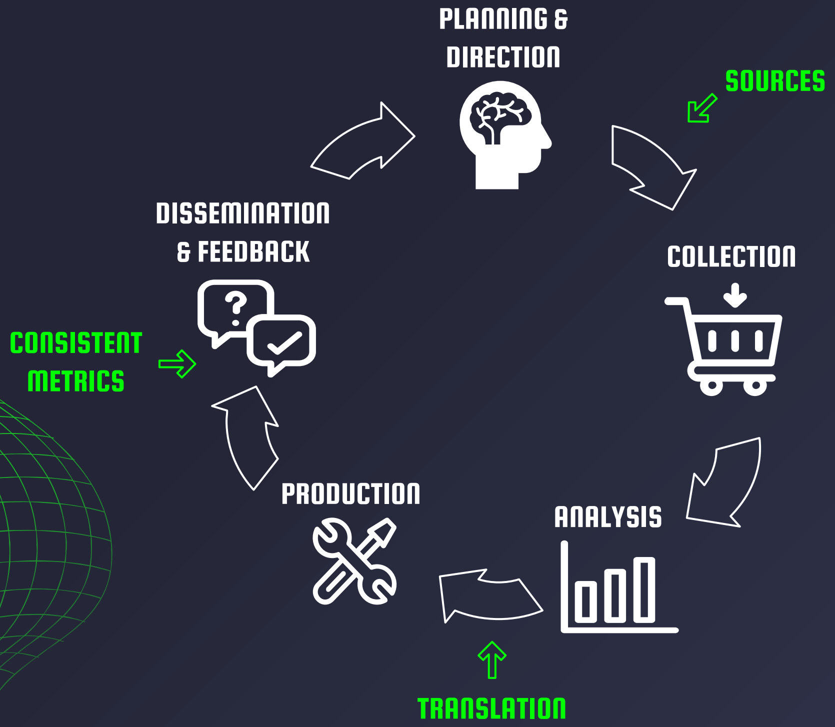
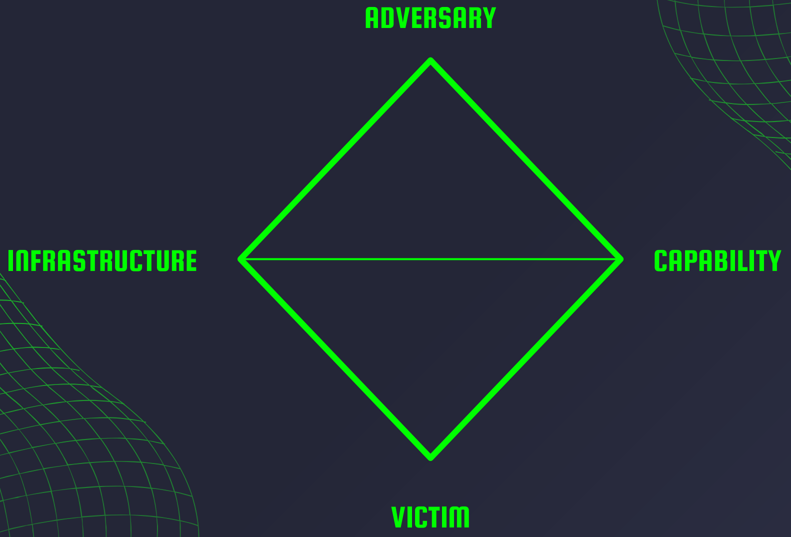
Helping Organizations Anticipate and Approach Emerging Technology Threats

