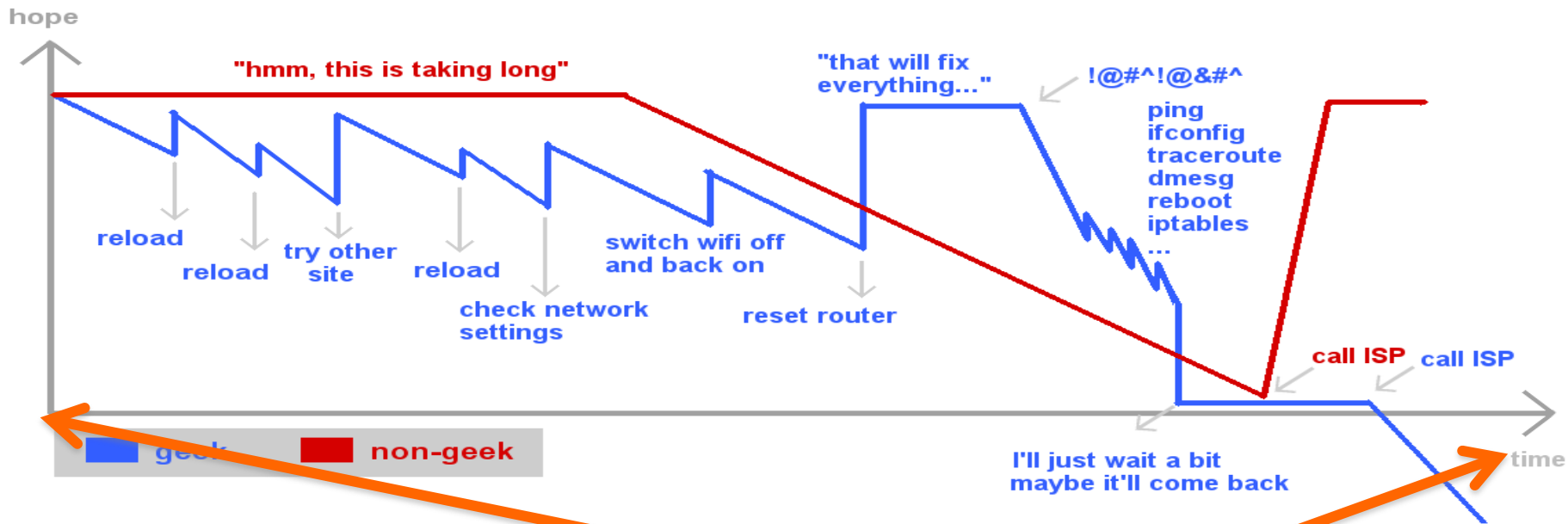
plus.google.com/+BrunoOliveira



How technical are you?

geek vs. non-geek reaction to flaky internet connection

plus.google.com/+BrunoOliveira

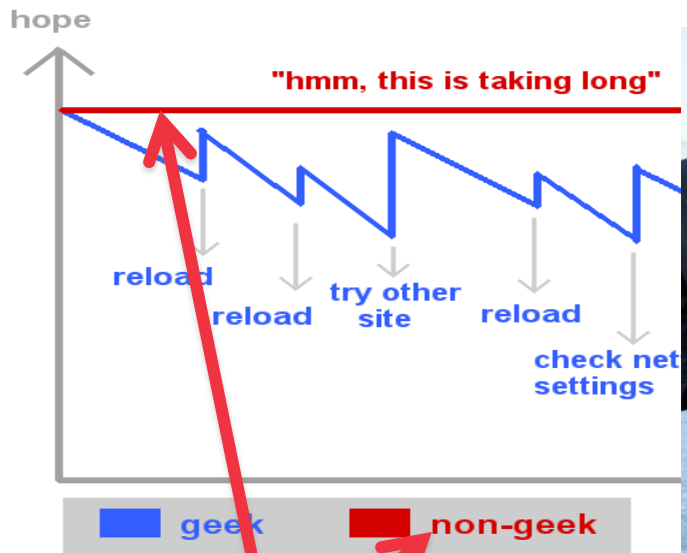


X-Axis: Time

How technical are you?

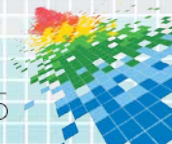
geek vs. non-geek reaction to flaky internet connection

plus.google.com/+BrunoOliveira



time

Non-Geeks – The Beautiful People

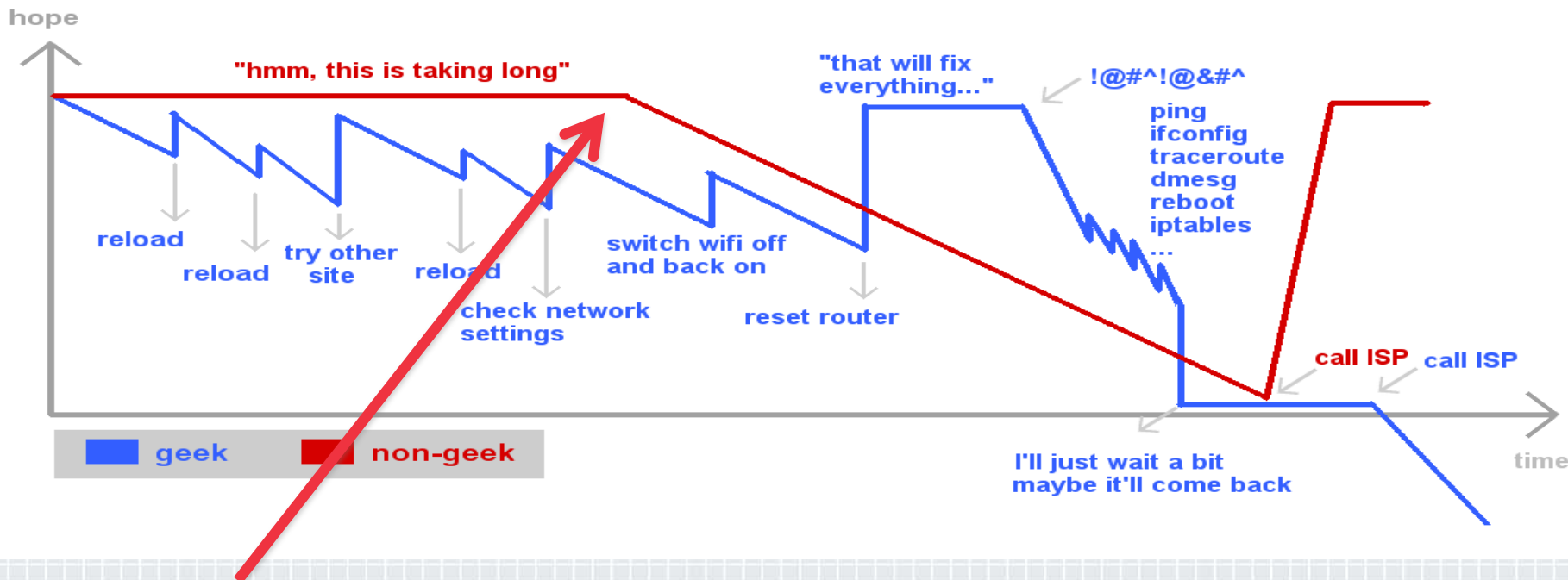


How technical are you?

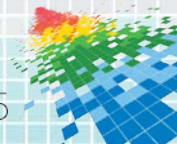


plus.google.com/+BrunoOliveira

geek vs. non-geek reaction to flaky internet connection



Non-Geeks – The Beautiful People

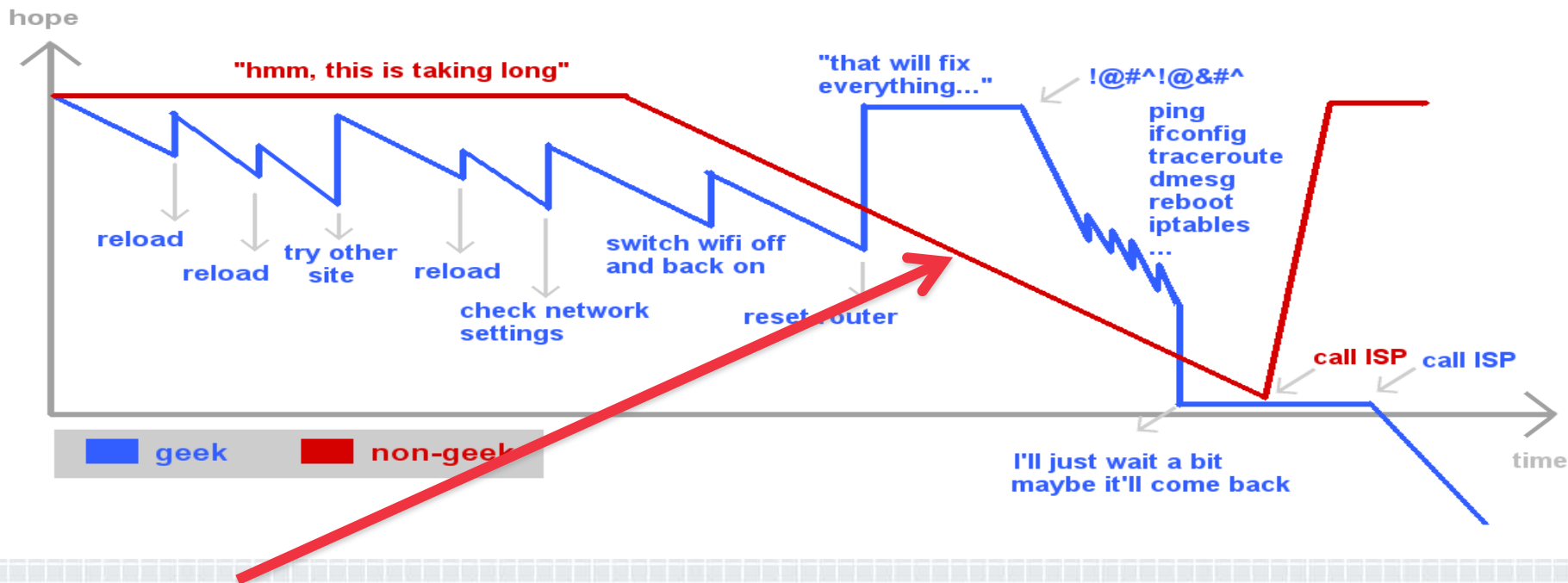


How technical are you?

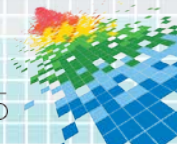


plus.google.com/+BrunoOliveira

geek vs. non-geek reaction to flaky internet connection



Non-Geeks – The Beautiful People

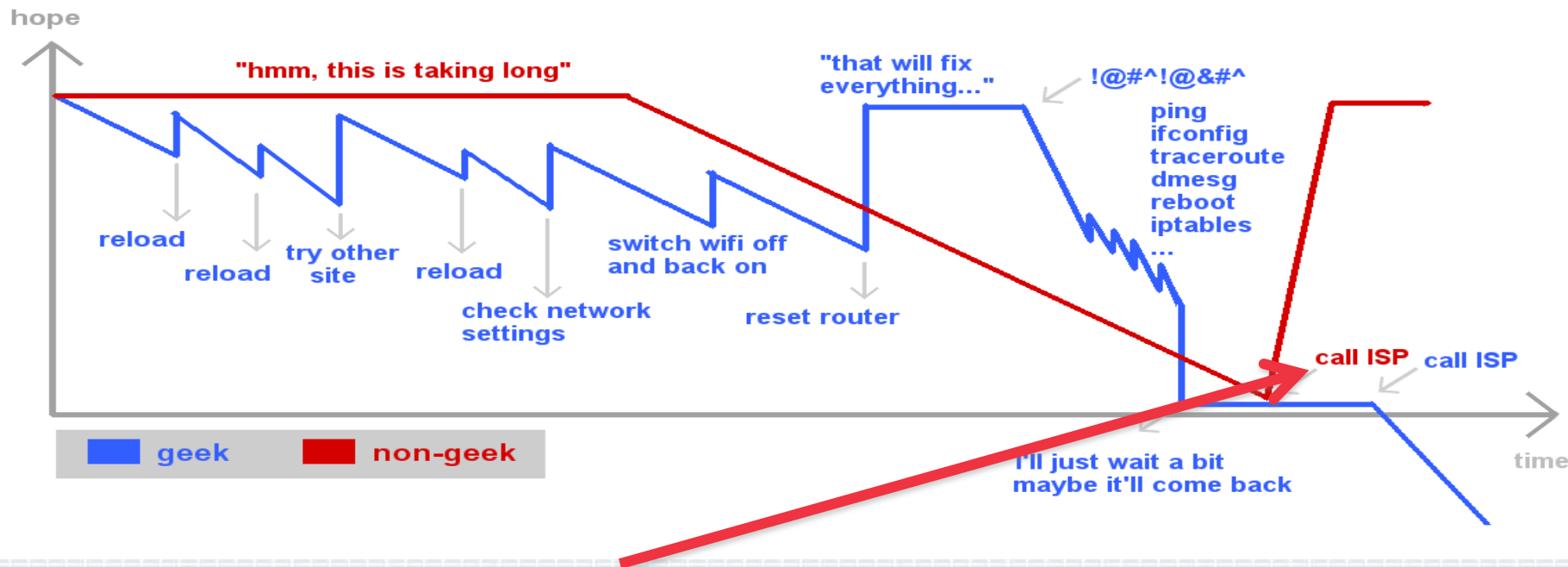


How technical are you?

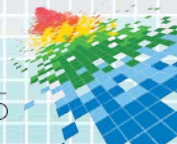


plus.google.com/+BrunoOliveira

geek vs. non-geek reaction to flaky internet connection



Non-Geeks – The Beautiful People

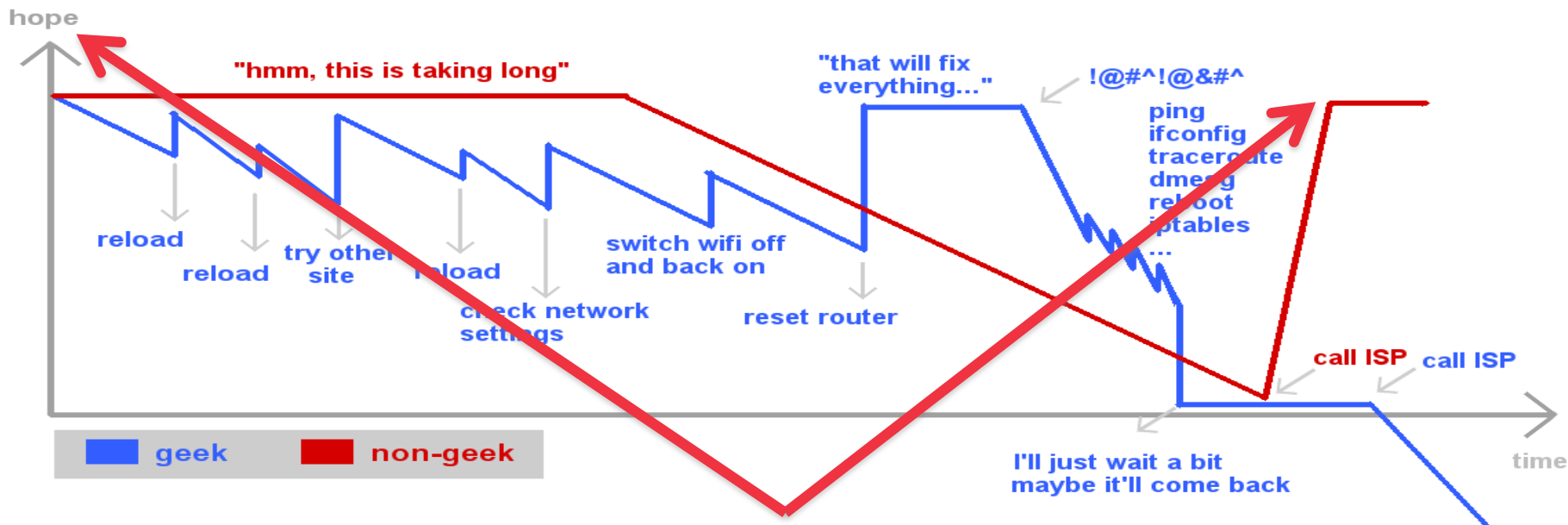


How technical are you?

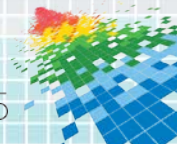


plus.google.com/+BrunoOliveira

geek vs. non-geek reaction to flaky internet connection



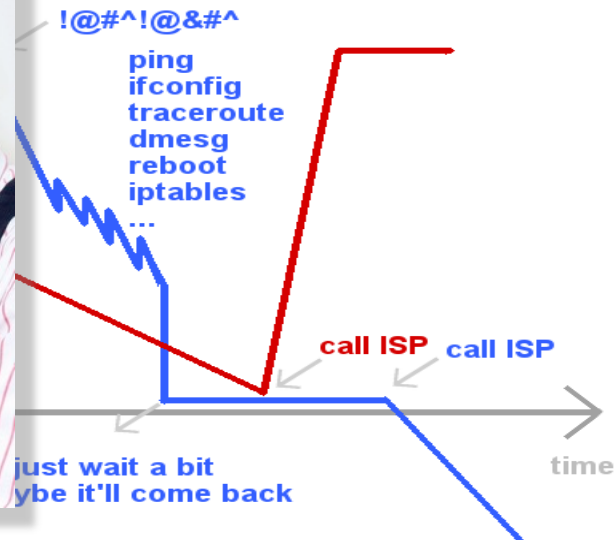
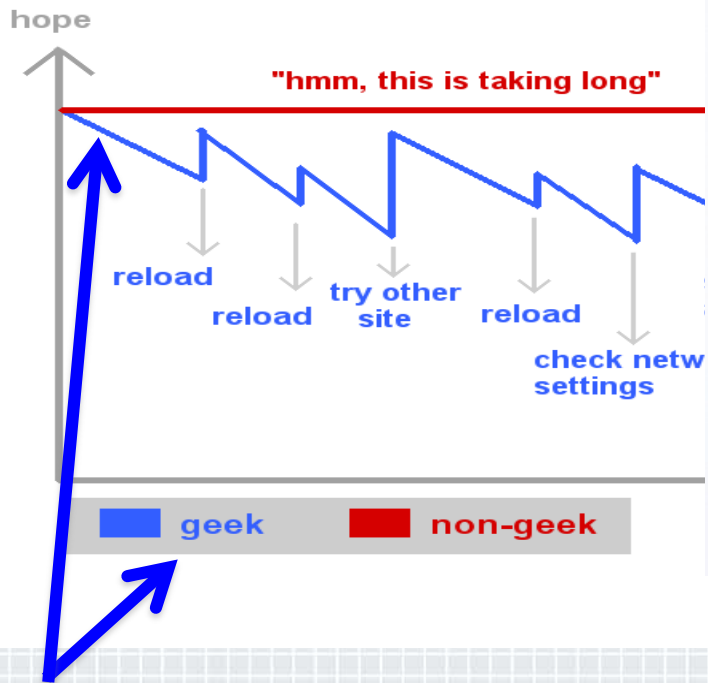
Non-Geeks – The Beautiful People



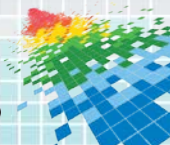
How technical are you?

geek vs. non-geek reaction to flaky internet connection

plus.google.com/+BrunoOliveira



Geeks – My Peeps

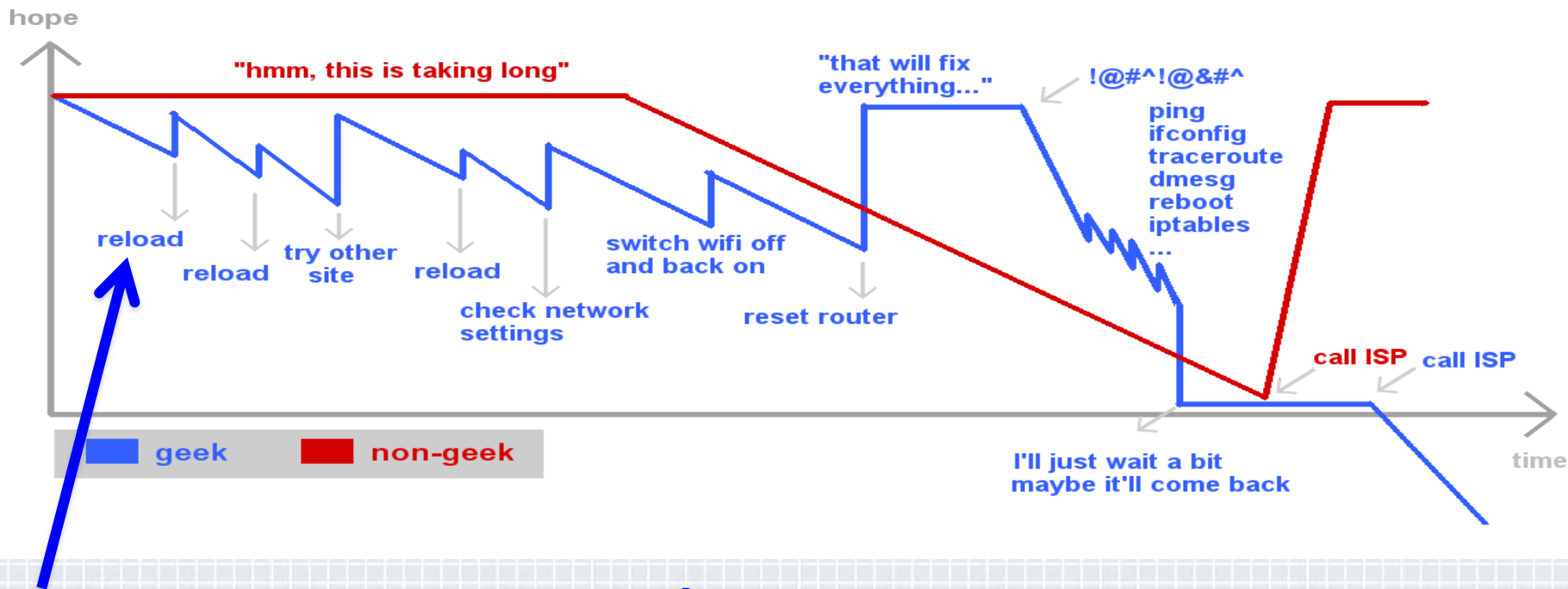


How technical are you?

