CANBERRA HALF DAY SECURITY CONFERENCE 2019

Thursday 12 September 2019

Welcome and opening address

Leonard Kleinman

Canberra Branch Chair at AISA

Thank you to our sponsors

JACOBS®

dimension data

NTT

The journey of cyber security in Australia: What’s happened; where’re we headed and what does the next generation of quantum computing and cryptography look like?

Julian Fay
Chief Technology Officer at Senetas

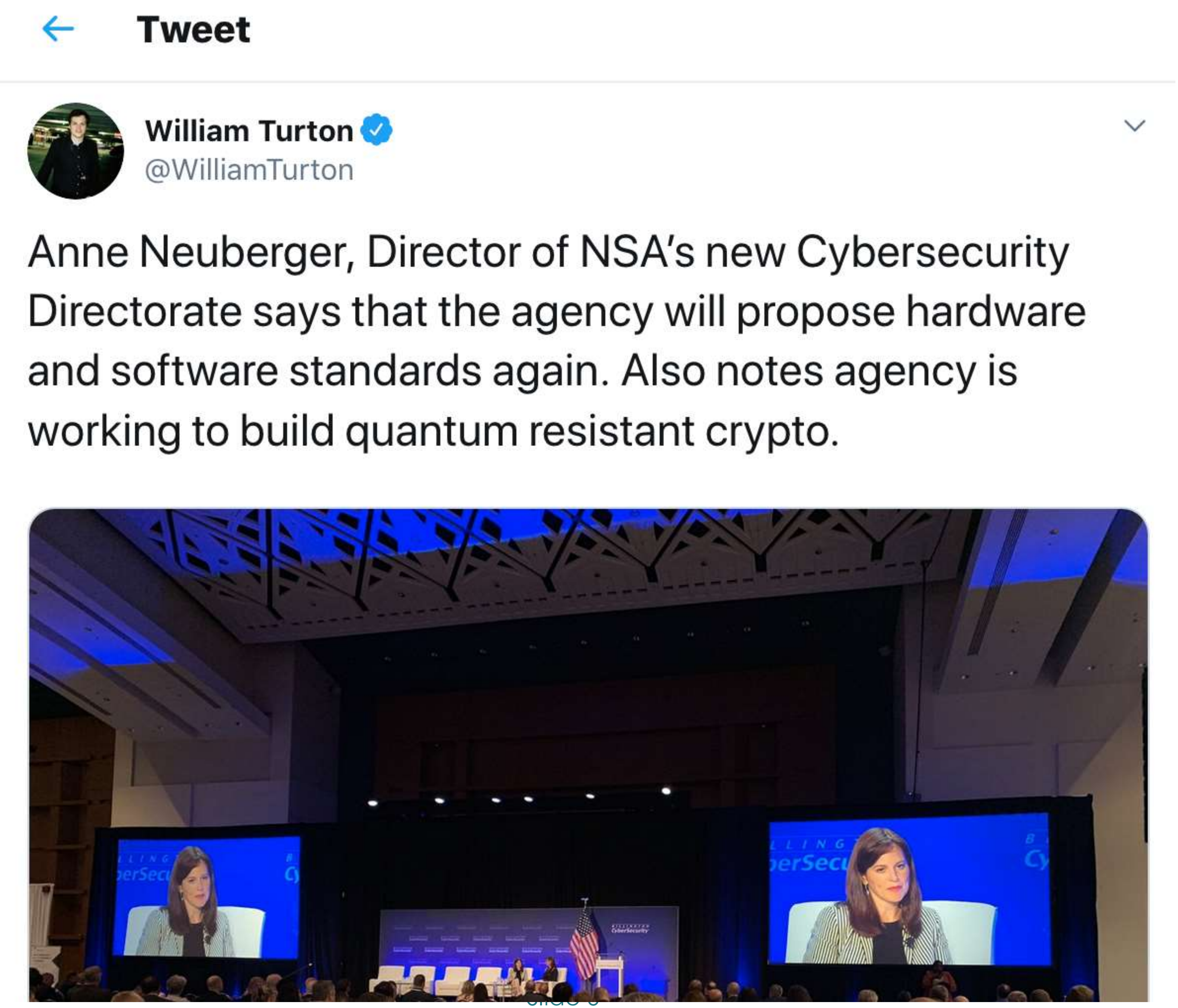
SENETAS

Security without compromise

AISA Security Conference Canberra 2019

Julian Fay CISSP

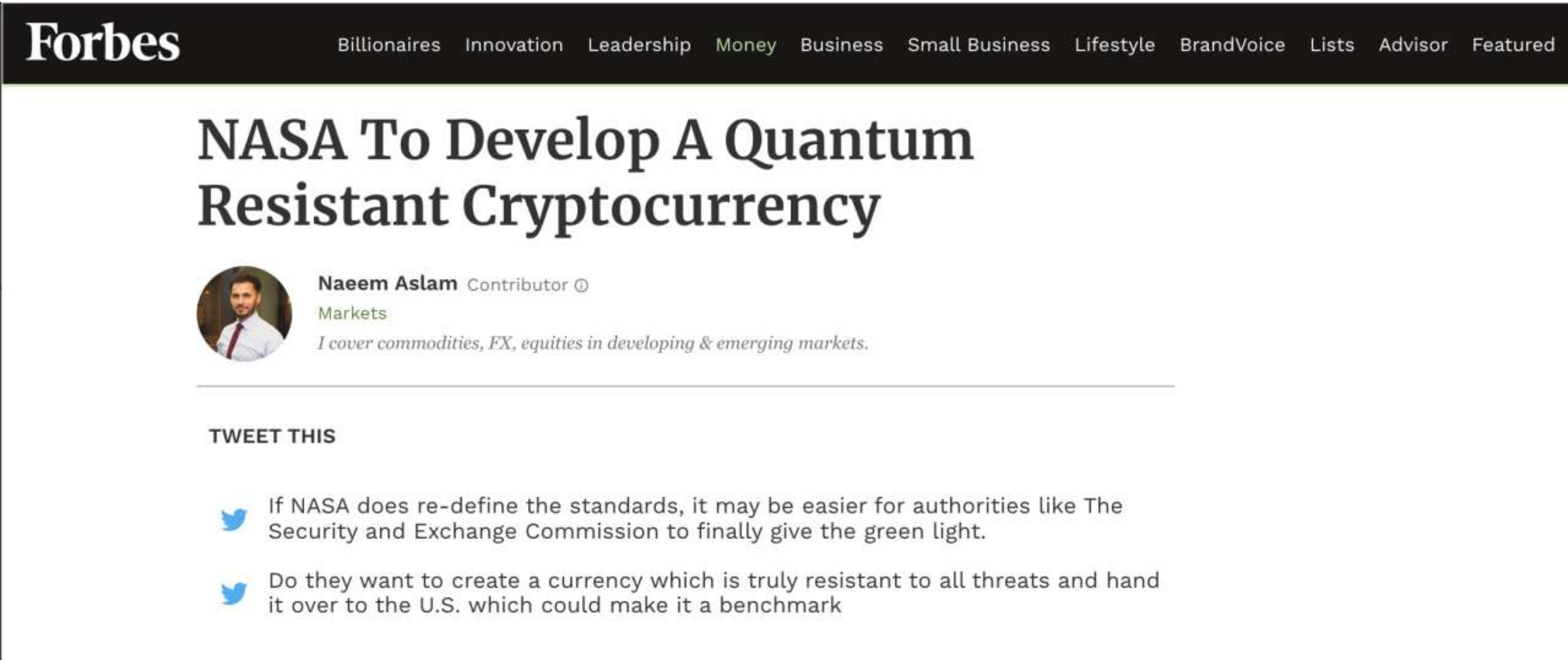
CTO Senetas



Tweet

William Turton
@WilliamTurton

Anne Neuberger, Director of NSA's new Cybersecurity Directorate says that the agency will propose hardware and software standards again. Also notes agency is working to build quantum resistant crypto.



NASA To Develop A Quantum Resistant Cryptocurrency

Naeem Aslam Contributor ⓘ

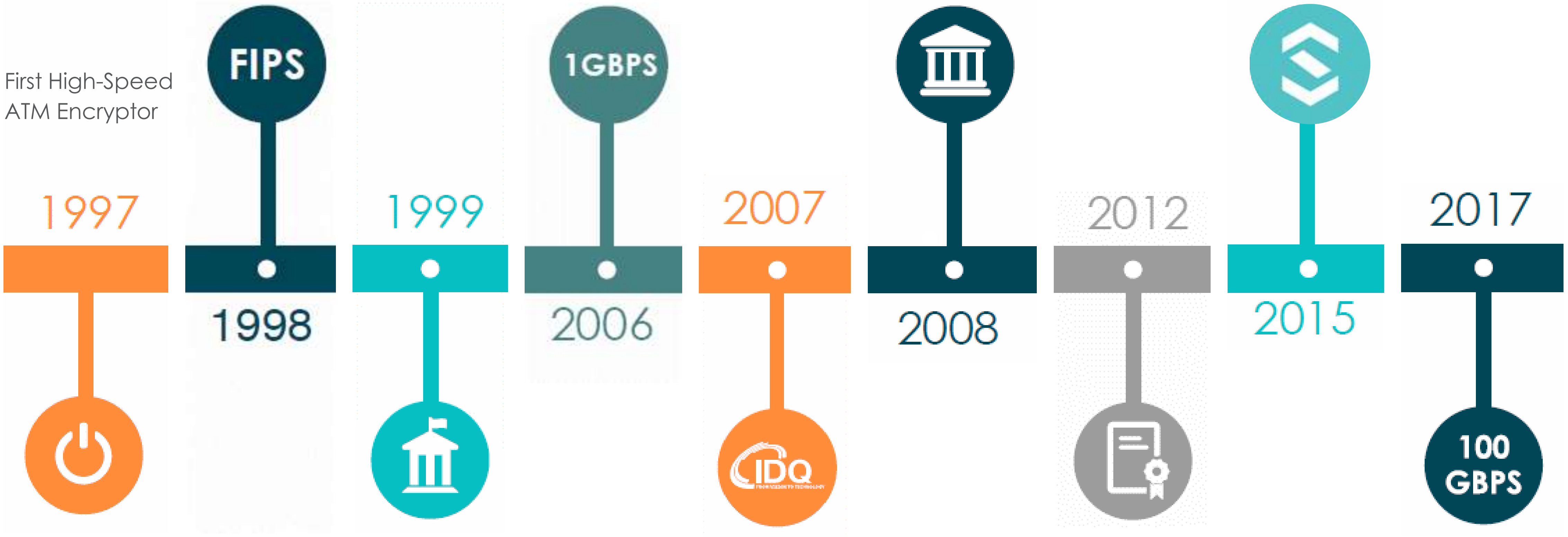
Markets

I cover commodities, FX, equities in developing & emerging markets.

TWEET THIS

- If NASA does re-define the standards, it may be easier for authorities like The Security and Exchange Commission to finally give the green light.
- Do they want to create a currency which is truly resistant to all threats and hand it over to the U.S. which could make it a benchmark

Senetas - History



1997

First High-Speed ATM Encryptor

1998

First FIPS Certified High-Assurance Layer 2 Network Encryptor

1999

First Global Deployment Of High-Assurance Layer 2 Encryptors

2006

Launch Of 1Gbps, High-Assurance Ethernet Encryptor

2007

World’s First Quantum-Powered Encryptors

2008

World’s First SONET Encryptor

2012

First Multi-Certified Layer 2 Ethernet Encryptors

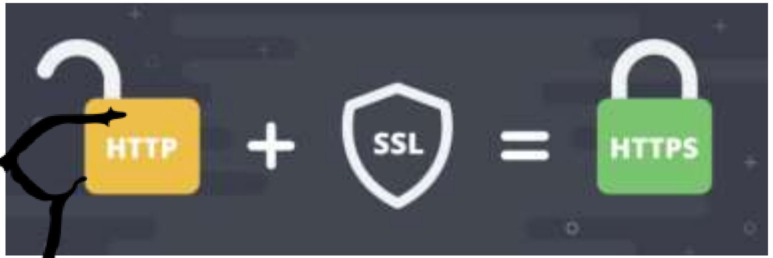
2015

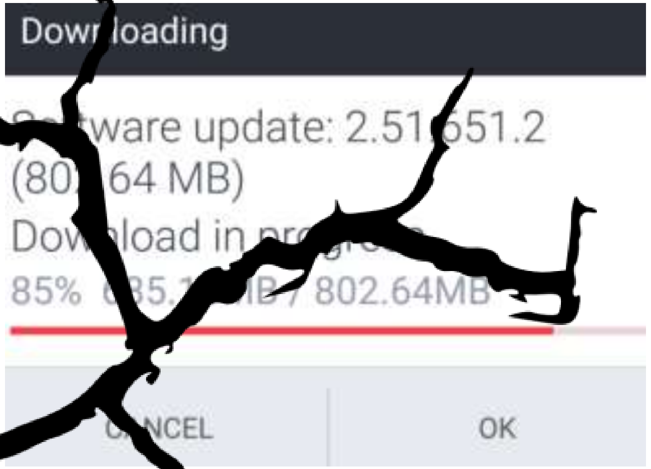
World's First ‘High-Assurance’ Encryption Based File Sharing And Collaboration Tool

2017

First Certified Ultra-Fast 100Gbps Ethernet Encryptor To Support All Topologies

Encryption=digital cement





Downloading

Software update: 2.51.651.2
(802.64 MB)

Download in progress

85% 685.1 MB / 802.64MB

Encryption for Everyone

PGP

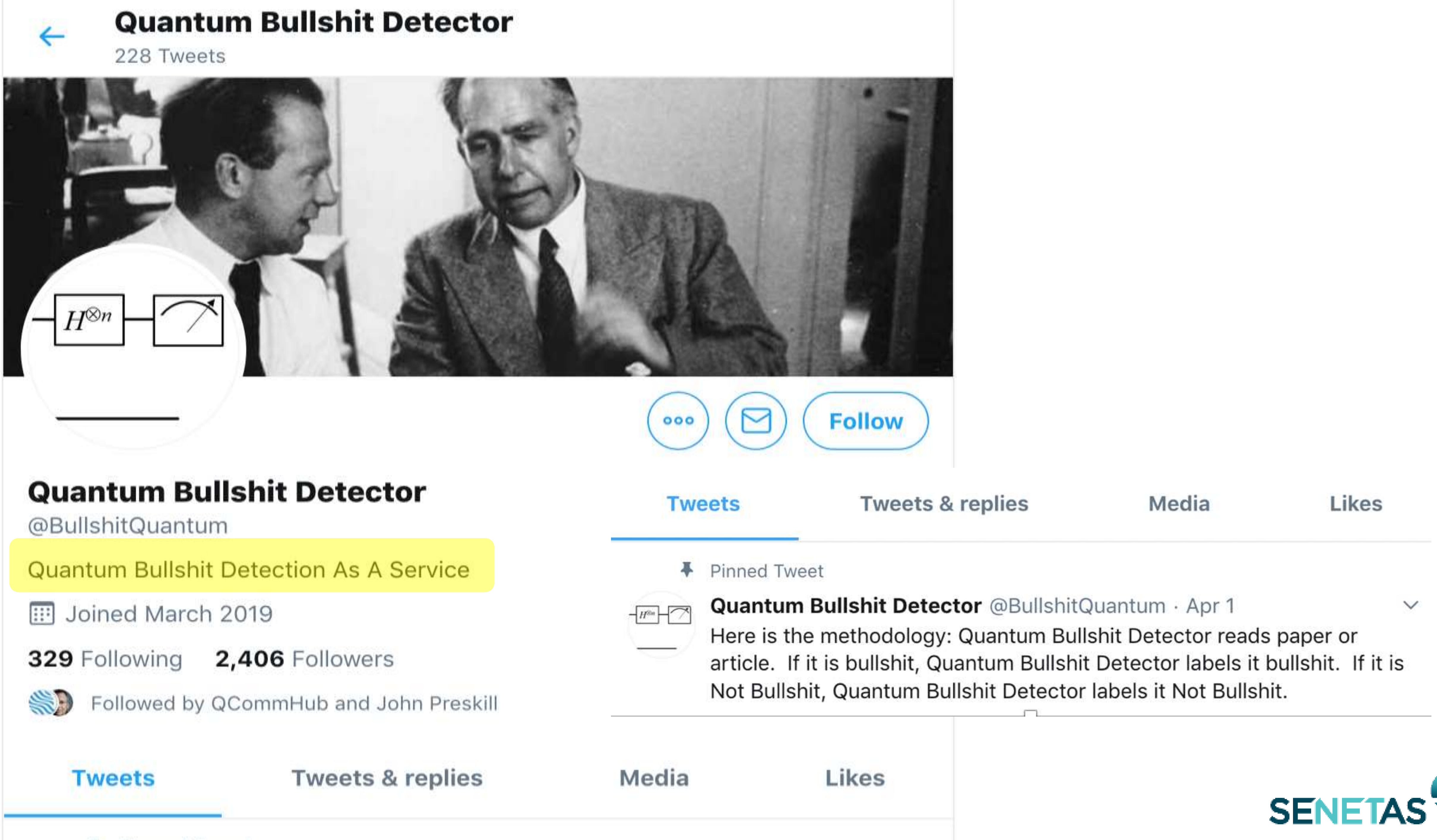
Pretty Good Privacy

HARDENED

PGP

Simson Garfinkel

O'Reilly & Associates, Inc.



Quantum Bullshit Detector

228 Tweets

Quantum Bullshit Detector

@BullshitQuantum

Quantum Bullshit Detection As A Service

Joined March 2019

329 Following **2,406** Followers

Followed by QCommHub and John Preskill

Pinned Tweet

Quantum Bullshit Detector @BullshitQuantum · Apr 1

Here is the methodology: Quantum Bullshit Detector reads paper or article. If it is bullshit, Quantum Bullshit Detector labels it bullshit. If it is Not Bullshit, Quantum Bullshit Detector labels it Not Bullshit.

What is a quantum computer?

A *proposed* new type of computer that seeks to exploit the properties of quantum mechanics such as entanglement and superposition to exponentially speedup computing performance for *some* hard problems

What is a quantum computer?