NATALIE KILBER | JOHN DOYLE | FIRST CTI 23

CTI LIFECYCLE EXTENDED

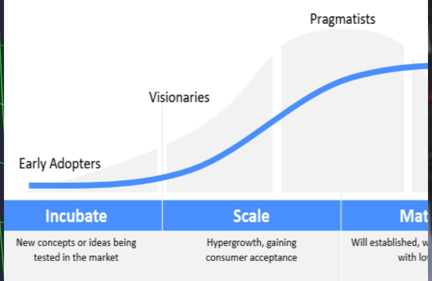


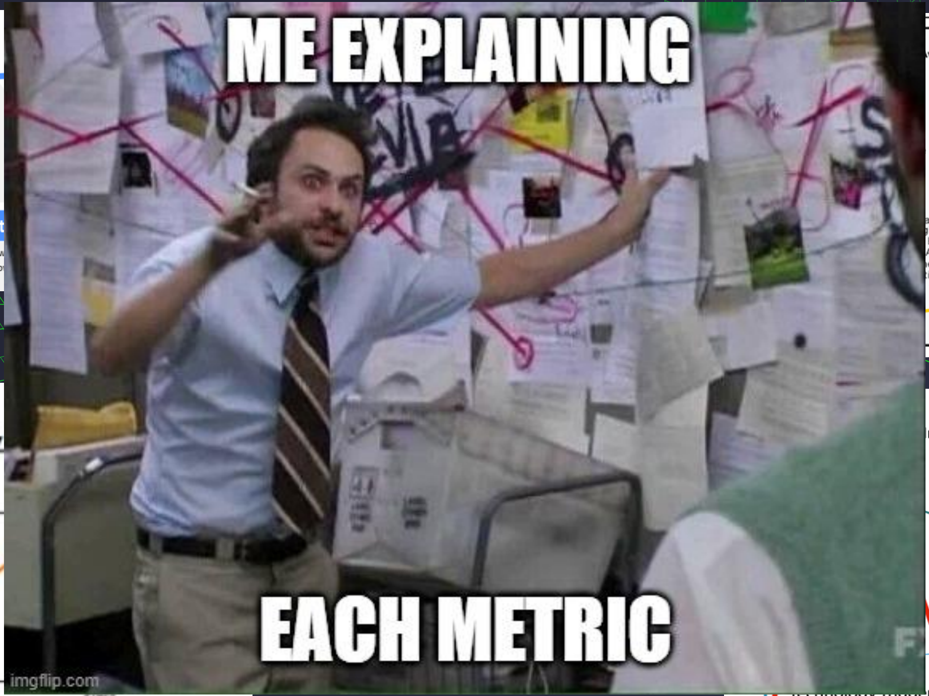
COMMON LANGUAGE MODELS

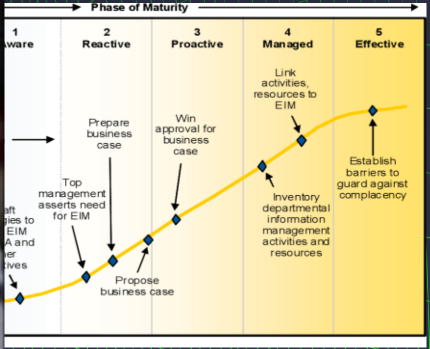


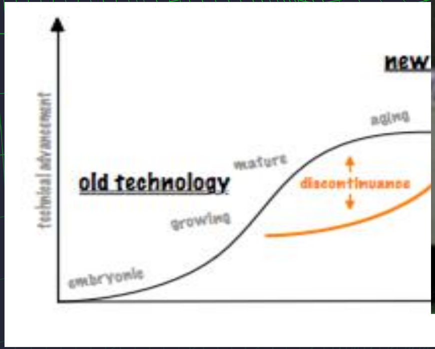
ATTACK PATH → MITRE | ATT&CK®

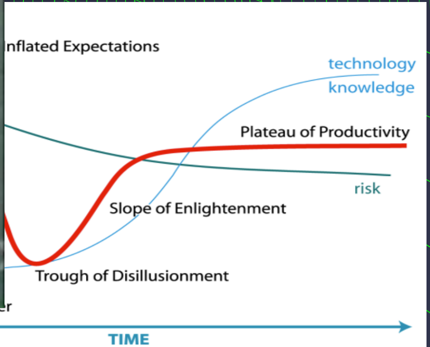
USING TECHNOLOGY MATURITY MODELS



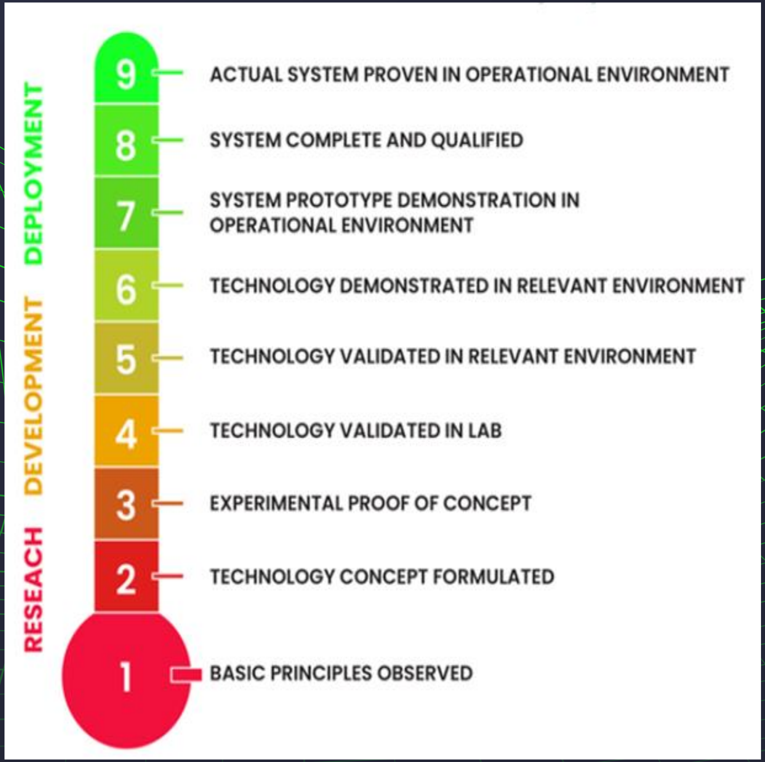








NASA TECHNOLOGY READINESS LEVELS



9 ACTUAL SYSTEM PROVEN IN OPERATIONAL ENVIRONMENT

8 SYSTEM COMPLETE AND QUALIFIED

7 SYSTEM PROTOTYPE DEMONSTRATION IN OPERATIONAL ENVIRONMENT

6 TECHNOLOGY DEMONSTRATED IN RELEVANT ENVIRONMENT

5 TECHNOLOGY VALIDATED IN RELEVANT ENVIRONMENT

4 TECHNOLOGY VALIDATED IN LAB

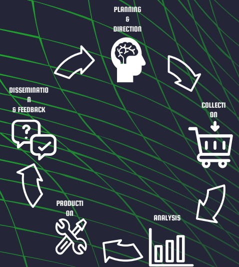
3 EXPERIMENTAL PROOF OF CONCEPT

2 TECHNOLOGY CONCEPT FORMULATED

1 BASIC PRINCIPLES OBSERVED

DIRECTION

EXTENDED



PLANNING
&
DIRECTION

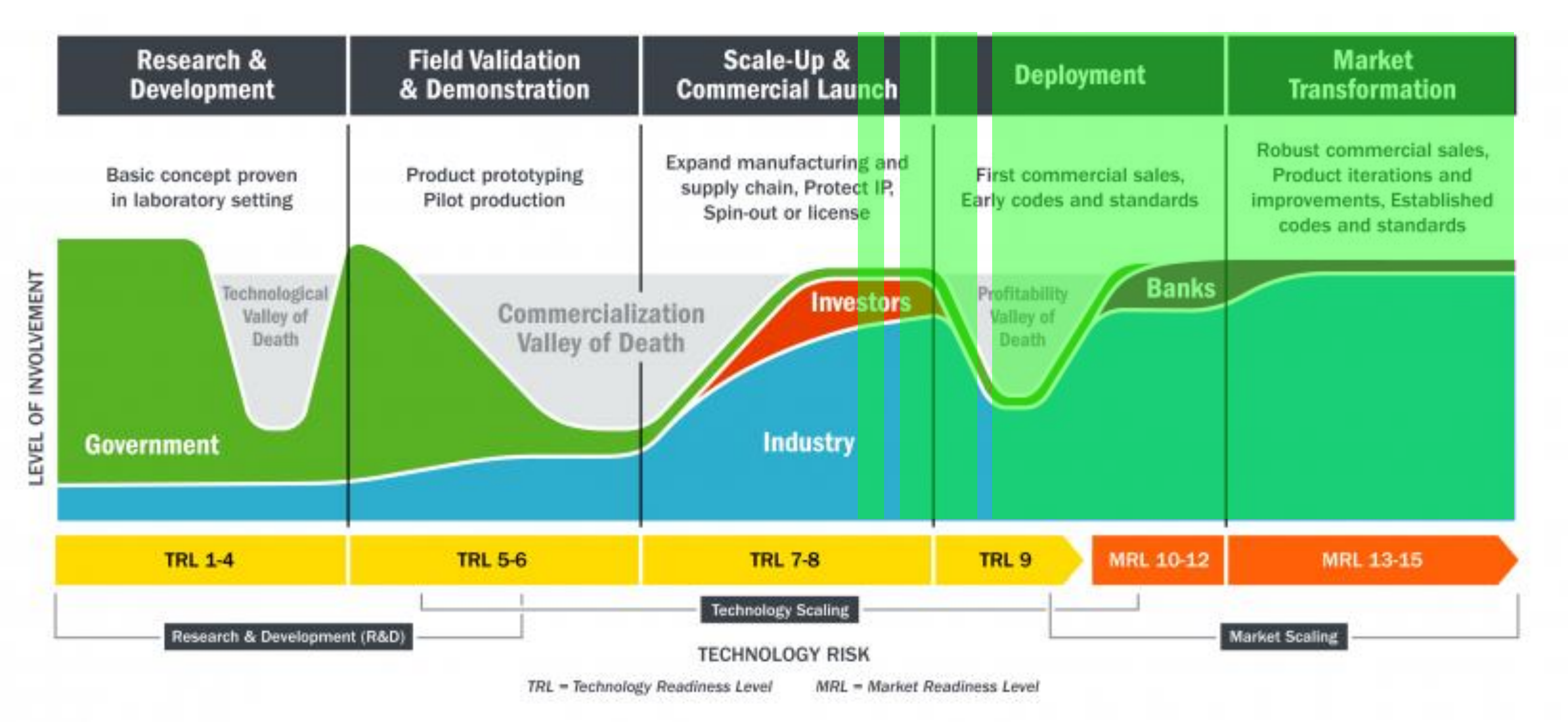
COLLECTI
ON

ANALYSIS

PRODUCTI
ON

DISSEMINATIO
N
& FEEDBACK

MARKET READINESS LEVELS


Research & Development
Field Validation & Demonstration
Scale-Up & Commercial Launch
Deployment
Market Transformation
Basic concept proven in laboratory setting
Product prototyping Pilot production
Expand manufacturing and supply chain, Protect IP, Spin-out or license
First commercial sales, Early codes and standards
Robust commercial sales, Product iterations and improvements, Established codes and standards
LEVEL OF INVOLVEMENT
Technological Valley of Death
Commercialization Valley of Death
Investors
Profitability Valley of Death
Banks
Government
Industry
TRL 1-4
TRL 5-6
TRL 7-8
TRL 9
MRL 10-12
MRL 13-15
Technology Scaling
Research & Development (R&D)
Market Scaling
TECHNOLOGY RISK
TRL = Technology Readiness Level
MRL = Market Readiness Level

DIFFERENT SOURCES

PLANNING & DIRECTION

PLANNING & DIRECTION
COLLECTI ON
ANALYSIS
PRODUCTI ON
DISSEMINATIO N & FEEDBACK

DIFFERENT INTELLIGENCE SOURCES REQUIRED PER TECH READINESS LEVEL (TRL)