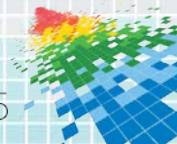


geek vs. non-geek reaction to flaky internet connection

plus.google.com/+BrunoOliveira



Geeks – My Peeps

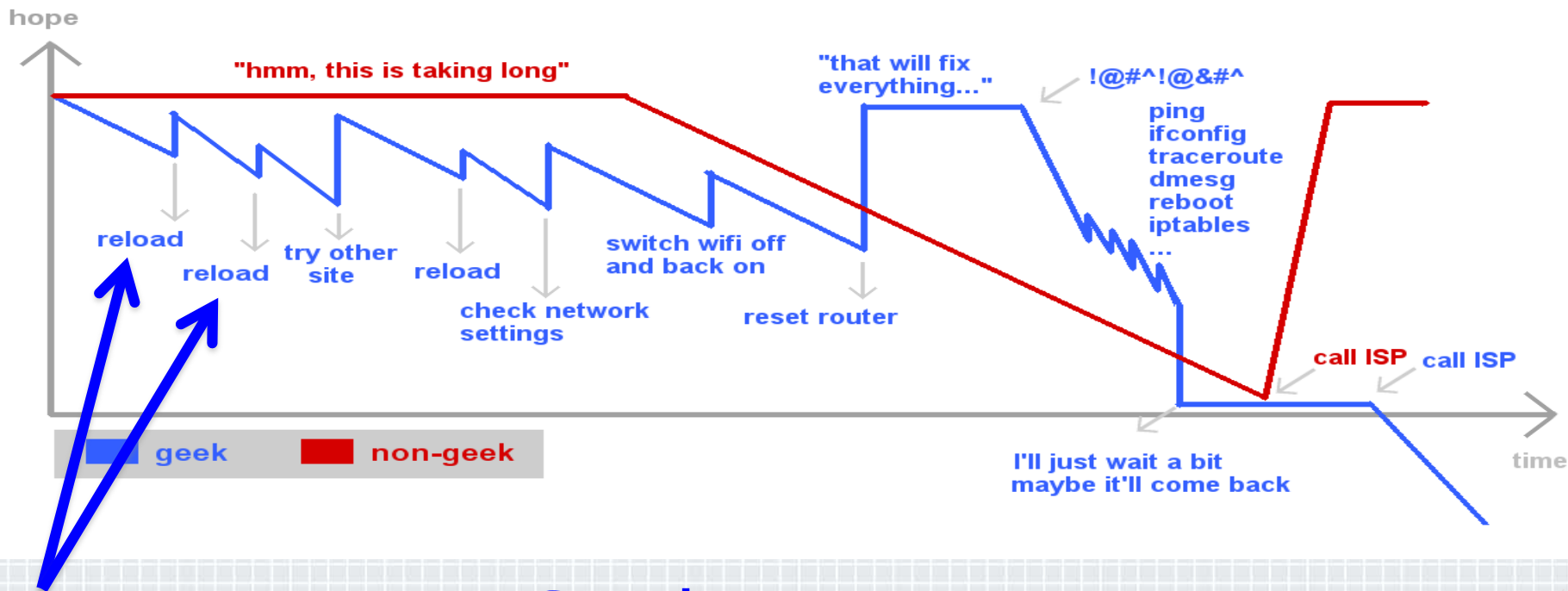


How technical are you?

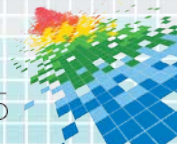


geek vs. non-geek reaction to flaky internet connection

plus.google.com/+BrunoOliveira



Geeks – My Peeps

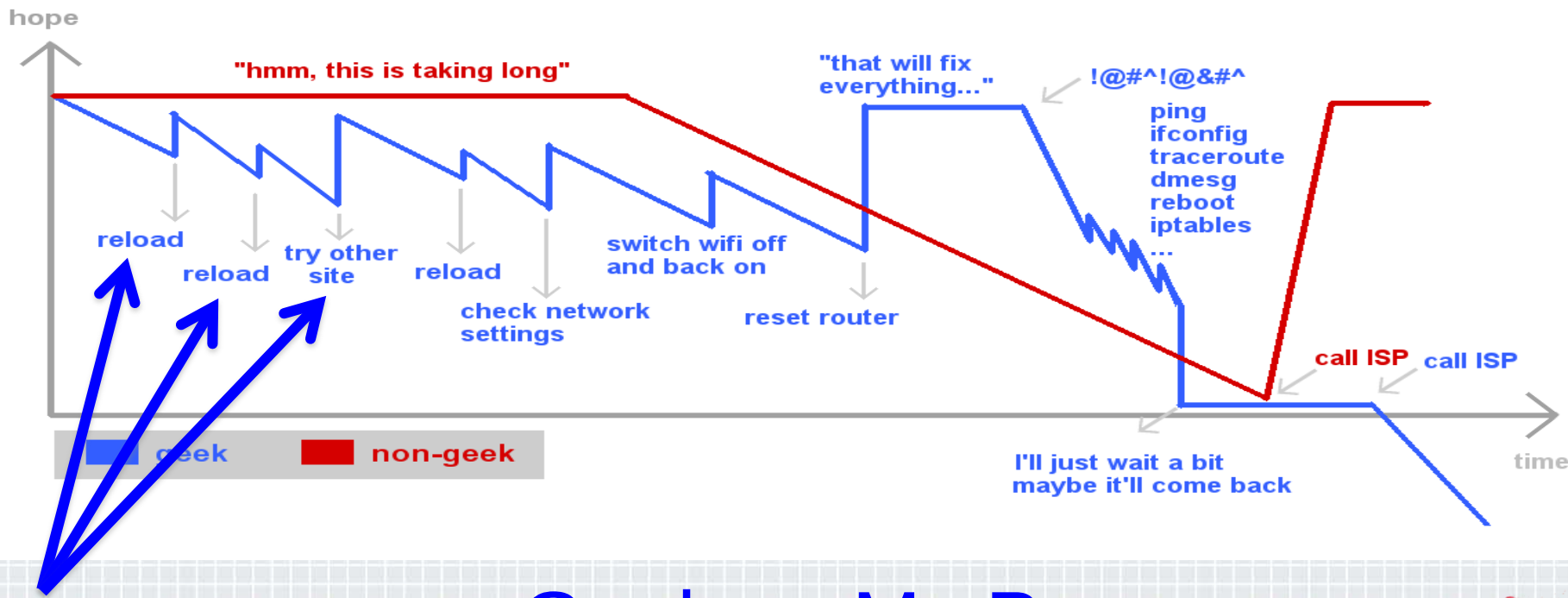


How technical are you?

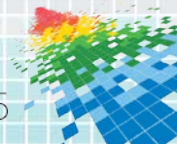


geek vs. non-geek reaction to flaky internet connection

plus.google.com/+BrunoOliveira



Geeks – My Peeps

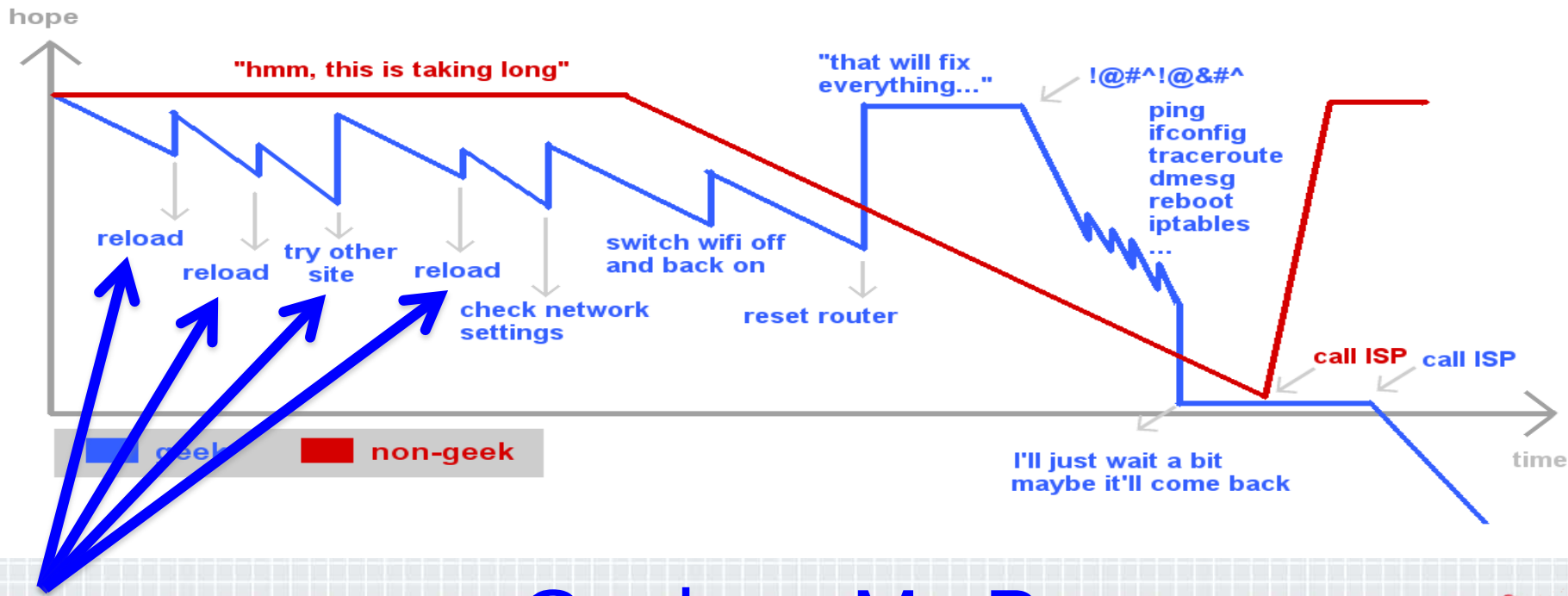


How technical are you?

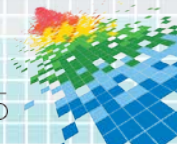


geek vs. non-geek reaction to flaky internet connection

plus.google.com/+BrunoOliveira



Geeks – My Peeps

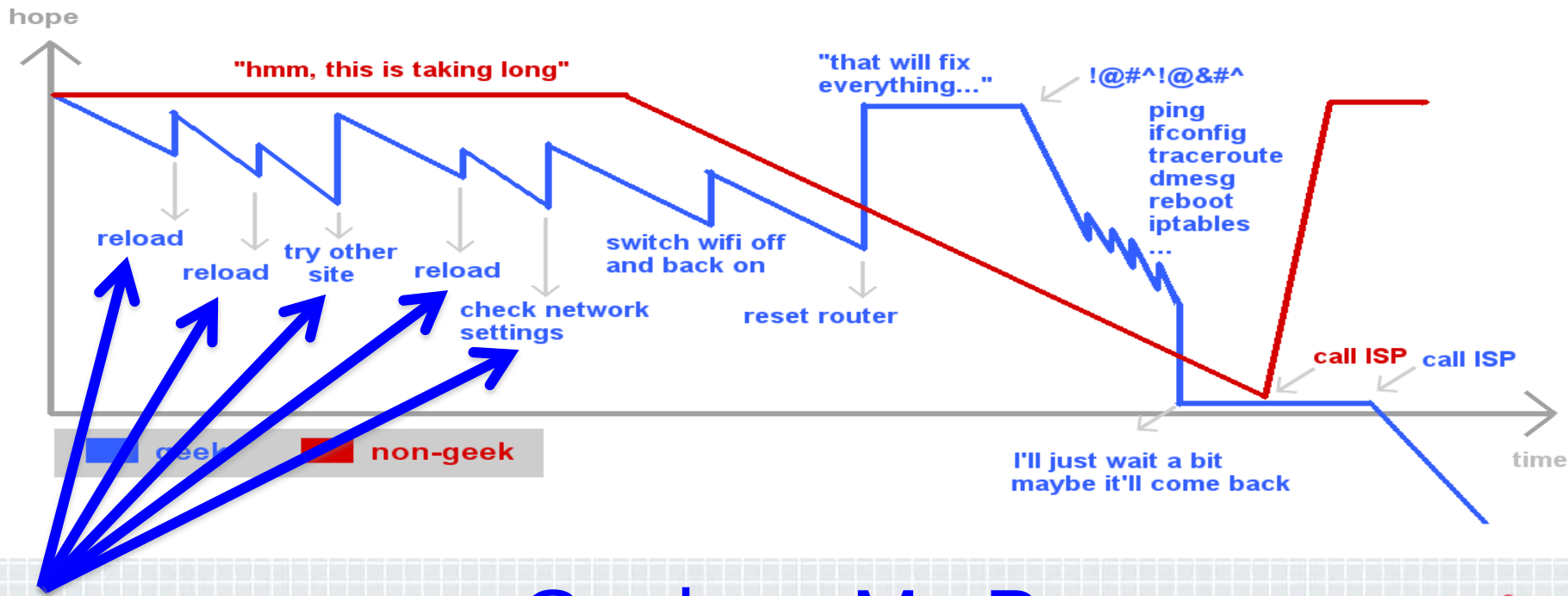


How technical are you?

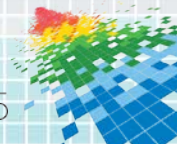


geek vs. non-geek reaction to flaky internet connection

plus.google.com/+BrunoOliveira



Geeks – My Peeps

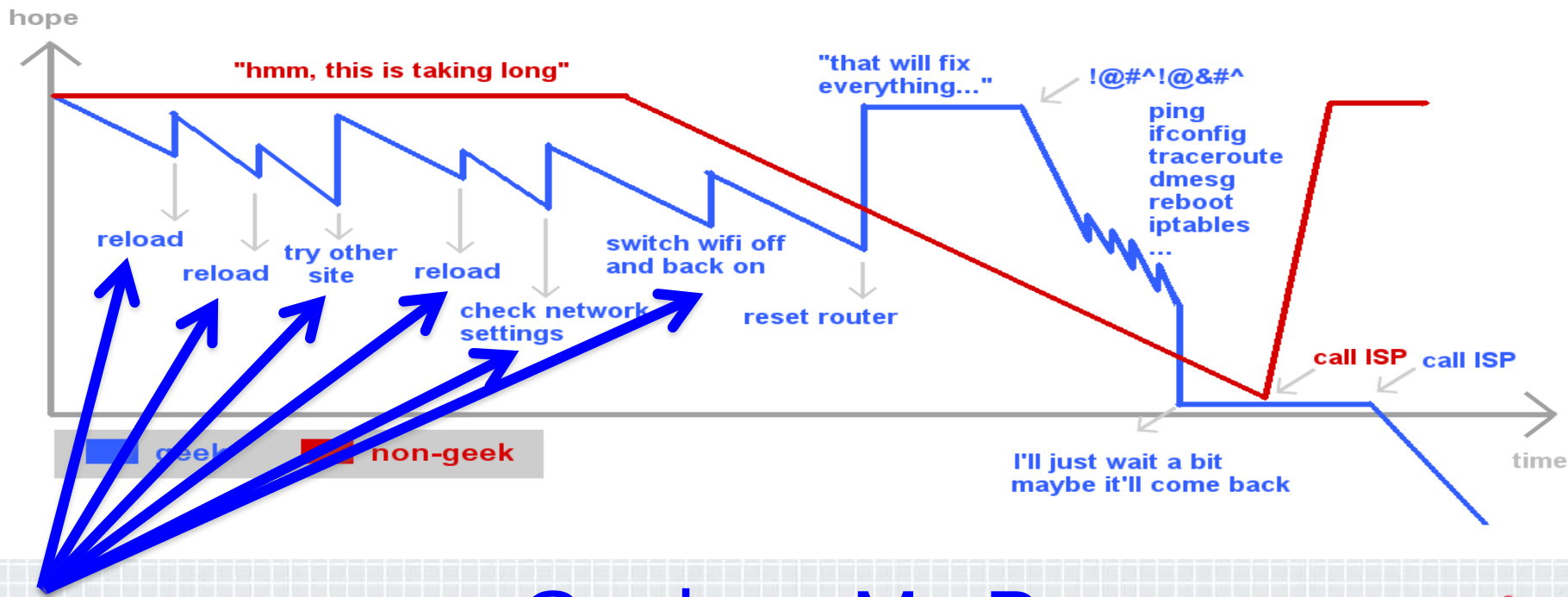


How technical are you?

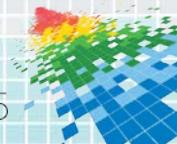


geek vs. non-geek reaction to flaky internet connection

plus.google.com/+BrunoOliveira



Geeks – My Peeps

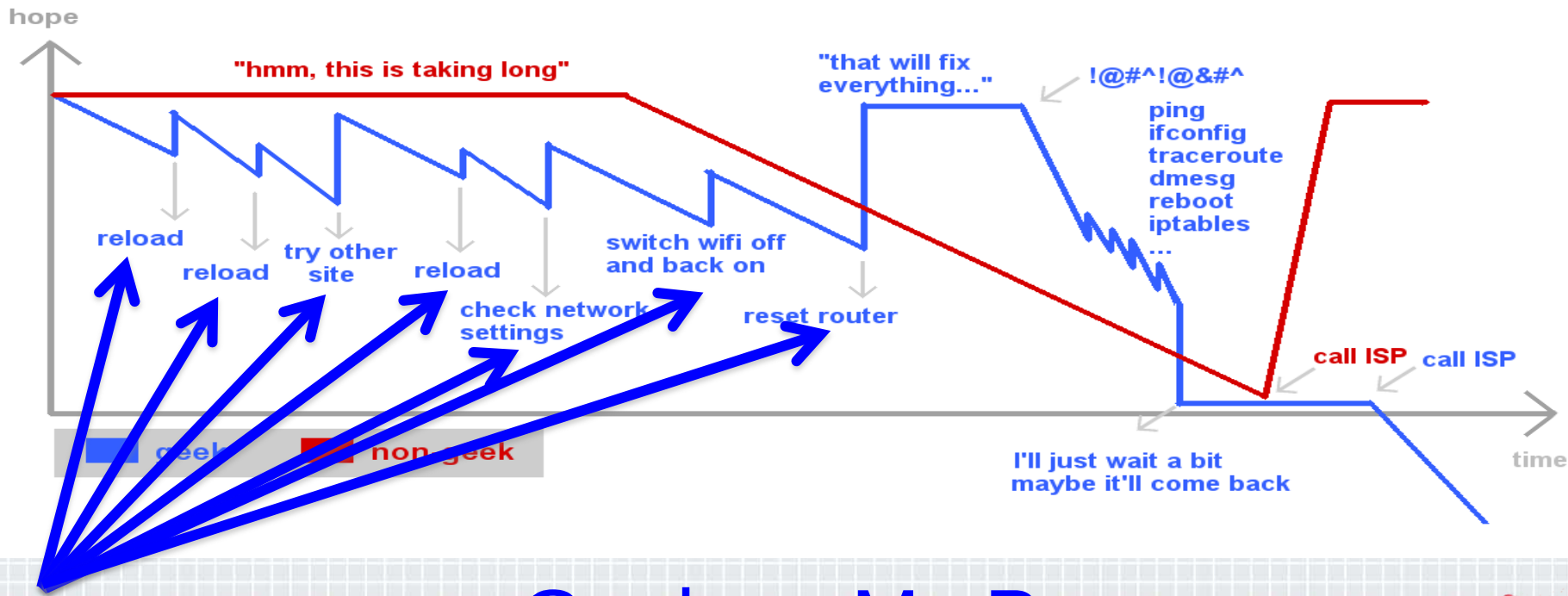


How technical are you?

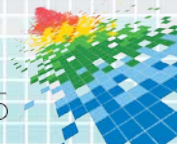


geek vs. non-geek reaction to flaky internet connection

plus.google.com/+BrunoOliveira



Geeks – My Peeps

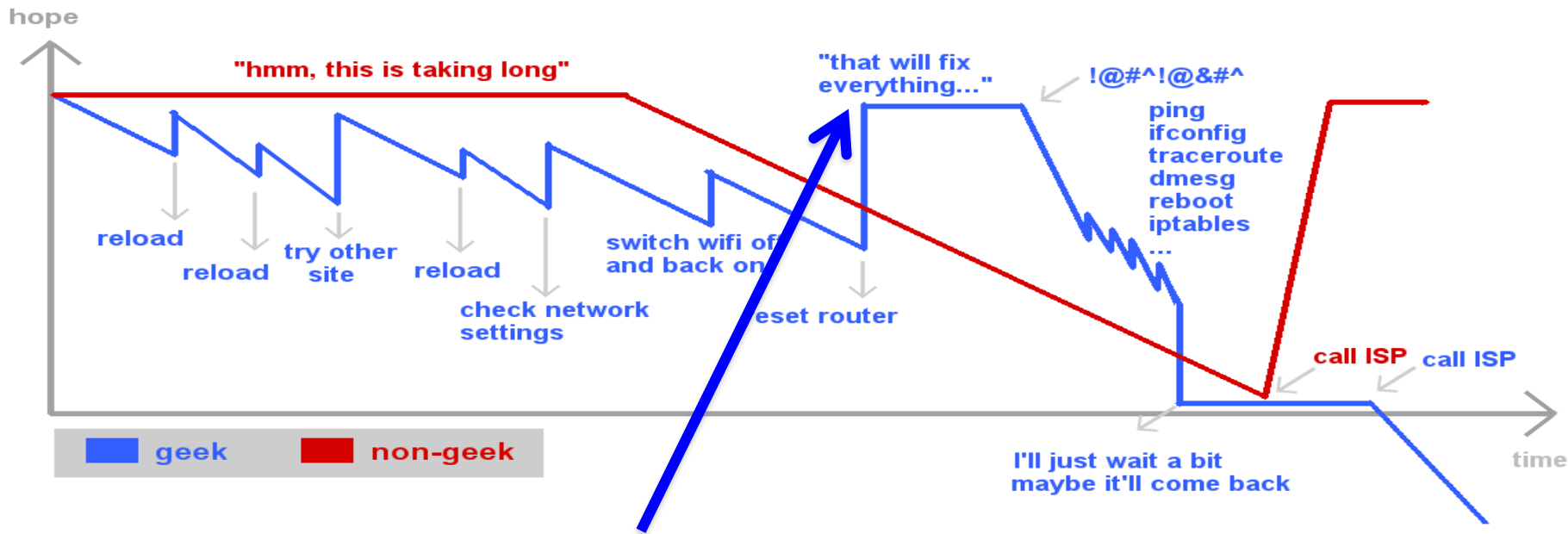


How technical are you?