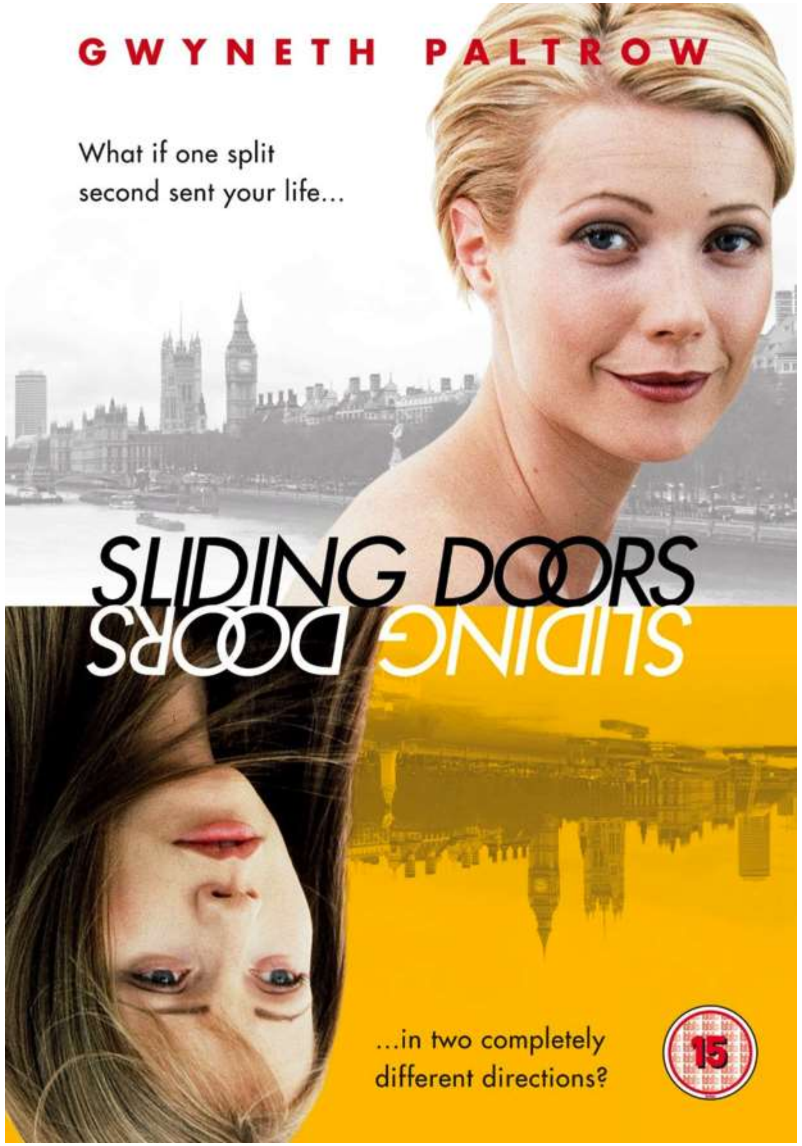
What Quantum Computing Isn’t – Scott Aaronson TED

“The study of what we can’t do with computers we don’t have”

What Quantum Computing Isn't | Scott Aaronson | TEDxDresden

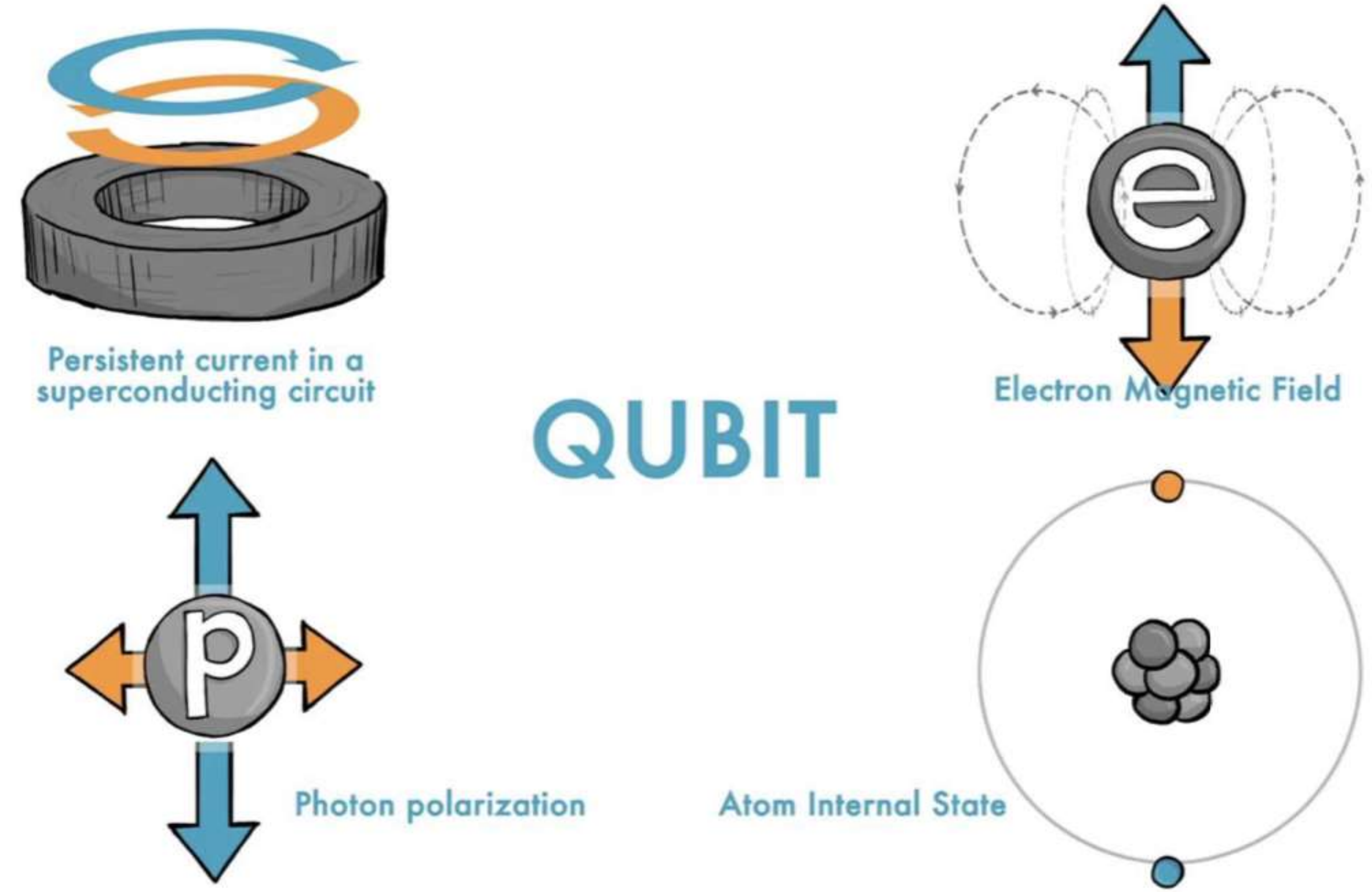
Gwyneth Paltrow interpretation of quantum computing

- ‘Many-worlds’ theory


GWYNETH PALTROW
What if one split second sent your life...
SLIDING DOORS
SLIDING DOORS
...in two completely different directions?
15

SENETAS

How to build a Qubit



Credit John Prescott @ Cornell Quantum NISQ and Beyond 2019

How to build a Quantum Computer from Qubits

1. You must be able to build qubits and build them in a way that allows you “scale up” to thousands or millions of qubits for a full quantum computer.

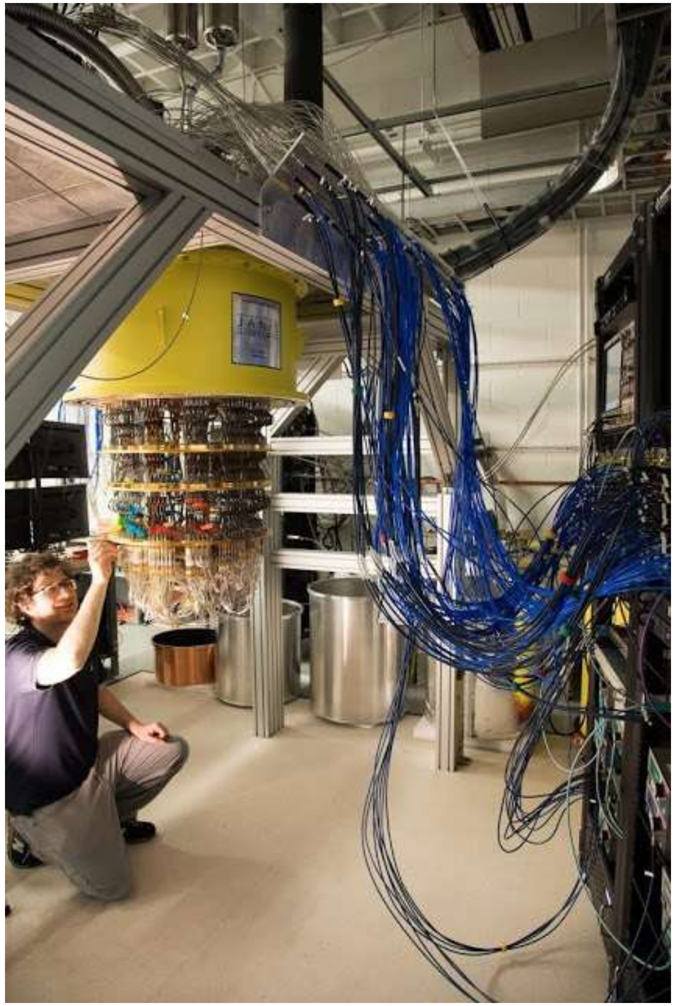
2. You must be able to initialise these qubits in some known state.

3. These qubits must have long decoherence times.

4. You must be able to apply operations or gates to these qubits which are “universal”.

5. You must be able to measure (at least some of) the qubits.

Quantum computers are not science fiction



Google Bristlecone - 76 Qubits

IBM Q – 20 Qubits

Noisy Intermediate Scale Quantum (NISQ)

- NISQ technology will be available in the near future
- Noise in quantum gates will limit the size to 50-100’s qubits
- May surpass abilities of classical digital computers (***quantum supremacy***)

- This is a significant step towards more powerful quantum computers
- But ……it will not change the world

How a Quantum Computer impacts cryptography

Grover

1

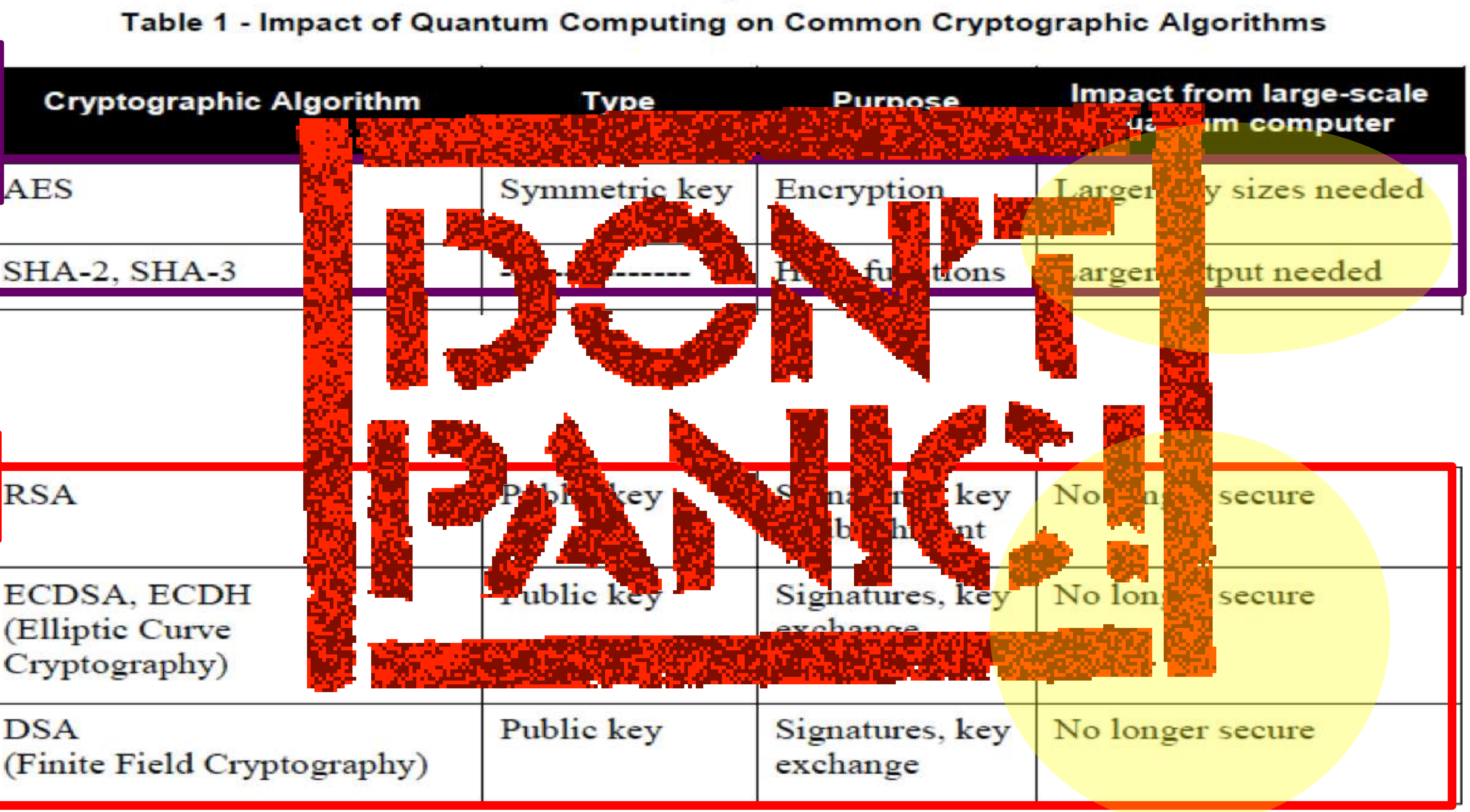


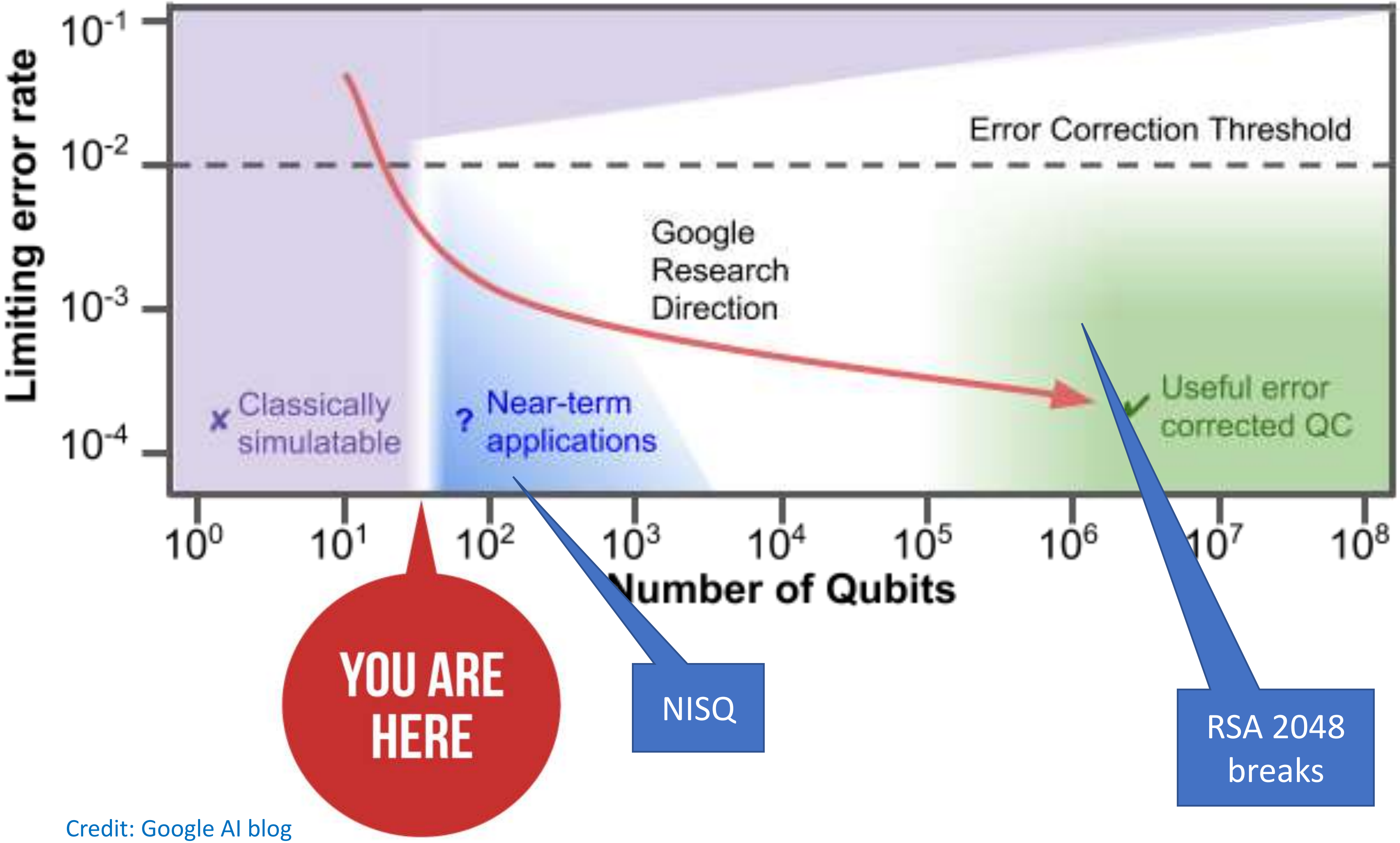
Table 1 - Impact of Quantum Computing on Common Cryptographic Algorithms

Cryptographic Algorithm	Type	Purpose	Impact from large-scale quantum computer
AES	Symmetric key	Encryption	Larger key sizes needed
SHA-2, SHA-3	-----------	Hash functions	Larger output needed
RSA	Public key	Signatures, key establishment	No longer secure
ECDSA, ECDH (Elliptic Curve Cryptography)	Public key	Signatures, key exchange	No longer secure
DSA (Finite Field Cryptography)	Public key	Signatures, key exchange	No longer secure

Shor

2

DON'T PANIC!



YOU ARE HERE

NISQ

RSA 2048 breaks

Credit: Google AI blog

How real is the threat?

Timeframe **(to develop large scale QC)**	**Impact**	**Likelihood**	**Risk**
Short term *(1-5 years)*	HIGH	LOW	MEDIUM
Medium term *(5-10 years)*	HIGH	MEDIUM	HIGH
Long term *(10-20 years)*	HIGH	HIGH	EXTREME

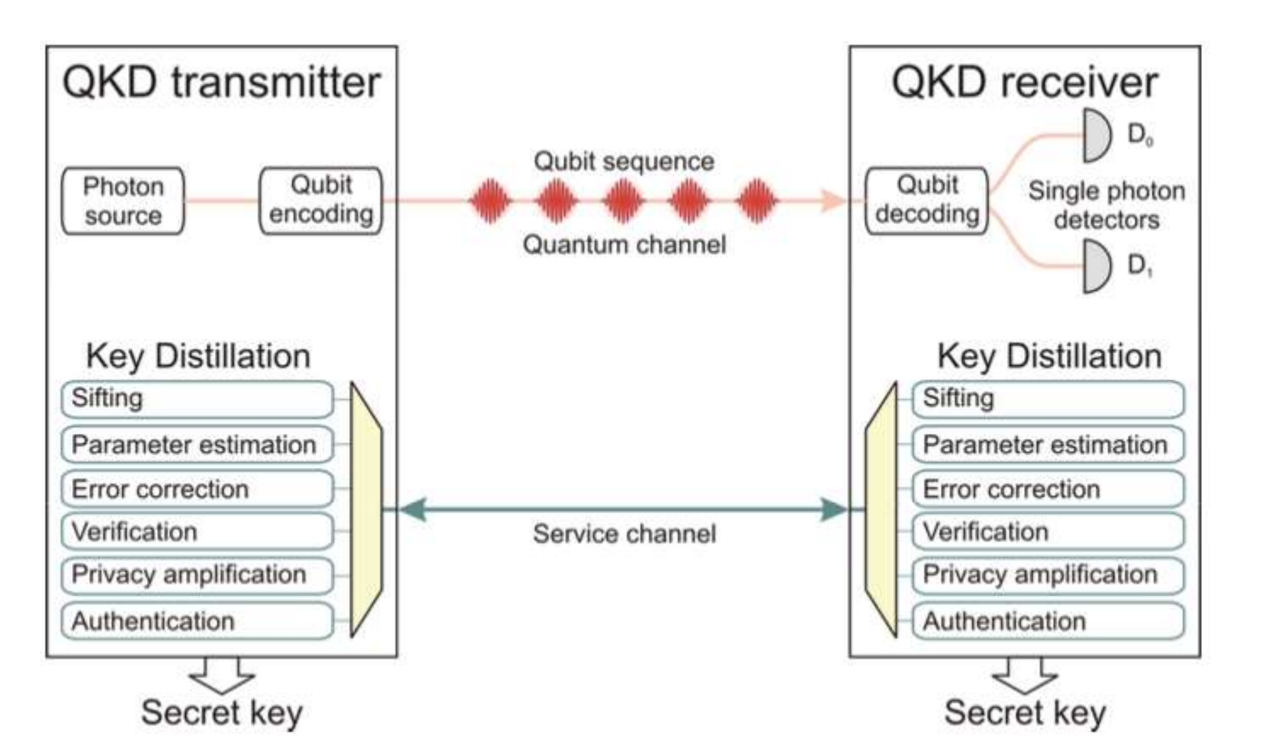
NO low risk outcome

“Hope is not a strategy”