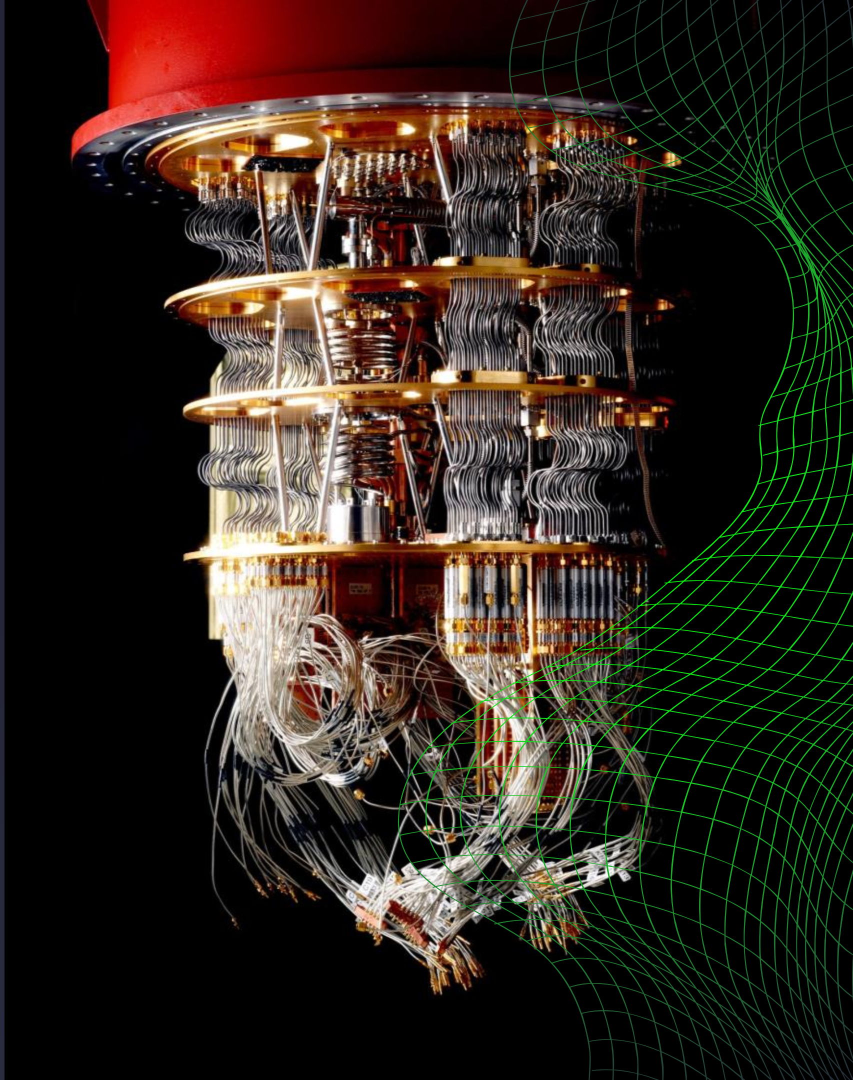
MATURE	TRLs 7 – 9	Mainstream Industry News Initial Public Offering Stock Market
DEVELOPMENT	TRLs 4 – 6	VC investment Market Analysis Patents Technology licensing
RESEARCH	TRLs 1 – 3	Scientific publications Research Funding
HYPE	Presented as TRL 7 – 9 whereas in fact it is at TRLs 1 – 3, if at all.	TRL 7-9 sources, but mainly driven through TRL1-3 sources