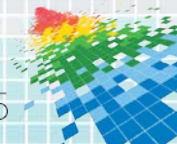


geek vs. non-geek reaction to flaky internet connection

plus.google.com/+BrunoOliveira



Geeks – My Peeps

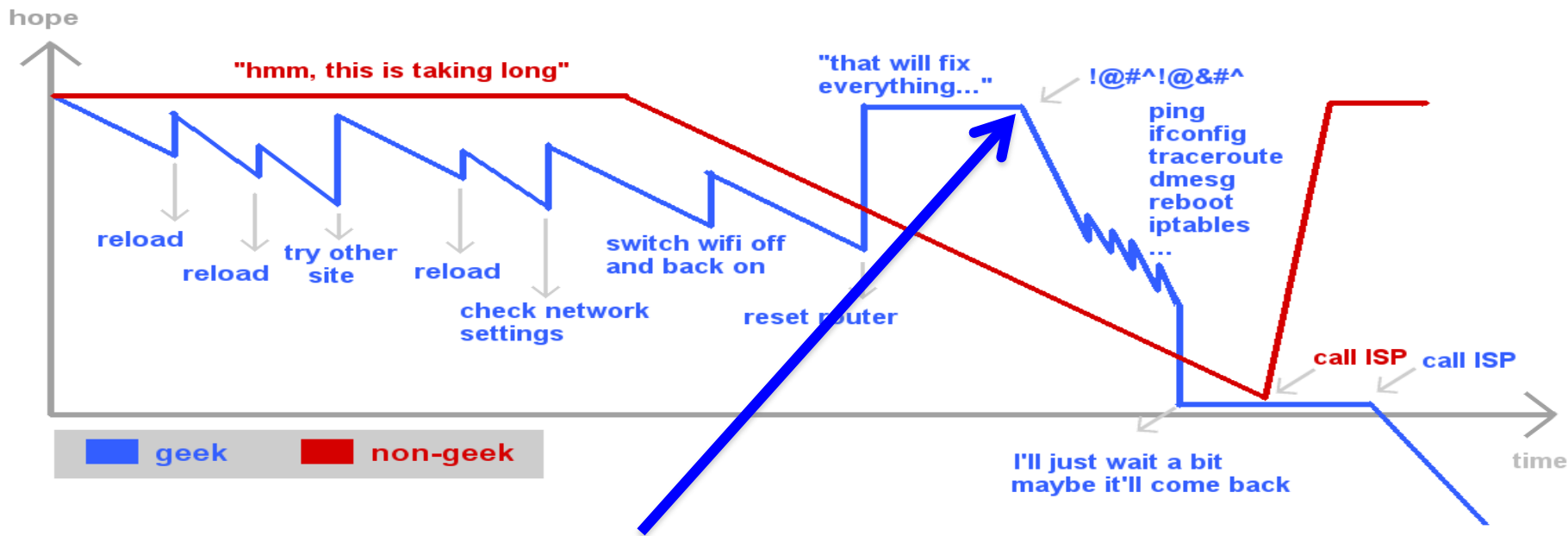


How technical are you?

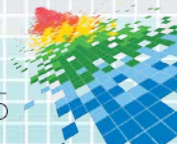


geek vs. non-geek reaction to flaky internet connection

plus.google.com/+BrunoOliveira



Geeks – My Peeps

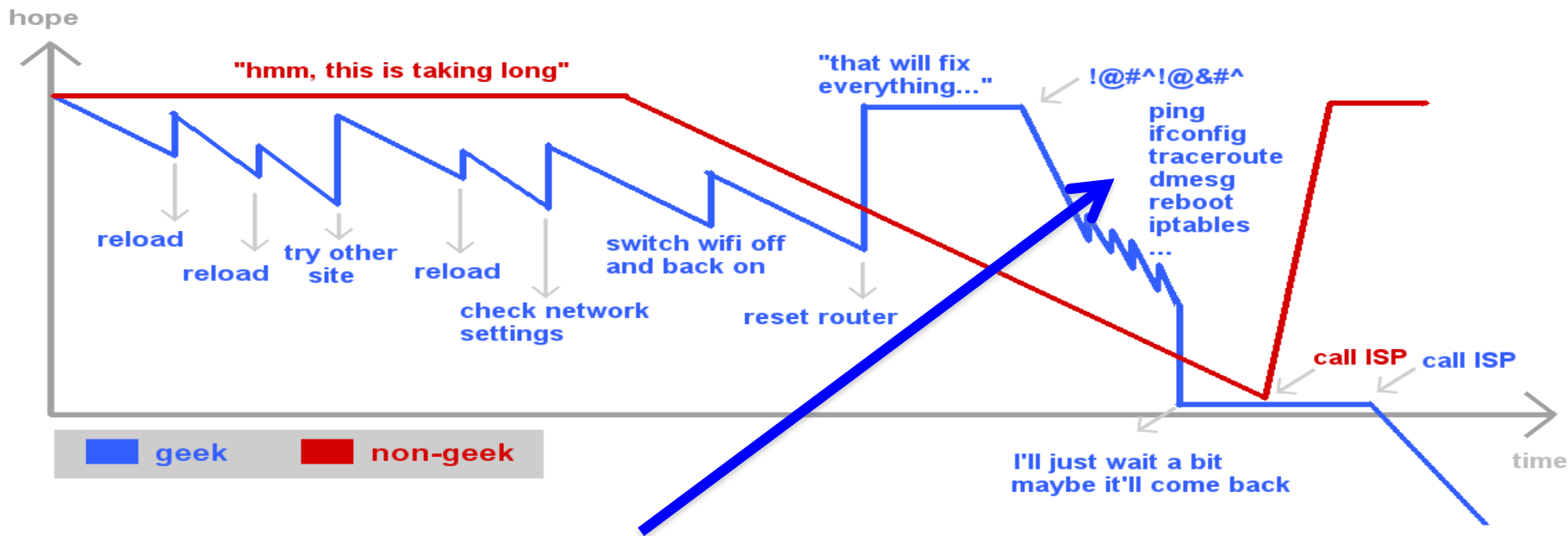


How technical are you?

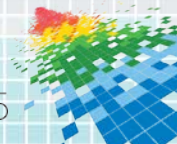


geek vs. non-geek reaction to flaky internet connection

plus.google.com/+BrunoOliveira



Geeks – My Peeps

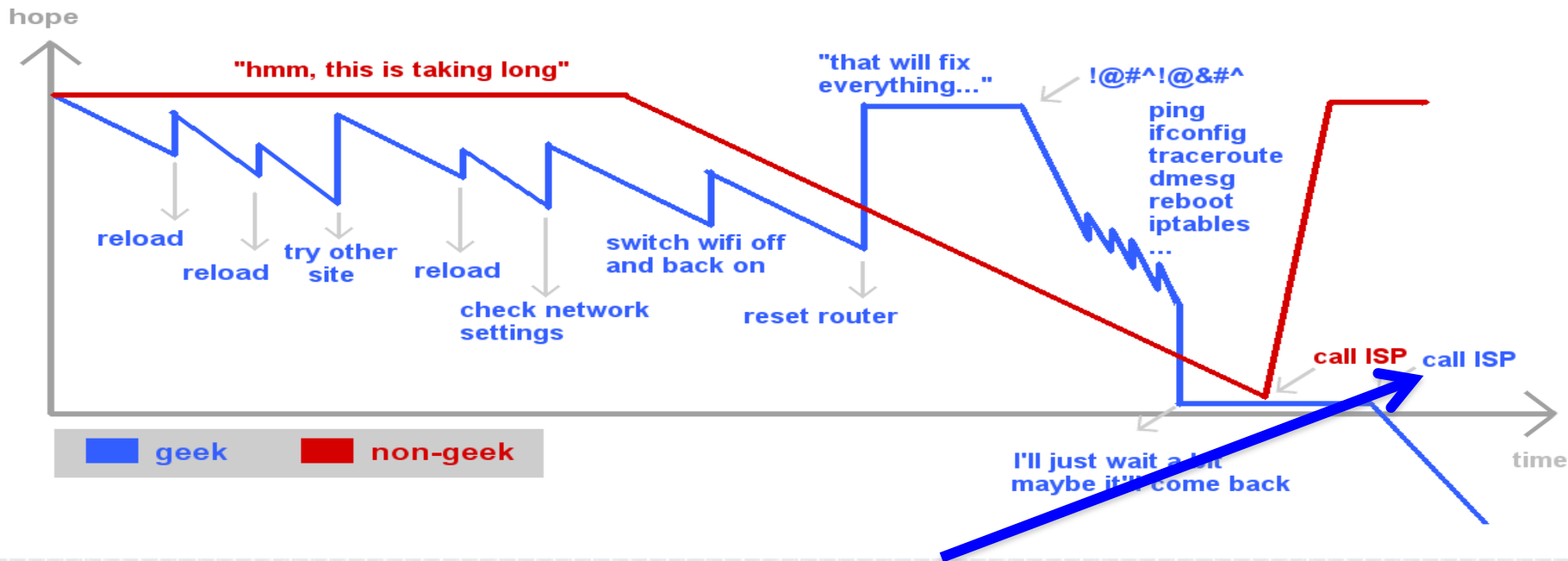


How technical are you?

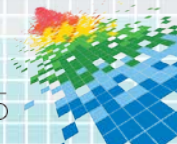


geek vs. non-geek reaction to flaky internet connection

plus.google.com/+BrunoOliveira

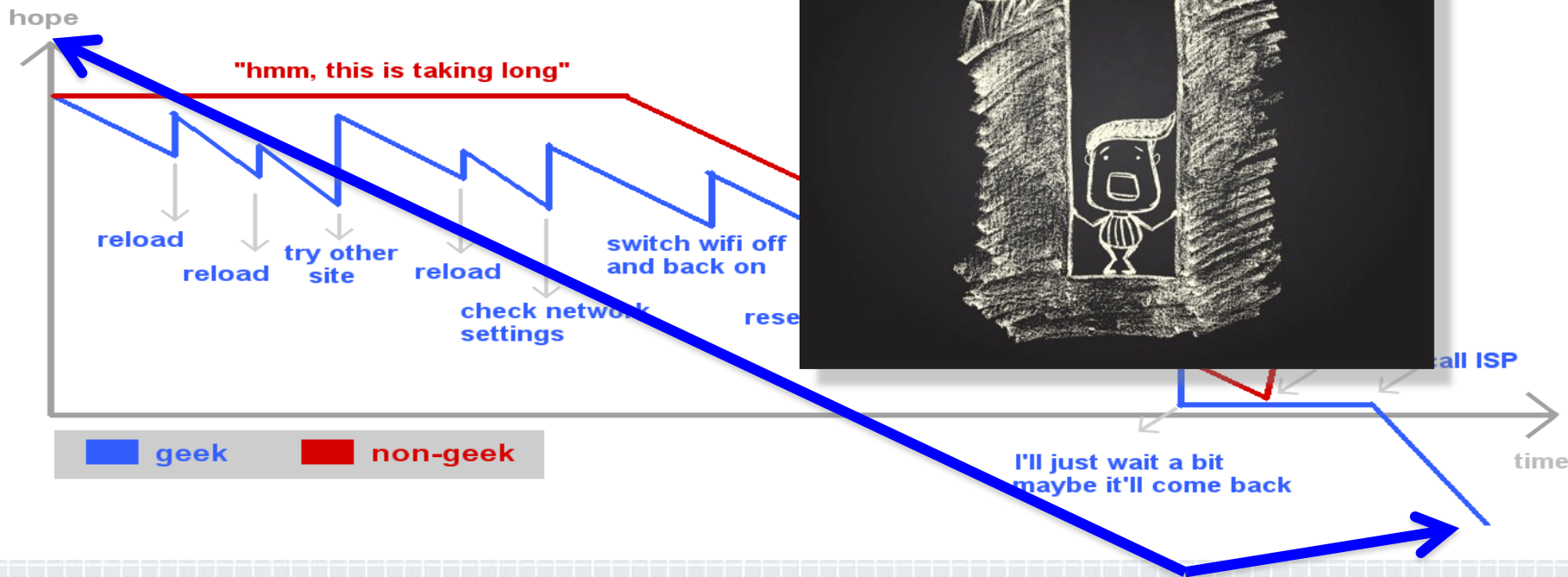


Geeks – My Peeps



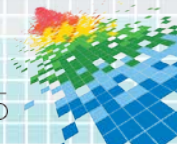
How technical are you?

geek vs. non-geek reaction to flaky internet conn



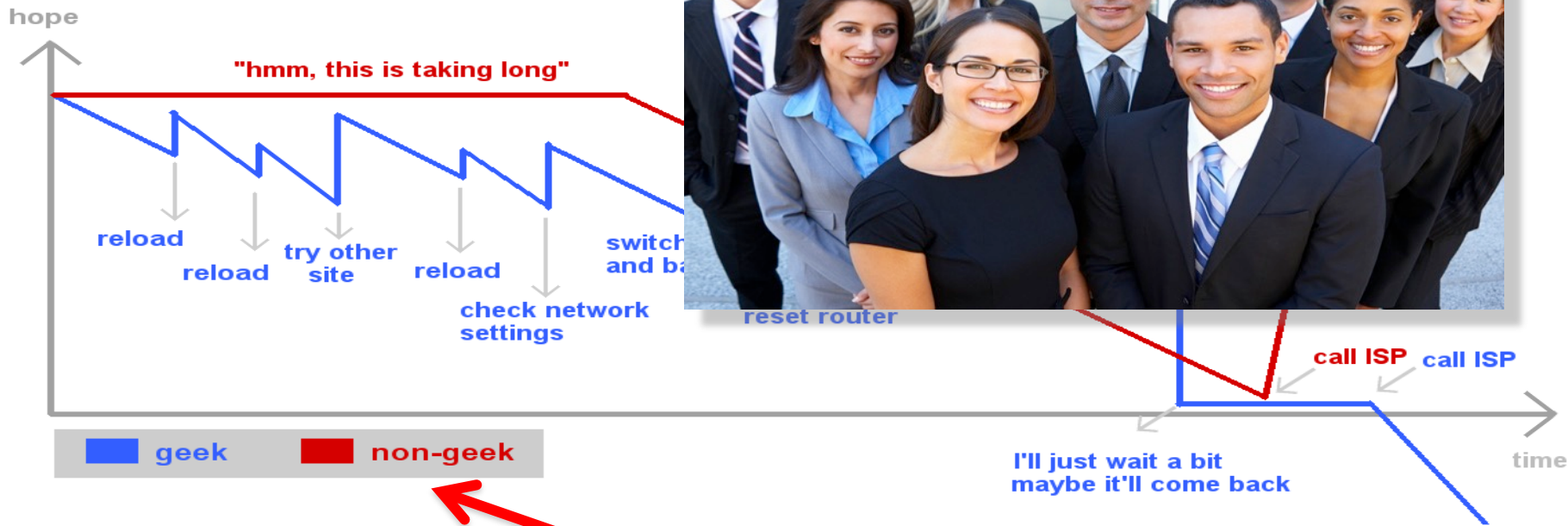
/+BrunoOliveira

Geeks – My Peeps

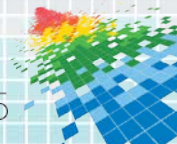


How technical are you?

geek vs. non-geek reaction to flaky internet

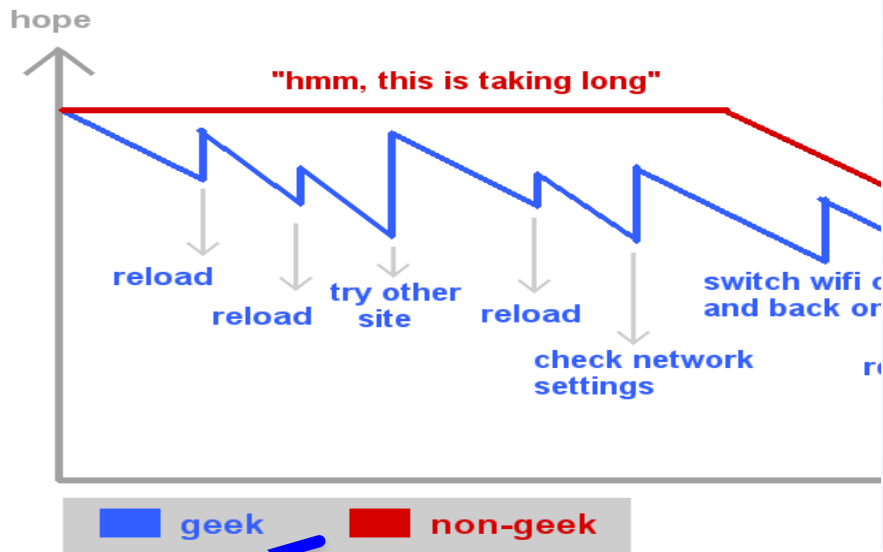


oOliveira

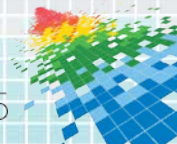
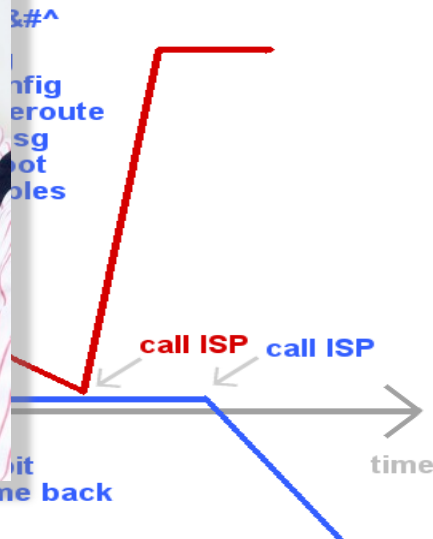


How technical are you?

geek vs. non-geek reaction to flaky internet connection



plus.google.com/+BrunoOliveira

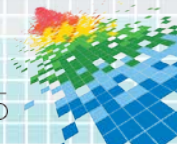


How technical are you?



FEAR UNCERTAINTY AND DOUBT COMMITTEE

STATE OF CALIFORNIA



How technical are you?

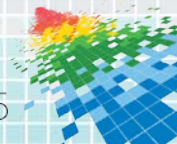


WORTHY

FEAR UNCERTAINTY AND DOUBT COMMITTEE



STATE OF CALIFORNIA



RSA®Conference2015

San Francisco | April 20-24 | Moscone Center

Setting the Stage:

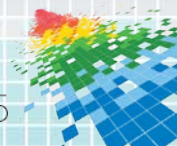
The Cybersecurity Canon
Project: Books You Should
Have Read By Now



My Library



My Library



My Blog



My Blog

VERISIGN® **iDefense®**



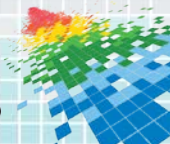
My Blog

VERISIGN® **iDefense®**



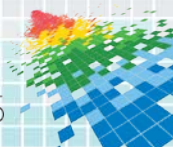
Terebrate

Piercing the fog of cyber security.



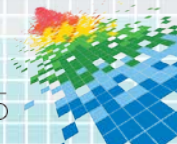
My Blog

Epitome



My Blog

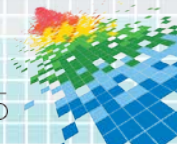
Epitome



My Blog

Epitome

History

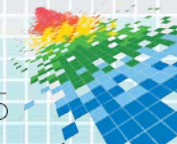


My Blog

Epitome

History

Culture



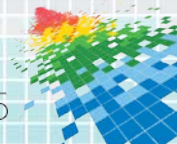
My Blog

Epitome

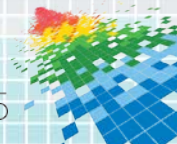
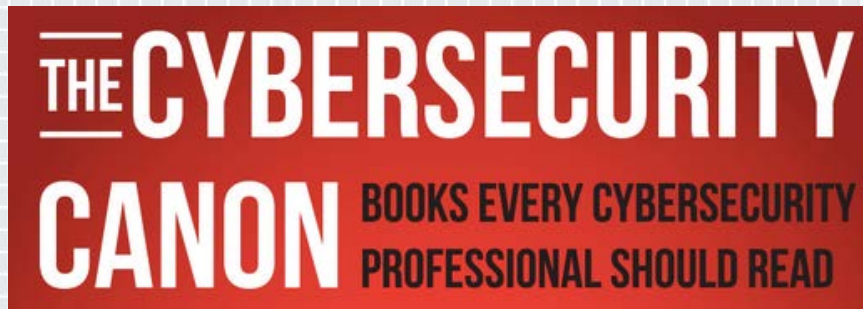
History

Culture

Best Thinking



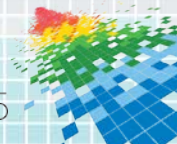
The Cybersecurity Canon



Definition of the Cyber Security Canon



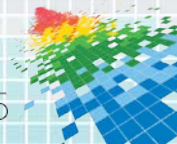
can·on
/kanən/
noun



Definition of the Cyber Security Canon

can·on
/kanən/
noun

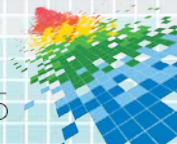
1. A **group** of literary works that are **generally accepted** as **representing a field**: *"the durable canon of American short fiction"* (William Styron).



