Helping Organizations
Anticipate and Approach
Emerging Technology Threats
COMMON LANGUAGE MODELS

ADVERSARY

INFRASTRUCTURE

VICTIM

CAPABILITY

ATTACK PATH → MITRE | ATT&CK®
USING TECHNOLOGY MATURITY MODELS

ME EXPLAINING EACH METRIC
NASA TECHNOLOGY READINESS LEVELS

1. BASIC PRINCIPLES OBSERVED
2. TECHNOLOGY CONCEPT FORMULATED
3. EXPERIMENTAL PROOF OF CONCEPT
4. TECHNOLOGY VALIDATED IN LAB
5. TECHNOLOGY VALIDATED IN RELEVANT ENVIRONMENT
6. TECHNOLOGY DEMONSTRATED IN RELEVANT ENVIRONMENT
7. SYSTEM PROTOTYPE DEMONSTRATION IN OPERATIONAL ENVIRONMENT
8. SYSTEM COMPLETE AND QUALIFIED
9. ACTUAL SYSTEM PROVEN IN OPERATIONAL ENVIRONMENT
DIFFERENT SOURCES
PLANNING & DIRECTION
## Different Intelligence Sources Required per Tech Readiness Level (TRL)

<table>
<thead>
<tr>
<th>Level</th>
<th>TRLs</th>
<th>Sources</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mature</td>
<td>7–9</td>
<td>Mainstream Industry News, Initial Public Offering, Stock Market</td>
</tr>
<tr>
<td>Development</td>
<td>4–6</td>
<td>VC investment, Market Analysis, Patents, Technology licensing</td>
</tr>
<tr>
<td>Research</td>
<td>1–3</td>
<td>Scientific publications, Research Funding</td>
</tr>
<tr>
<td>Hype</td>
<td>Presented as TRL 7–9 whereas in fact it is at TRLs 1–3, if at all.</td>
<td>TRL 7-9 sources, but mainly driven through TRL1-3 sources</td>
</tr>
</tbody>
</table>
COLLECTION
EXTENDED INTELLIGENCE SOURCES
CASE STUDY:
QUANTUM THREAT
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.
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 Nachrig, Krysta M. Svore, and Kristin Lauter
Microsoft Research, USA

An Efficient Quantum Factoring Algorithm
Oded Regev*

Abstract
We show that n-bit integers can be factored by independently running a quantum circuit with $O(n^{5/3})$ gates for $n = 4$ 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 sub-exponential 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.
Scientific paper/Publication database analytics:

- Web of science
- Scopus
- Google Ngram Viewer

#quantum cryptography

**Documents by country or territory**

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

- China: 5259
- United States: 2686
- United Kingdom: 1272
- Germany: 1072
- Japan: 1059
- India: 1027
- Canada: 888
- France: 667
- Russian Federation: 491
- Italy: 483
WHAT ARE THE ATTACK SCENARIOS?

BRUTE FORCE

HARVEST NOW / DECRYPT LATER

NETWORK SNIFFING
THREAT ACTORS
CAPABILITIES, MOTIVE, SKILL LEVEL, SIZE

Picture Source: Threatpost, Crowdstrike
TRANSLATION INTO COMMON LANGUAGE MODELS
Risk posed to public key cryptography

**QUANTUM THREAT**

- **Government proximity**
- Data with long **INT lifetime**
- **BGP hijacking** (victim agnostic)
- **C2 Channel**

→ **questionable adversary cost**

**Physical access to QC**

**Initial Access**

**Lateral Movement**

**Defense**

**Evasion**

**Network Sniffing**

**Exfiltration**
Risk posed to public key cryptography

**QUANTUM THREAT**

**INFRASTRUCTURE**
- BGP hijacking (victim agnostic)
- C2 Channel
  ...

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

**ADVERSARY**
- United States
- China
- Russia
- Criminals

→questionable adversary cost

**VICTIM**
- Government proximity
- Data with long INT lifetime
QUANTUM THREAT TAKEAWAYS – FOR SENIOR LEADERSHIP

Risks posed to public key cryptography

- 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
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!
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 infographics by Freepik.