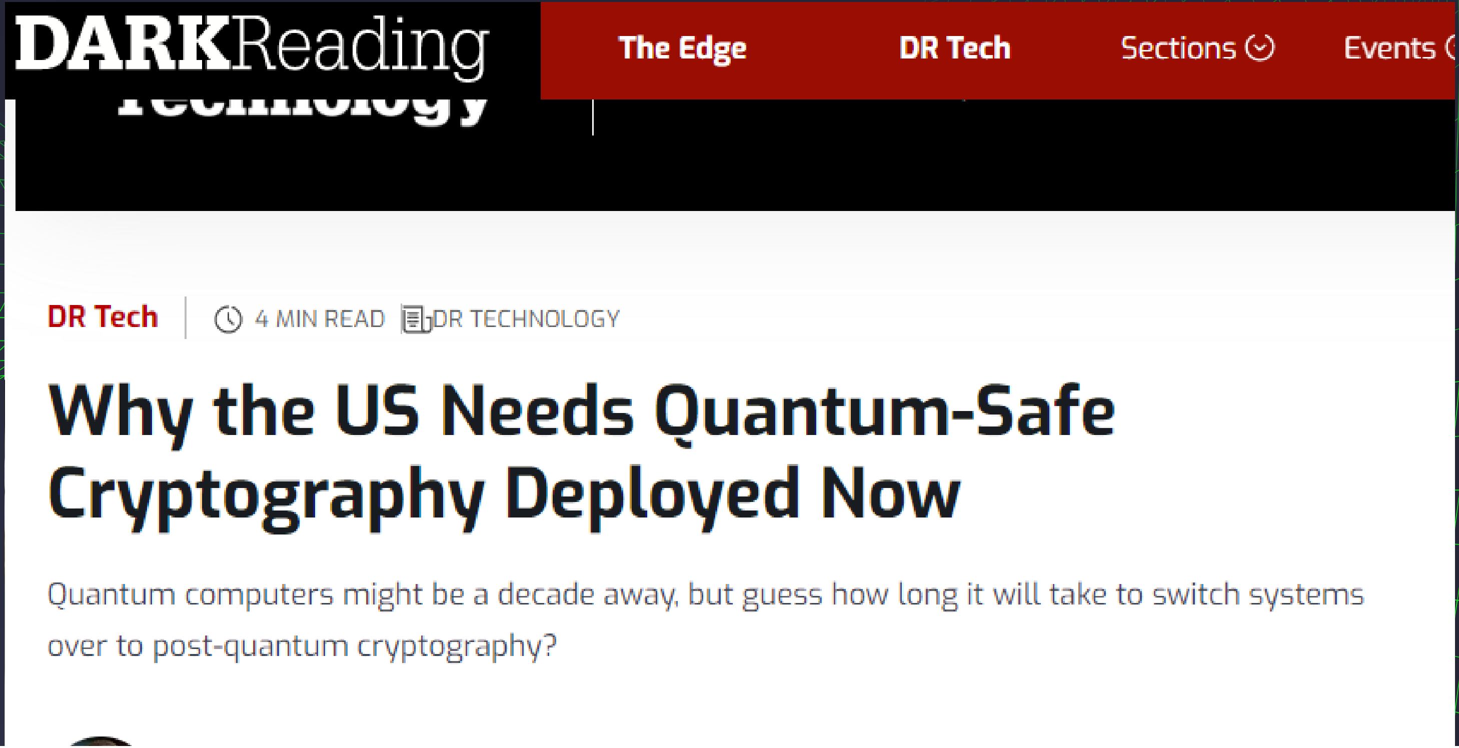
COLLECTION

EXTENDED INTELLIGENCE SOURCES

PLANNING & DIRECTION
COLLECTI ON
ANALYSIS
PRODUCTI ON
DISSEMINATIO N & FEEDBACK

CASE STUDY: QUANTUM THREAT

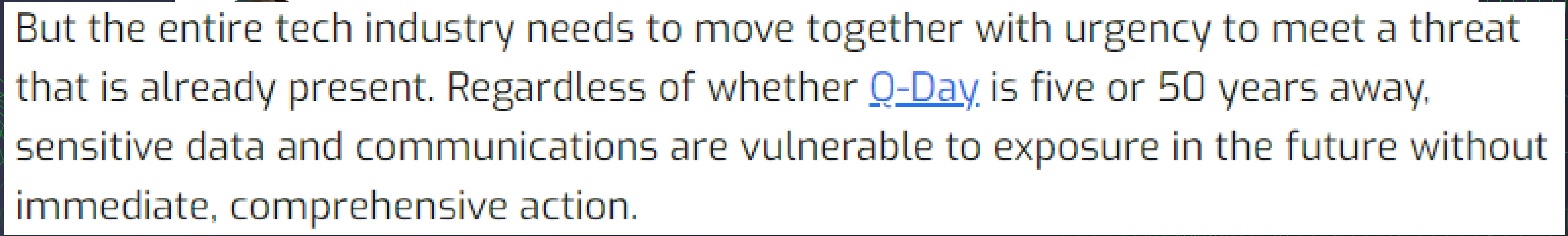




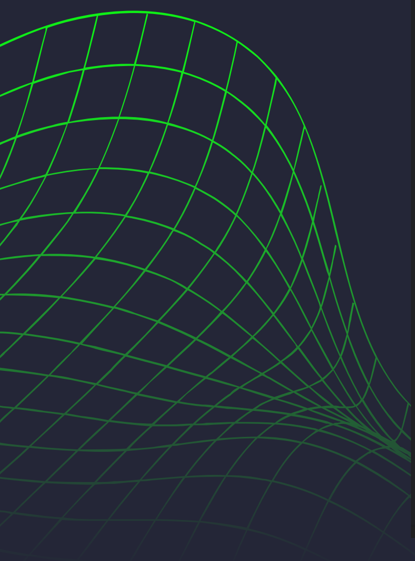
DR Tech | 4 MIN READ DR TECHNOLOGY

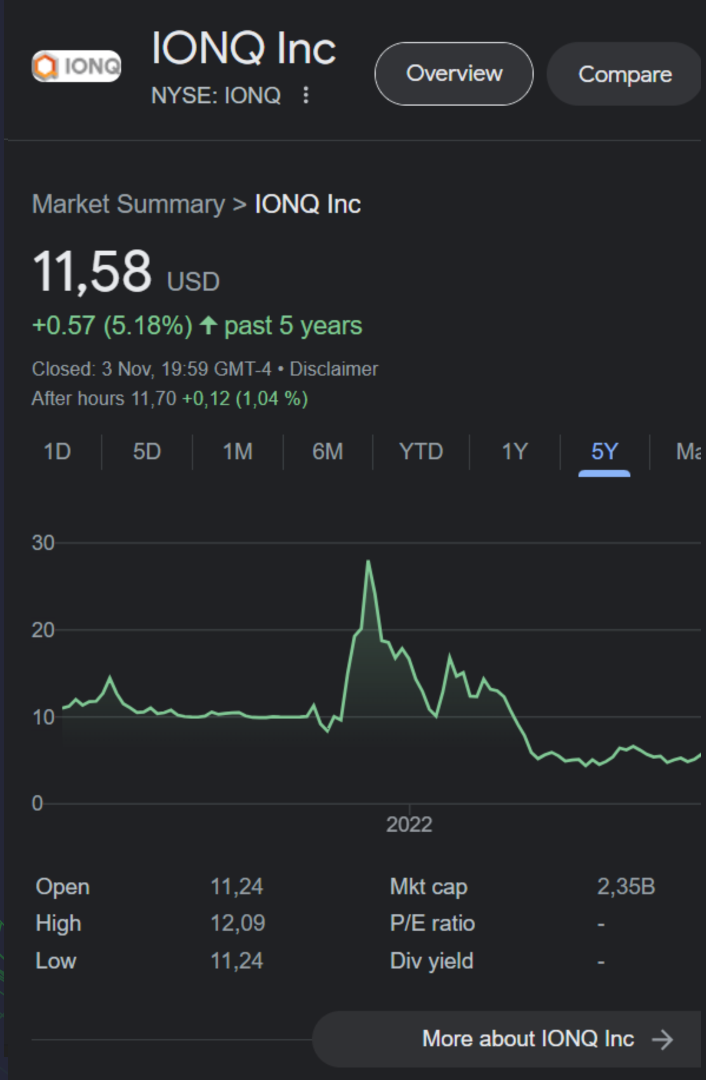
Why the US Needs Quantum-Safe Cryptography Deployed Now

Quantum computers might be a decade away, but guess how long it will take to switch systems over to post-quantum cryptography?



But the entire tech industry needs to move together with urgency to meet a threat that is already present. Regardless of whether Q-Day is five or 50 years away, sensitive data and communications are vulnerable to exposure in the future without immediate, comprehensive action.





IONQ Inc
NYSE: IONQ

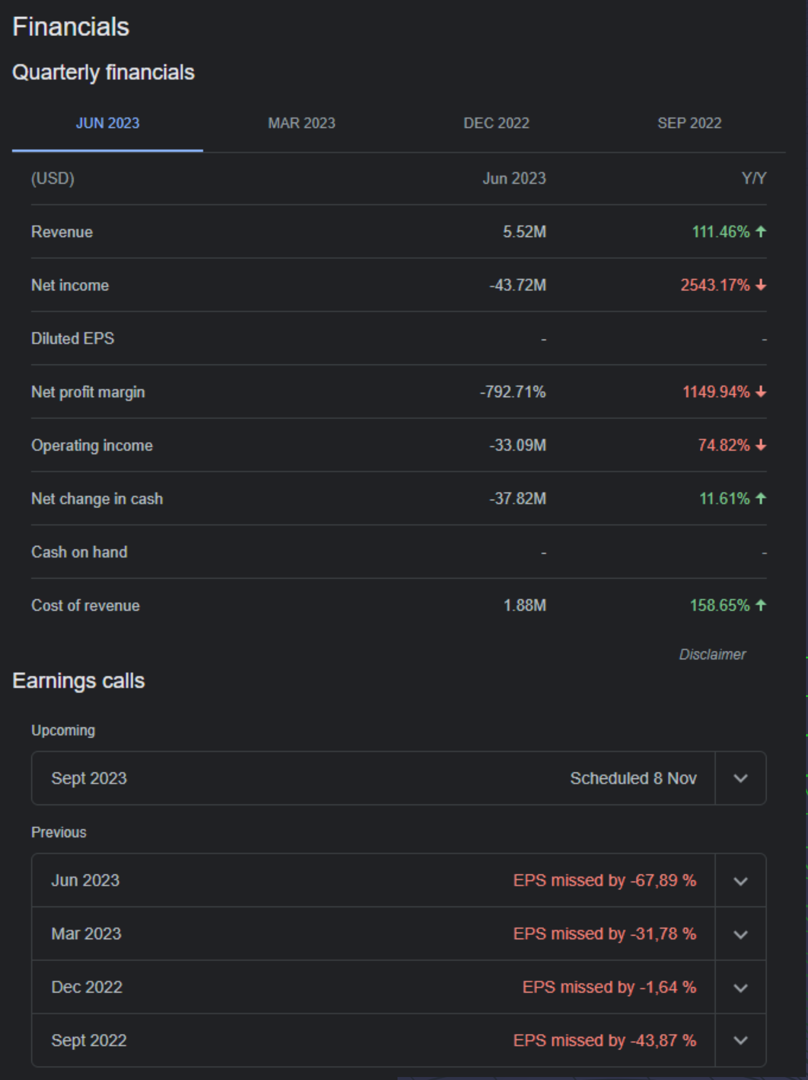
Market Summary > IONQ Inc

11,58 USD

+0.57 (5.18%) ↑ past 5 years

Closed: 3 Nov, 19:59 GMT-4 • Disclaimer
After hours 11,70 +0,12 (1,04 %)

Open	11,24	Mkt cap	2,35B
High	12,09	P/E ratio	-
Low	11,24	Div yield	-



Financials

Quarterly financials

(USD)	Jun 2023	Y/Y
Revenue	5.52M	111.46% ↑
Net income	-43.72M	2543.17% ↓
Diluted EPS	-	-
Net profit margin	-792.71%	1149.94% ↓
Operating income	-33.09M	74.82% ↓
Net change in cash	-37.82M	11.61% ↑
Cash on hand	-	-
Cost of revenue	1.88M	158.65% ↑

Disclaimer

Earnings calls

Upcoming

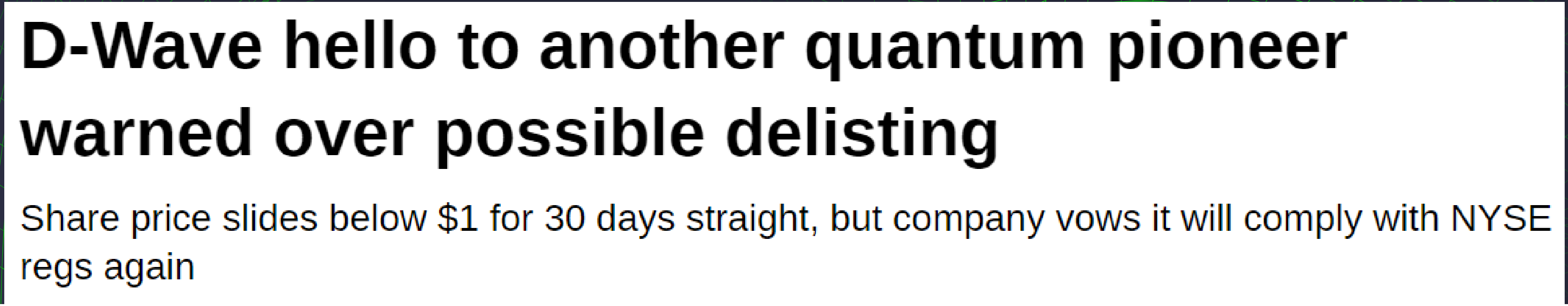
Sept 2023	Scheduled 8 Nov

Previous

Jun 2023	EPS missed by -67,89 %
Mar 2023	EPS missed by -31,78 %
Dec 2022	EPS missed by -1,64 %
Sept 2022	EPS missed by -43,87 %