Definition of the Cyber Security Canon

can·on
/kanən/
noun

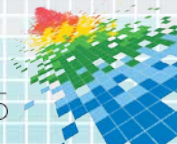
1. A **group** of literary works that are **generally accepted** as **representing a field**: *"the durable canon of American short fiction"* (William Styron).
2. A **list of writings** officially **recognized as genuine**.



Definition of the Cyber Security Canon

can·on
/kanən/
noun

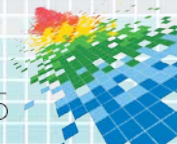
1. A **group** of literary works that are **generally accepted** as **representing a field**: *"the durable canon of American short fiction" (William Styron).*
2. A **list of writings** officially **recognized as genuine**.
3. **The list of works considered** to be **permanently established** as being of the **highest quality**: *"Hopkins was firmly established in the canon of English poetry."*



Definition of the Cyber Security Canon

can·on
/kanən/
noun

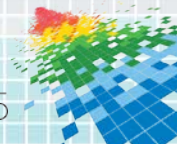
1. A **group** of literary works that are **generally accepted** as **representing a field**: *"the durable canon of American short fiction" (William Styron).*
2. A **list of writings** officially **recognized as genuine**.
3. **The list of works considered** to be **permanently established** as being of the **highest quality**: *"Hopkins was firmly established in the canon of English poetry."*



Definition of the Cyber Security Canon

can·on
/kanən/
noun

1. A **group** of literary works that are **generally accepted** as **representing a field**: *"the durable canon of American short fiction" (William Styron).*
2. A **list of writings** officially **recognized as genuine**.
3. **The list of works considered** to be **permanently established** as being of the **highest quality**: *"Hopkins was firmly established in the canon of English poetry."*



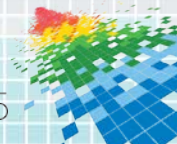
Definition of the Cyber Security Canon

can·on
/kanən/
noun

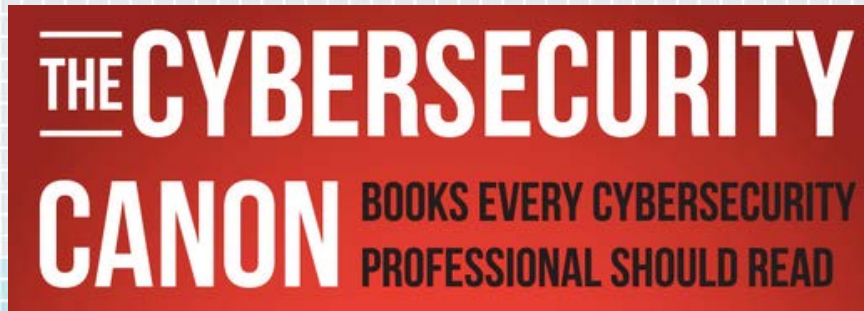
1. A **group** of literary works that are **generally accepted** as **representing a field**: *"the durable canon of American short fiction"* (William Styron).
2. A **list of writings** officially **recognized as genuine**.
3. **The list of works considered** to be **permanently established** as being of the **highest quality**: *"Hopkins was firmly established in the canon of English poetry."*



For Cybersecurity Books



The Cybersecurity Canon First Award



The Cybersecurity Canon First Award



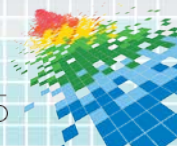
CYBERSECURITY CANON AWARD WINNERS

2014 AWARD WINNER

Cyber Hactivism:
We Are Anonymous



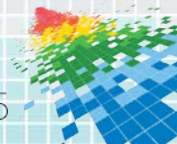
Watch Palo Alto Networks' CSO Rick Howard present the inaugural Cybersecurity Canon award to Parag Olson, author of "We Are Anonymous"



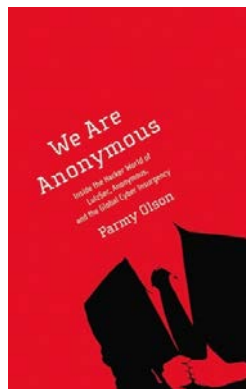
The Cybersecurity Canon Committee



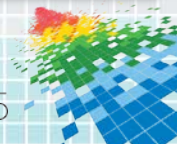
THE CYBERSECURITY
CANON BOOKS EVERY CYBERSECURITY
PROFESSIONAL SHOULD READ



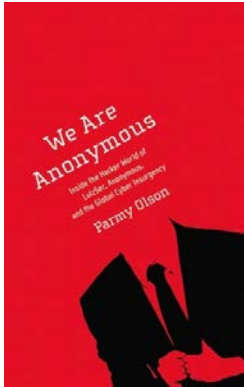
2014 Inductee



THE CYBERSECURITY
CANON BOOKS EVERY CYBERSECURITY
PROFESSIONAL SHOULD READ



2014 Inductee

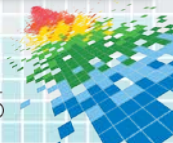


MARCH 2014

Author Parmy Olson was inducted into the Palo Alto Networks Cybersecurity Canon for her novel, *We Are Anonymous*.

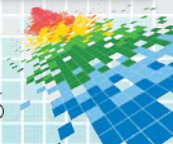


THE CYBERSECURITY
CANON BOOKS EVERY CYBERSECURITY
PROFESSIONAL SHOULD READ

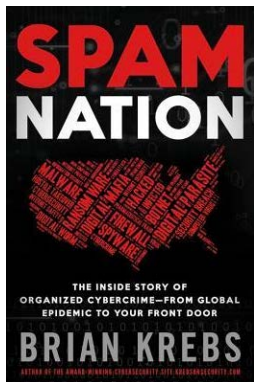


2015 Inductees

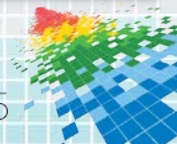
THE CYBERSECURITY
CANON BOOKS EVERY CYBERSECURITY
PROFESSIONAL SHOULD READ



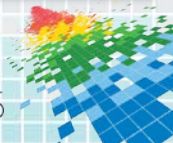
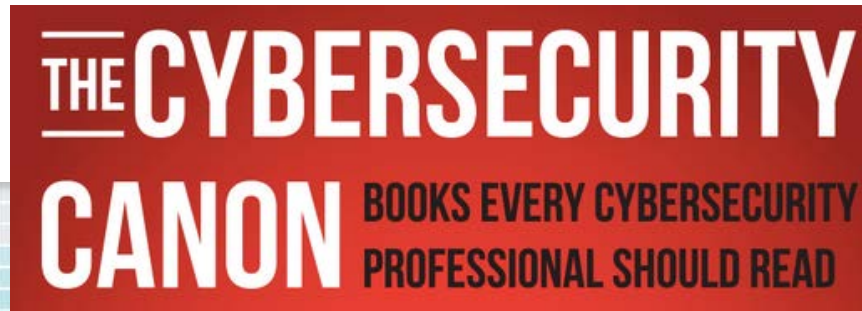
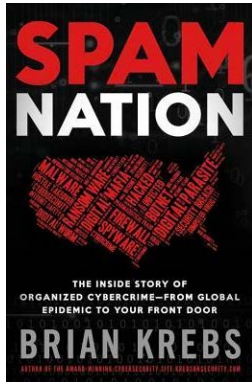
2015 Inductees



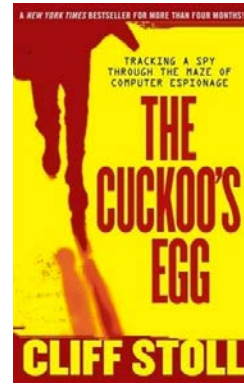
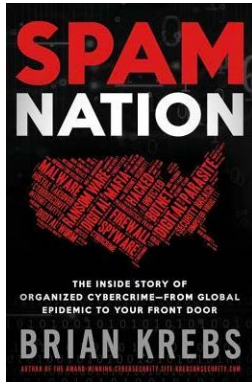
THE CYBERSECURITY
CANON BOOKS EVERY CYBERSECURITY
PROFESSIONAL SHOULD READ



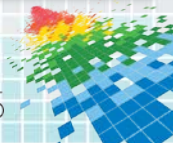
2015 Inductees



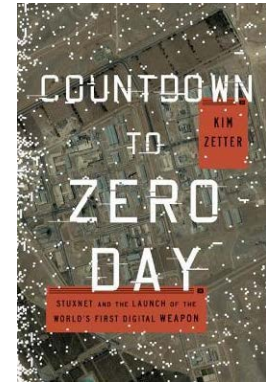
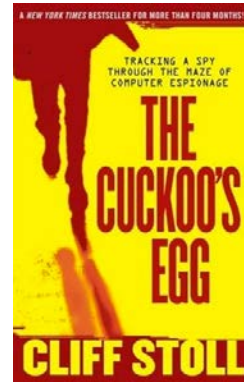
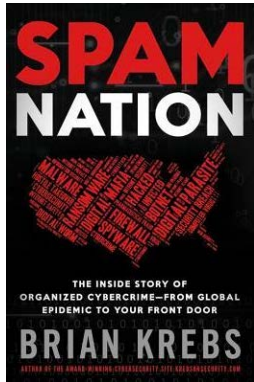
2015 Inductees



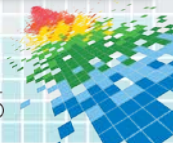
THE CYBERSECURITY
CANON BOOKS EVERY CYBERSECURITY
PROFESSIONAL SHOULD READ



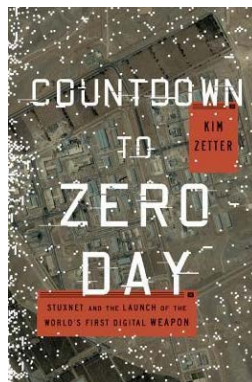
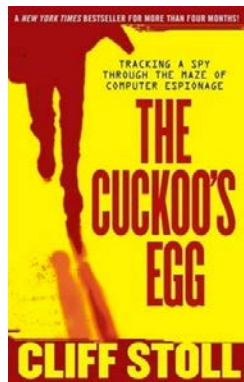
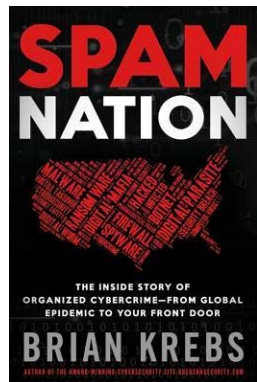
2015 Inductees



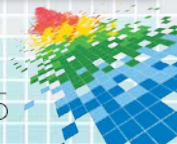
THE CYBERSECURITY
CANON BOOKS EVERY CYBERSECURITY
PROFESSIONAL SHOULD READ



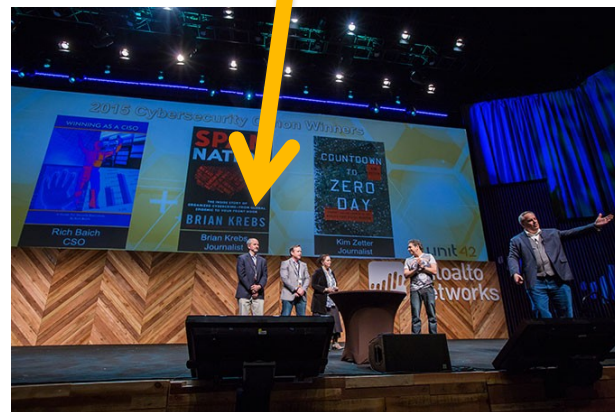
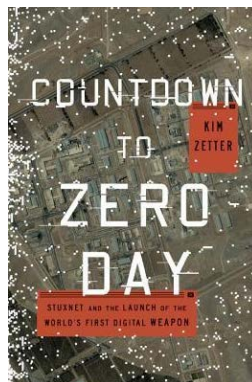
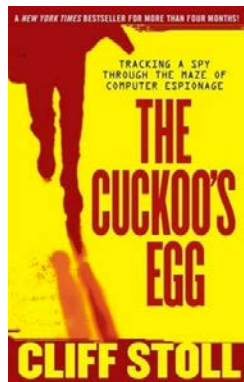
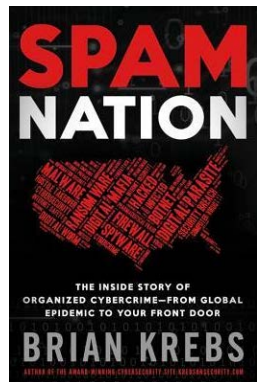
2015 Inductees



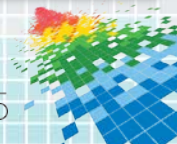
THE CYBERSECURITY CANON BOOKS EVERY CYBERSECURITY PROFESSIONAL SHOULD READ



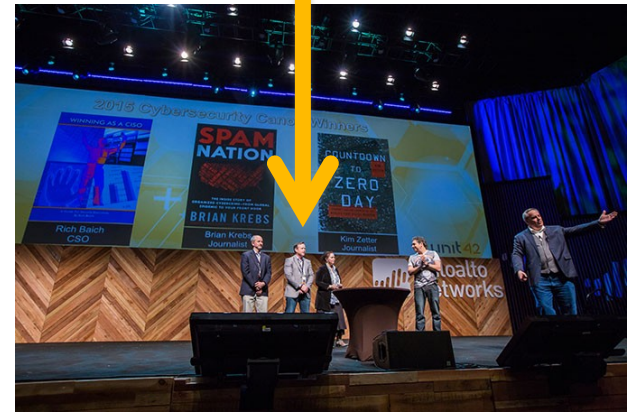
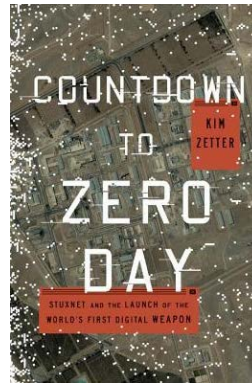
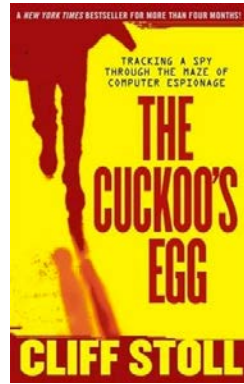
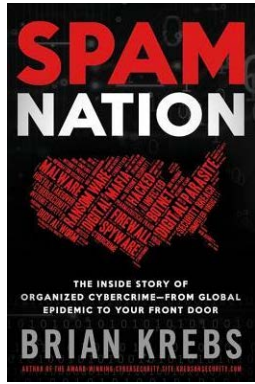
2015 Inductees



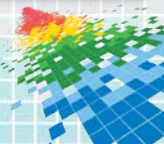
THE CYBERSECURITY
CANON BOOKS EVERY CYBERSECURITY
PROFESSIONAL SHOULD READ



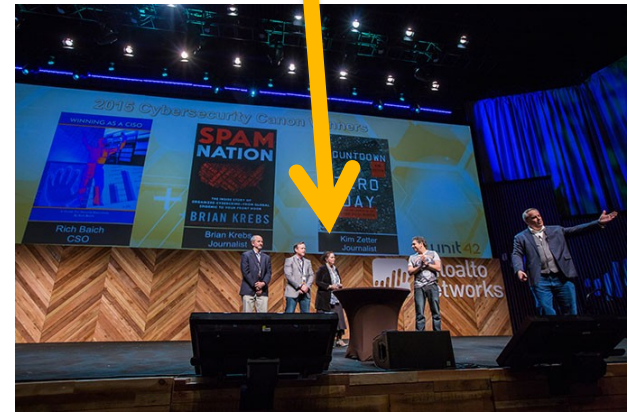
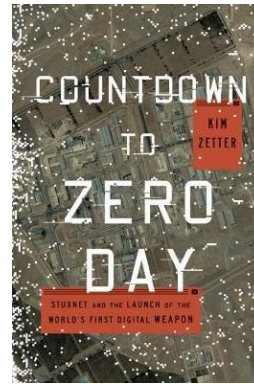
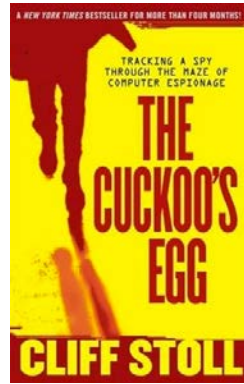
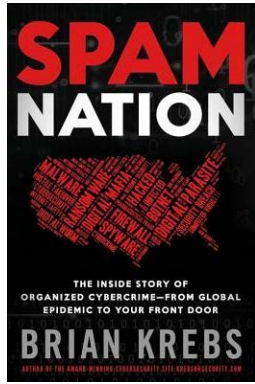
2015 Inductees



THE CYBERSECURITY
CANON BOOKS EVERY CYBERSECURITY
PROFESSIONAL SHOULD READ

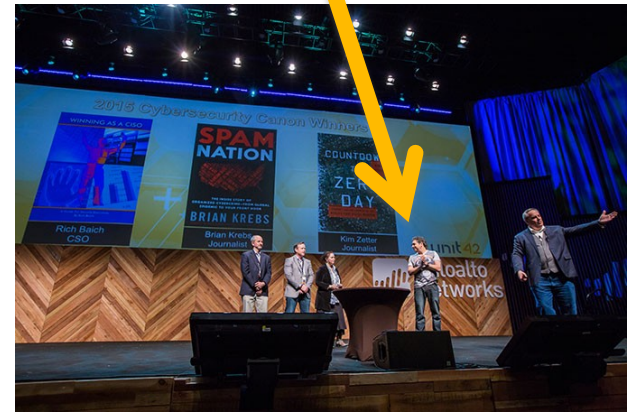
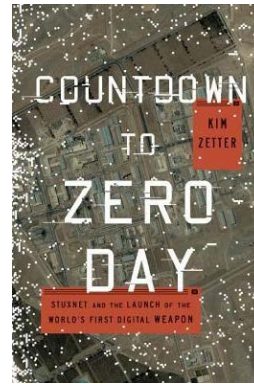
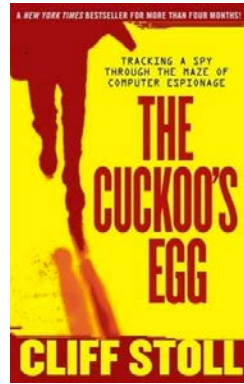
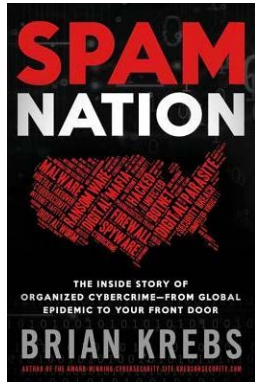


2015 Inductees



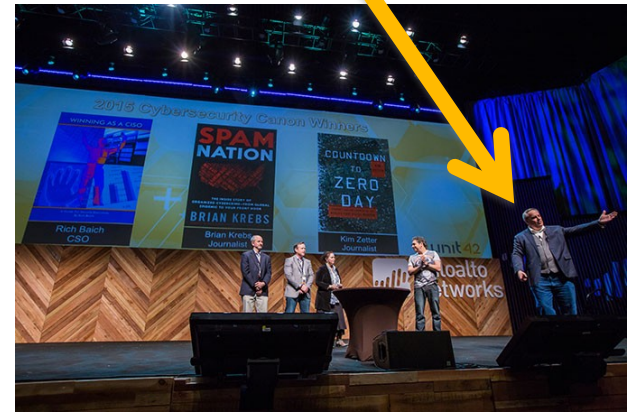
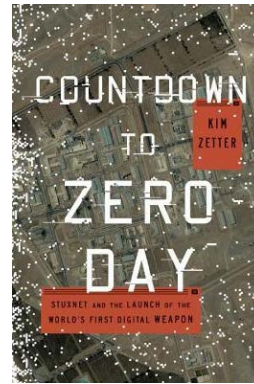
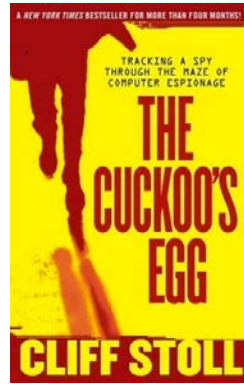
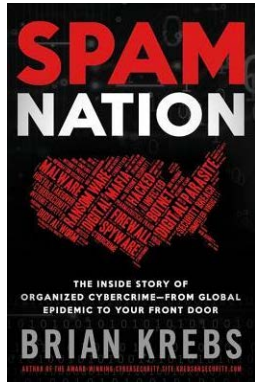
THE CYBERSECURITY
CANON BOOKS EVERY CYBERSECURITY
PROFESSIONAL SHOULD READ

2015 Inductees



THE CYBERSECURITY
CANON BOOKS EVERY CYBERSECURITY
PROFESSIONAL SHOULD READ

2015 Inductees



THE CYBERSECURITY CANON BOOKS EVERY CYBERSECURITY PROFESSIONAL SHOULD READ

San Francisco | April 20-24 | Moscone Center

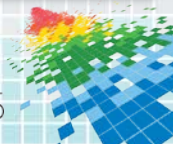
Today:

2016 Cybersecurity Canon Candidates



2016 Candidates

THE CYBERSECURITY
CANON BOOKS EVERY CYBERSECURITY
PROFESSIONAL SHOULD READ

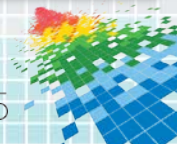


Cyber Crime

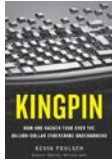


2016 Candidates

THE CYBERSECURITY
CANON BOOKS EVERY CYBERSECURITY
PROFESSIONAL SHOULD READ

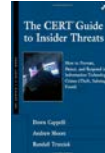
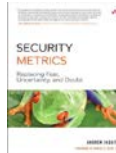
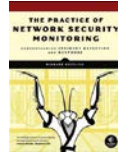


Cyber Crime

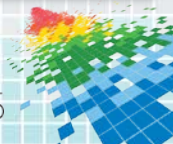


2016 Candidates

Technical



THE CYBERSECURITY
CANON BOOKS EVERY CYBERSECURITY
PROFESSIONAL SHOULD READ

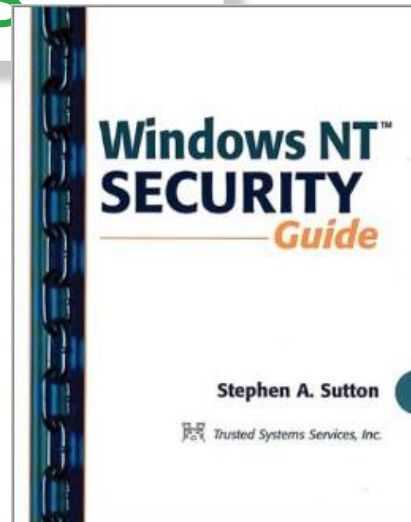
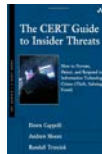
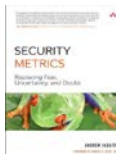
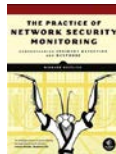


Cyber Crime

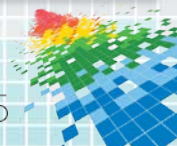


2016 Candidates

Technical



THE CYBERSECURITY
CANON BOOKS EVERY CYBERSECURITY
PROFESSIONAL SHOULD READ



Cyber Crime



2016 Candidates

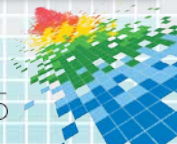
Cyber Warfare



Technical



THE CYBERSECURITY
CANON BOOKS EVERY CYBERSECURITY
PROFESSIONAL SHOULD READ

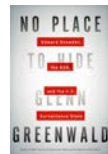


Cyber Crime

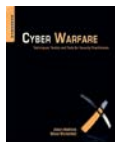
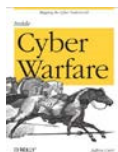
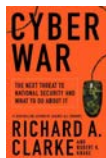


2016 Candidates

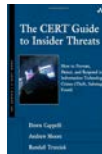
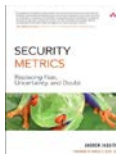
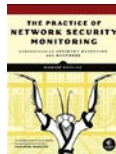
Cyber History and Culture



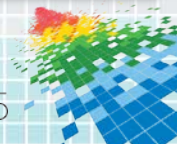
Cyber Warfare



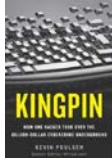
Technical



**THE CYBERSECURITY
CANON** BOOKS EVERY CYBERSECURITY
PROFESSIONAL SHOULD READ

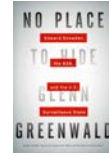
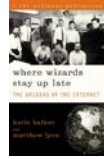
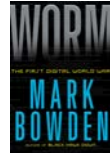


Cyber Crime

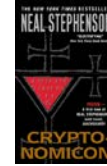


2016 Candidates

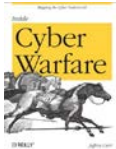
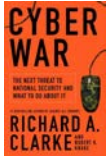
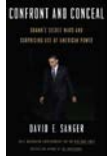
Cyber History and Culture



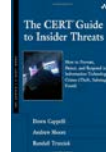
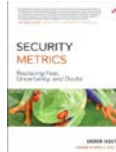
Novels



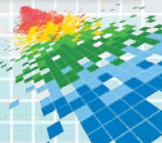
Cyber Warfare



Technical



THE CYBERSECURITY CANON BOOKS EVERY CYBERSECURITY PROFESSIONAL SHOULD READ



RSACConference2015

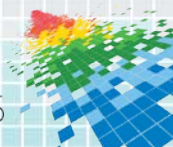
San Francisco | April 20-24 | Moscone Center

6 Books:

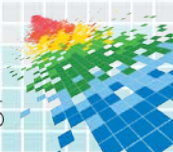
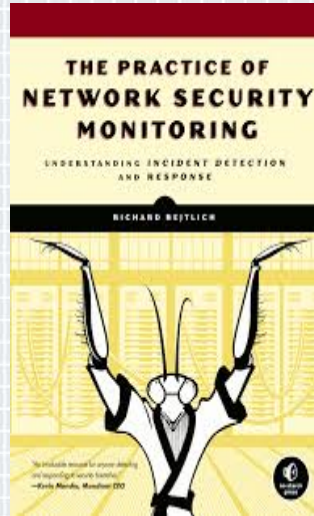
2016 Cybersecurity Canon Candidates



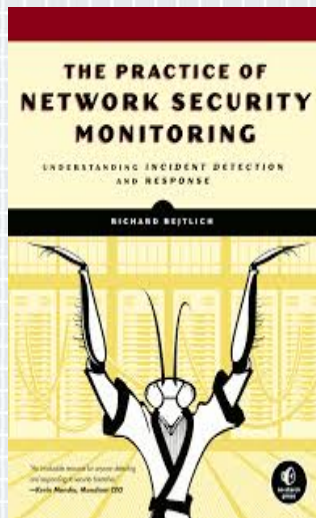
Technical



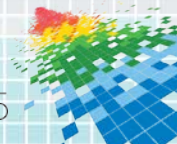
Technical



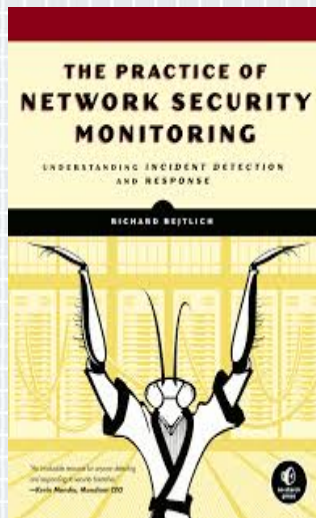
Technical



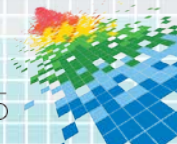
Richard Bejtlich



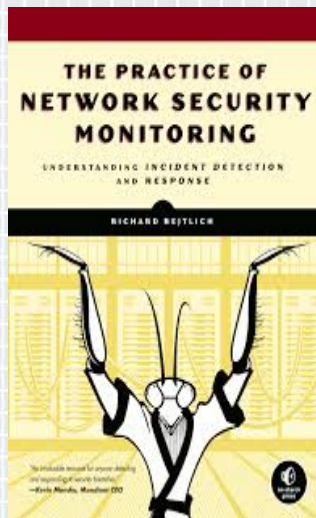
Technical



Richard Bejtlich



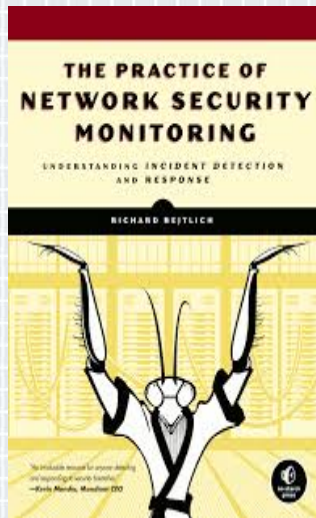
Technical



Richard Bejtlich

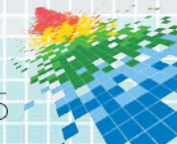


Technical

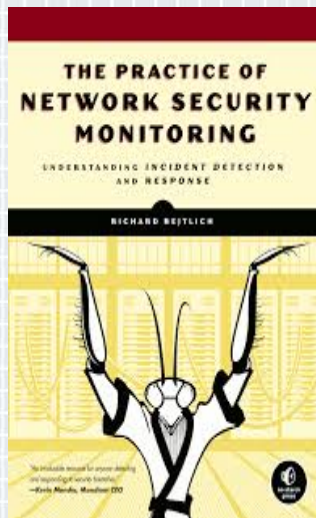


Richard Bejtlich

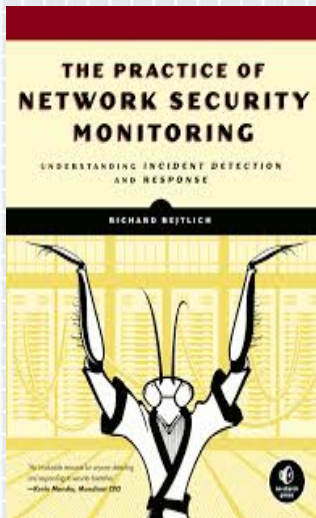
ManTech
International Corporation®



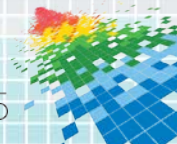
Technical



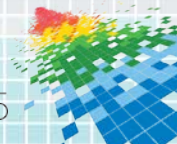
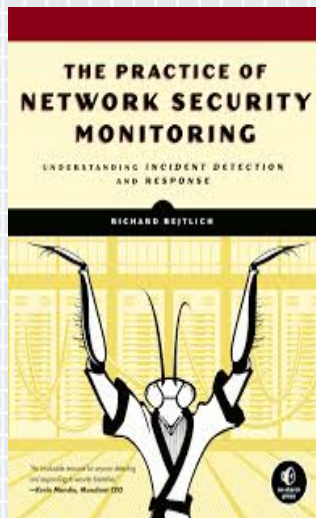
Technical



**OPEN
SOURCE**



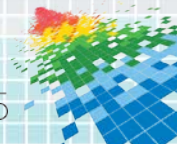
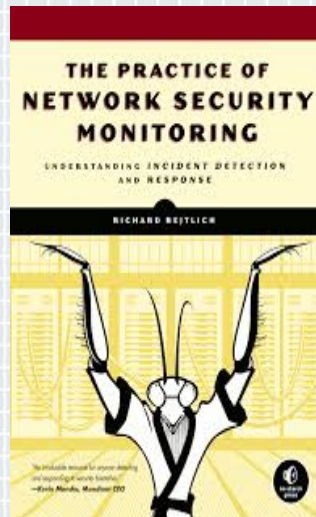
Technical



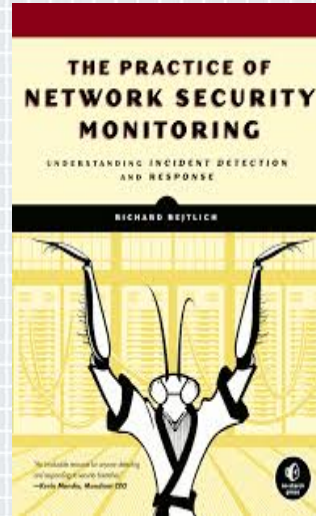
Technical



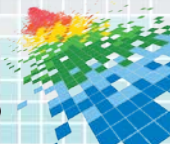
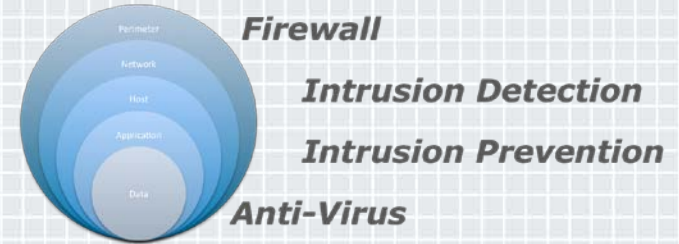
Conga Line of Security Vendor Solutions



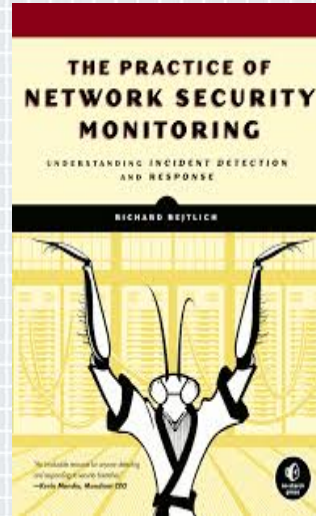
Technical



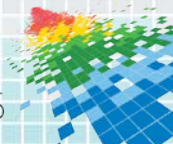
Defense in Depth



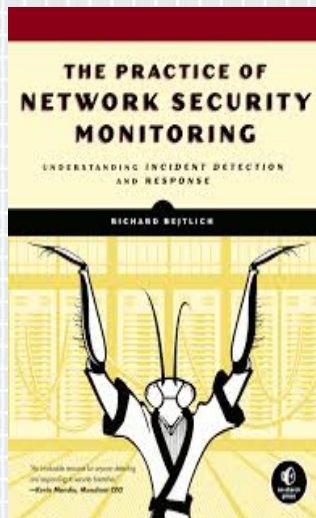
Technical



KILL CHAIN

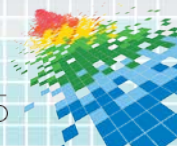


Technical

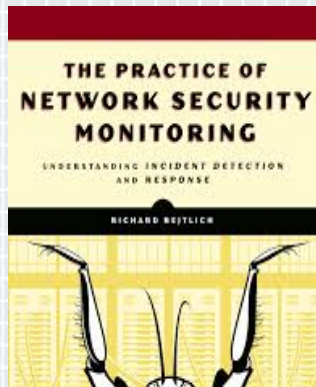


CYBER ESPIONAGE	
CYBER CRIME	
CYBER HACKTIVISM	
CYBER WARFARE	
CYBER MISCHIEF	
CYBER TERRORISM	

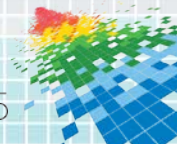
KILL CHAIN



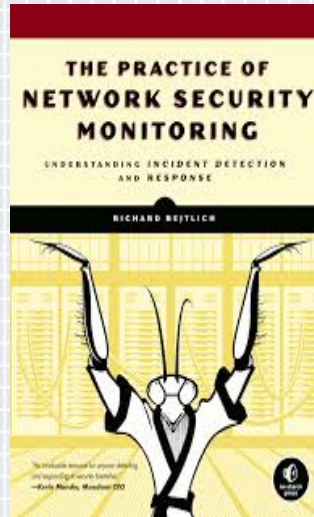
Technical



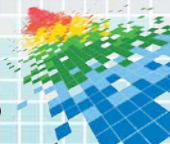
*“It’s become smarter to operate as though your enterprise is
always compromised.”*



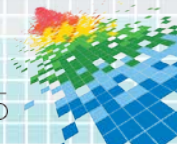
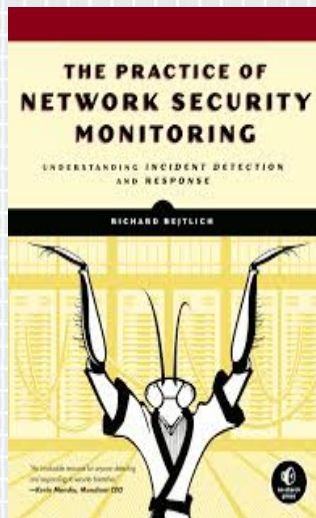
Technical



OPEN
SOURCE



Technical

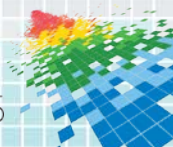
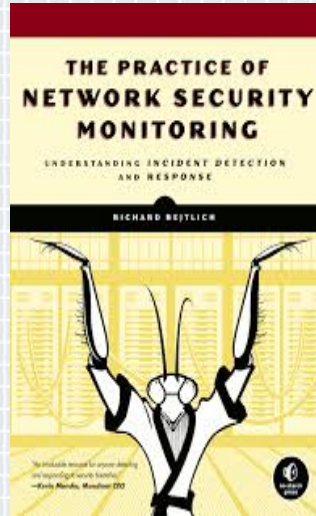


Technical



Data Collection Tool

Argus

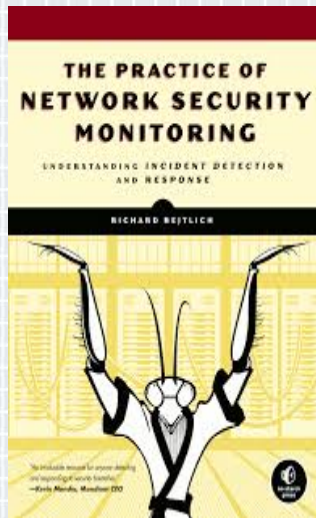


Technical



Data Collection Tool

Argus



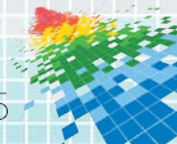
Data Presentation Tools

Tcpdump

Tshark

Argus Ra Client

Dumpcap

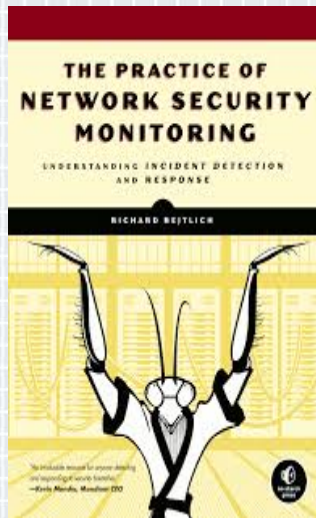


Technical



Data Collection Tool

Argus



Data Presentation Tools

Tcpdump

Tshark

Argus Ra Client

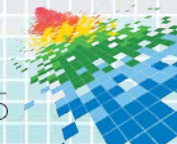
Dumpcap

Packet Analysis Tools

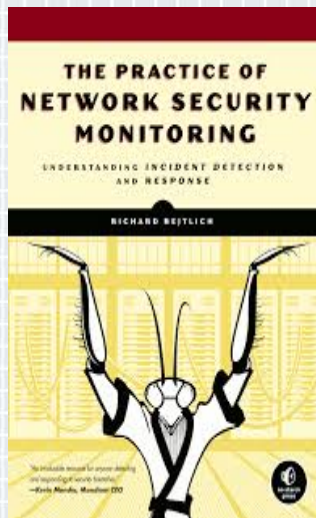
Wireshark

Xpilco

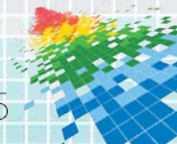
NetworkMiner



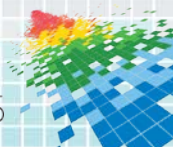
Technical



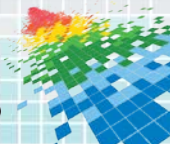
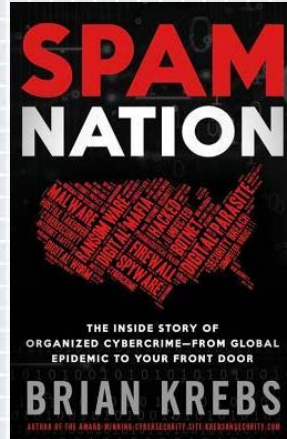
You Should Have Read this by Now!