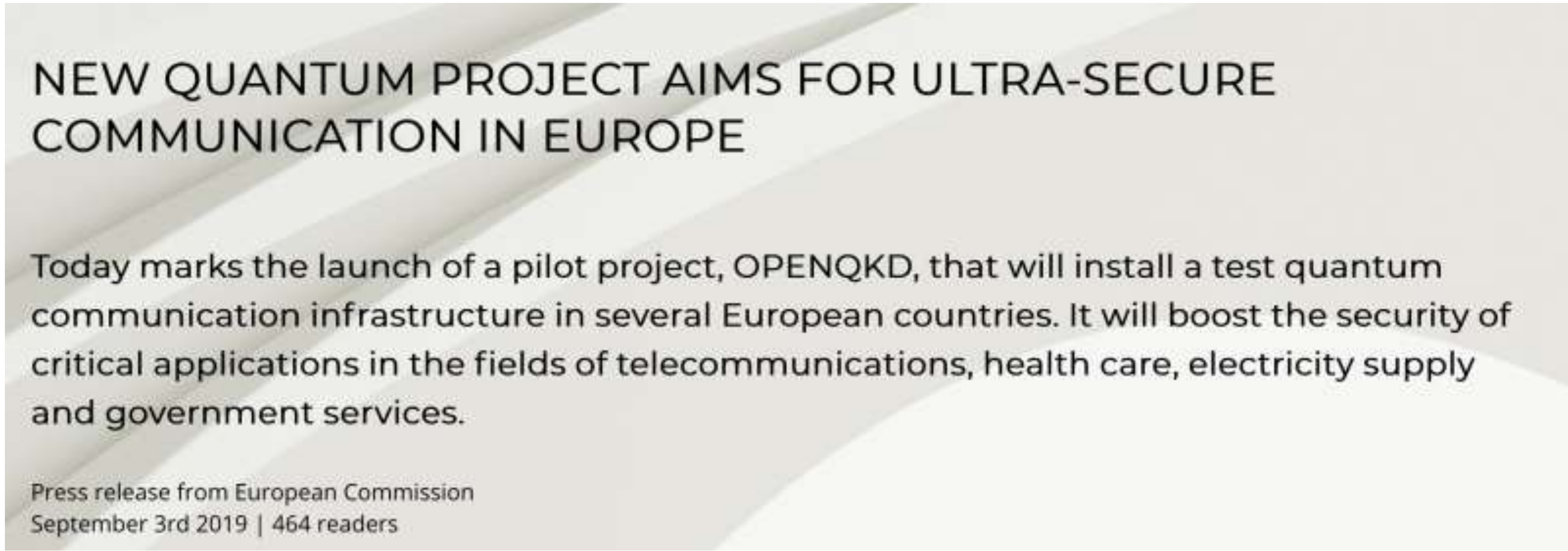
Quantum Safe Security

#1 Quantum Key Distribution (QKD)

- Fundamentally different approach
- Distributes keys based on principles of physics not mathematics



SENETAS



NEW QUANTUM PROJECT AIMS FOR ULTRA-SECURE COMMUNICATION IN EUROPE

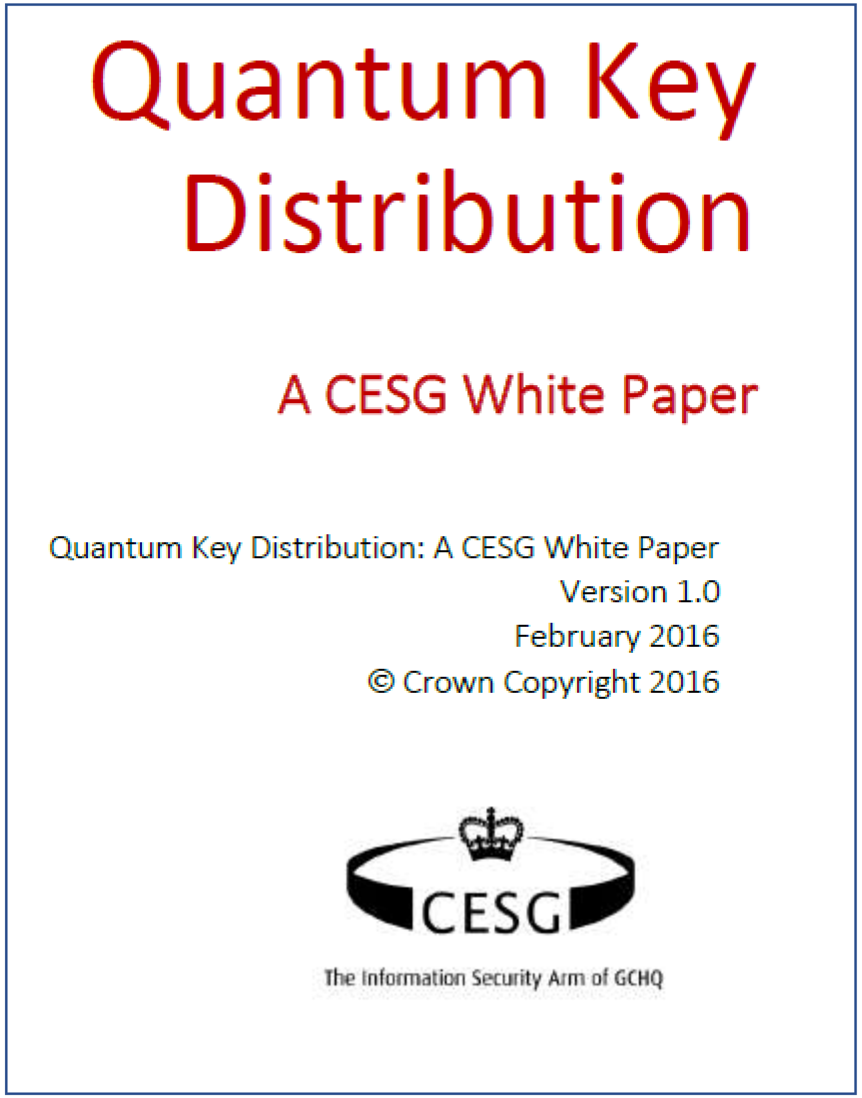
Today marks the launch of a pilot project, OPENQKD, that will install a test quantum communication infrastructure in several European countries. It will boost the security of critical applications in the fields of telecommunications, health care, electricity supply and government services.

Press release from European Commission
September 3rd 2019 | 464 readers

Open European Quantum Key Distribution Testbed

- Establishment of QKD-based secure communication
- Access to robust and reliable crypto technology to secure traditional industries and vertical application sectors
- Preparation for pan-European QKD infrastructure

Intelligence agency view

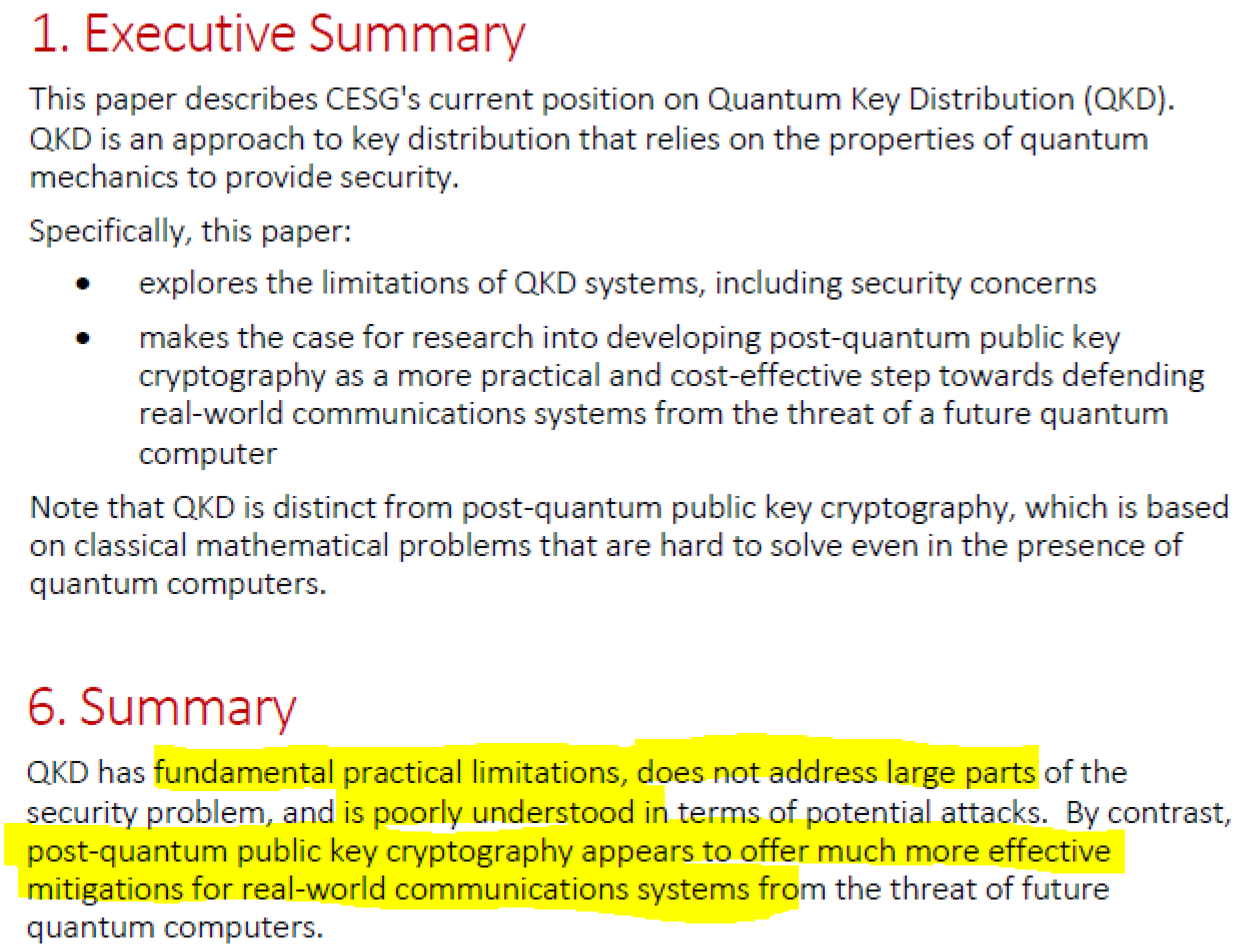


Quantum Key Distribution

A CESG White Paper

Quantum Key Distribution: A CESG White Paper
Version 1.0
February 2016
© Crown Copyright 2016

CESG
The Information Security Arm of GCHQ



1. Executive Summary

This paper describes CESG's current position on Quantum Key Distribution (QKD). QKD is an approach to key distribution that relies on the properties of quantum mechanics to provide security.

Specifically, this paper:

- explores the limitations of QKD systems, including security concerns
- makes the case for research into developing post-quantum public key cryptography as a more practical and cost-effective step towards defending real-world communications systems from the threat of a future quantum computer

Note that QKD is distinct from post-quantum public key cryptography, which is based on classical mathematical problems that are hard to solve even in the presence of quantum computers.

6. Summary

QKD has fundamental practical limitations, does not address large parts of the security problem, and is poorly understood in terms of potential attacks. By contrast, post-quantum public key cryptography appears to offer much more effective mitigations for real-world communications systems from the threat of future quantum computers.

Quantum Safe Security

#2 Quantum Resistant Algorithms (QRA)

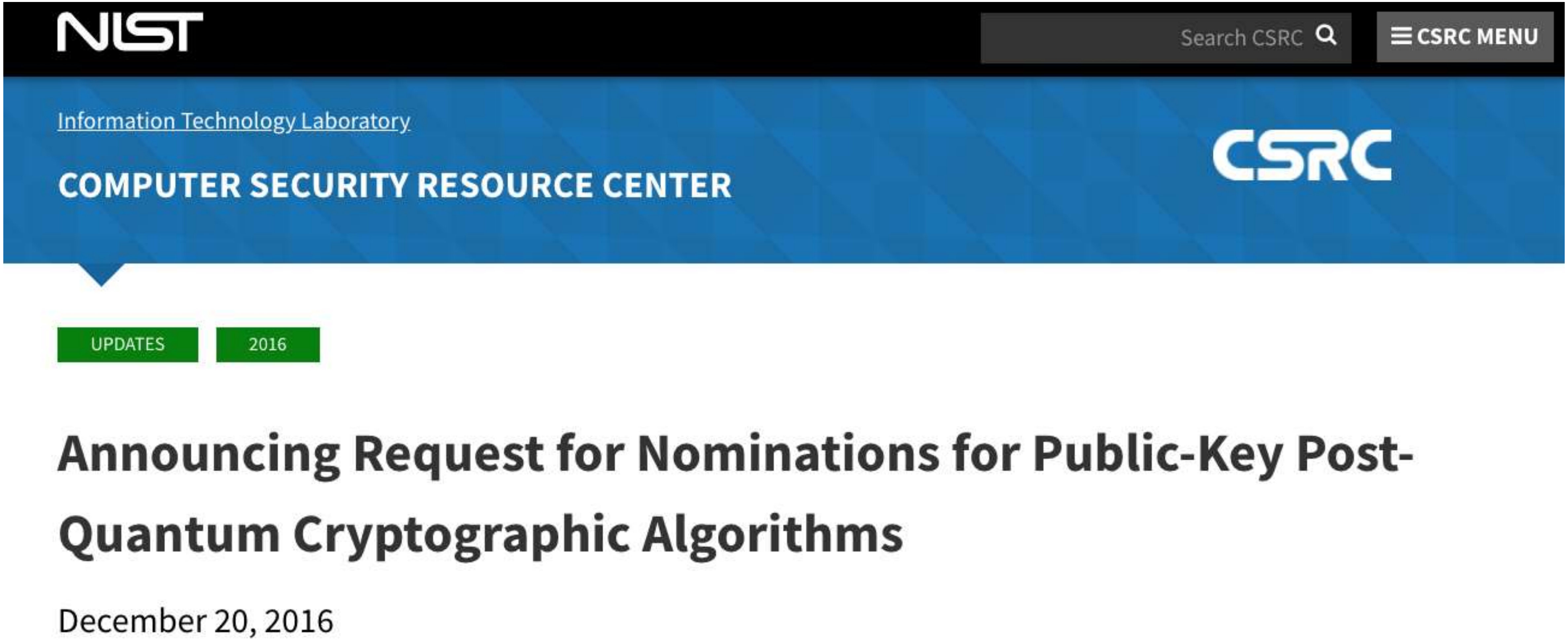
- Quantum safe algorithms
- Lattice based cryptography
- Multivariate cryptography
- Hash based cryptography
- Code-based cryptography
- E.g. New Hope

What we require:

Secure against all known and future classical attacks

Secure against all known and future quantum attacks

Post Quantum Cryptography Standardisation



Information Technology Laboratory

COMPUTER SECURITY RESOURCE CENTER

UPDATES 2016

Announcing Request for Nominations for Public-Key Post-Quantum Cryptographic Algorithms

December 20, 2016

SUBMISSIONS TO NIST CALL FOR PROPOSALS

- 82 total submissions received from 26 Countries, 6 Continents
  - The submitters in USA are from 16 States
- 69 accepted as "complete and proper"   (5 since withdrawn)

	Signatures	KEM/Encryption	Overall
Lattice-based	5	21	26
Code-based	2	17	19
Multi-variate	7	2	9
Stateless Hash-based/Symmetric based	3		3
Other	2	5	7
Total	**19**	**45**	**64**

NIST TIMELINE AND REMARKS

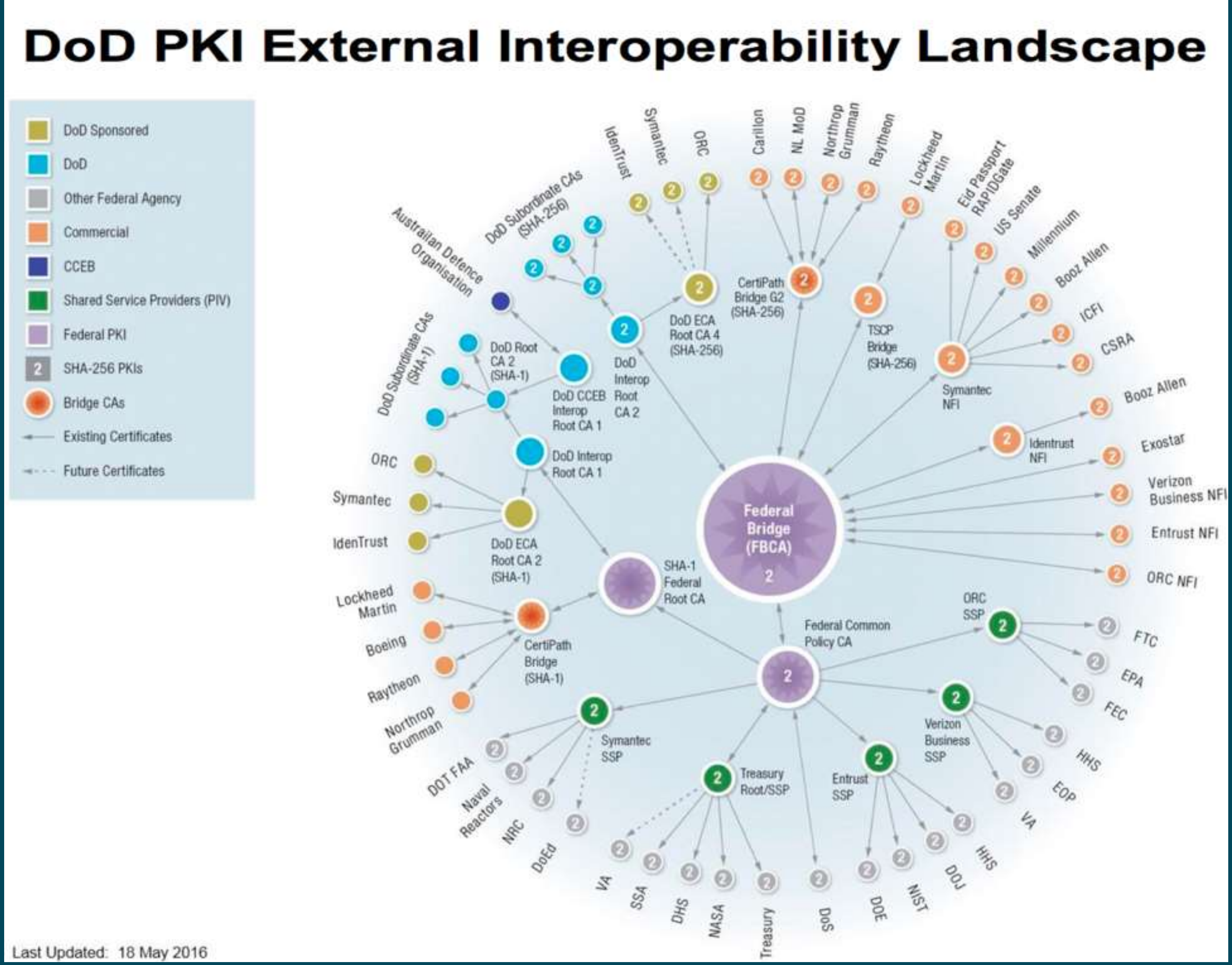
- After the 1st NIST PQC Standardization Conference
  - Allow similar submissions to merge and submit before November 30
- 2018/2019 – 2nd Round begins (smaller number of submissions)
  - minor changes/tweaks allowed
- Aug 2019 – 2nd NIST PQC Workshop
- 2020/2021 - Select algorithms or start a 3rd Round
- 2022-2024 - Draft standards available

Some submitted algorithms may not be selected in the second round and neither be excluded for future consideration.

We may select one or two to standardize and leave others as 3rd round candidates and maintain a separate list for future consideration. It may not be the case to select winners and exclude all the others in one pass.

The standard development may last longer than two or three years based on the development of quantum computers and the maturity of the PQC algorithms.