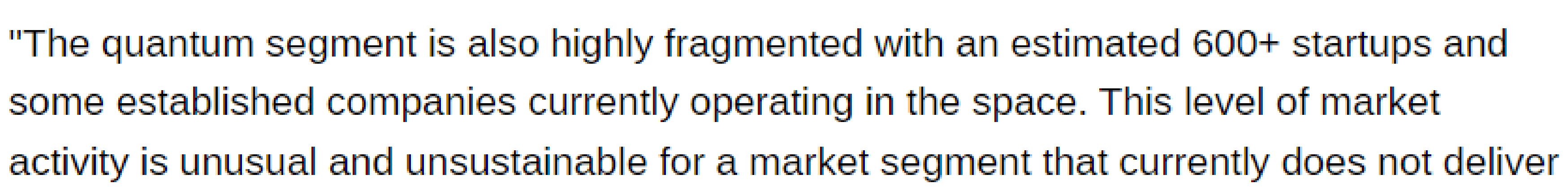
TRL 4-6

MARKET ANALYSIS OUTLETS / TECH BLOGs

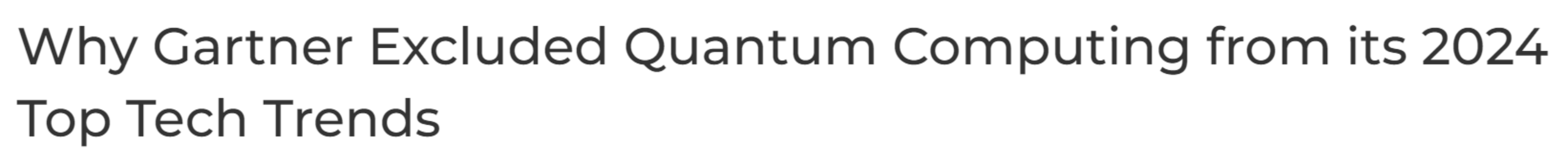


D-Wave hello to another quantum pioneer warned over possible delisting

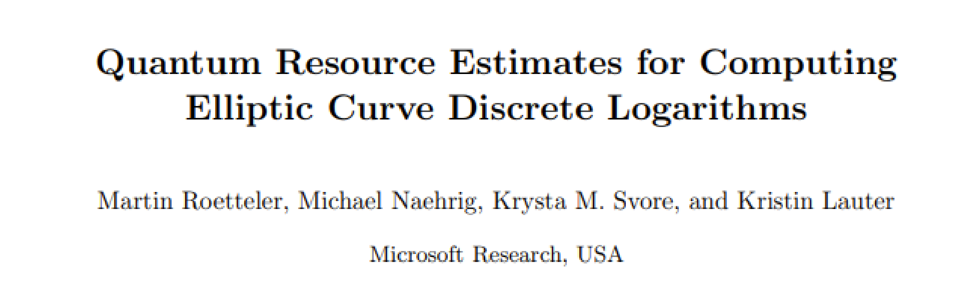
Share price slides below $1 for 30 days straight, but company vows it will comply with NYSE regs again



"The quantum segment is also highly fragmented with an estimated 600+ startups and some established companies currently operating in the space. This level of market activity is unusual and unsustainable for a market segment that currently does not deliver



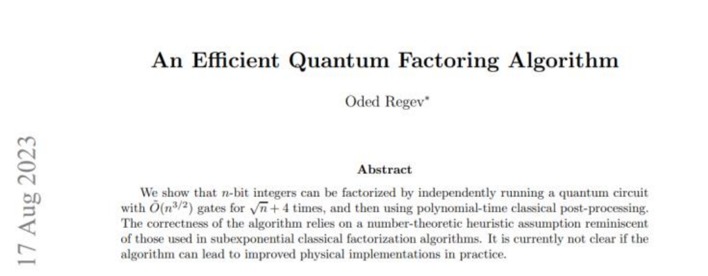
Why Gartner Excluded Quantum Computing from its 2024 Top Tech Trends



Quantum Resource Estimates for Computing Elliptic Curve Discrete Logarithms

Martin Roetteler, Michael Naehrig, Krysta M. Svore, and Kristin Lauter

Microsoft Research, USA



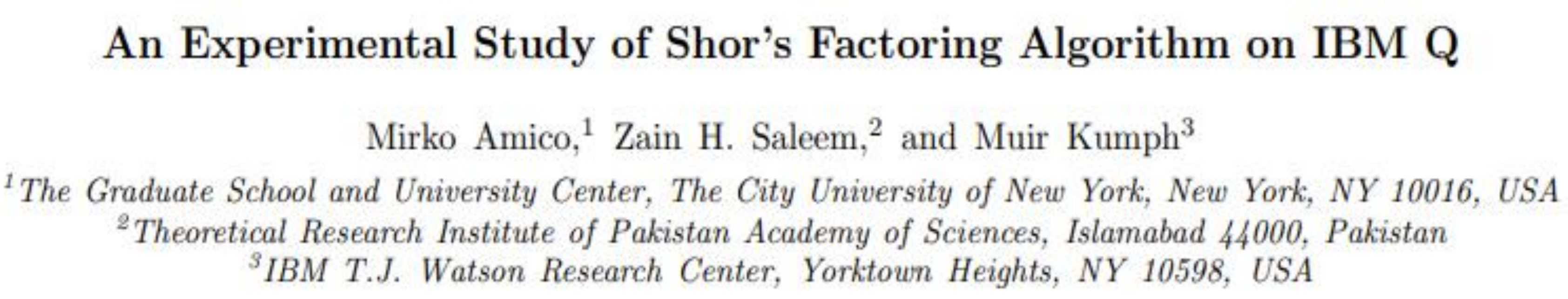
An Efficient Quantum Factoring Algorithm

Oded Regev*

17 Aug 2023

Abstract

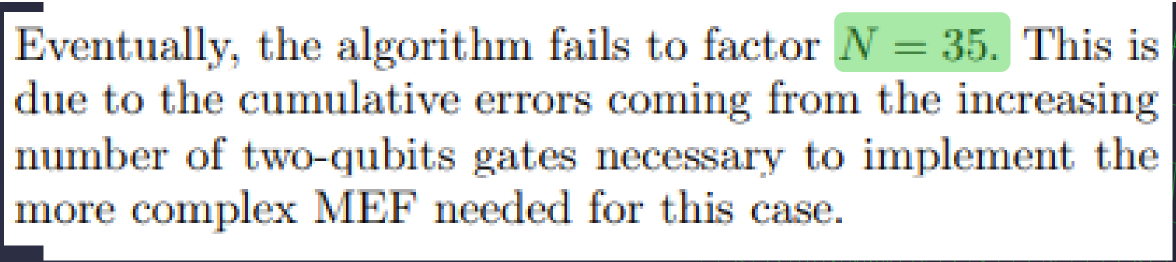
We show that n-bit integers can be factorized by independently running a quantum circuit with $\tilde{O}(n^{3/2})$ gates for $\sqrt{n}+4$ times, and then using polynomial-time classical post-processing. The correctness of the algorithm relies on a number-theoretic heuristic assumption reminiscent of those used in subexponential classical factorization algorithms. It is currently not clear if the algorithm can lead to improved physical implementations in practice.



An Experimental Study of Shor's Factoring Algorithm on IBM Q

Mirko Amico,[1] Zain H. Saleem,[2] and Muir Kumph[3]

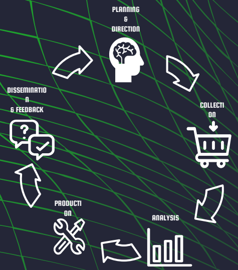
[1] The Graduate School and University Center, The City University of New York, New York, NY 10016, USA
[2] Theoretical Research Institute of Pakistan Academy of Sciences, Islamabad 44000, Pakistan
[3] IBM T.J. Watson Research Center, Yorktown Heights, NY 10598, USA



Eventually, the algorithm fails to factor $N = 35.$ This is due to the cumulative errors coming from the increasing number of two-qubits gates necessary to implement the more complex MEF needed for this case.