Cyber Crime



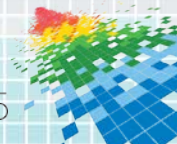
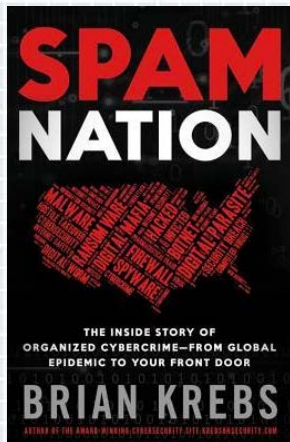
Cyber Crime



Cyber Crime



Brian Krebs





SPAM

NATION

THE INSIDE STORY OF
ORGANIZED CYBERCRIME—FROM GLOBAL
EPIDEMIC TO YOUR FRONT DOOR

BRIAN KREBS

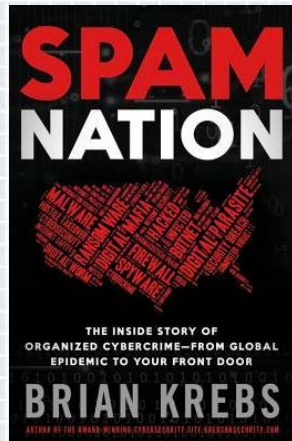
AUTHOR OF THE GRAB-BURNING, STEAL-SCHEMERY, SELL: HACKING SCHEMES FOR DUMMIES

Cyber Crime

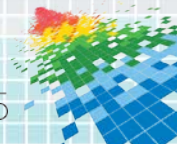


Brian Krebs

Krebs on Security
In-depth security news and investigation



2007-2013



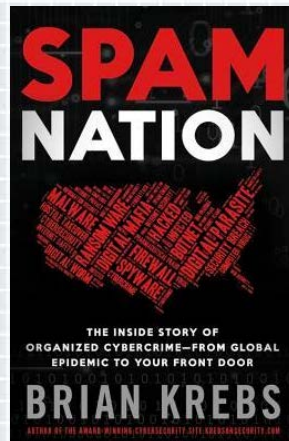
Cyber Crime

Symbiotic Relationship



Brian Krebs

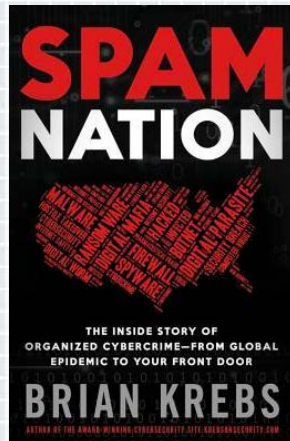
Krebs on Security
In-depth security news and investigation



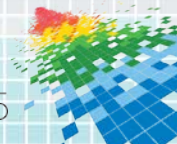
Cyber Crime



Symbiotic Relationship



Krebs on Security
In-depth security news and investigation

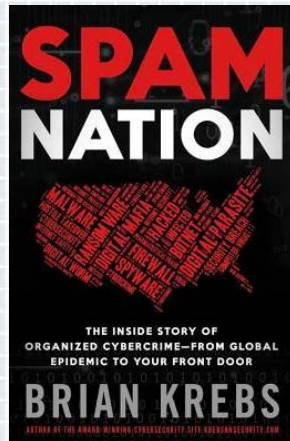


Cyber Crime

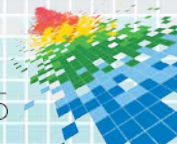
Symbiotic Relationship



AKA: RedEye



Krebs on Security
In-depth security news and investigation

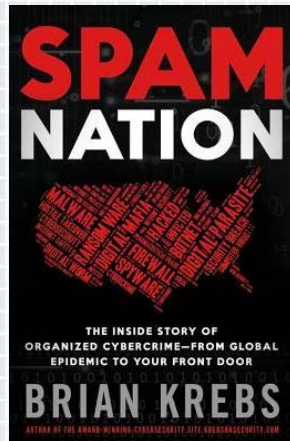


Cyber Crime

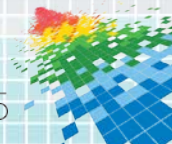


AKA: RedEye
AKA: DespDuck

Symbiotic Relationship



Krebs on Security
In-depth security news and investigation



Cyber Crime

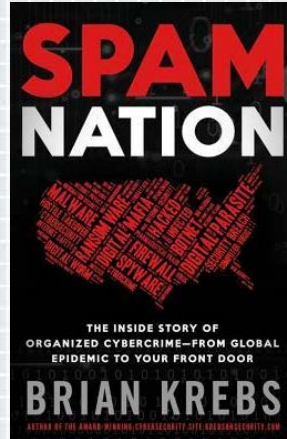


Pavel Vrulevsky

AKA: RedEye

AKA: DespDuck

Symbiotic Relationship

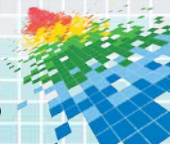


Brian Krebs

Krebs on Security
In-depth security news and investigation



Dimitry Nechvolod



Cyber Crime

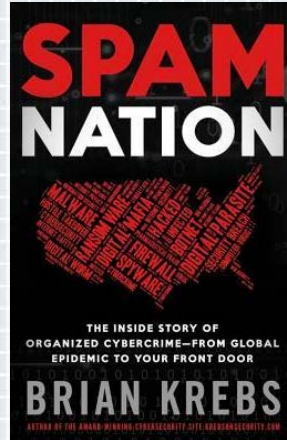


Pavel Vrulevsky

AKA: RedEye

AKA: DespDuck

Symbiotic Relationship



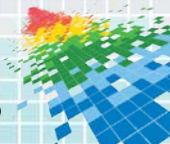
Brian Krebs

Krebs on Security
In-depth security news and investigation



Dimitry Nechvolod

AKA: Gugle

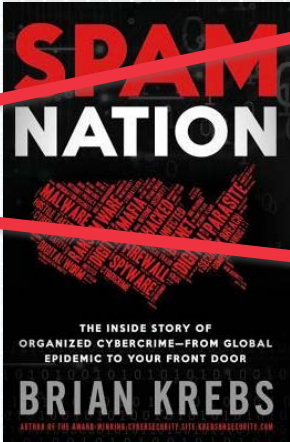


Cyber Crime

Symbiotic Relationship



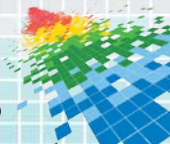
AKA: RedEye
AKA: DespDuck



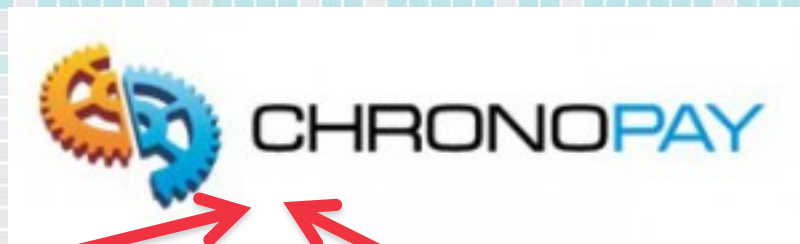
Krebs on Security
In-depth security news and investigation



AKA: Gugle

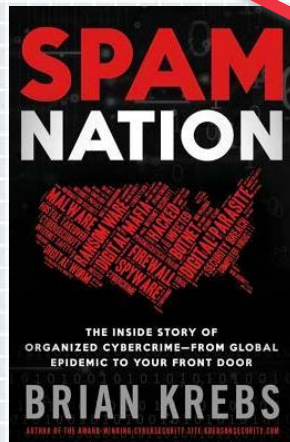


Cyber Crime



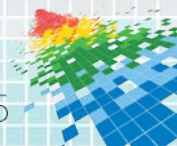
Pavel Vrulevsky

AKA: RedEye
AKA: DespDuck



Dimitry Nechvolod

2003



Cyber Crime

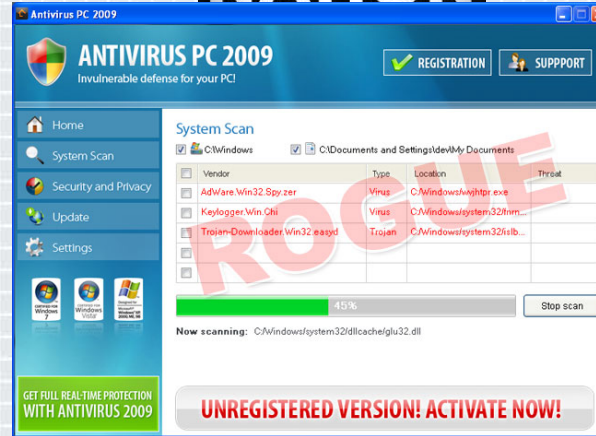


AKA: RedEye
AKA: DespDuck

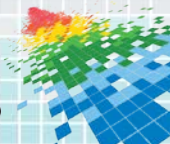


Payment Processor

**SPAM
NATION**



2003

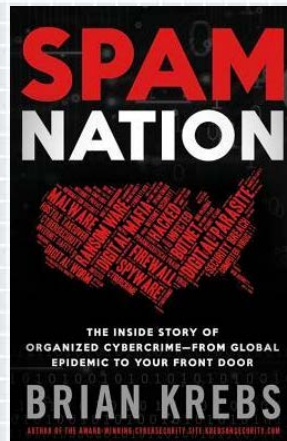


Cyber Crime



Brian Krebs

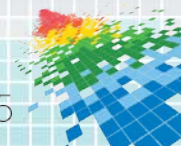
Krebs on Security
In-depth security news and investigation



Dimitry Nechvolod

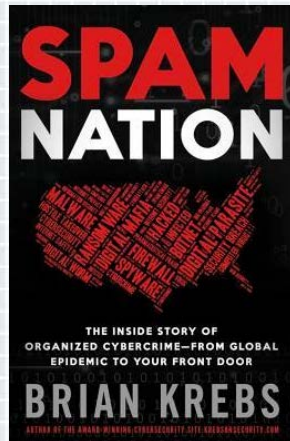
AKA: Gugle

2006



Cyber Crime

Pharmaceutical Spam



Brian Krebs

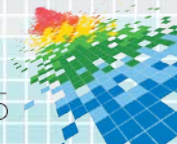
Krebs on Security
In-depth security news and investigation



Dimitry Nechvolod

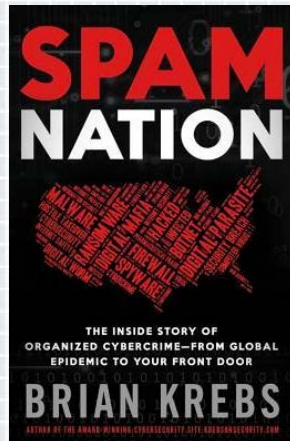
AKA: Gugle

2006



Cyber Crime

Pharmaceutical Spam



Brian Krebs

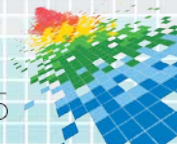
Krebs on Security
In-depth security news and investigation



Dimitry Nechvolod

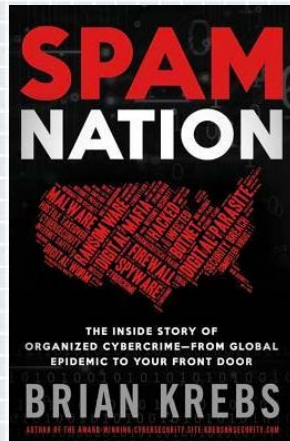
AKA: Gugle

2006



Cyber Crime

Pharmaceutical Spam



Brian Krebs

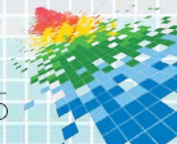
Krebs on Security
In-depth security news and investigation



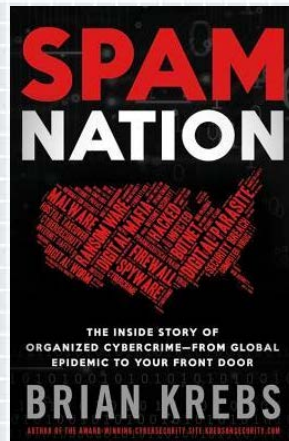
Dimitry Nechvolod

AKA: Gugle

2006

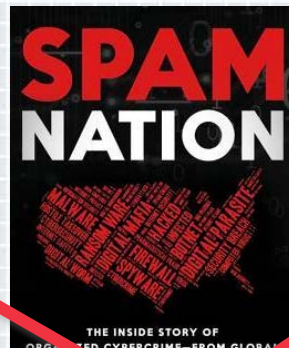


Cyber Crime



Pharmaceutical Spam

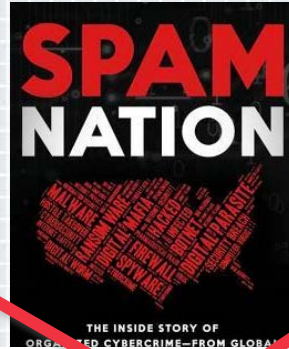
Cyber Crime



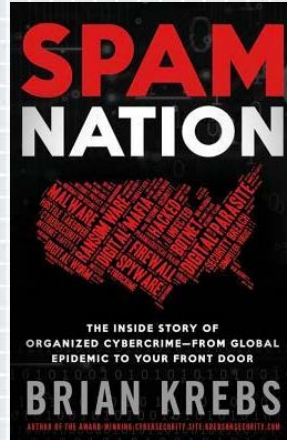
Krebs on Security
In-depth security news and investigation



Cyber Crime



Cyber Crime



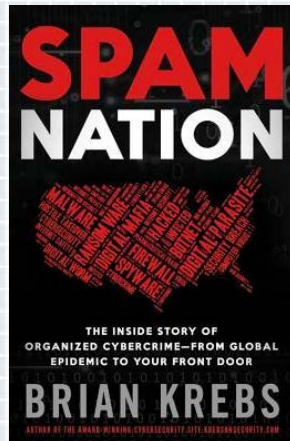
Krebs on Security
In-depth security news and investigation



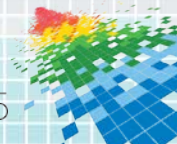
Pharmaceutical Spam

Cyber Crime

Take A-ways



Krebs on Security
In-depth security news and investigation



Cyber Crime

Famous Botnets



Pavel Vrublevsky

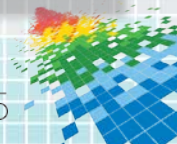
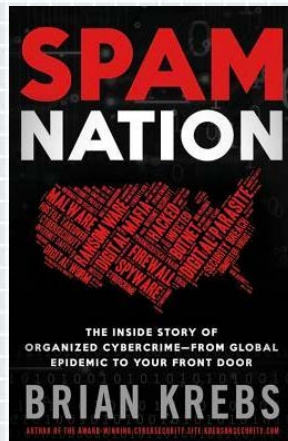


Dimitry Nechvolod



Brian Krebs

Krebs on Security
In-depth security news and investigation



Cyber Crime

Famous Botnets

Conficker



Pavel Vrublevsky

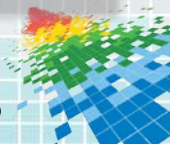
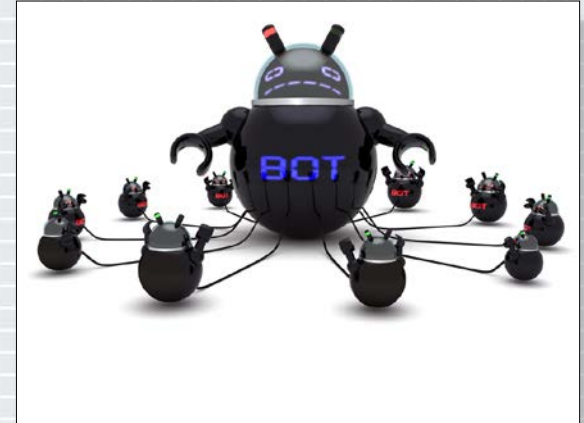
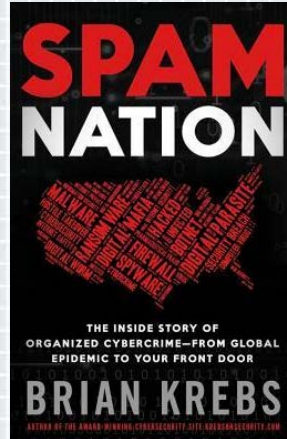


Dimitry Nechvolod



Brian Krebs

Krebs on Security
In-depth security news and investigation



Cyber Crime

Famous Botnets

Conficker

Cutwail



Pavel Vrulevsky

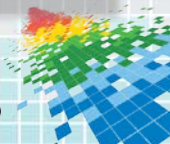
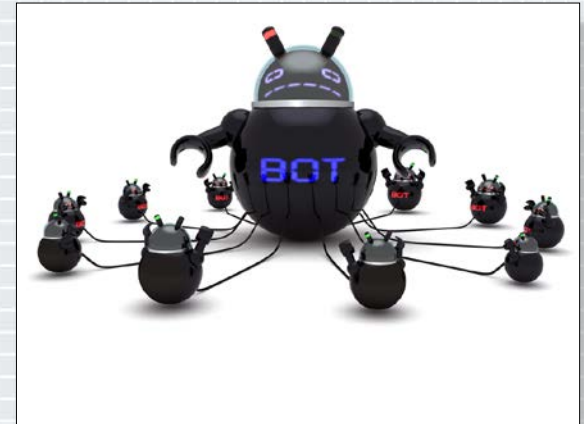
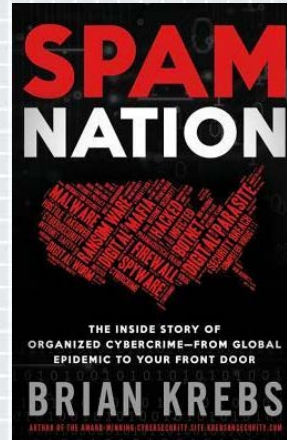


Dimitry Nechvolod



Brian Krebs

Krebs on Security
In-depth security news and investigation



Cyber Crime

Famous Botnets

Conficker

Cutwail

Grum

Festi



Pavel Vrulevsky

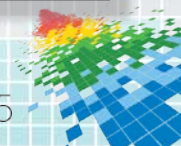
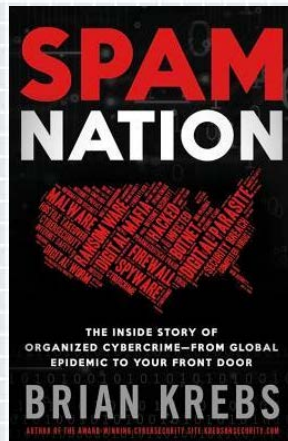


Dimitry Nechvolod



Brian Krebs

Krebs on Security
In-depth security news and investigation



Cyber Crime

Famous Botnets

Conficker Rustock

Cutwail

Grum

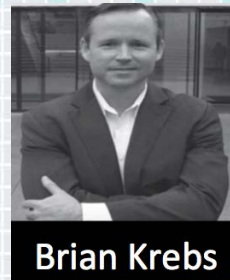
Festi



Pavel Vrublevsky

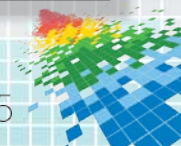
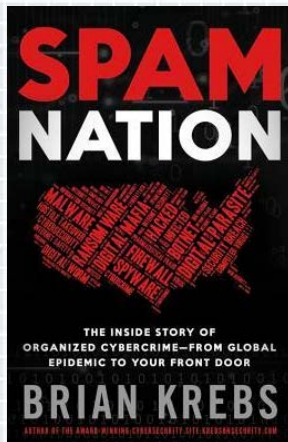


Dimitry Nechvolod



Brian Krebs

Krebs on Security
in-depth security news and investigation



Cyber Crime

Famous Botnets

Conficker Rustock

Cutwail Storm

Grum

Festi



Pavel Vrublevsky

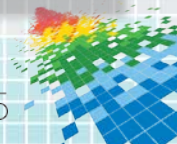
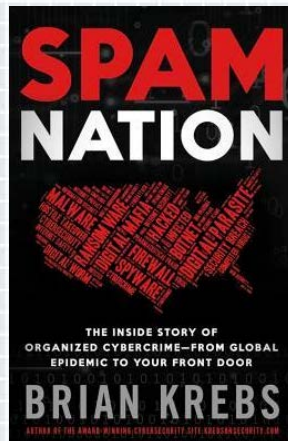


Dimitry Nechvolod



Brian Krebs

Krebs on Security
In-depth security news and investigation



Cyber Crime

Famous Botnets

Conficker Rustock

Cutwail Storm

Grum Waledock

Festi



Pavel Vrulevsky

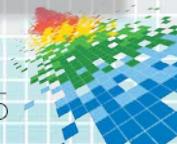
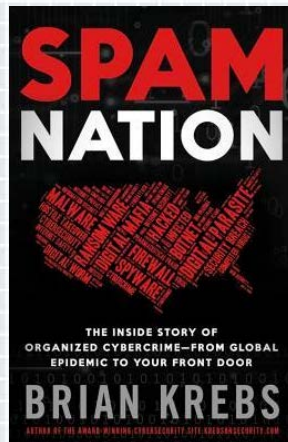


Dimitry Nechvolod



Brian Krebs

Krebs on Security
In-depth security news and investigation

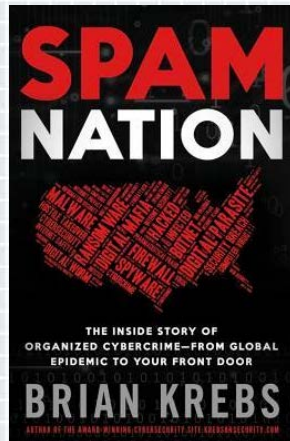


Cyber Crime

Take A-ways

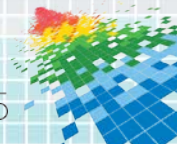
Famous Botnets

Criminal Business
Operations

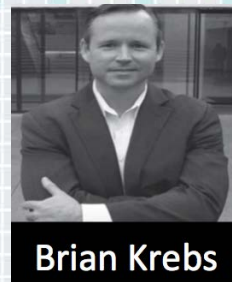
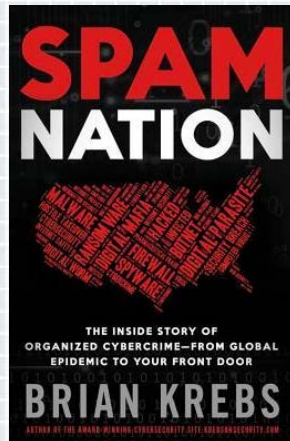


Brian Krebs

Krebs on Security
In-depth security news and investigation

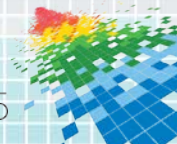


Cyber Crime

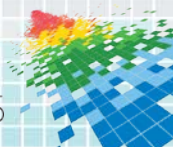


Krebs on Security
In-depth security news and investigation

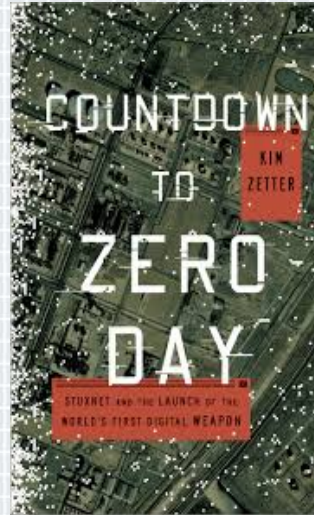
You Should Have Read this by Now



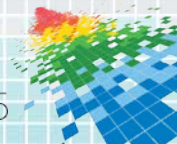
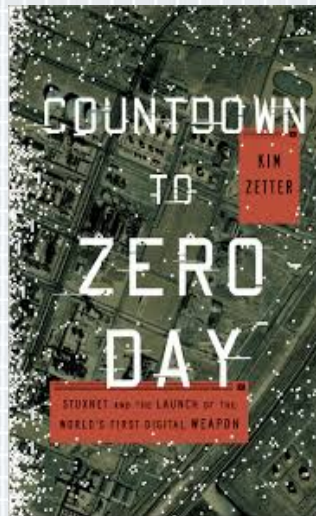
Cyber Warfare