Industry Impact

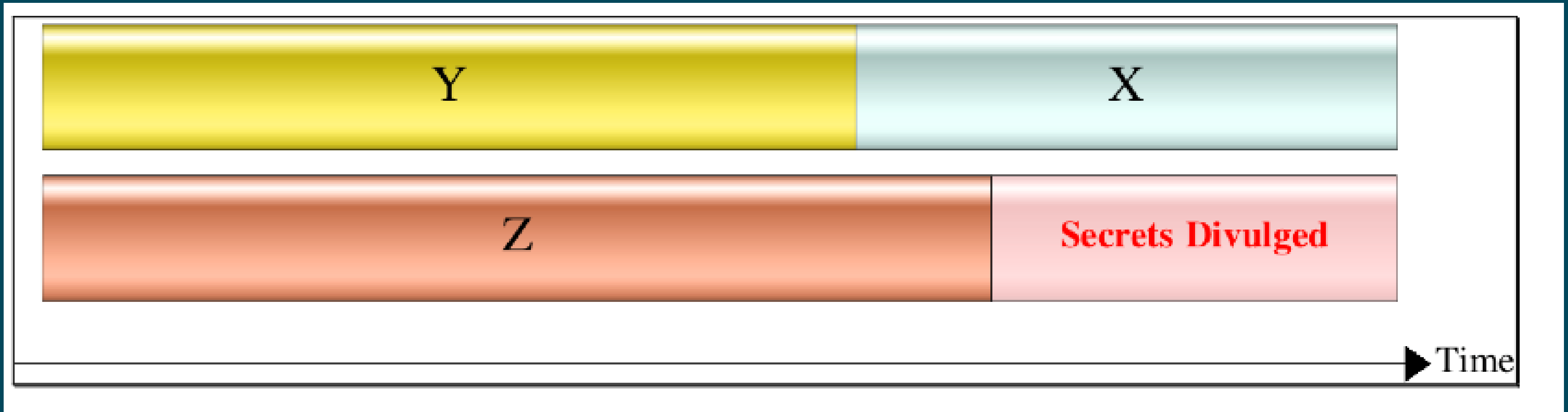


DoD PKI External Interoperability Landscape

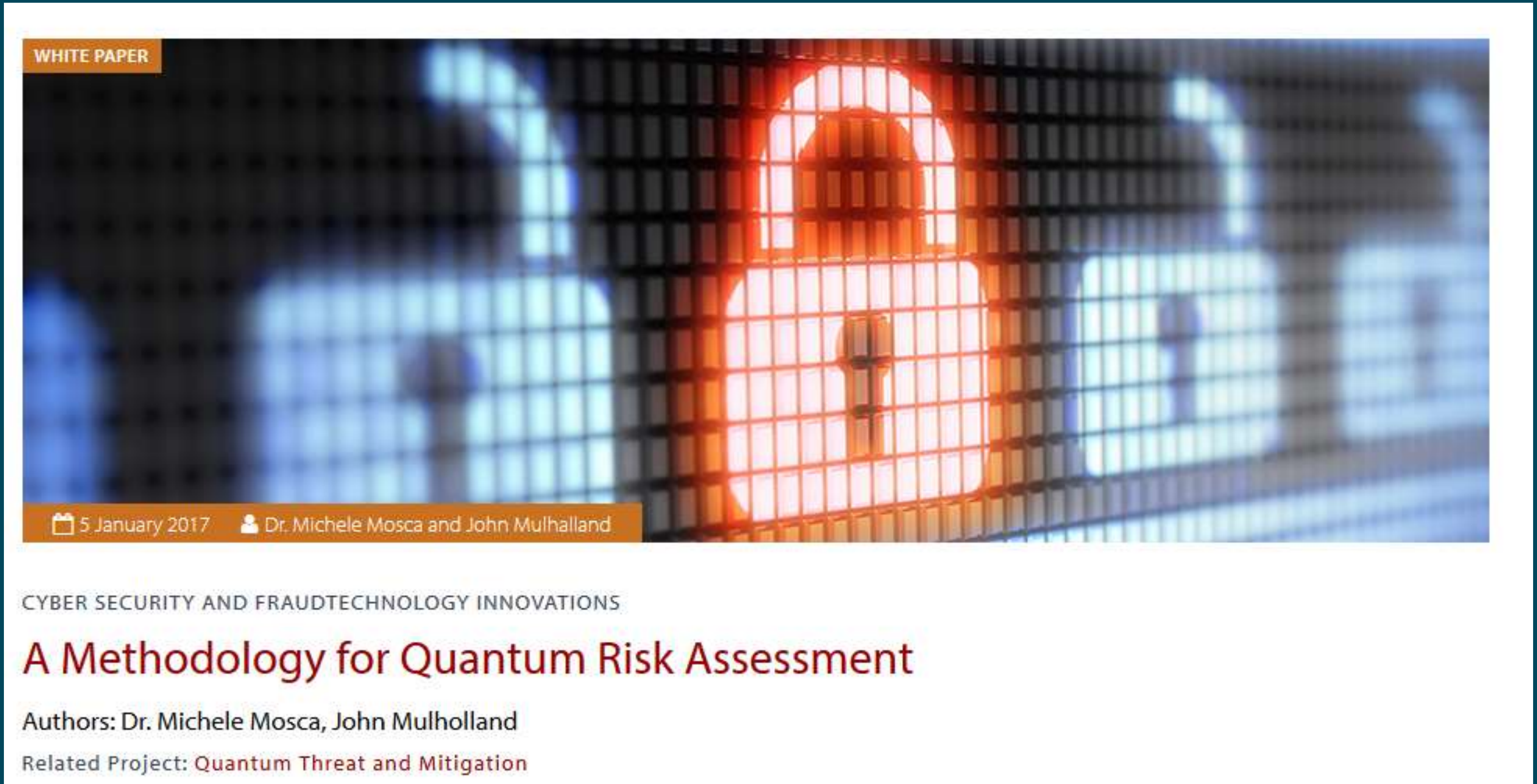
Last Updated: 18 May 2016

Harvest & Decrypt Threat: Mosca's law

- X: "how many years we need to keep our encrypted data"
- Y: "how many years it will take us to make our IT infrastructure quantum-safe"
- Z: "how many years before a large-scale quantum computer will be built"



Quantum Risk Assessment



WHITE PAPER

5 January 2017 Dr. Michele Mosca and John Mulhalland

CYBER SECURITY AND FRAUDTECHNOLOGY INNOVATIONS

A Methodology for Quantum Risk Assessment

Authors: Dr. Michele Mosca, John Mulholland

Related Project: Quantum Threat and Mitigation

Quantum Risk Assessment Model

- **Phase 1-** Identify and document information assets, and their current cryptographic protection.
- **Phase 2-** Research the state of emerging quantum computers and quantum-safe cryptography. Estimate the timelines for availability of these technologies. Influence the development and validation of quantum-safe cryptography.
- **Phase 3-** Identify threat actors, and estimate their time to access quantum technology "z".
- **Phase 4-** Identify the lifetime of your assets "x", and the time required to transform the organization's technical infrastructure to a quantum-safe state "y".
- **Phase 5-** Determine quantum risk by calculating whether business assets will become vulnerable before the organization can move to protect them. ($x + y > z$?)
- **Phase 6-** Identify and prioritize the activities required to maintain awareness, and to migrate the organization's technology to a quantum-safe state.

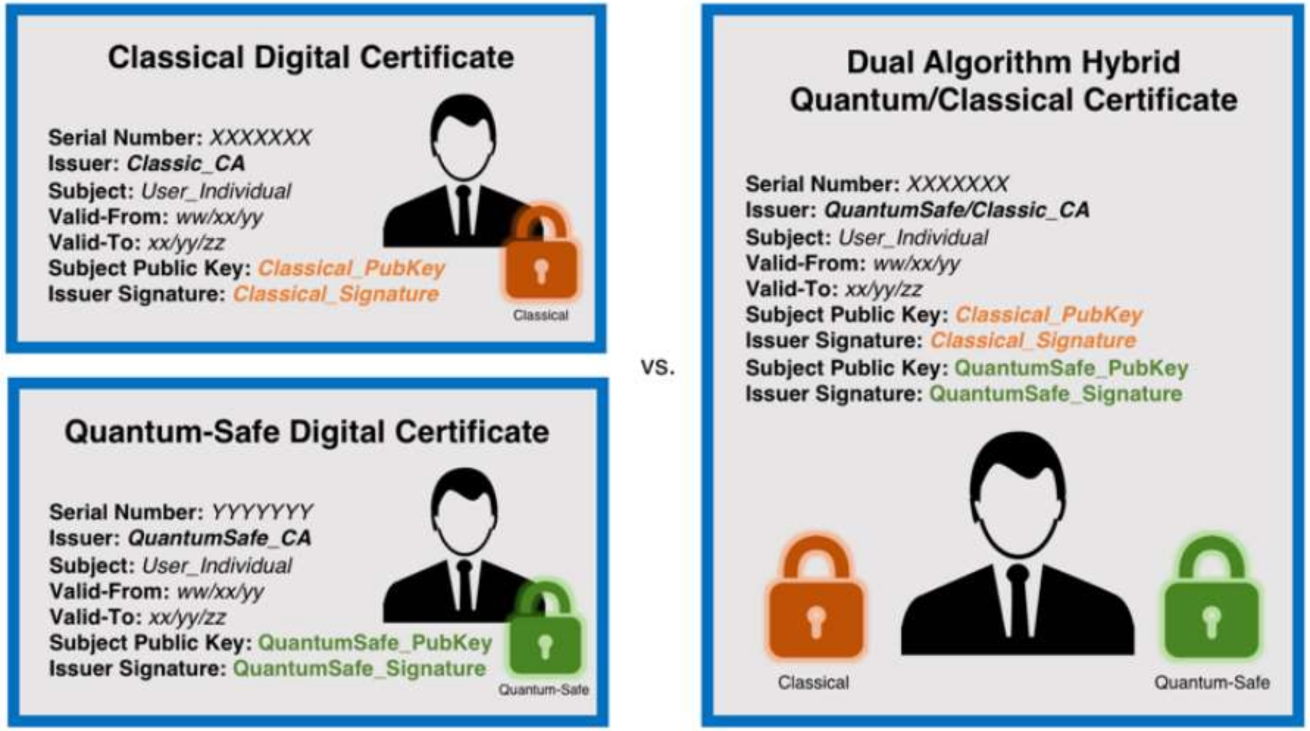
http://www.evolutionq.com/methodology-for-qra.html

The importance of Crypto-Agility

> The ability to quickly modify underlying crypto primitives of a system in the face of new and emerging attack vectors.

Quantum Safe Multi-Key Certificate mechanisms

- Multiple Certificates
- “Hybrid” v3 extensions
- “Composite” concatenated keys and signatures



Classical Digital Certificate

Serial Number: *XXXXXXX*
Issuer: ***Classic_CA***
Subject: *User_Individual*
Valid-From: *ww/xx/yy*
Valid-To: *xx/yy/zz*
Subject Public Key: *Classical_PubKey*
Issuer Signature: *Classical_Signature*

vs.

Quantum-Safe Digital Certificate

Serial Number: *YYYYYYY*
Issuer: ***QuantumSafe_CA***
Subject: *User_Individual*
Valid-From: *ww/xx/yy*
Valid-To: *xx/yy/zz*
Subject Public Key: QuantumSafe_PubKey
Issuer Signature: QuantumSafe_Signature

Dual Algorithm Hybrid Quantum/Classical Certificate

Serial Number: *XXXXXXX*
Issuer: ***QuantumSafe/Classic_CA***
Subject: *User_Individual*
Valid-From: *ww/xx/yy*
Valid-To: *xx/yy/zz*
Subject Public Key: *Classical_PubKey*
Issuer Signature: *Classical_Signature*
Subject Public Key: QuantumSafe_PubKey
Issuer Signature: QuantumSafe_Signature

Credit: https://www.isara.com/cryptographic-certificates-quantum-safe/

Our advice to customers

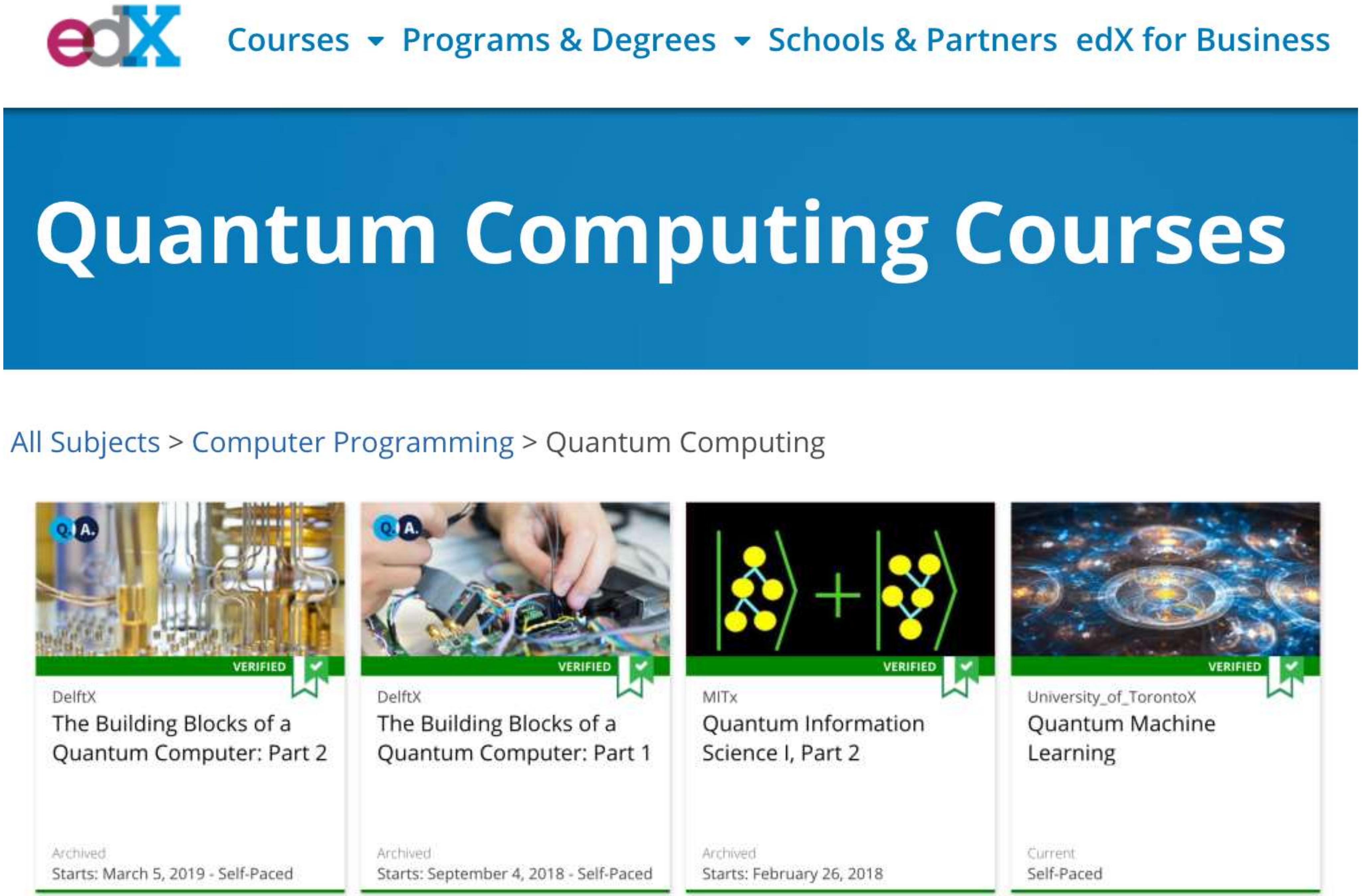
- Trust the maths – encryption is still strong
- Be sceptical of implementations more than algorithms
- Look for some assurance beyond the vendors word – independent certifications or testing can help
- Change is coming so start thinking about this now
  - Consider a Quantum Risk Assessment
  - Ask your vendors if they are building crypto-agile solutions

Resources to get more information

- Quantum Information Science
  - https://www.nist.gov/topics/quantum-information-science
  - https://www.scottaaronson.com/blog/
  - http://www.cornell.edu/video/john-preskill-quantum-computing-nisq-era-beyond

- Post Quantum Cryptography
  - https://csrc.nist.gov/Projects/Post-Quantum-Cryptography

- Quantum Resistant Software libraries
  - https://openquantumsafe.org/
  - https://libpqcrypto.org/
  - https://www.microsoft.com/en-us/research/project/post-quantum-cryptography/



Courses ▾ Programs & Degrees ▾ Schools & Partners edX for Business

Quantum Computing Courses

All Subjects > Computer Programming > Quantum Computing

VERIFIED

DelftX

The Building Blocks of a Quantum Computer: Part 2

Archived

Starts: March 5, 2019 - Self-Paced

VERIFIED

DelftX

The Building Blocks of a Quantum Computer: Part 1

Archived

Starts: September 4, 2018 - Self-Paced

VERIFIED

MITx

Quantum Information Science I, Part 2

Archived

Starts: February 26, 2018

VERIFIED

University_of_TorontoX

Quantum Machine Learning

Current

Self-Paced

Thank You

Questions?

LUNCH

CYBER
smart
safe
secure

Please be back by **1:45pm**

AISA

Management lessons learnt: Security operations and incident response

Andrew Scully

Head of Cyber Security at Shelde

One bloke's lessons learnt –

Failing, winning, but always learning.

What are we going to cover?