ANALYSIS

CONTEXTUALIZATION



PLANNING
&
DIRECTION

COLLECTI
ON

ANALYSIS

PRODUCTI
ON

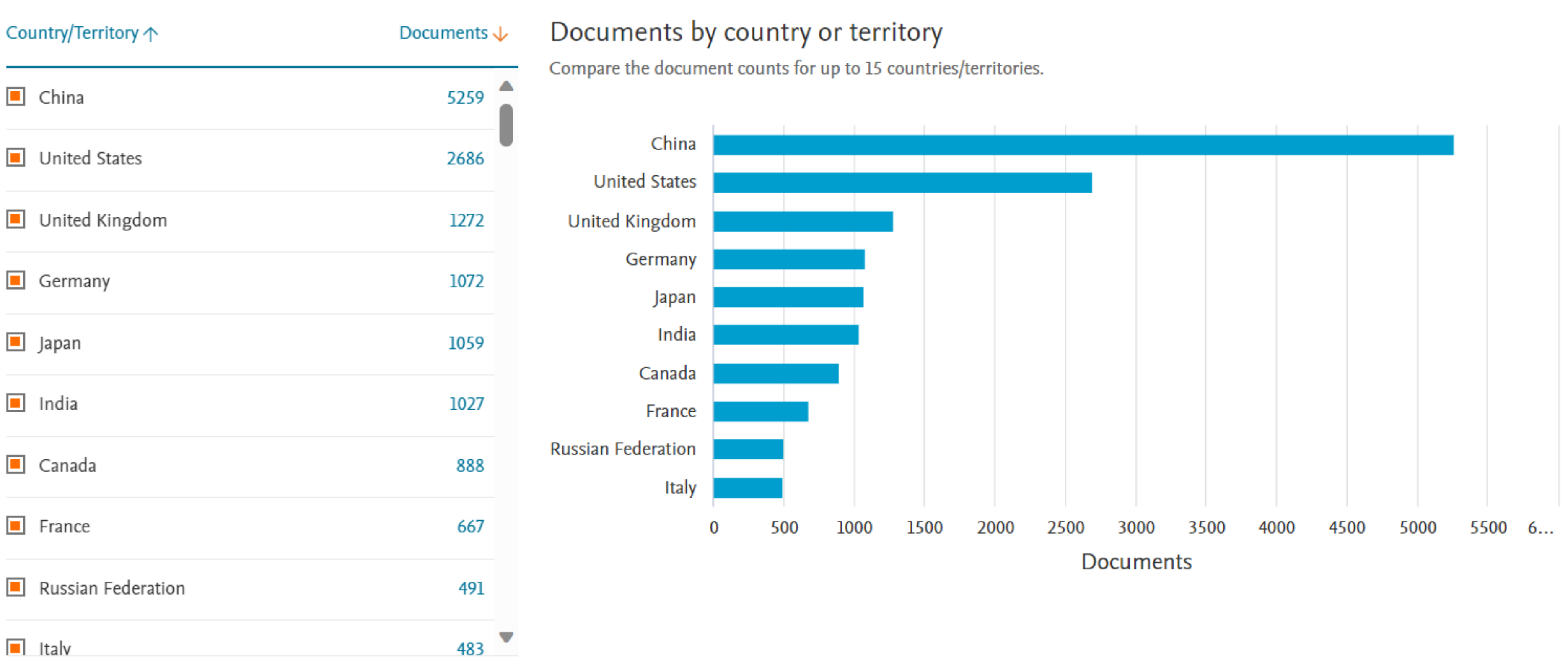
DISSEMINATIO
N
& FEEDBACK

#quantum cryptography

Funding sponsor ↓ | Documents ↓

Documents by funding sponsor

Compare the document counts for up to 15 funding sponsors.



Documents by country or territory

Compare the document counts for up to 15 countries/territories.

Country/Territory ↑	Documents ↓
☑ China	5259
☑ United States	2686
☑ United Kingdom	1272
☑ Germany	1072
☑ Japan	1059
☑ India	1027
☑ Canada	888
☑ France	667
☑ Russian Federation	491
☑ Italy	483

☑ National Research Foundation of Korea	3
☑ China Postdoctoral Science	2

WHAT ARE THE ATTACK SCENARIOS?