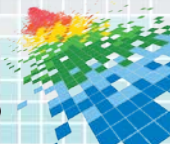
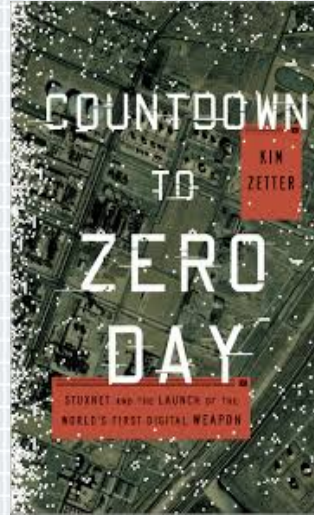
Cyber Warfare



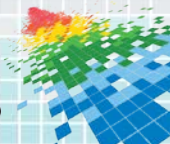
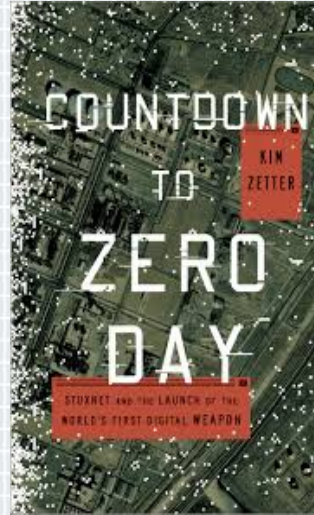
Cyber Warfare



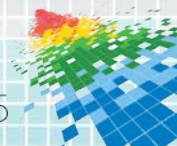
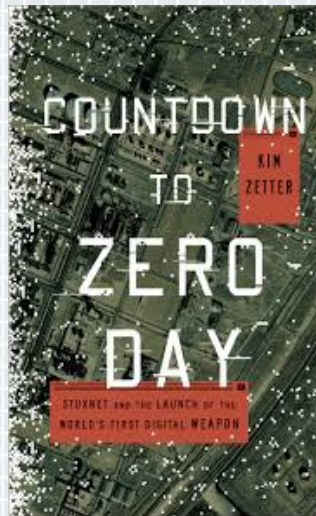
Cyber Warfare



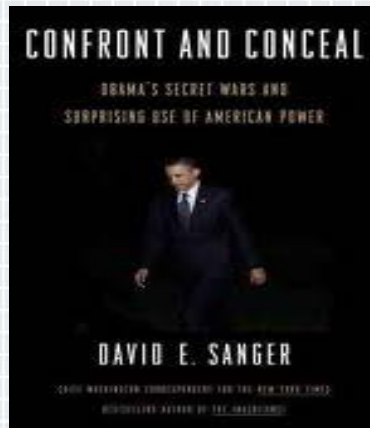
Cyber Warfare



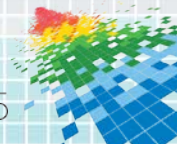
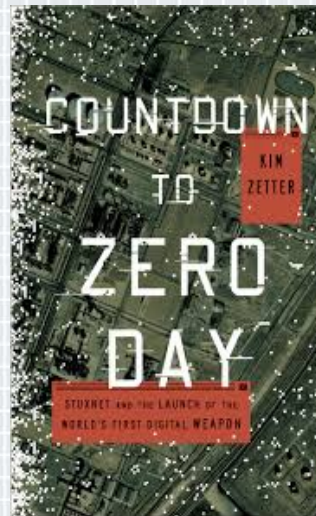
Cyber Warfare



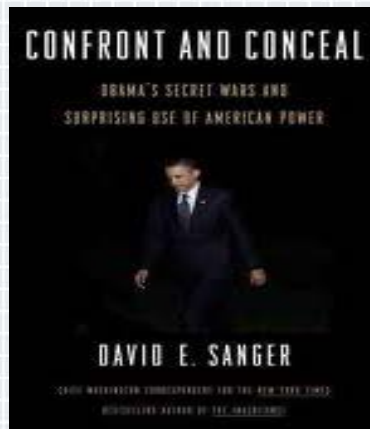
Cyber Warfare



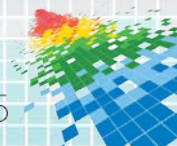
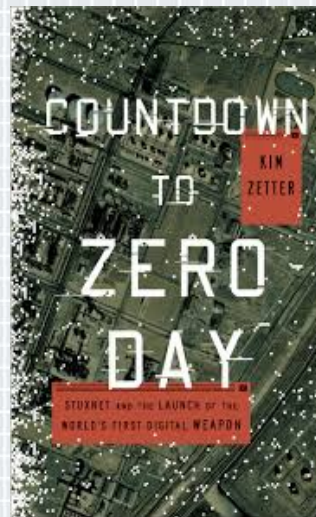
The New York Times



Cyber Warfare

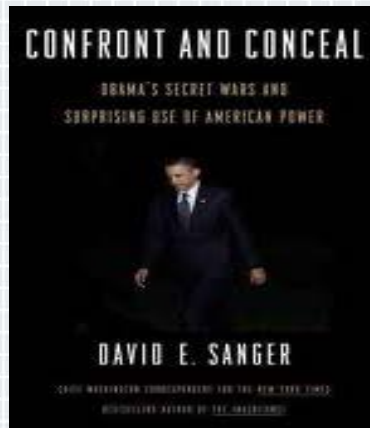


The New York Times



Cyber Warfare

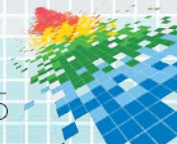
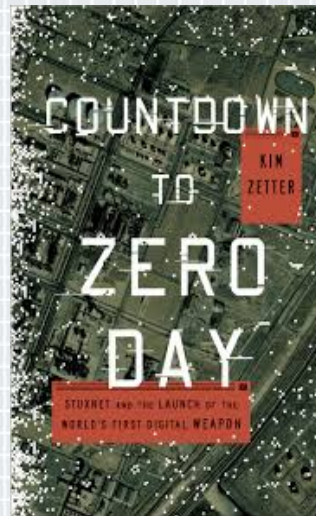
Foreign Policy



The New York Times



David Sanger



Cyber Warfare

People



Eugene Kaspersky



Liam O Murchu



Eric Chien



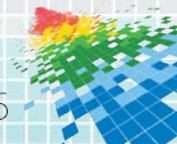
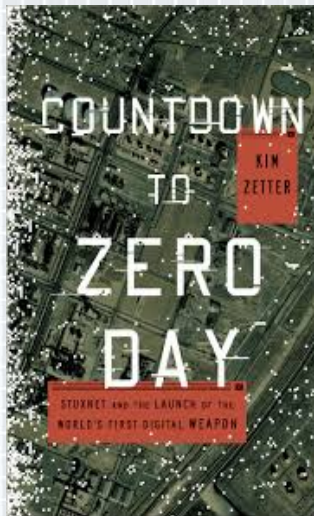
Nicolas Falliere



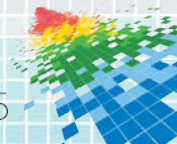
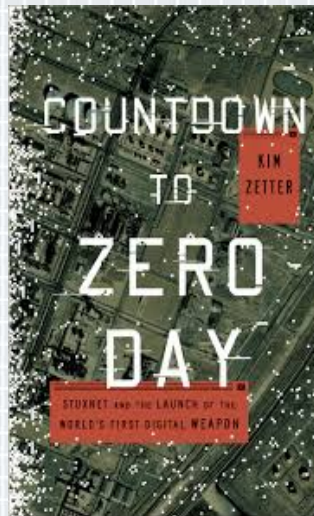
Ralph Langer



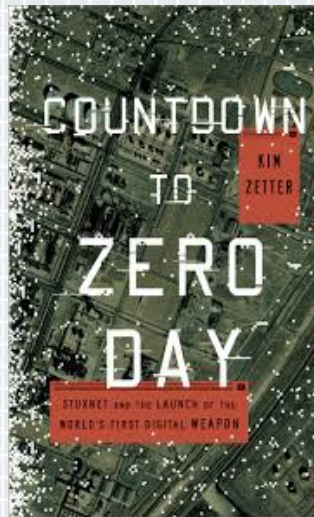
Technical Details



Cyber Warfare



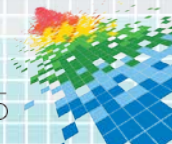
Cyber Warfare



2800 Power Plants

300,000 Oil & Natural Gas Sites

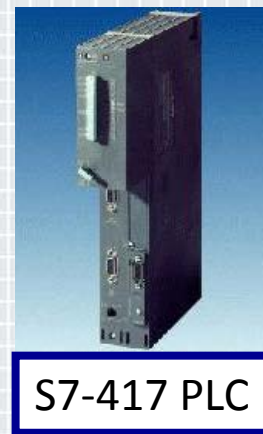
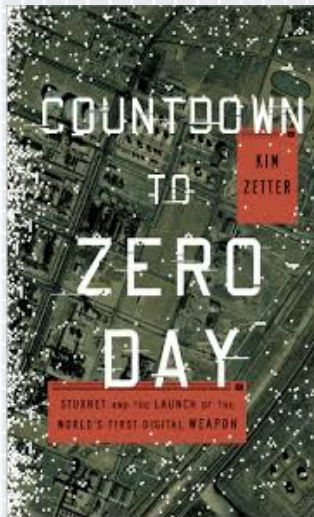
170,000 Public Water Systems



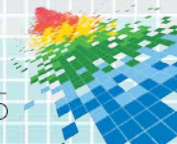
Cyber Warfare



Technical Details



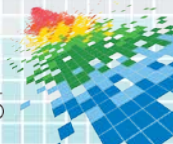
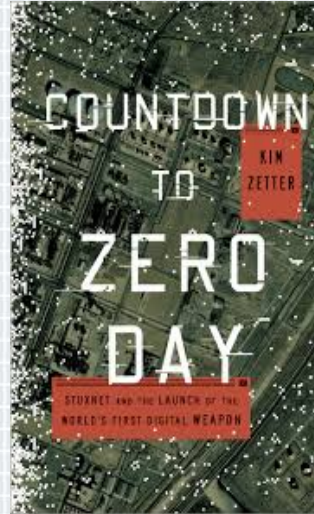
Programmable Logic Controllers (PLCs)



Cyber Warfare



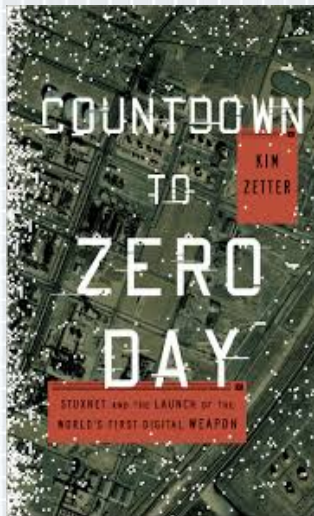
2: Philosophical Conundrums



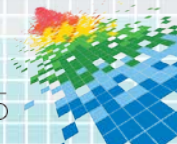
Cyber Warfare



2: Philosophical Conundrums



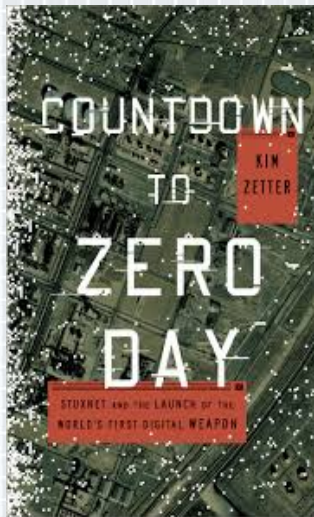
Intelligence Dilemma



Cyber Warfare

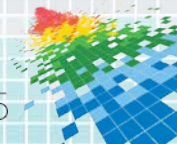


2: Philosophical Conundrums

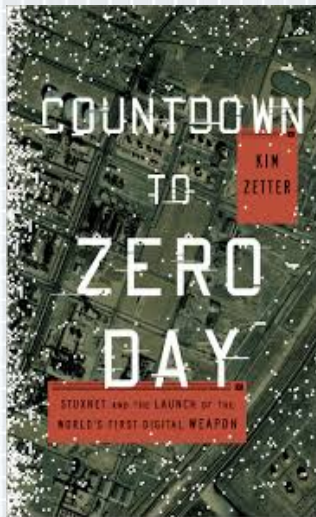


Intelligence Dilemma

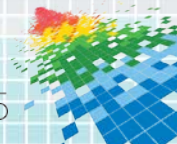
Simultaneous Offense and Defense Operations



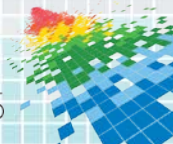
Cyber Warfare



You Should Have Read this by Now!