1 Scully has Cyber Performance Anxiety

2 Cyber security is a team sport - The Continuous Cyber Maturity Model

3 When stuff goes bang - Cyber response will make or break you.

ACRONYMS –

SOB - Scully Observations

SFLL - Scully Fail Lesson Learnt

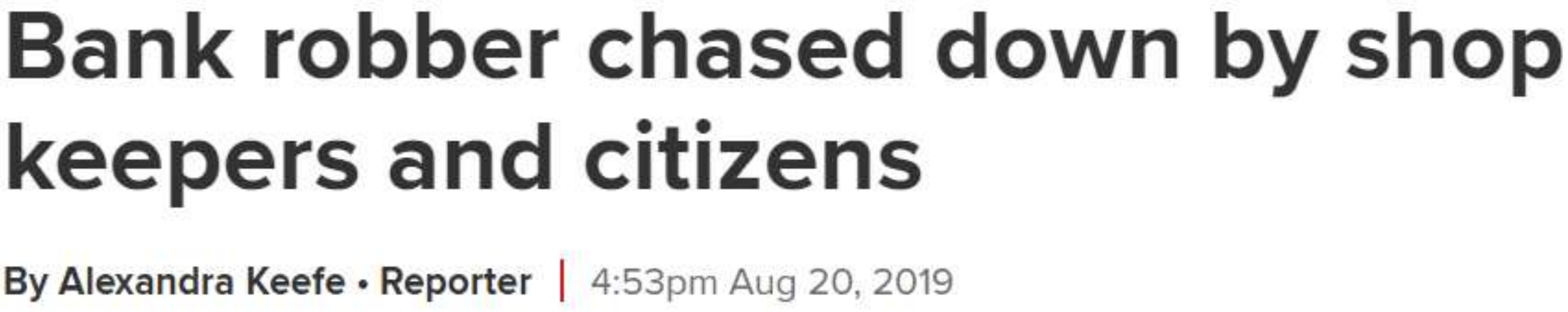
SOBFLL - Scully Observations Lessons Learnt

I HAVE CYBER PERFORMANCE ANXIETY

SOB

Cyber security is in its infancy

SOB – We need to be realistic about what we CAN and SHOULD achieve



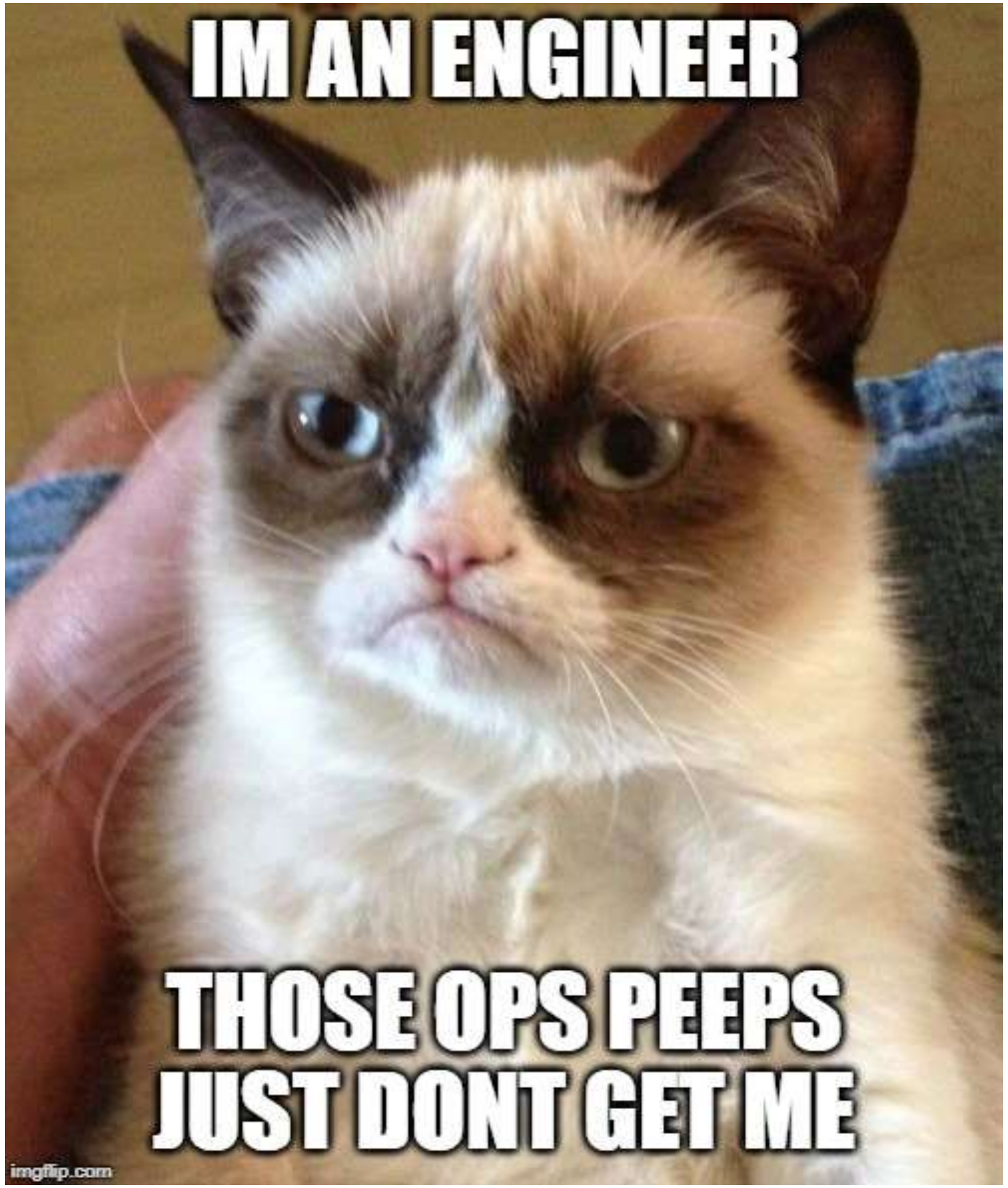
Bank robber chased down by shop keepers and citizens

By Alexandra Keefe • Reporter | 4:53pm Aug 20, 2019

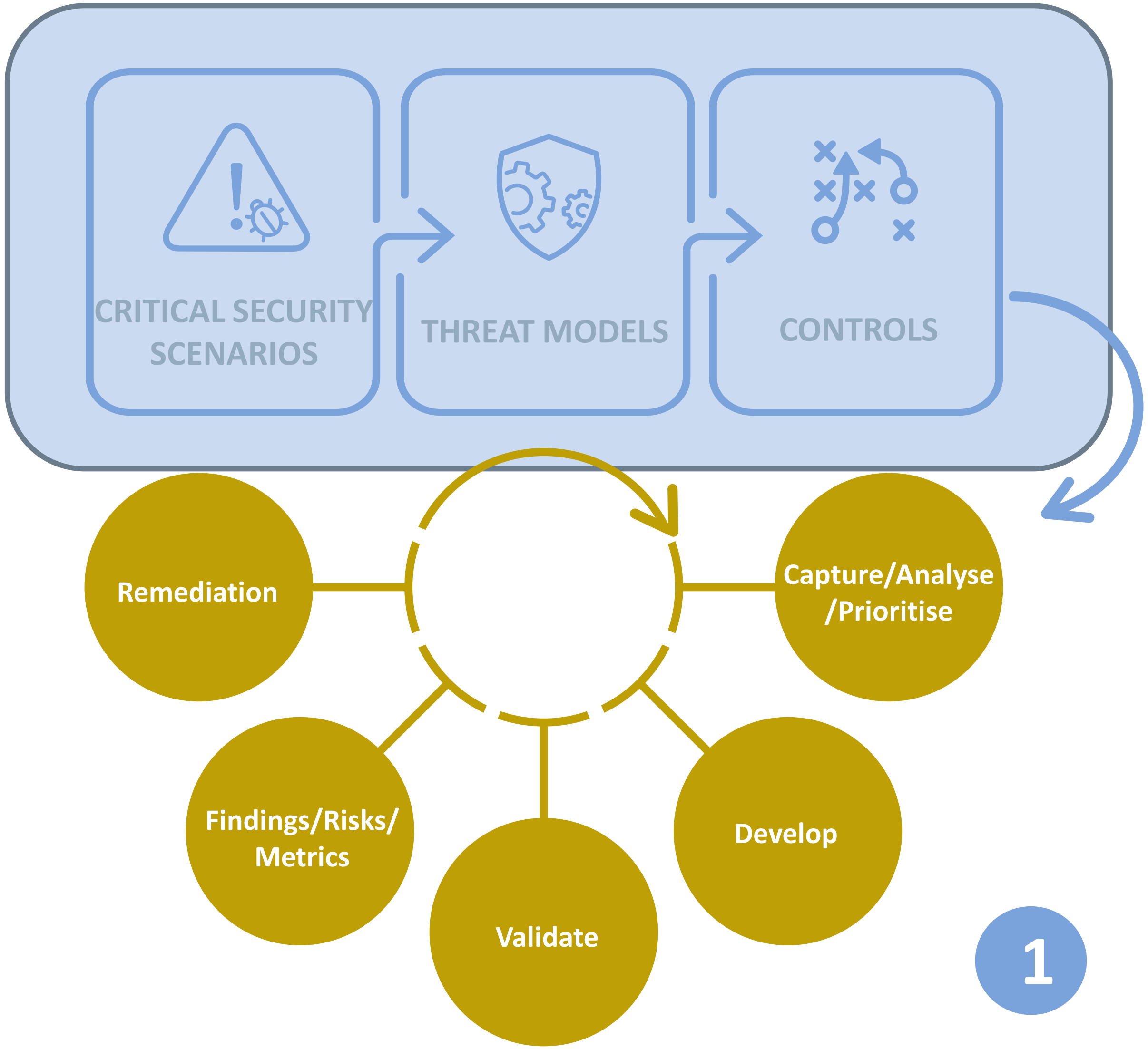
SODELL

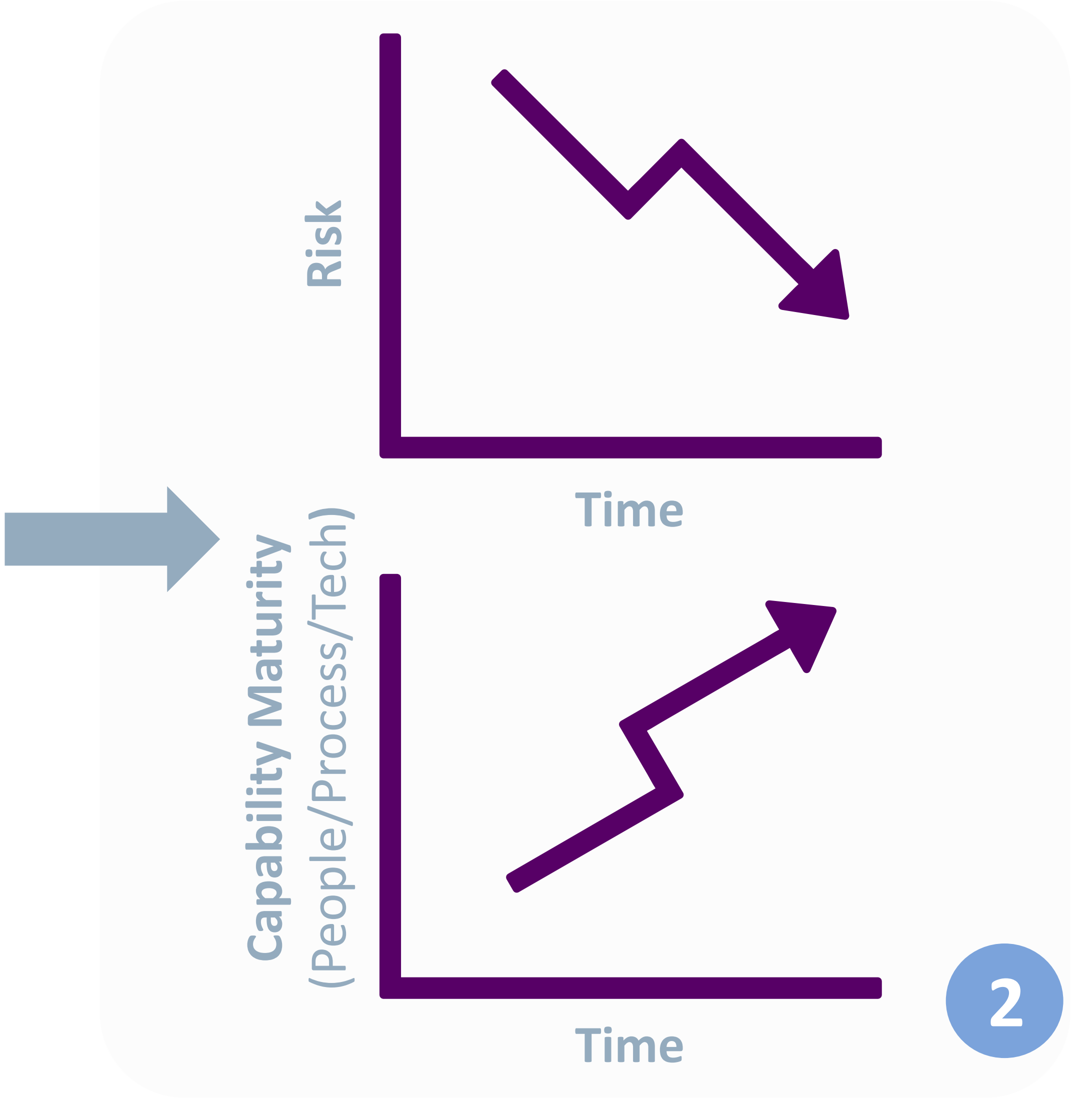
Articulating HOW the team works together is 'problematic'

Cyber security operations is a team sport



CONOPS – "CONTINUOUS CYBER MATURITY"





SOBFLL

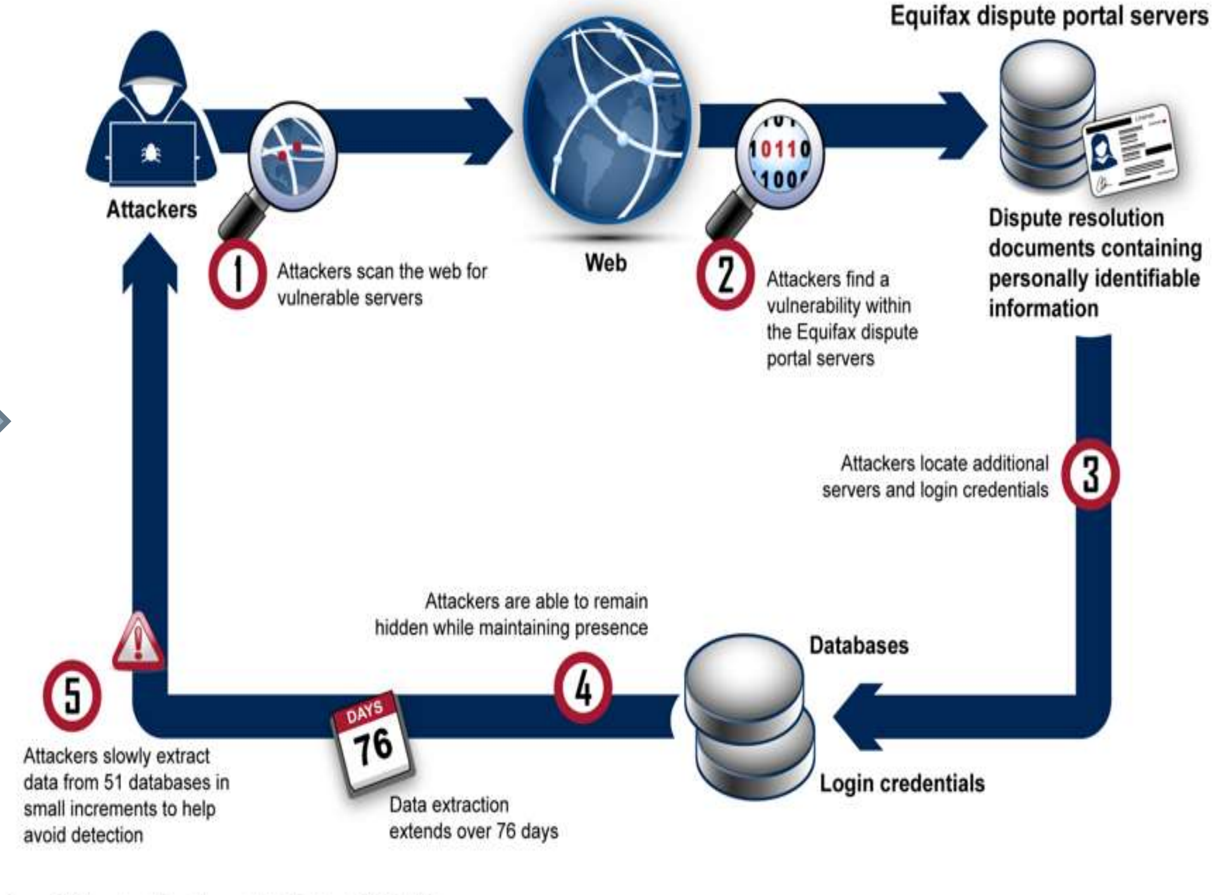
Understand your organisations "Critical Security Scenarios (CSS)"

CSS > Threat Models

EXAMPLE CSS – *“A large scale public data breach resulting in catastrophic* impact to brand, reputation and revenue”*

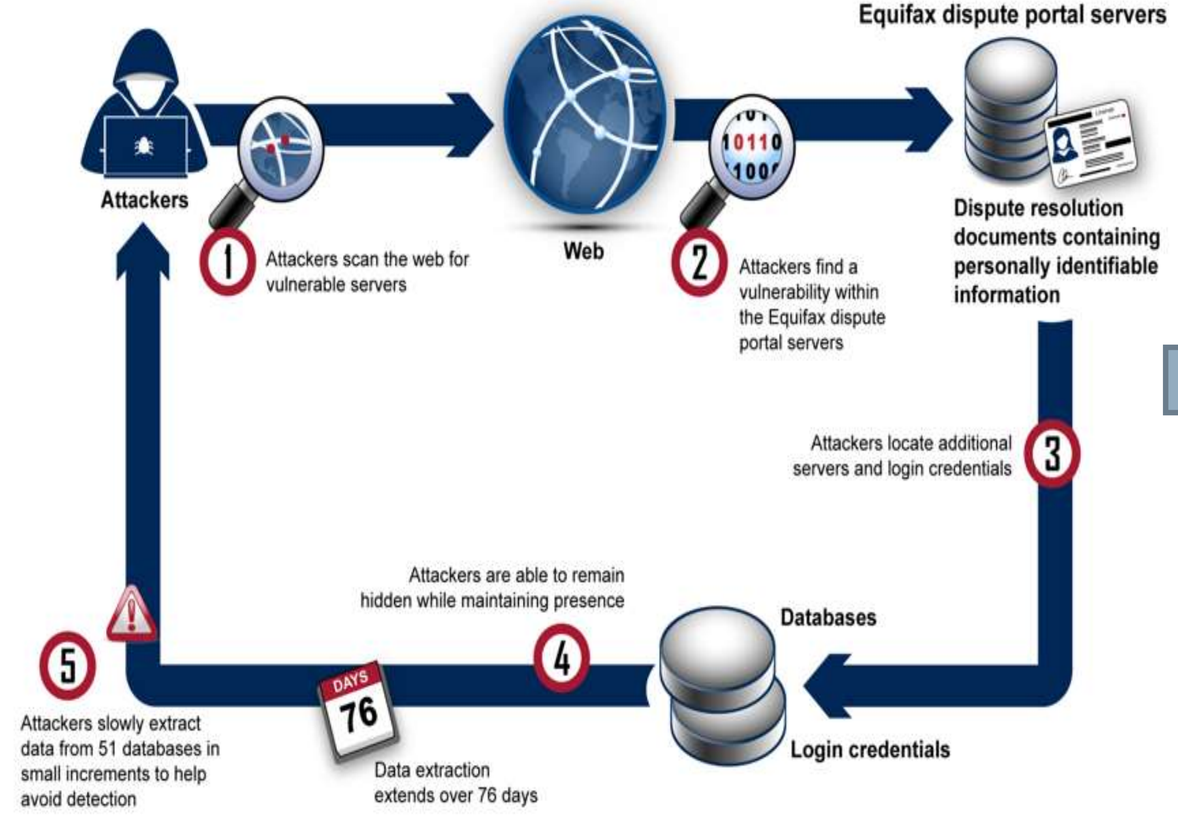
ISO 27001

NIST 800-53


Attackers
1 Attackers scan the web for vulnerable servers
Web
2 Attackers find a vulnerability within the Equifax dispute portal servers
Equifax dispute portal servers
Dispute resolution documents containing personally identifiable information
Attackers locate additional servers and login credentials 3
Databases
Login credentials
Attackers are able to remain hidden while maintaining presence 4
DAYS 76
Data extraction extends over 76 days
5 Attackers slowly extract data from 51 databases in small increments to help avoid detection

Source: GAO, based on information provided by Equifax. | GAO-18-559

Threat Models > Controls (Prevent, Detect, Respond Recover)



Equifax dispute portal servers

Attackers

Web

1 Attackers scan the web for vulnerable servers

2 Attackers find a vulnerability within the Equifax dispute portal servers

Dispute resolution documents containing personally identifiable information

3 Attackers locate additional servers and login credentials

Databases

Login credentials

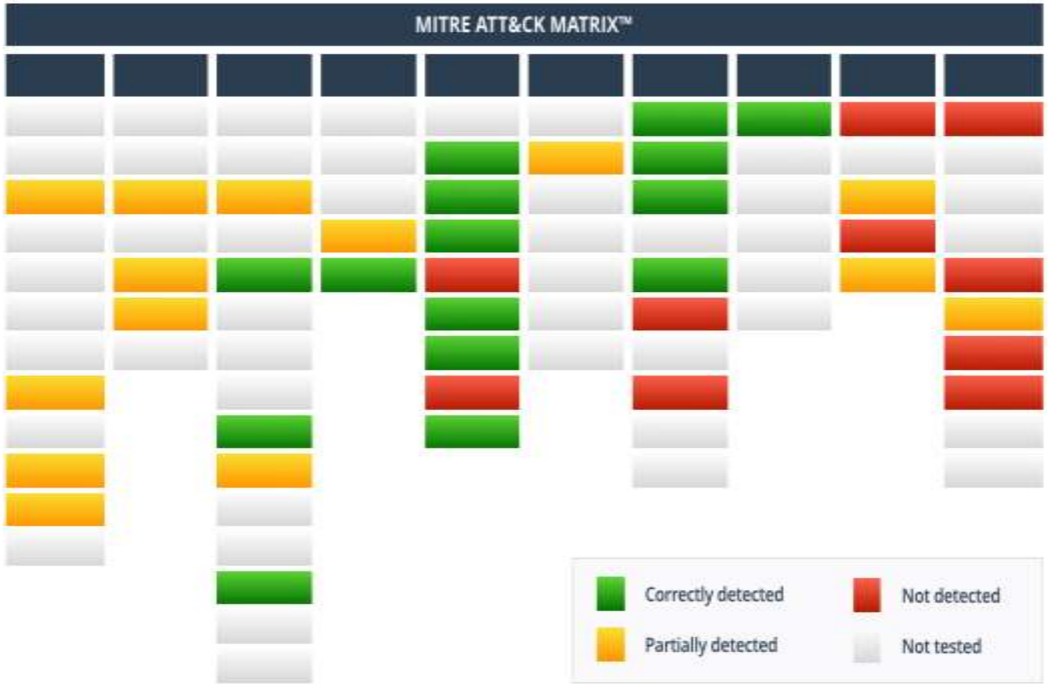
4 Attackers are able to remain hidden while maintaining presence