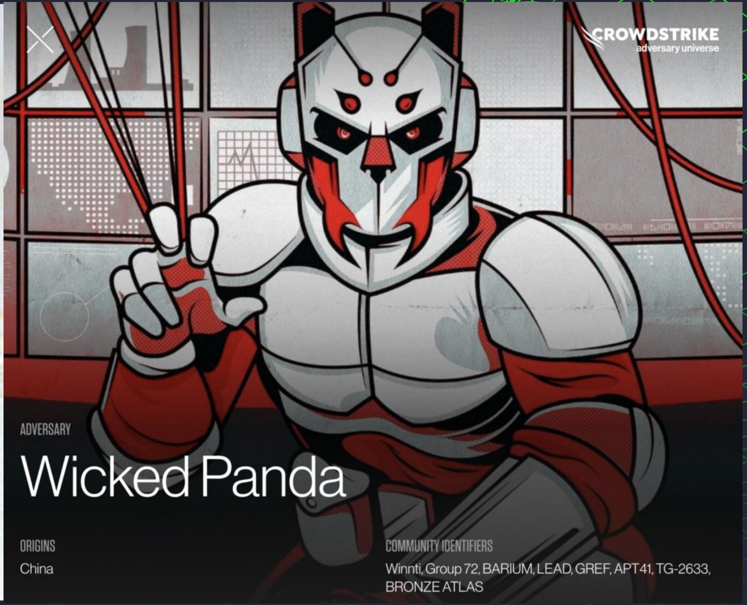
BRUTE FORCE

HARVEST NOW / DECRYPT LATER

NETWORK SNIFFING

THREAT ACTORS

CAPABILITIES, MOTIVE, SKILL LEVEL, SIZE



ADVERSARY

Wicked Panda

ORIGINS

China

COMMUNITY IDENTIFIERS

Winnti, Group 72, BARIUM, LEAD, GREF, APT41, TG-2633, BRONZE ATLAS

Picture Source: Threatpost, Crowdstrike

TRANSLATION

INTO COMMON LANGUAGE MODELS

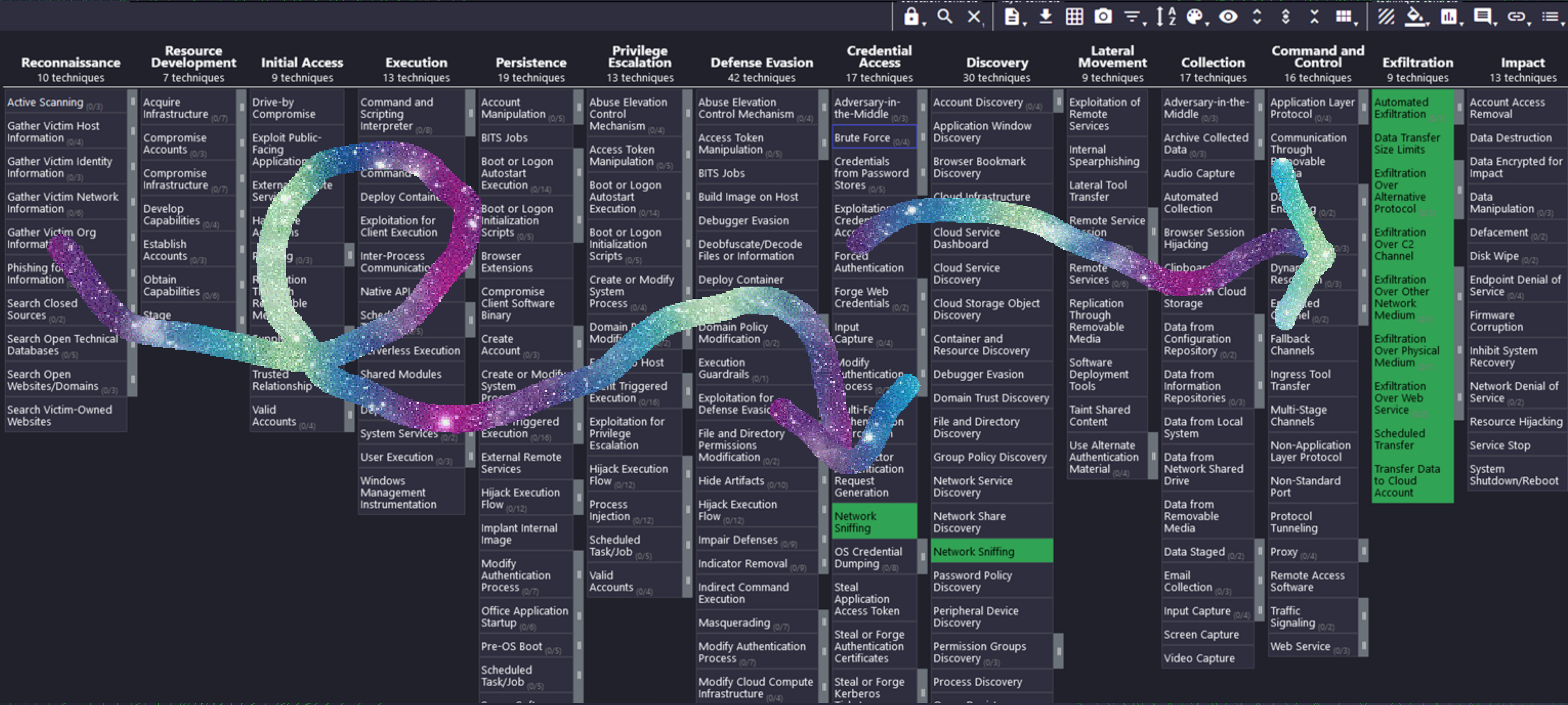
PLANNING
&
DIRECTION

COLLECTI
ON

ANALYSIS

PRODUCTI
ON

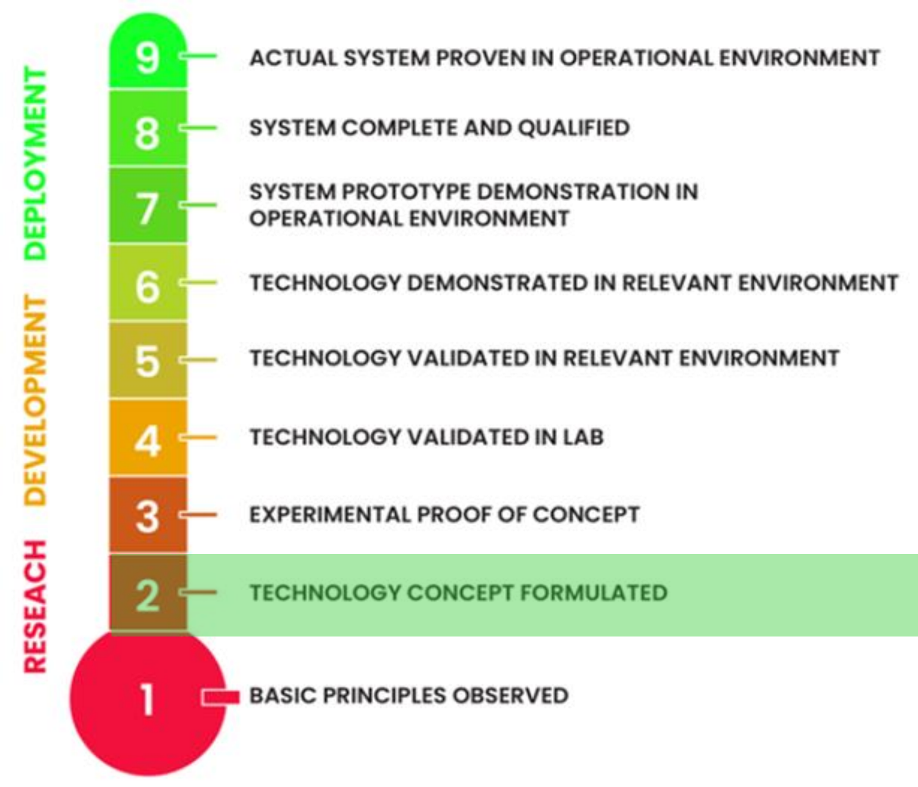
DISSEMINATIO
N
& FEEDBACK



Reconnaissance 10 techniques	Resource Development 7 techniques	Initial Access 9 techniques	Execution 13 techniques	Persistence 19 techniques	Privilege Escalation 13 techniques	Defense Evasion 42 techniques	Credential Access 17 techniques	Discovery 30 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 16 techniques	Exfiltration 9 techniques	Impact 13 techniques
Active Scanning (0/3)	Acquire Infrastructure (0/7)	Drive-by Compromise	Command and Scripting Interpreter (0/8)	Account Manipulation (0/5)	Abuse Elevation Control Mechanism (0/4)	Abuse Elevation Control Mechanism (0/4)	Adversary-in-the-Middle (0/3)	Account Discovery (0/4)	Exploitation of Remote Services	Adversary-in-the-Middle (0/3)	Application Layer Protocol (0/4)	Automated Exfiltration (0/1)	Account Access Removal
Gather Victim Host Information (0/4)	Compromise Accounts (0/3)	Exploit Public-Facing Application	Container Administration Command	BITS Jobs	Access Token Manipulation (0/5)	Access Token Manipulation (0/5)	Brute Force (0/4)	Application Window Discovery	Internal Spearphishing	Archive Collected Data (0/3)	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Gather Victim Identity Information (0/3)	Compromise Infrastructure (0/7)	External Remote Services	Deploy Container	Boot or Logon Autostart Execution (0/14)	Boot or Logon Autostart Execution (0/14)	BITS Jobs	Credentials from Password Stores (0/5)	Browser Bookmark Discovery	Lateral Tool Transfer	Audio Capture	Data Encoding (0/2)	Exfiltration Over Alternative Protocol (0/3)	Data Encrypted for Impact
Gather Victim Network Information (0/6)	Develop Capabilities (0/4)	Hardware Additions	Exploitation for Client Execution	Boot or Logon Initialization Scripts (0/5)	Boot or Logon Initialization Scripts (0/5)	Build Image on Host	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking	Automated Collection	Data Obfuscation (0/3)	Exfiltration Over C2 Channel	Data Manipulation (0/3)
Gather Victim Org Information	Establish Accounts (0/3)	Phishing (0/3)	Inter-Process Communication	Browser Extensions	Create or Modify System Process (0/4)	Debugger Evasion	Forced Authentication	Cloud Service Dashboard	Remote Services (0/6)	Browser Session Hijacking	Dynamic Resolution (0/3)	Exfiltration Over Other Network Medium (0/1)	Defacement (0/2)
Phishing for Information	Obtain Capabilities (0/6)	Replication Through Removable Media	Native API	Compromise Client Software Binary	Domain Policy Modification (0/2)	Deobfuscate/Decode Files or Information	Forge Web Credentials (0/2)	Cloud Service Discovery	Replication Through Removable Media	Clipboard Data	Encrypted Channel (0/2)	Exfiltration Over Physical Medium (0/1)	Disk Wipe (0/2)
Search Closed Sources (0/2)	Stage	Supply Chain Compromise	Scheduled Task/Job (0/5)	Create Account (0/3)	Escape to Host	Deploy Container	Input Capture (0/4)	Cloud Storage Object Discovery	Software Deployment Tools	Data from Cloud Storage	Fallback Channels	Exfiltration Over Web Service (0/2)	Endpoint Denial of Service (0/4)
Search Open Technical Databases (0/5)		Trusted Relationship	Serverless Execution	Create or Modify System Process	Event Triggered Execution (0/16)	Domain Policy Modification (0/2)	Modify Authentication Process	Container and Resource Discovery	Taint Shared Content	Data from Configuration Repository (0/2)	Ingress Tool Transfer	Scheduled Transfer	Firmware Corruption
Search Open Websites/Domains (0/3)		Valid Accounts (0/4)	Shared Modules	Event Triggered Execution (0/16)	Exploitation for Privilege Escalation	Execution Guardrails (0/1)	Multi-Factor Authentication Interception	Debugger Evasion	Use Alternate Authentication Material (0/4)	Data from Information Repositories (0/3)	Multi-Stage Channels	Transfer Data to Cloud Account	Inhibit System Recovery
Search Victim-Owned Websites			Software Deployment Tools	External Remote Services	Hijack Execution Flow (0/12)	Exploitation for Defense Evasion	Multi-Factor Authentication Request Generation	Domain Trust Discovery		Data from Local System	Non-Application Layer Protocol		Network Denial of Service (0/2)
			System Services (0/2)	Hijack Execution Flow (0/12)	Process Injection (0/12)	File and Directory Permissions Modification (0/2)	Network Sniffing	File and Directory Discovery		Data from Network Shared Drive	Non-Standard Port		Resource Hijacking
			User Execution (0/3)	Implant Internal Image	Scheduled Task/Job (0/5)	Hide Artifacts (0/10)	OS Credential Dumping (0/8)	Group Policy Discovery		Data from Removable Media	Protocol Tunneling		Service Stop
			Windows Management Instrumentation	Modify Authentication Process (0/7)	Valid Accounts (0/4)	Hijack Execution Flow (0/12)	Steal Application Access Token	Network Service Discovery		Data Staged (0/2)	Proxy (0/4)		System Shutdown/Reboot
				Office Application Startup (0/6)		Impair Defenses (0/9)	Steal or Forge Authentication Certificates	Network Share Discovery		Email Collection (0/3)	Remote Access Software		
				Pre-OS Boot (0/5)		Indicator Removal (0/9)	Steal or Forge Kerberos	Network Sniffing		Input Capture (0/4)	Traffic Signaling (0/2)		
				Scheduled Task/Job (0/5)		Indirect Command Execution		Password Policy Discovery		Screen Capture	Web Service (0/3)		
						Masquerading (0/7)		Peripheral Device Discovery		Video Capture			
						Modify Authentication Process (0/7)		Permission Groups Discovery (0/3)					
						Modify Cloud Compute Infrastructure (0/4)		Process Discovery					

QUANTUM THREAT

Risk posed to public key cryptography



9 ACTUAL SYSTEM PROVEN IN OPERATIONAL ENVIRONMENT

8 SYSTEM COMPLETE AND QUALIFIED

7 SYSTEM PROTOTYPE DEMONSTRATION IN OPERATIONAL ENVIRONMENT

6 TECHNOLOGY DEMONSTRATED IN RELEVANT ENVIRONMENT

5 TECHNOLOGY VALIDATED IN RELEVANT ENVIRONMENT

4 TECHNOLOGY VALIDATED IN LAB

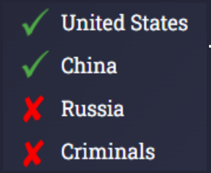
3 EXPERIMENTAL PROOF OF CONCEPT

2 TECHNOLOGY CONCEPT FORMULATED

1 BASIC PRINCIPLES OBSERVED

QUANTUM THREAT

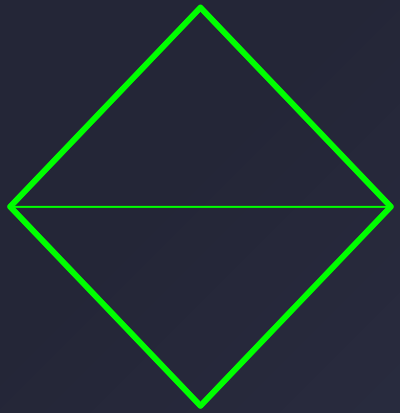
Risk posed to public key cryptography



- ✓ United States
- ✓ China
- ✗ Russia
- ✗ Criminals

→questionable adversary cost

ADVERSARY



INFRASTRUCTURE

BGP hijacking
(victim agnostic)

C2 Channel
….