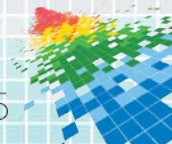
Cyber History and Culture



Cyber History and Culture



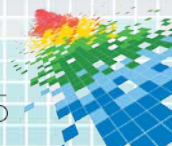
2005



Cyber History and Culture



2005



Cyber History and Culture



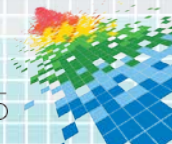
2005



Cyber History and Culture



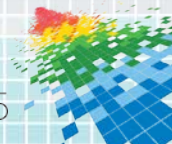
2005



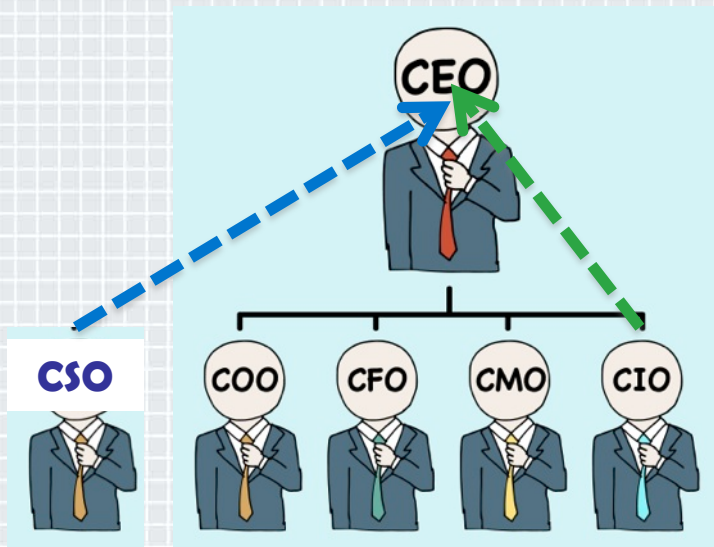
Cyber History and Culture



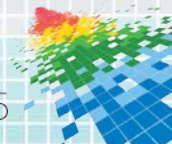
3



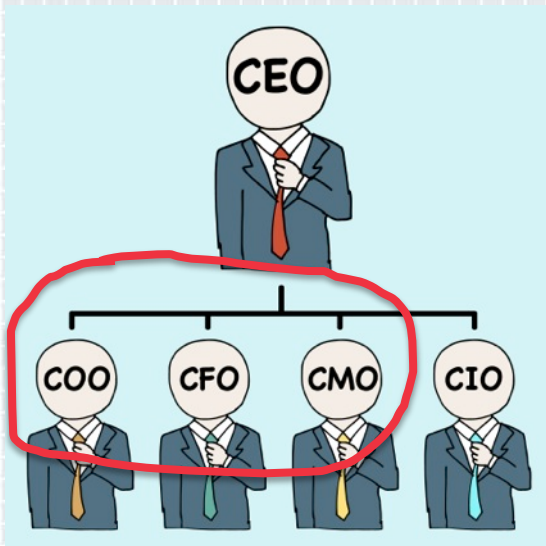
Cyber History and Culture



1



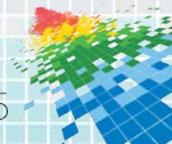
Cyber History and Culture



1



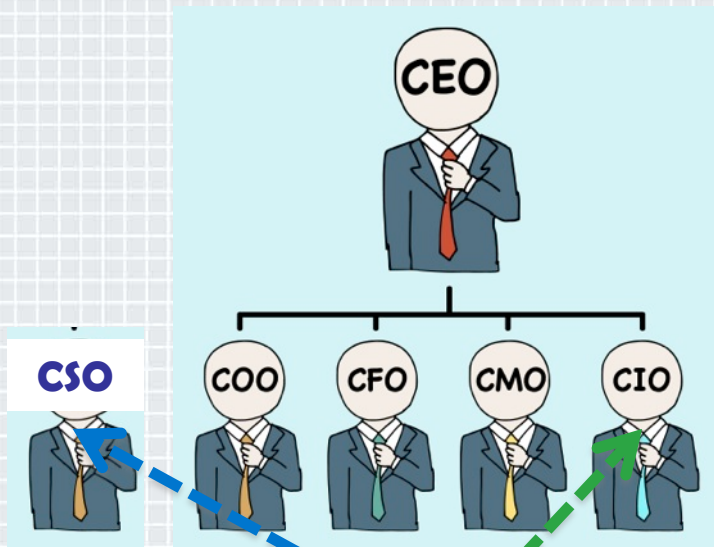
Not



Cyber History and Culture

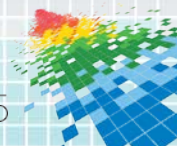


1

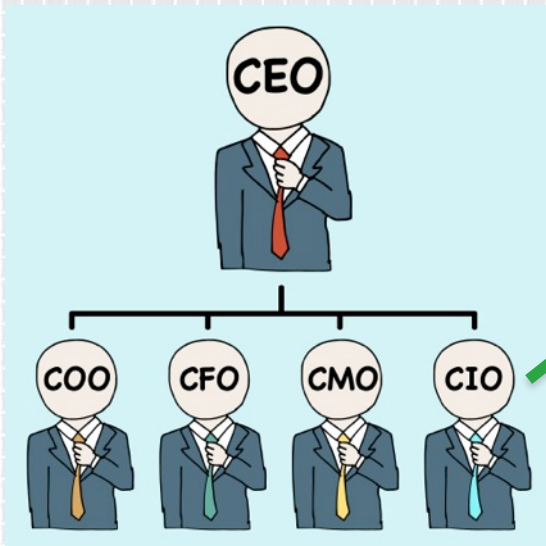


Healthy

Tension



Cyber History and Culture

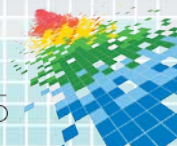


I

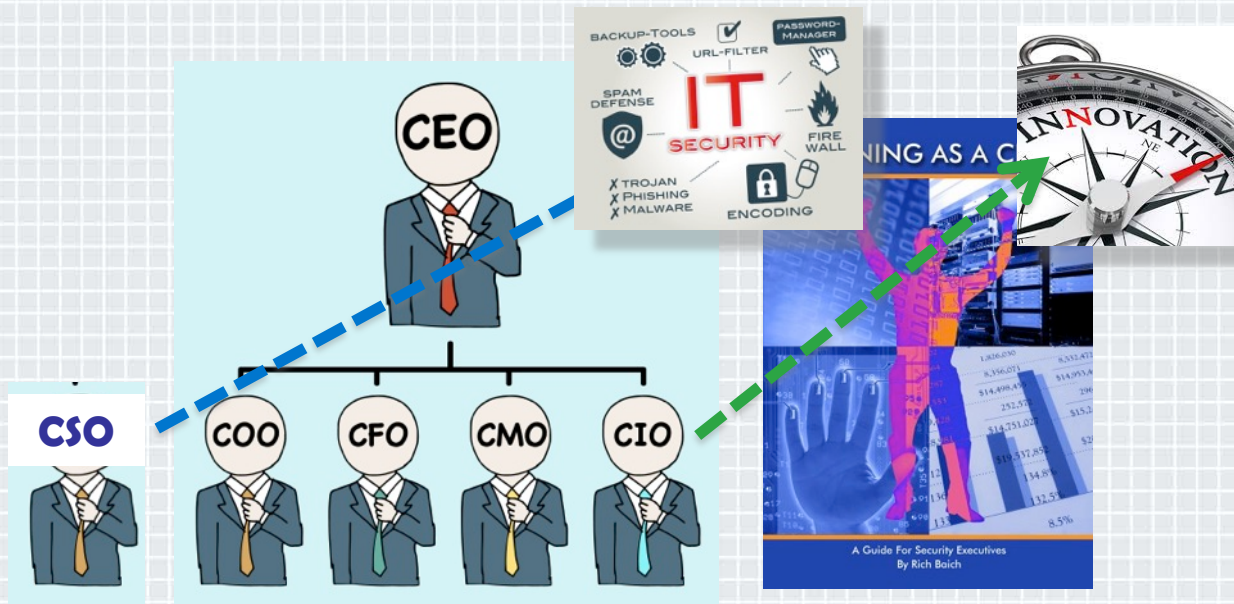


Healthy

Tension



Cyber History and Culture

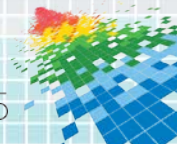


1



Healthy

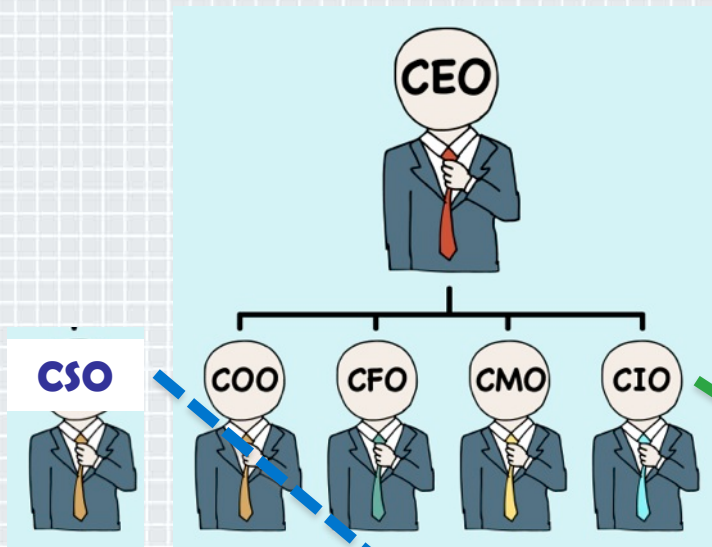
Tension



Cyber History and Culture

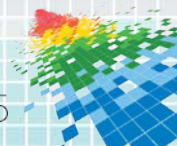


1



Healthy

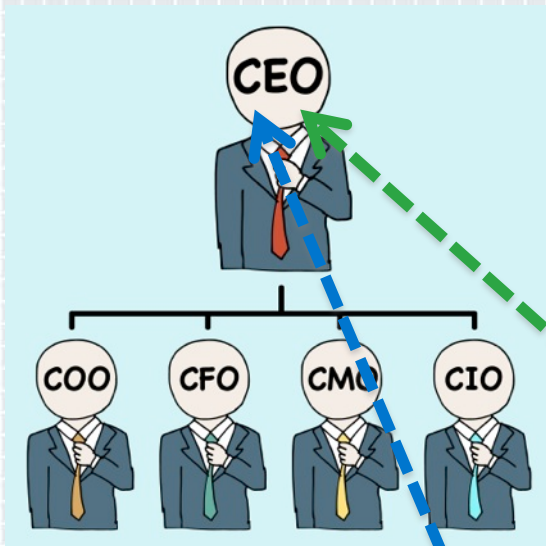
Tension



Cyber History and Culture

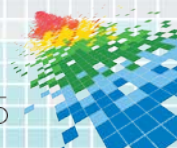


1



Healthy

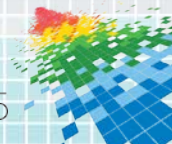
Tension



Cyber History and Culture



2

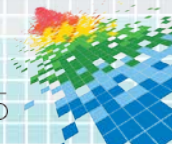


Cyber History and Culture

Business



2



Cyber History and Culture

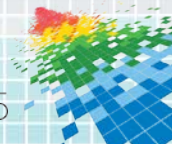
Business



Product



2



Cyber History and Culture

Business

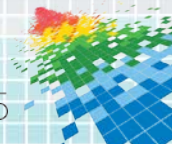


Product

Marketing



2



Cyber History and Culture

Business



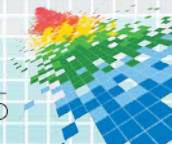
Product

Marketing

Profit & Loss



2



Cyber History and Culture

Business



Product

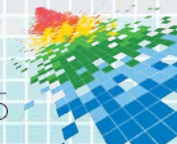
Marketing

Profit & Loss

Customer Service



2



Cyber History and Culture

Business

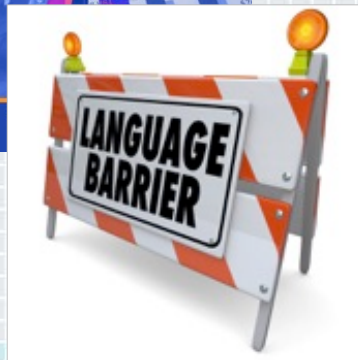


Product

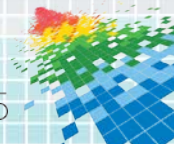
Marketing

Profit & Loss

Customer Service



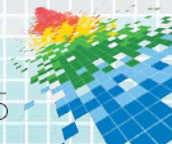
2



Cyber History and Culture



3

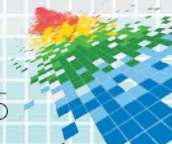


Cyber History and Culture

CISO Skills



3



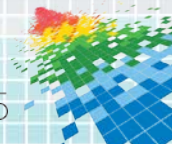
Cyber History and Culture

CISO Skills

- Must have an MBA



3



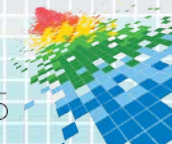
Cyber History and Culture

CISO Skills

- Must have an MBA
- Prior budget or P&L experience



3



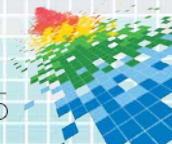
Cyber History and Culture

CISO Skills

- Must have an MBA
- Prior budget or P&L experience
- A proven ability to lead an effective information security organization



3

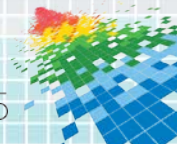


Cyber History and Culture

CISO Skills

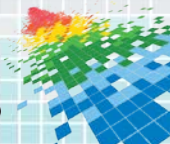
- Must have an MBA
- Prior budget or P&L experience
- A proven ability to lead an effective information security organization

“If performing vulnerability assessments, configuring firewalls, and performing network forensics makes you happy then becoming Chief Information Security Officer may not be the right career choice for you.”

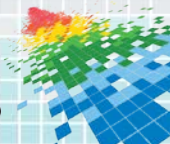
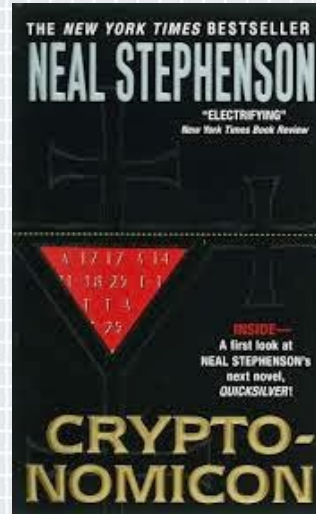




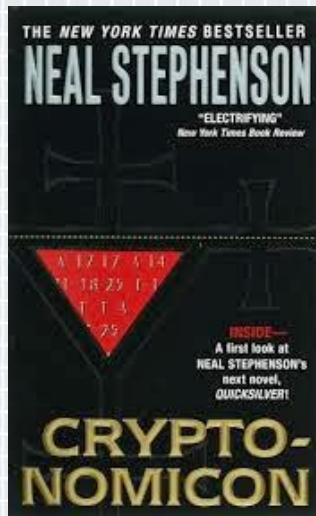
Novel



Novel

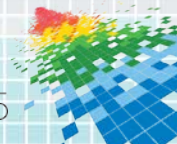


Novel



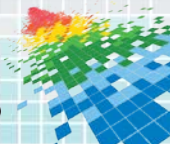
Neil Stephenson

Quintessential

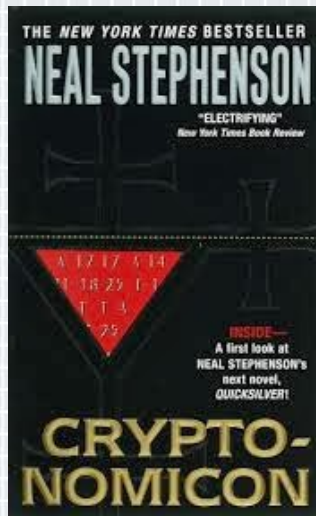




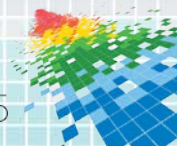
Quintessential



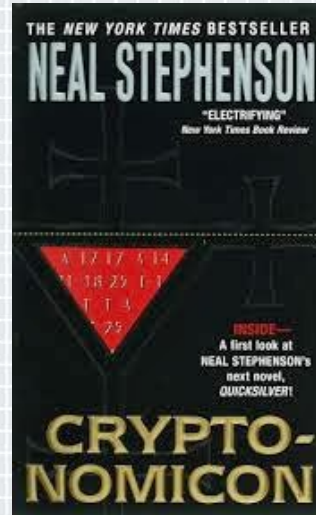
Novel



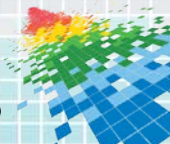
Quintessential



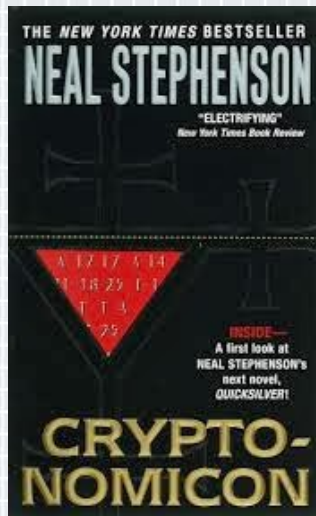
Novel



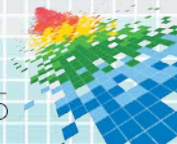
Quintessential



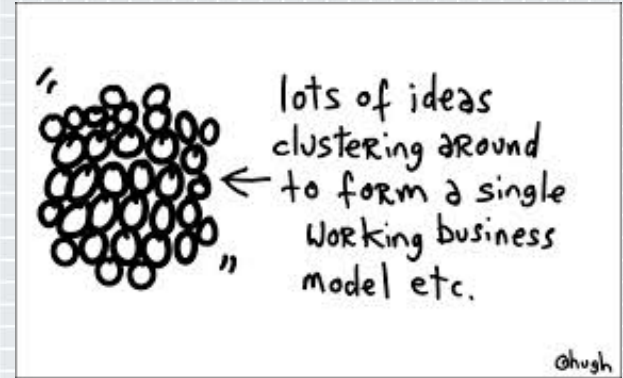
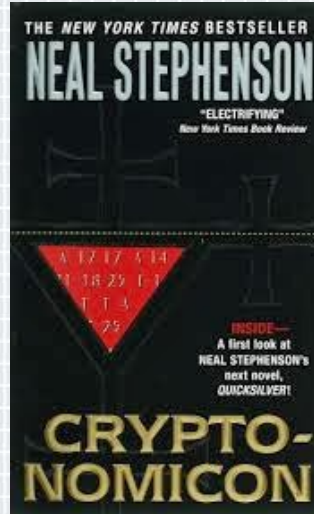
Novel



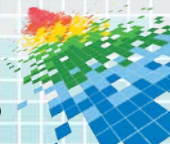
Quintessential



Novel

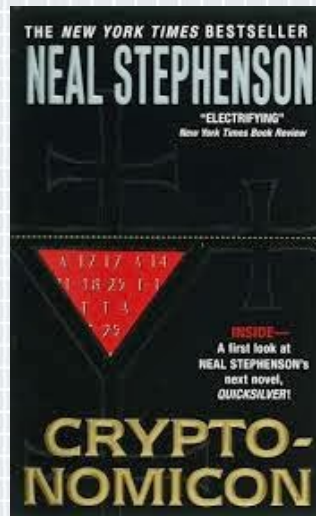


Quintessential

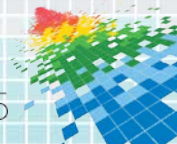


Novel

CYBER SECURITY HISTORY



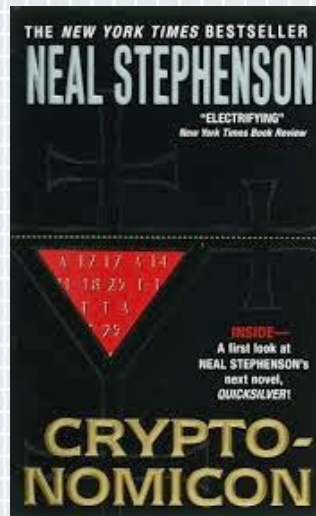
Quintessential



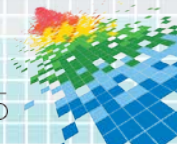
Novel

CYBER SECURITY HISTORY

TRAGEDY



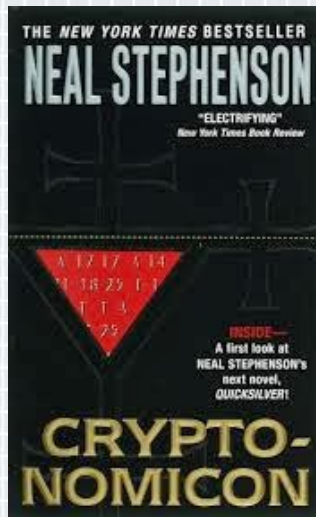
Quintessential



Novel

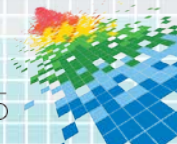
CYBER SECURITY HISTORY

TRAGEDY



ADVENTURE

Quintessential



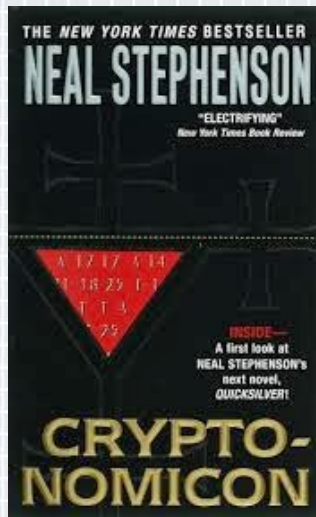
Novel

CYBER SECURITY HISTORY

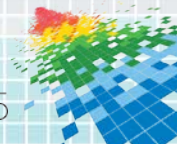
TRAGEDY

GEEK LOVE STORIES

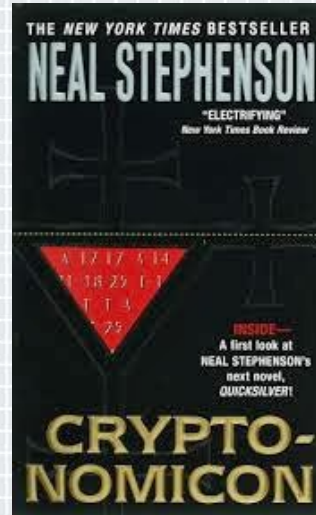
ADVENTURE



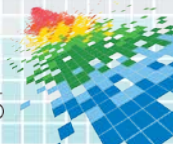
Quintessential



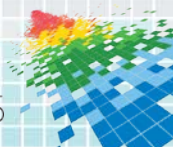
Novel



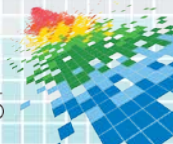
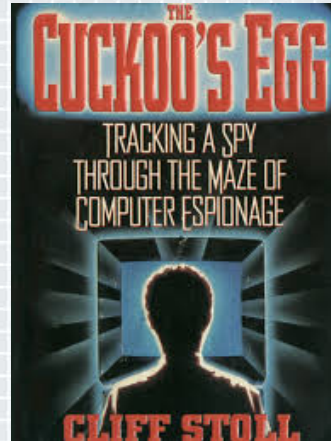
You Should Have Read this by Now



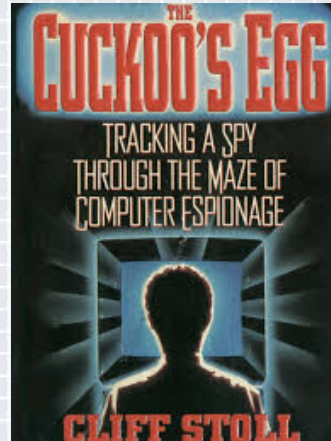
Cyber Espionage



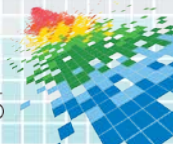
Cyber Espionage



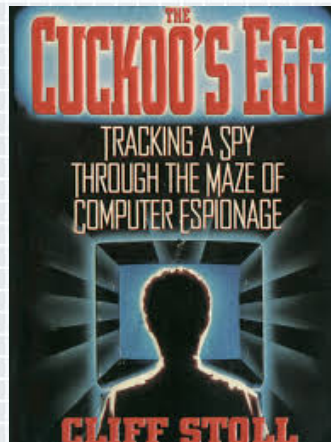
Cyber Espionage



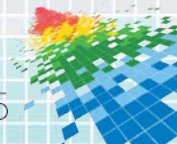
1989



Cyber Espionage

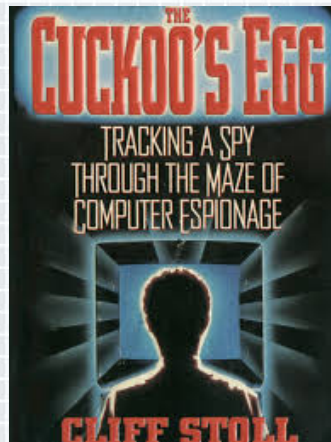


1989

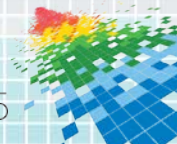


Cyber Espionage

Information Sharing



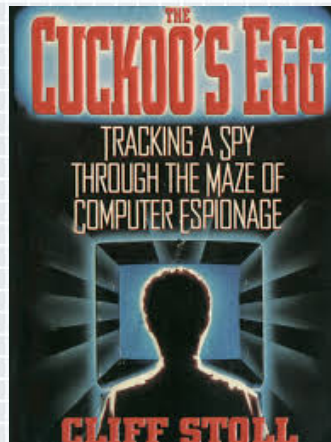
1989



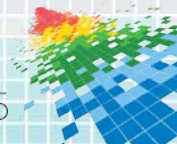
Cyber Espionage

Information Sharing

Privacy vs Security (R)
Liberty vs Control (D)



1989

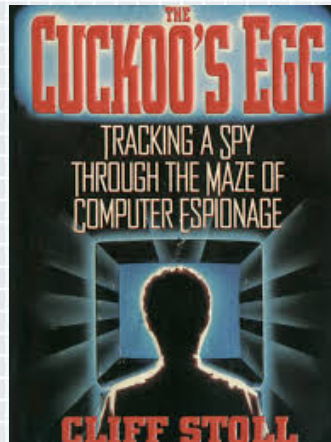


Cyber Espionage

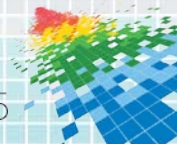
Information Sharing

Privacy vs Security (R)
Liberty vs Control (D)

Cyber Espionage



1989



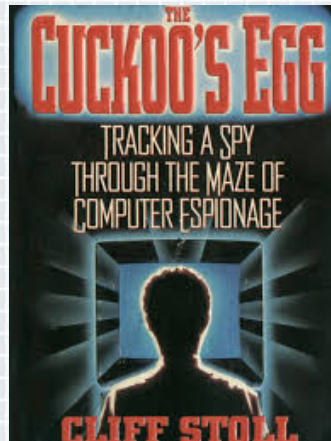
Cyber Espionage

Information Sharing

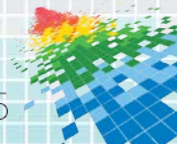
Privacy vs Security (R)
Liberty vs Control (D)

Cyber Espionage

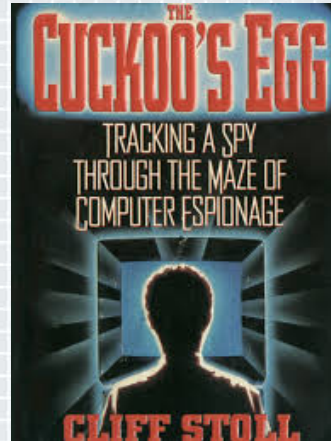
Intelligence Dilemma



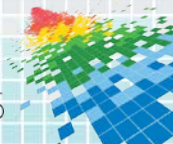
1989



Cyber Espionage



You Should Have Read this by Now



RSA®Conference2015

San Francisco | April 20-24 | Moscone Center

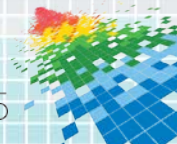
Conclusion:

Cybersecurity Canon Project



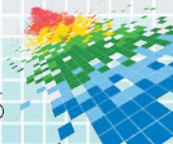
Apply What You Have Learned Today

- ◆ Next week you should:



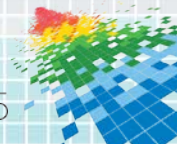
Apply What You Have Learned Today

- ◆ Next week you should:
 - ◆ **Go to the Canon Website and read the reviews**



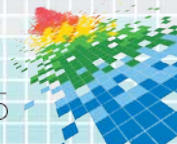
Apply What You Have Learned Today

- ◆ Next week you should:
 - ◆ Go to the Canon Website and read the reviews
- ◆ In the first three months following this presentation you should:



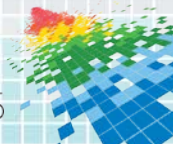
Apply What You Have Learned Today

- ◆ Next week you should:
 - ◆ Go to the Canon Website and read the reviews
- ◆ In the first three months following this presentation you should:
 - ◆ **Compile a list of your favorite books that are not already on the candidate list**
 - ◆ **Send them to me.**



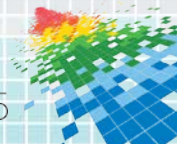
Apply What You Have Learned Today

- ◆ Next week you should:
 - ◆ Go to the Canon Website and read the reviews
- ◆ In the first three months following this presentation you should:
 - ◆ Compile a list of your favorite books that are not already on the candidate list
 - ◆ Send them to me.
- ◆ Within six months you should:



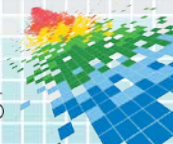
Apply What You Have Learned Today

- ◆ Next week you should:
 - ◆ Go to the Canon Website and read the reviews
- ◆ In the first three months following this presentation you should:
 - ◆ Compile a list of your favorite books that are not already on the candidate list
 - ◆ Send them to me.
- ◆ Within six months you should:
 - ◆ **Write a review of your favorite book and submit it to the project.**



Apply What You Have Learned Today

- ◆ Next week you should:
 - ◆ Go to the Canon Website and read the reviews
- ◆ In the first three months following this presentation you should:
 - ◆ Compile a list of your favorite books that are not already on the candidate list
 - ◆ Send them to me.
- ◆ Within six months you should:
 - ◆ Write a review of your favorite book and submit it to the project.



Questions?

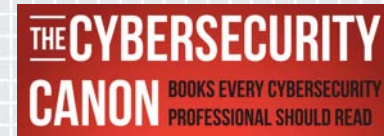
Rick Howard: CSO Palo Alto Networks

Email: rhoward@paloaltonetworks.com

Twitter: [@raceBannon99](https://twitter.com/raceBannon99)



<https://paloaltonetworks.com/threat-research.html>



<https://paloaltonetworks.com/threat-research/cybercanon.html>



<http://cyberthreatalliance.org/>