DAYS 76

Data extraction extends over 76 days

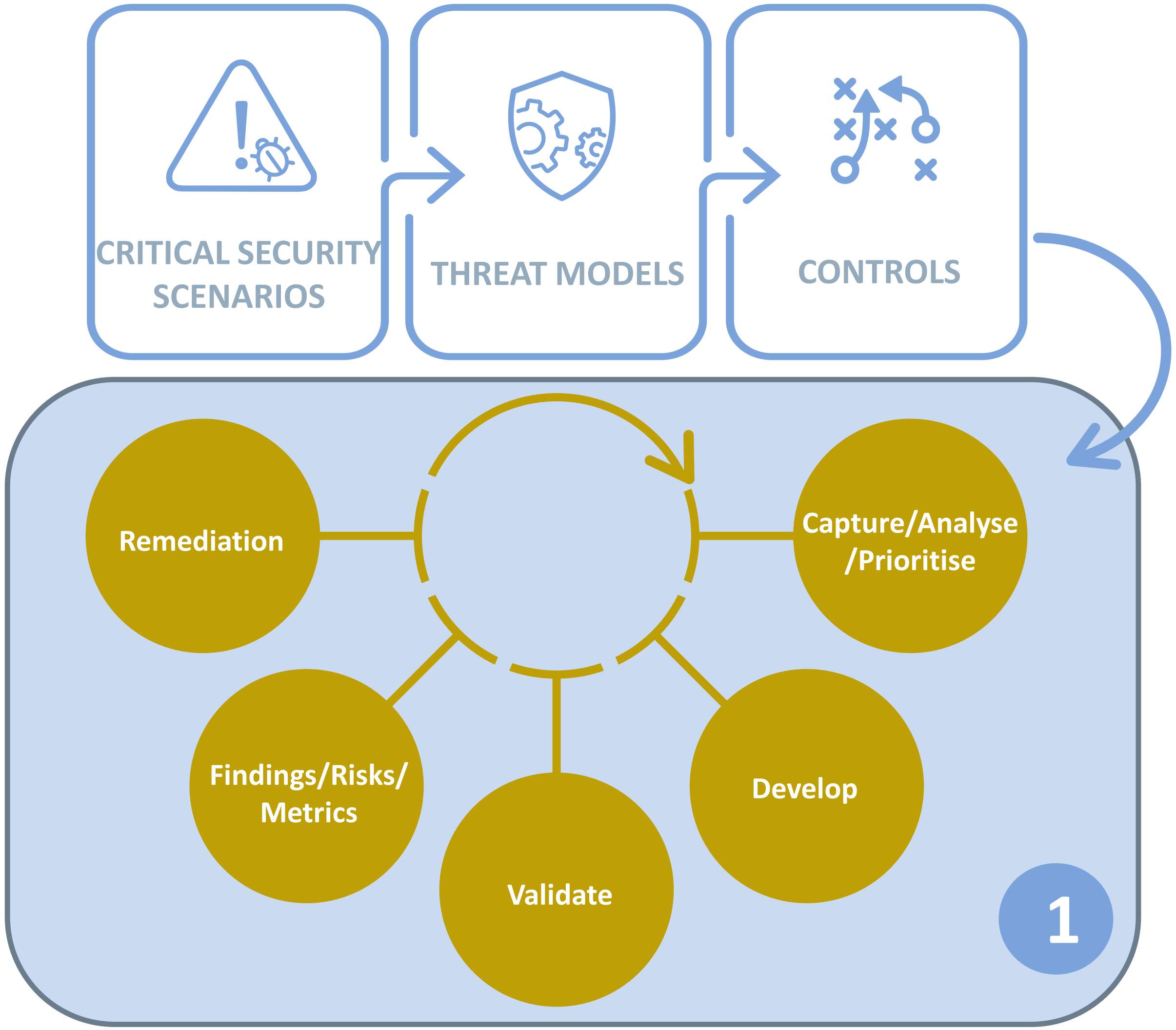
5 Attackers slowly extract data from 51 databases in small increments to help avoid detection

Source: GAO, based on information provided by Equifax. | GAO-18-559



MITRE | ATT&CK™

CONOPS – "CONTINUOUS CYBER MATURITY"



CRITICAL SECURITY SCENARIOS

THREAT MODELS

CONTROLS

Remediation

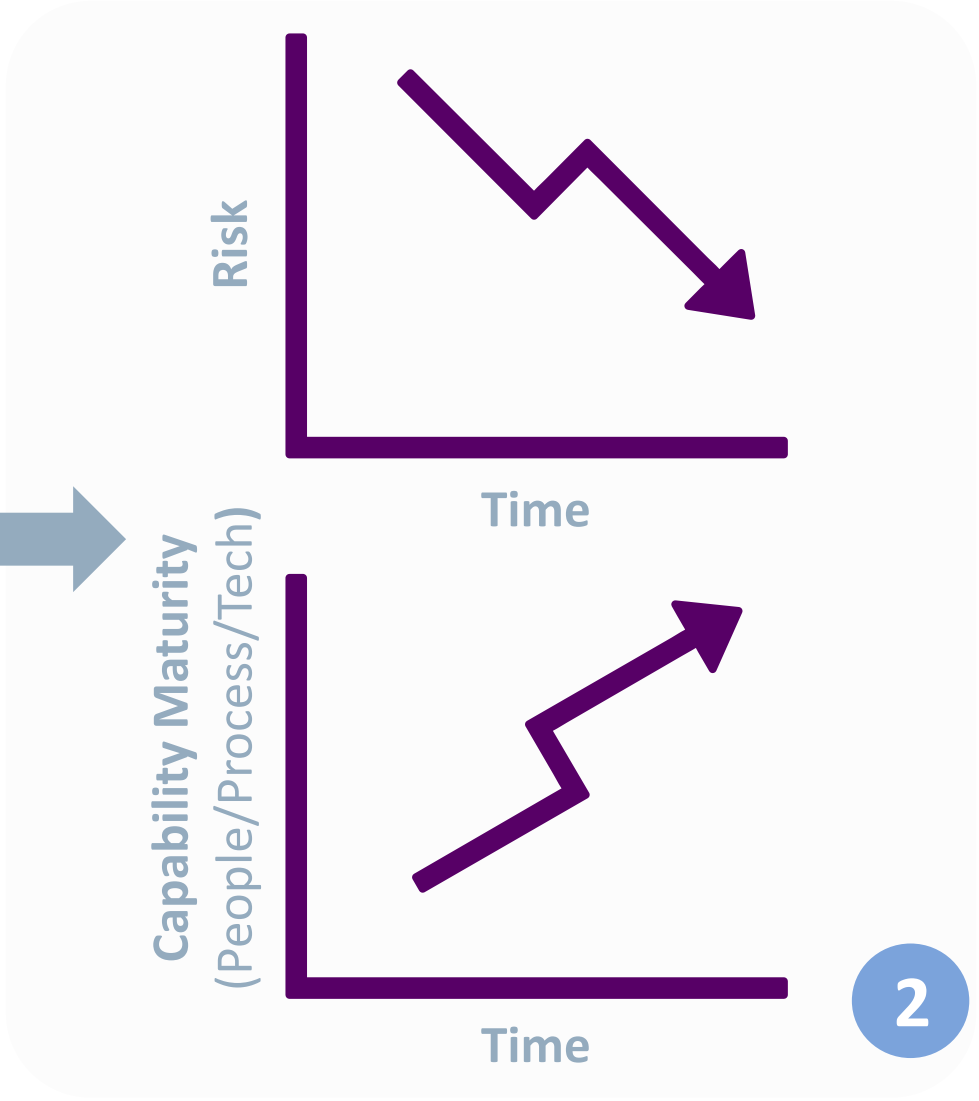
Capture/Analyse /Prioritise

Findings/Risks/ Metrics

Validate

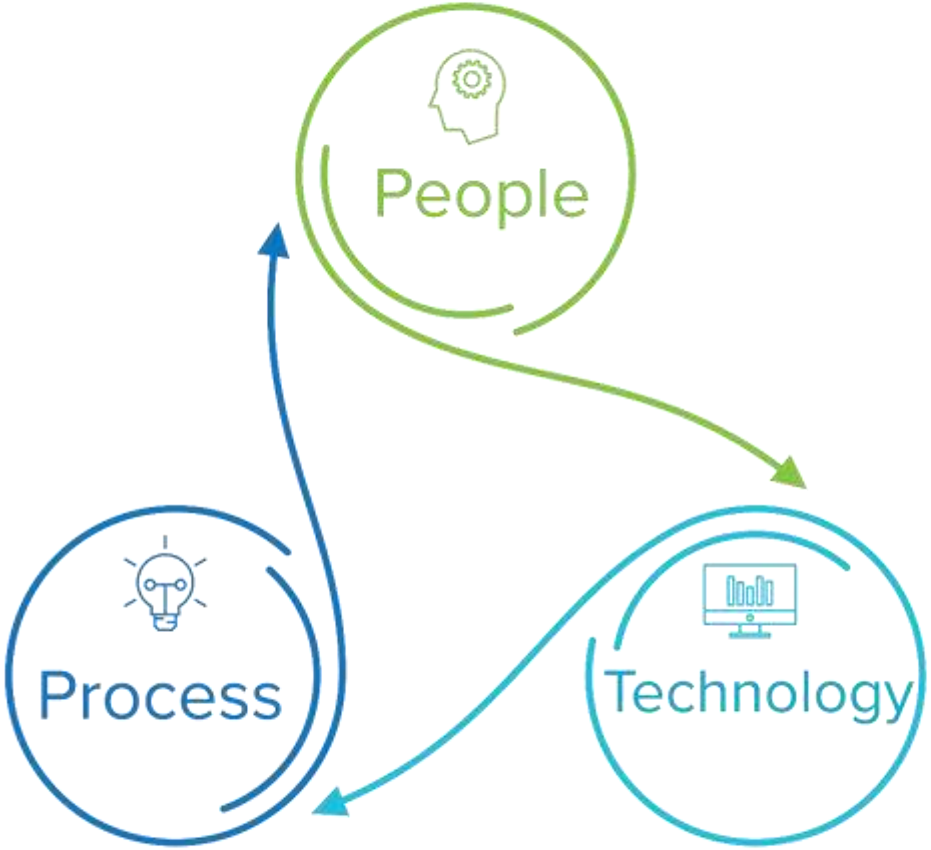
Develop

1

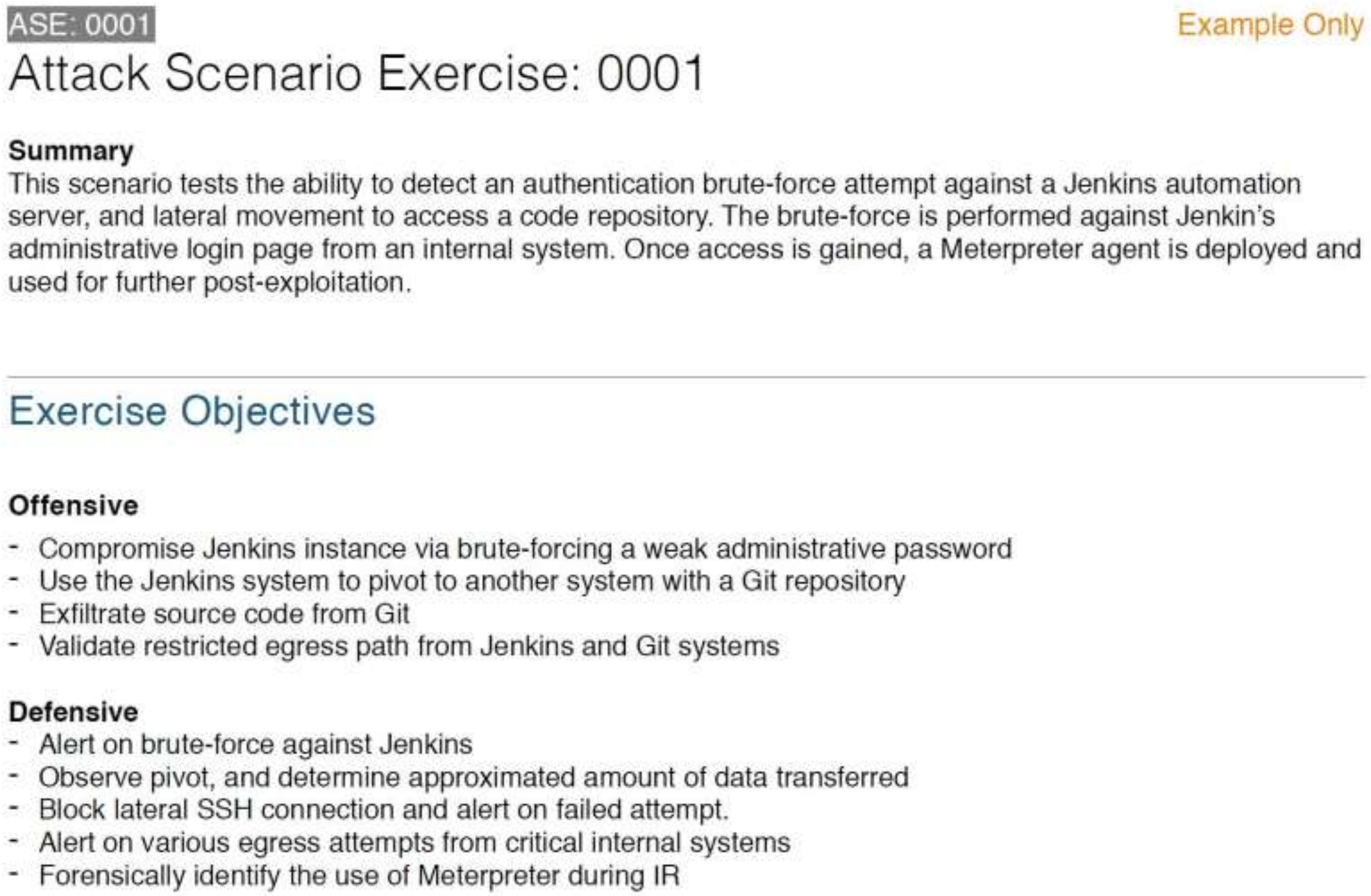


2

Capture/Analyse/Prioritise Maturity Requirements



Develop Master Scenario Event List (MSEL)



ASE: 0001

Example Only

Attack Scenario Exercise: 0001

Summary
This scenario tests the ability to detect an authentication brute-force attempt against a Jenkins automation server, and lateral movement to access a code repository. The brute-force is performed against Jenkin's administrative login page from an internal system. Once access is gained, a Meterpreter agent is deployed and used for further post-exploitation.

Exercise Objectives

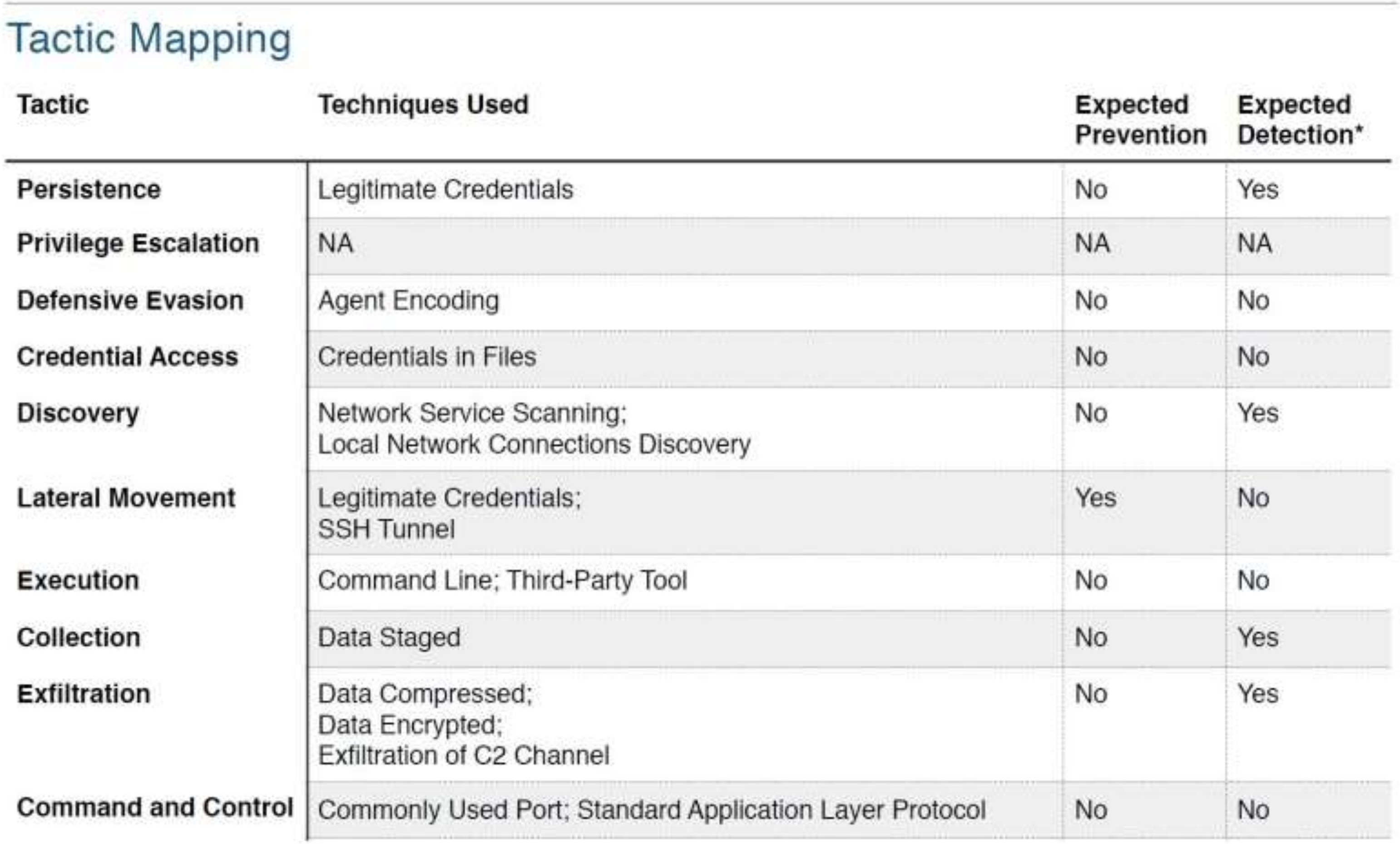
Offensive

- Compromise Jenkins instance via brute-forcing a weak administrative password
- Use the Jenkins system to pivot to another system with a Git repository
- Exfiltrate source code from Git
- Validate restricted egress path from Jenkins and Git systems

Defensive

- Alert on brute-force against Jenkins
- Observe pivot, and determine approximated amount of data transferred
- Block lateral SSH connection and alert on failed attempt.
- Alert on various egress attempts from critical internal systems
- Forensically identify the use of Meterpreter during IR