CAPABILITY

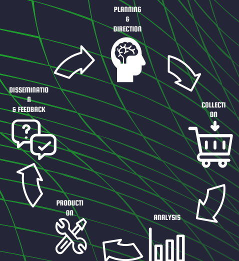
Physical access to QC
Initial Access
Lateral Movement
Defense Evasion
Network Sniffing
Exfiltration

VICTIM

Government proximity
Data with long INT lifetime

PRODUCTION

COMMUNICATION



PLANNING & DIRECTION

COLLECTION

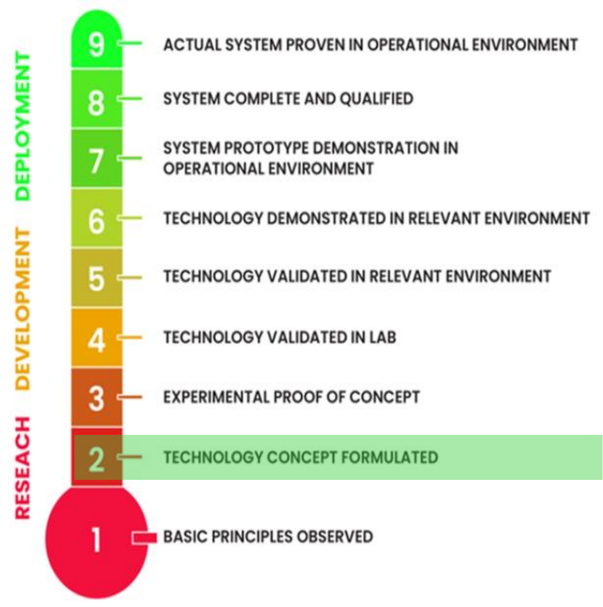
ANALYSIS

PRODUCTION

DISSEMINATION & FEEDBACK

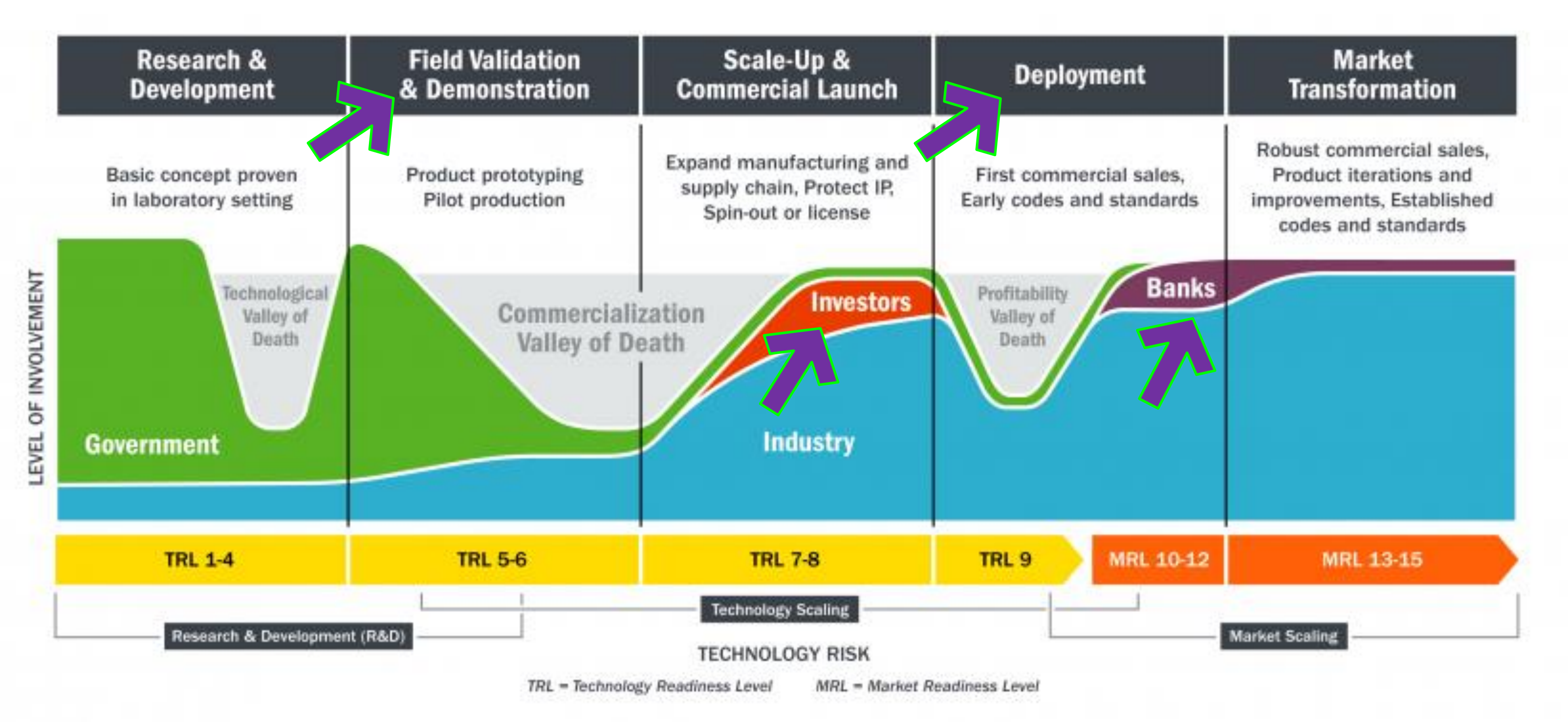
QUANTUM THREAT TAKEAWAYS – FOR SENIOR LEADERSHIP

Risks posed to public key cryptography


DEPLOYMENT
DEVELOPMENT
RESEACH
9 ACTUAL SYSTEM PROVEN IN OPERATIONAL ENVIRONMENT
8 SYSTEM COMPLETE AND QUALIFIED
7 SYSTEM PROTOTYPE DEMONSTRATION IN OPERATIONAL ENVIRONMENT
6 TECHNOLOGY DEMONSTRATED IN RELEVANT ENVIRONMENT
5 TECHNOLOGY VALIDATED IN RELEVANT ENVIRONMENT
4 TECHNOLOGY VALIDATED IN LAB
3 EXPERIMENTAL PROOF OF CONCEPT
2 TECHNOLOGY CONCEPT FORMULATED
1 BASIC PRINCIPLES OBSERVED

- Inflated threat! Will remain theoretical for at least 20 years
- Who likely should care?
  - those with Government proximity
- Predicates
  - Core fundamental research
  - Funding streams
  - QC skills, access to quantum computing HW, etc.
- Current State of Play
  - ✓ United States
  - ✓ China
  - ✗ Russia
  - ✗ Criminals

PROACTIVE SCOPING


Research & Development
Field Validation & Demonstration
Scale-Up & Commercial Launch
Deployment
Market Transformation
Basic concept proven in laboratory setting
Product prototyping Pilot production
Expand manufacturing and supply chain, Protect IP, Spin-out or license
First commercial sales, Early codes and standards
Robust commercial sales, Product iterations and improvements, Established codes and standards
LEVEL OF INVOLVEMENT
Technological Valley of Death
Commercialization Valley of Death
Profitability Valley of Death
Government
Investors
Banks
Industry
TRL 1-4
TRL 5-6
TRL 7-8
TRL 9
MRL 10-12
MRL 13-15
Technology Scaling
Research & Development (R&D)
Market Scaling
TECHNOLOGY RISK
TRL = Technology Readiness Level
MRL = Market Readiness Level

KEY TAKEAWAYS:

1. BE PROACTIVE IN EMERGENT TECHNOLOGY ASSESSMENTS
2. LEVERAGE COMMON LANGUAGE MODELS & STAY CONSISTENT
3. PROVIDE VALUE TO YOUR ORG BY CONTEXTUALIZATION SO LEADERS CAN TAKE INFORMED DECISIONS

THANK YOU!

QUANTUM PERCEPTION SURVEY

forms.gle/dH4CwyXmb3Bp5JMY9

LET'S TALK!

natalie.kilber@nablaco.com

linkedin.com/in/donuts

CREDITS: This presentation was created with a Slidesgo template, including icons by Flaticon and inforgraphics by Freepik.