Develop Master Scenario Event List (MSEL)



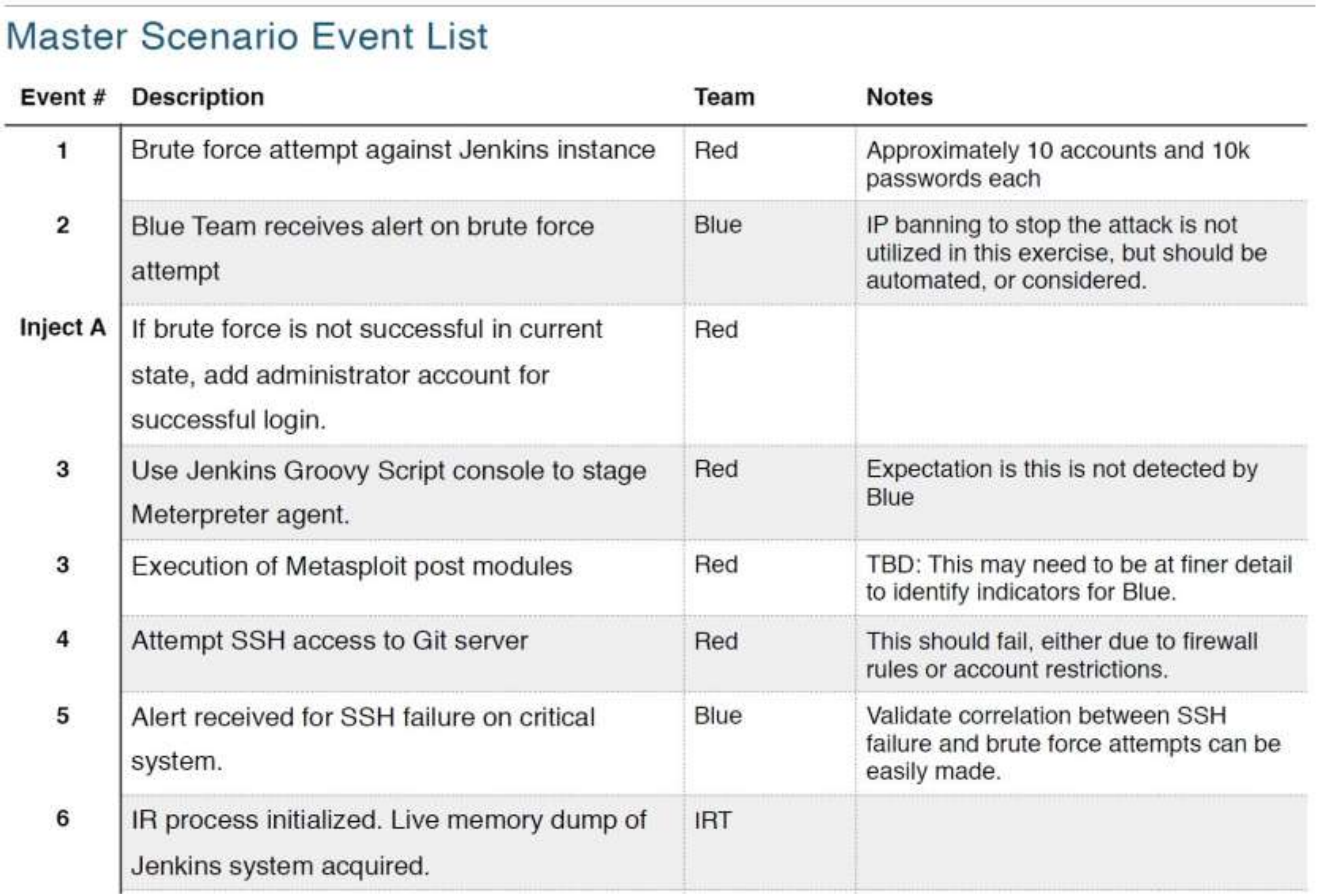
Tactic Mapping

Tactic	Techniques Used	Expected Prevention	Expected Detection*
Persistence	Legitimate Credentials	No	Yes
Privilege Escalation	NA	NA	NA
Defensive Evasion	Agent Encoding	No	No
Credential Access	Credentials in Files	No	No
Discovery	Network Service Scanning; Local Network Connections Discovery	No	Yes
Lateral Movement	Legitimate Credentials; SSH Tunnel	Yes	No
Execution	Command Line; Third-Party Tool	No	No
Collection	Data Staged	No	Yes

Exfiltration	Data Compressed;
	Data Encrypted;
	Exfiltration of C2 Channel
		No	Yes

Command and Control	Commonly Used Port; Standard Application Layer Protocol	No	No

Develop Master Scenario Event List (MSEL)

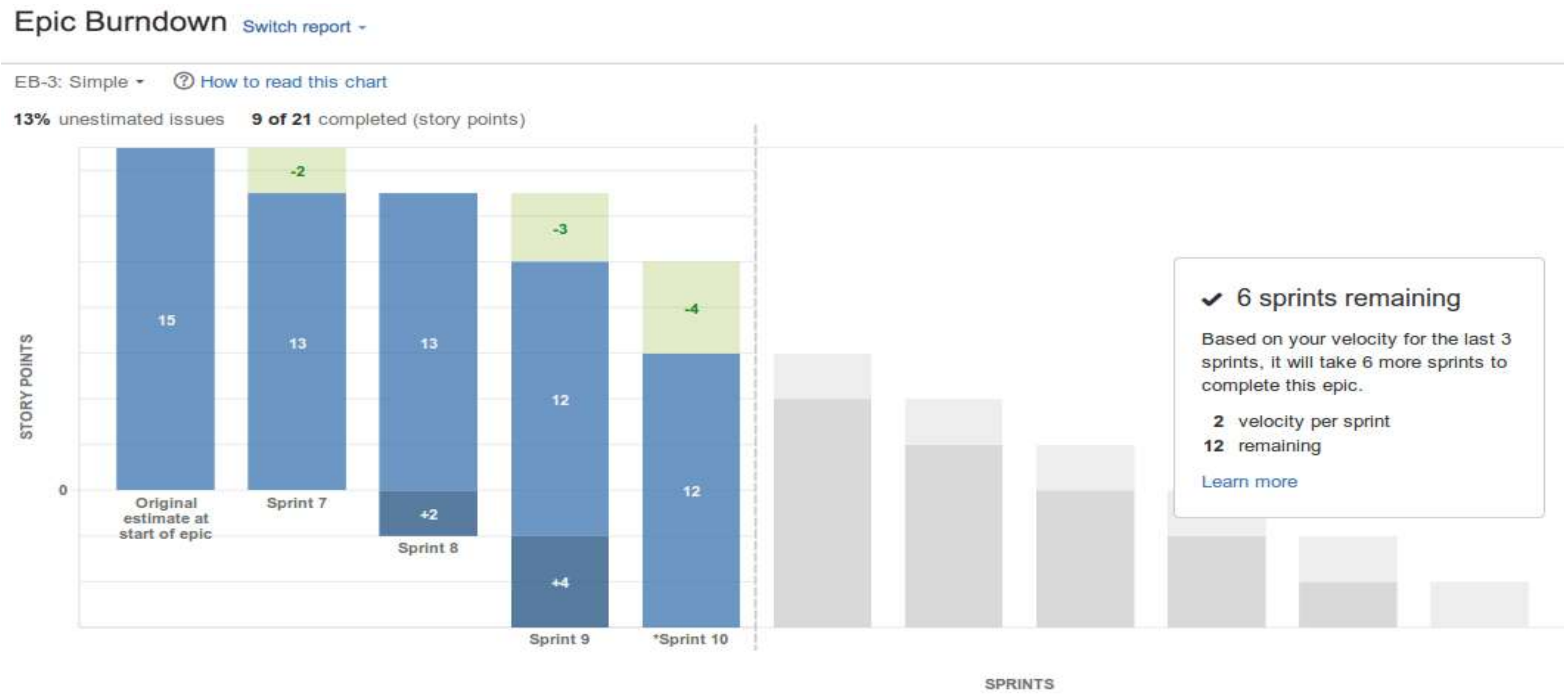


Master Scenario Event List

Event #	Description	Team	Notes
1	Brute force attempt against Jenkins instance	Red	Approximately 10 accounts and 10k passwords each
2	Blue Team receives alert on brute force attempt	Blue	IP banning to stop the attack is not utilized in this exercise, but should be automated, or considered.
Inject A	If brute force is not successful in current state, add administrator account for successful login.	Red	
3	Use Jenkins Groovy Script console to stage Meterpreter agent.	Red	Expectation is this is not detected by Blue
3	Execution of Metasploit post modules	Red	TBD: This may need to be at finer detail to identify indicators for Blue.
4	Attempt SSH access to Git server	Red	This should fail, either due to firewall rules or account restrictions.
5	Alert received for SSH failure on critical system.	Blue	Validate correlation between SSH failure and brute force attempts can be easily made.
6	IR process initialized. Live memory dump of Jenkins system acquired.	IRT	

HACK ALL THE THINGS

Findings Management



Epic Burndown

13% unestimated issues **9 of 21** completed (story points)

✔ 6 sprints remaining

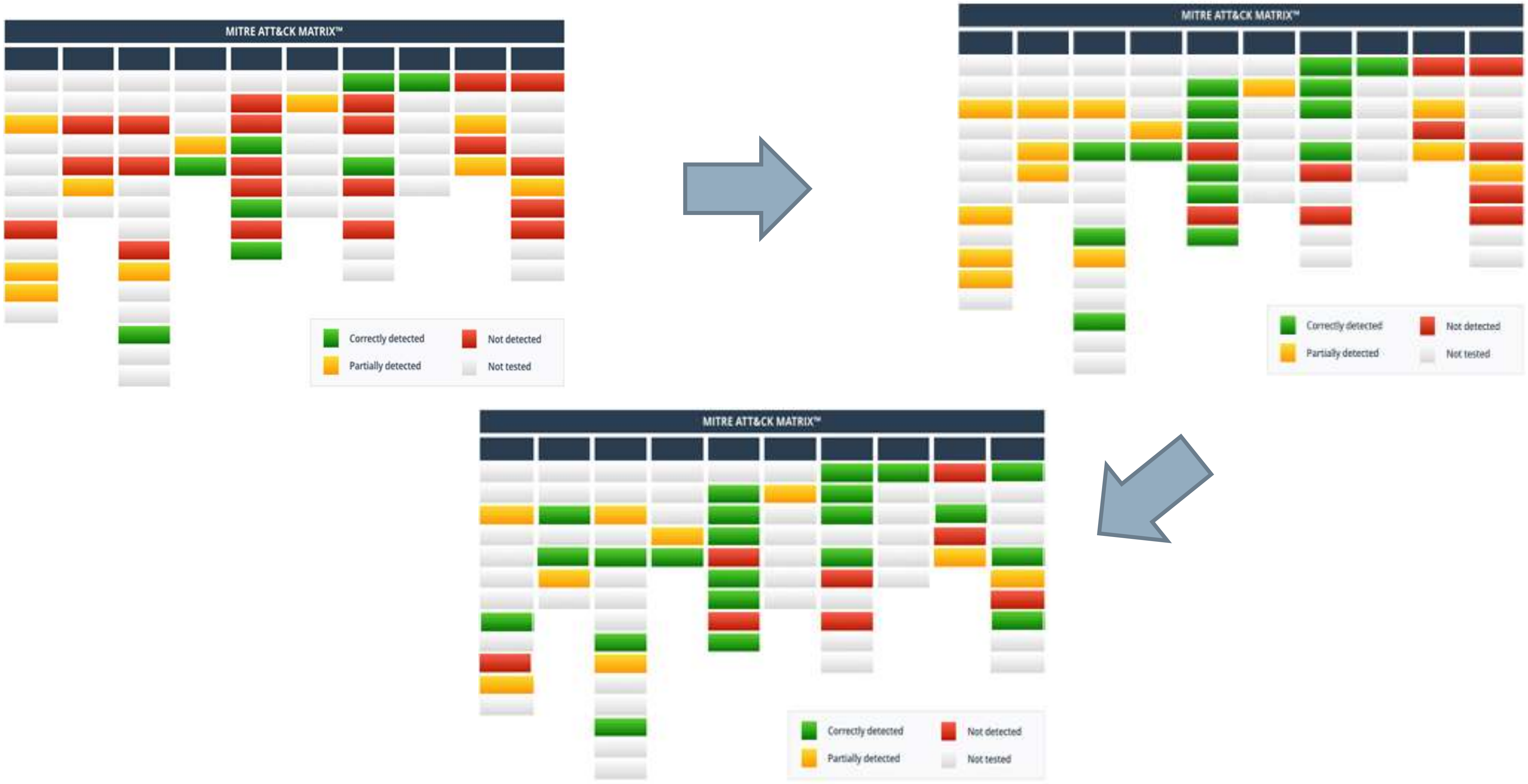
Based on your velocity for the last 3 sprints, it will take 6 more sprints to complete this epic.

2	velocity per sprint
12	remaining

Learn more

Remediation

What does maturity look like?



Security vs Privacy: Challenges emanating from the changing legislative environment

Patrick Fair

Partner at Baker Mckenzie

Baker McKenzie.

Challenges from the changing legislative environment

Patrick Fair | 12 September 2019

Agenda

1 Introduction

2 Assistance and Access Act

3 Security of Critical Infrastructure

4 Foreign Influence & Espionage

5 Abhorrent Violent Material

6 Mandatory Data Breach Notification

7 Questions and Discussion

1

Assistance and Access

Notices, Requests, warrants and assistance orders

- Part 15 of the Telco Act is generally applicable to IT services and service providers.
- Power to request or require listed acts or things without a warrant.
- Widened computer access warrants
- Assistance orders can be directed at an individual.

Key challenges

When to comply with a TAR?

Careful consultation with regulators

When to resist a TAN?

When to formally assess a TCN?

Employment policy Assistance orders

What code/system can stay in Australia?

2

Security of Critical Infrastructure

Reporting of ownership, control and changes

- Requirement apply to named ports, water and sewage, gas processing electricity network, system or interconnection of particular size.

- Can be applied to other assets in nominated “ relevant industries”.

- “operational information” and “ownership control information” must be updated within 30 days.

- Secretary has power to request information and Minister has power to direct the doing of any “act or thing” that may be prejudicial to security.

Key Challenges

If you are CI: reporting accurately

If you are CI: avoiding direction

If you are CI: ensuring report of changes

If a supplier: national security compliance

If a supplier: are you an acceptable supplier?

If you are an asset: avoid becoming Ci

3

Espionage and Foreign interference

Espionage and Foreign Interference Crimes

- Foreign influence Transparency Scheme requires registration if representing a foreign principle in certain public discourse/ lobbying.

- Range of new offences for Commonwealth officers and offences of:

  - “reckless as to national security” when dealing with information or an article that results in information or an article being made available to a foreign principal.

  - recklessly supporting a foreign intelligence agency.

  - recklessly funding or being funded by a foreign intelligence agency.

Key Challenges

Knowing who you are dealing with

Knowing who they are dealing with

Identifying foreign principals/ security agencies

Assessing national security interests

International collaboration/ research

Cost of defensive compliance

4

Abhorrent Violent Material

3 New offences in the Criminal Code

- Being reckless regarding the availability of abhorrent violent material on a content service or a hosting service.
- Failure to report to the AFP when AVM indicates action taking place in Australia.
- Maximum penalty $10m or 10% of global revenues whichever is >.
- Flow on impact requiring Telcos to block content under s313 obligations.

Key Challenges

Not to be “reckless”?!

Identification of some AVM content

When to unblock?

Compensation for blocking?

3

Mandatory Data Breach Notification

Mandatory data breach notification

- Notification required for any unauthorised access, disclosure likely to result in serious harm.

- A duty to investigate within 30 days if unsure.

- An ability to remediate if harm can be avoided by remediation.

Key Challenges

Serious harm is hard to assess

When is compensation remediation?

Is there a downside of notification?

Sometimes secondary actions cause harm

Who notifies when multiple parties are involved?

Contracts don’t address disclosure/ cooperation

Questions

Baker McKenzie.

patrick.fair@bakermckenzie.com

Baker & McKenzie, an Australian Partnership, is a member firm of Baker & McKenzie International, a global law firm with member law firms around the world. In accordance with the common terminology used in professional service organisations, reference to a "partner" means a person who is a partner, or equivalent, in such a law firm. Similarly, reference to an "office" means an office of any such law firm. This may qualify as “Attorney Advertising” requiring notice in some jurisdictions. Prior results do not guarantee a similar outcome.

AFTERNOON TEA

CYBER
smart
safe
secure

Please be back by **3:30pm**

The Cyber Ecosystem

Dr Lesley Seebeck

Chief Executive Officer at ANU Cyber Institute

CYBER INSTITUTE

A strategic initiative of
The Australian National University

The Cyber Ecosystem

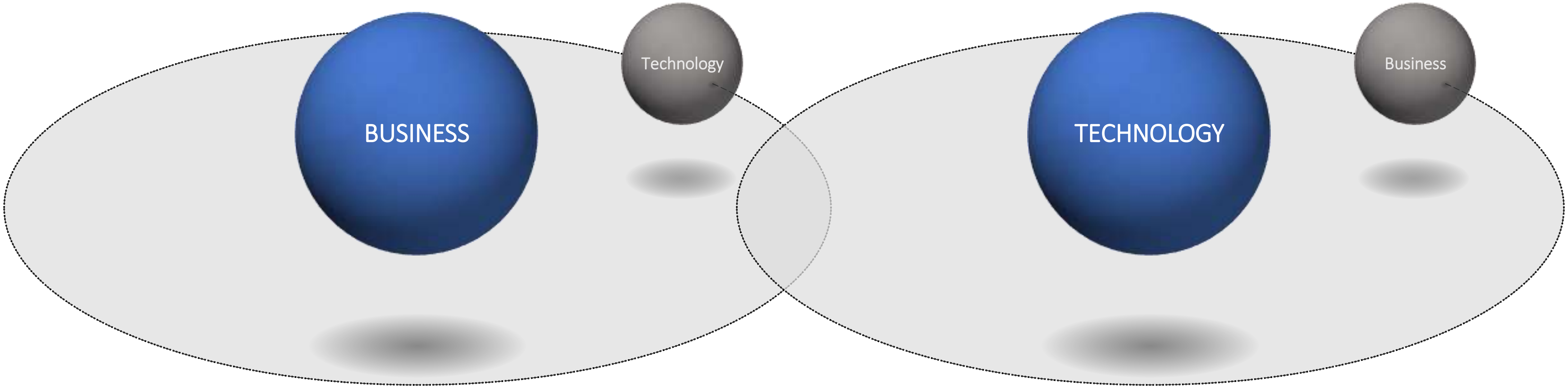
Dr Lesley Seebeck

CEO

cyber.anu.edu.au

Cyber: the unreconstructed view

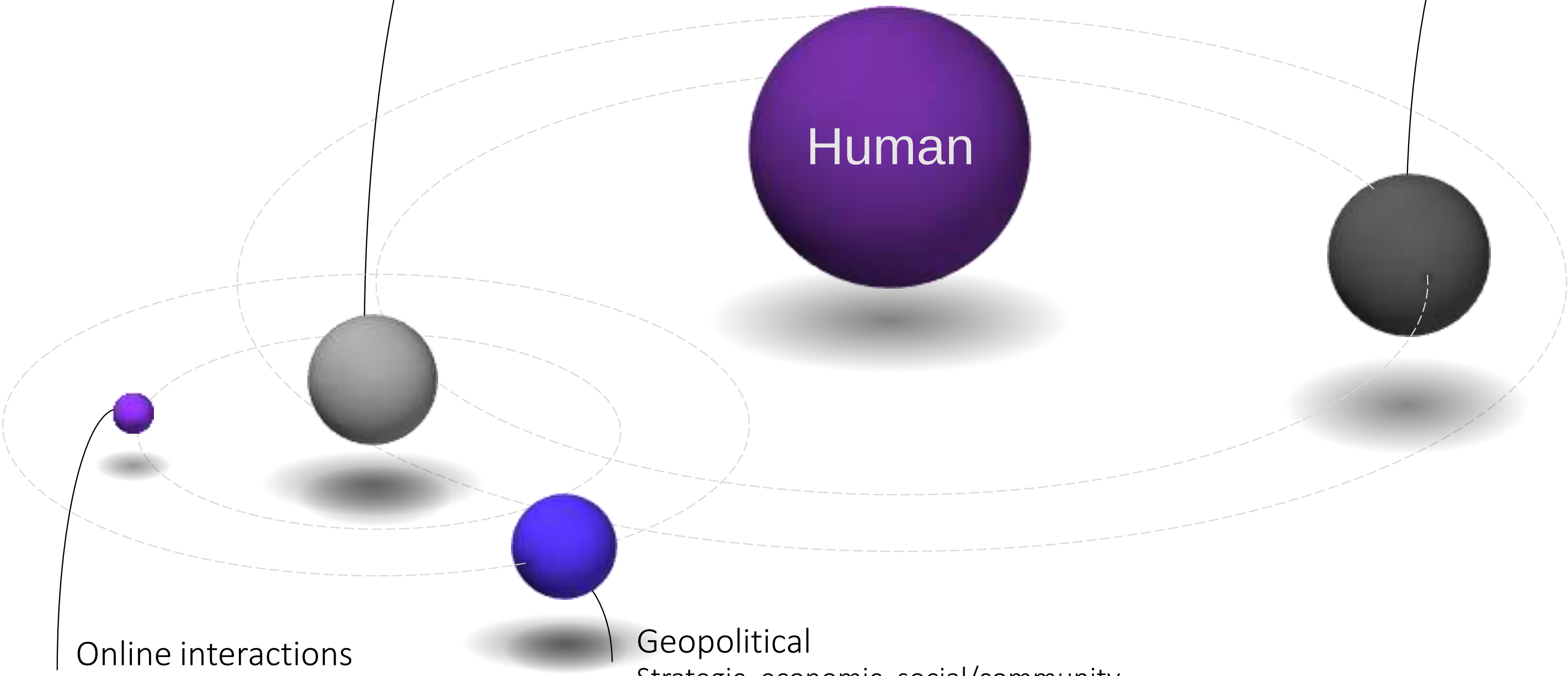
CYBER INSTITUTE
A strategic initiative of
The Australian National University



Intractability

CYBER INSTITUTE

A strategic initiative of
The Australian National University



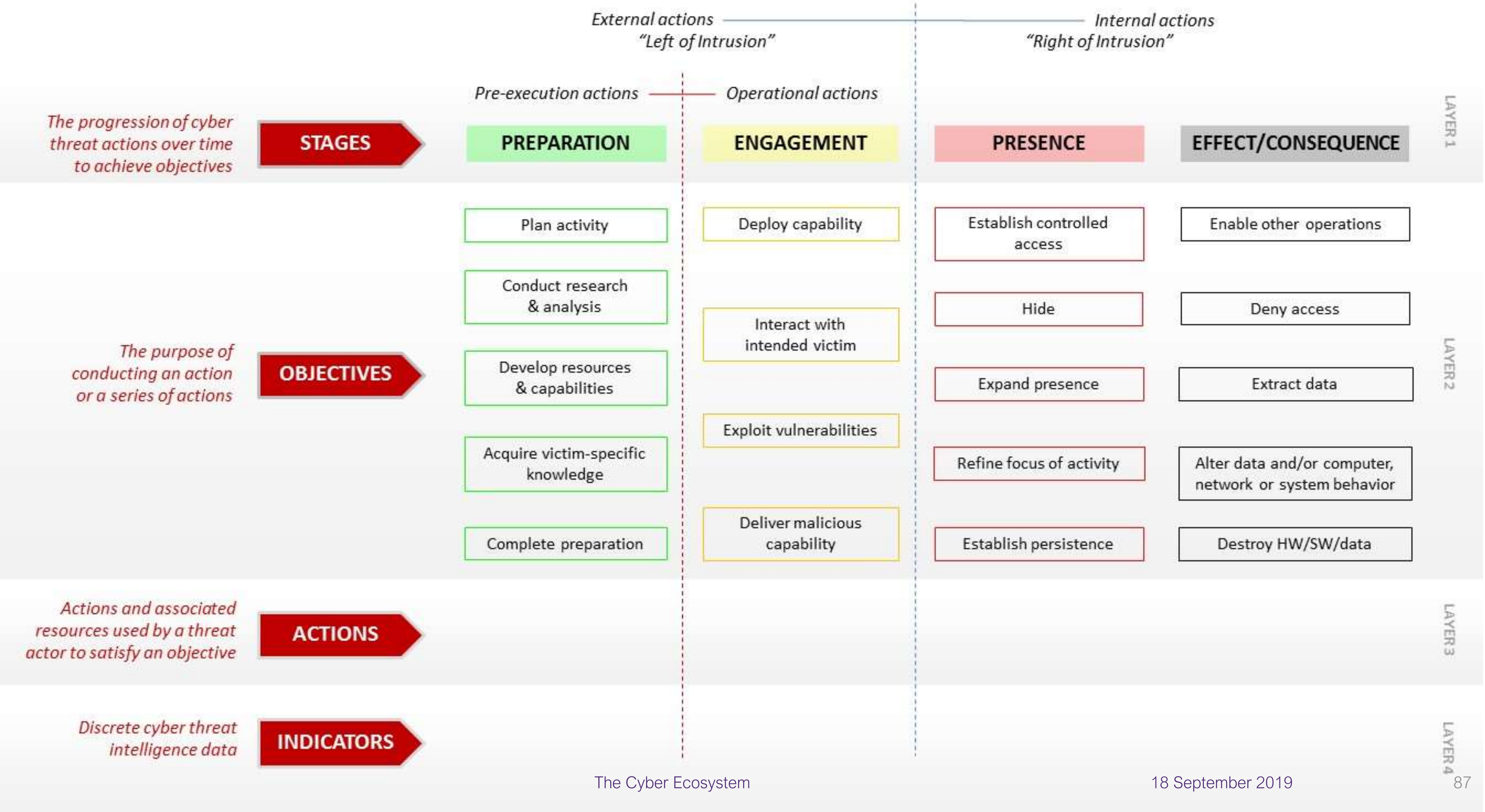
Digital environment
Because smartphones, cloud, data, tech stack

Business/workaday
Process, governance, other people

Online interactions
B2B, P2P, M2M, B2P

Geopolitical
Strategic, economic, social/community

CYBER THREAT FRAMEWORK



External actions "Left of Intrusion"

Internal actions "Right of Intrusion"

Pre-execution actions

Operational actions

The progression of cyber threat actions over time to achieve objectives — **STAGES**

The purpose of conducting an action or a series of actions — **OBJECTIVES**

Actions and associated resources used by a threat actor to satisfy an objective — **ACTIONS**

Discrete cyber threat intelligence data — **INDICATORS**

PREPARATION
- Plan activity
- Conduct research & analysis
- Develop resources & capabilities
- Acquire victim-specific knowledge
- Complete preparation

ENGAGEMENT
- Deploy capability
- Interact with intended victim
- Exploit vulnerabilities
- Deliver malicious capability

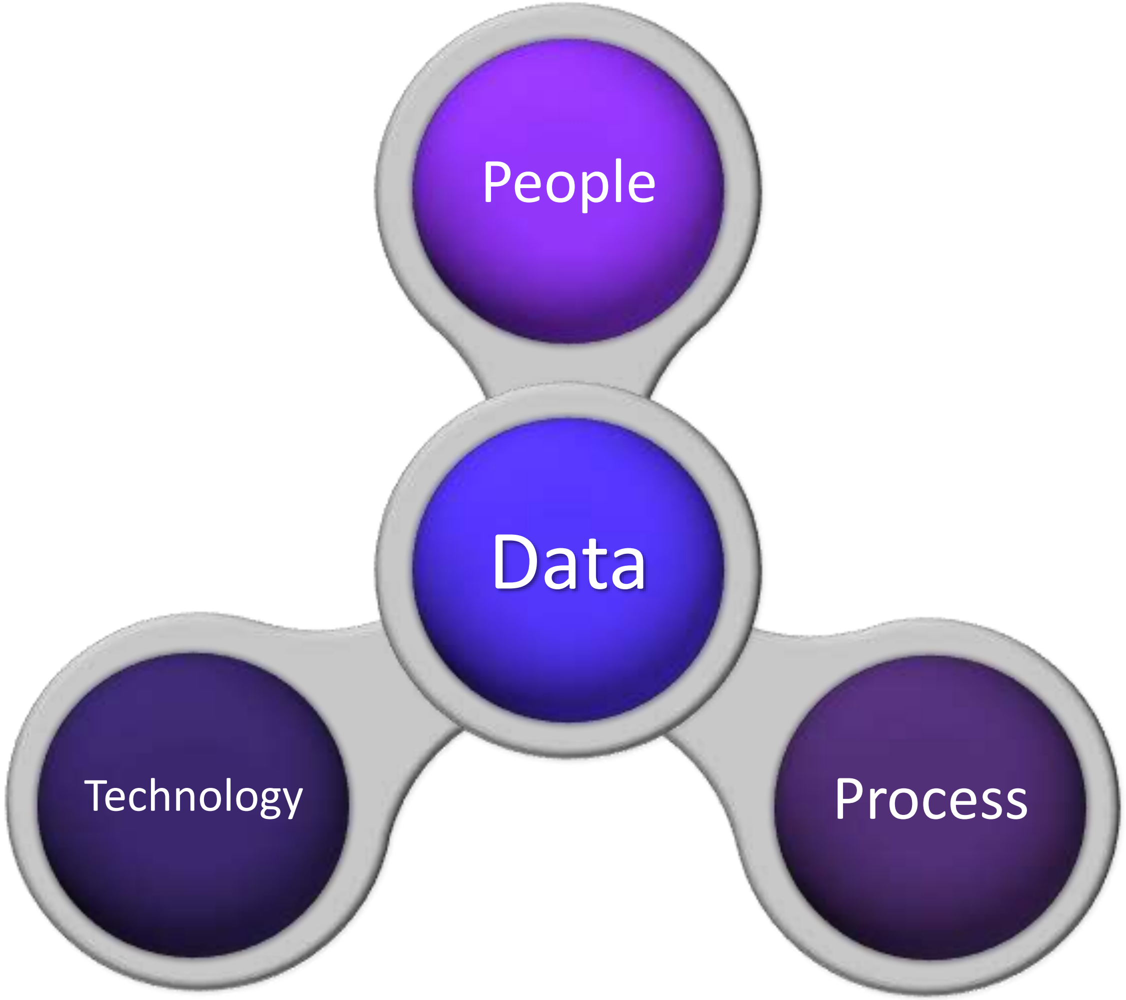
PRESENCE
- Establish controlled access
- Hide
- Expand presence
- Refine focus of activity
- Establish persistence

EFFECT/CONSEQUENCE
- Enable other operations
- Deny access
- Extract data
- Alter data and/or computer, network or system behavior
- Destroy HW/SW/data

Scaffolding

CYBER INSTITUTE

A strategic initiative of
The Australian National University



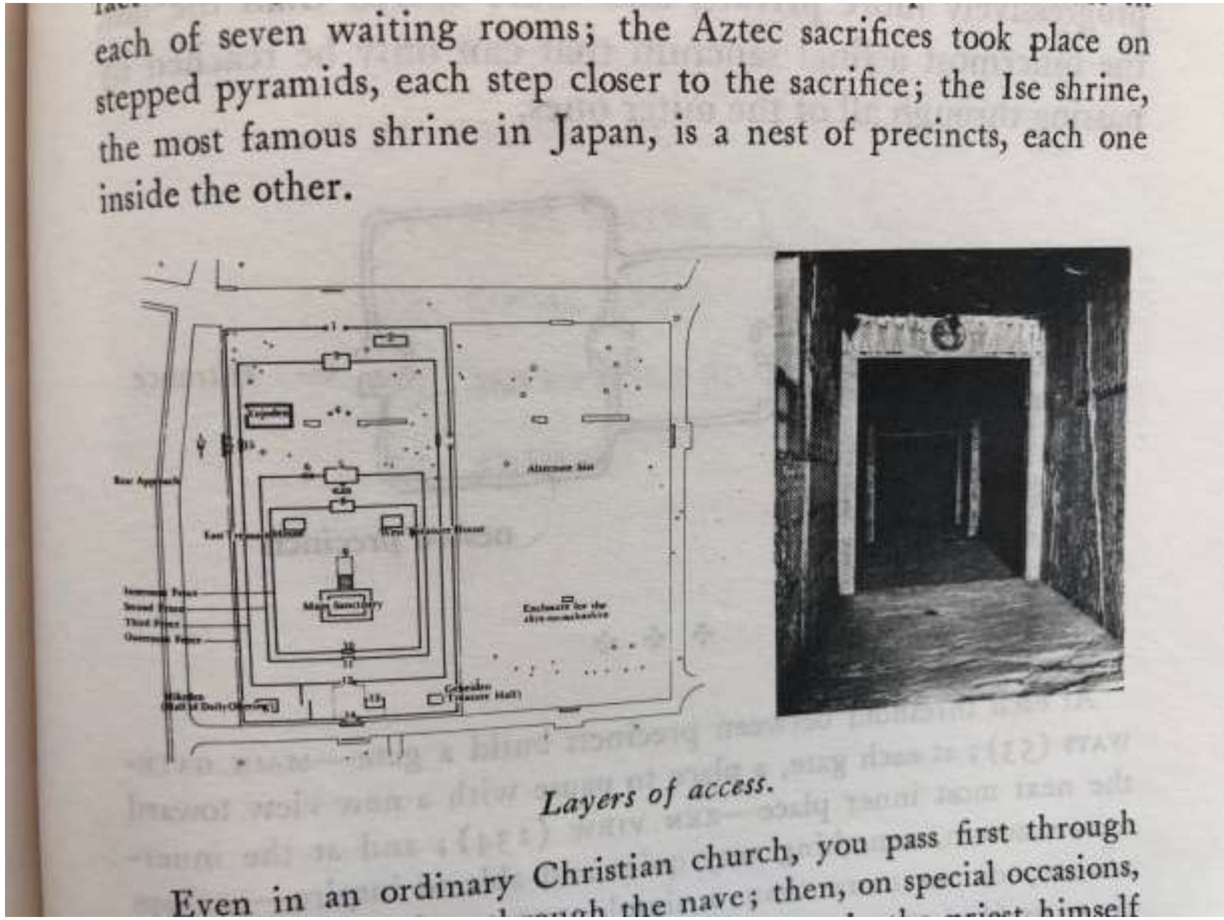
SATAY POWER
6

RO Permeate Reject
RO/CIP
RO Concentra
DRAIN

Some patterns for the whole of system

CYBER INSTITUTE
A strategic initiative of
The Australian National University

- Build for the human
- Resilience
- Modular architecture
- Defence-in-depth
- Zero trust
- Don’t collect what you don’t need
- Absolute encryption
- People own their own data



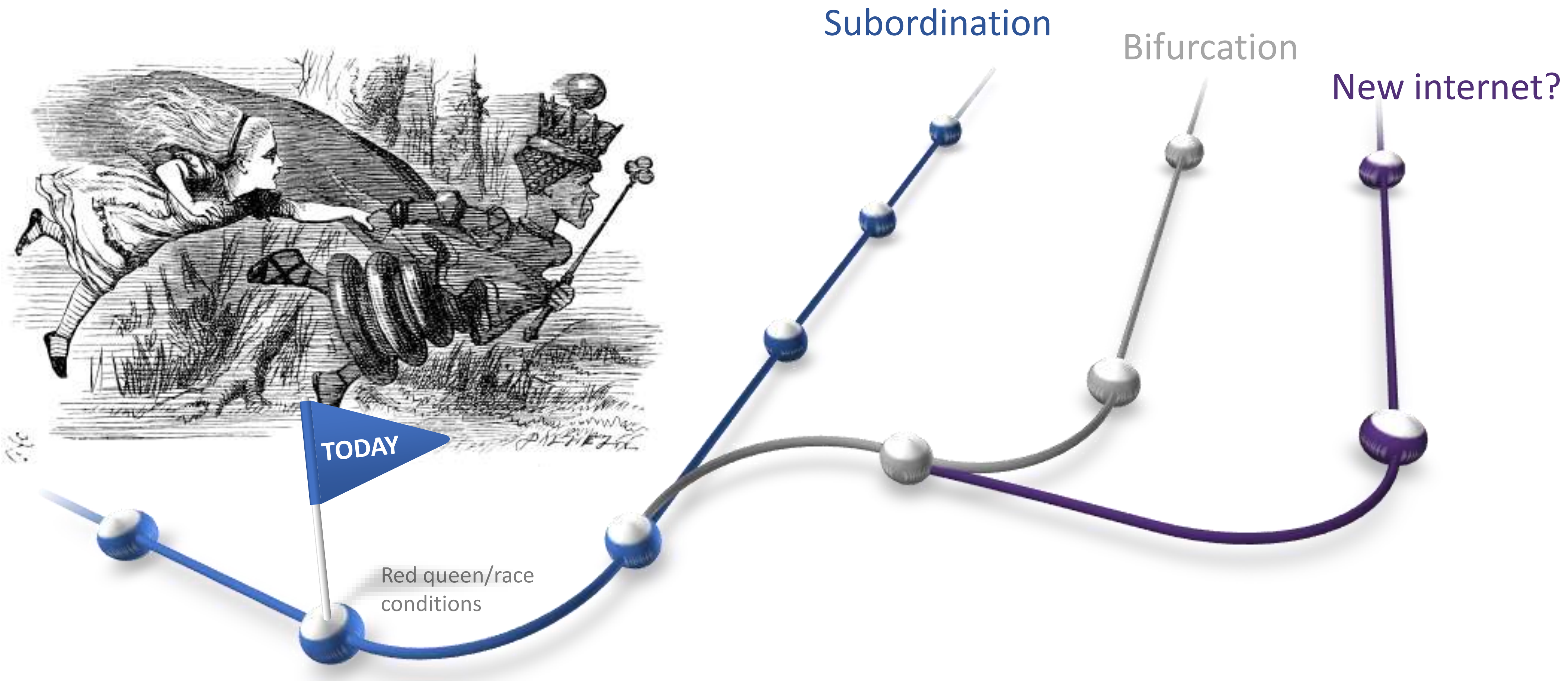
each of seven waiting rooms; the Aztec sacrifices took place on stepped pyramids, each step closer to the sacrifice; the Ise shrine, the most famous shrine in Japan, is a nest of precincts, each one inside the other.

Alternate Site
West Treasure House
Main Sanctuary
Mikeden
(Hall of Daily Offering)
Gehaiden
(Treasure Hall)

Layers of access.

Even in an ordinary Christian church, you pass first through ough the nave; then, on special occasions, priest himself

Futures


Subordination
Bifurcation
New internet?
TODAY
Red queen/race
conditions

Building a trusted ecosystem

Australia's NATIONAL University

Focus on the strategic, global problems

Direct ongoing access to policy-makers, advisers and operators

Developing people through innovative education

The best shape the best.

Co-design, co-develop and co-deliver the cyber professional and capability eco-system.

Learning by doing in real-time operations

The best way to learn—and to test new ideas and technology.

Help build a unique education facility for our future.

Shaping the future through research and innovation

Cyber will determine our future.

We need interdisciplinary and business/academic research to generate new capabilities, energy and change.

Khomsaz

How can we help you?

Email cyber@anu.edu.au

PANEL DISCUSSION:

What can industry and government do better, to be prepared for the future of the cyber security landscape?

Panel members:

Jamie Norton, Andrew Scully and Patrick Fair

Update of the Australian Cyber Security Centre

Rachel Noble PSM

Head of Australian Cyber Security Centre (ACSC)

Closing remarks

Damien Manuel
Board of Directors Chair at AISA

Thank you to our sponsors

CYBER
smart
safe
secure

JACOBS®

dimension
data

NTT

AISA