NATIONAL ACADEMIES *Sciences Engineering Medicine*

Cryptography and the Intelligence Community- The Future of Encryption Report Summary

Steve Lipner, Committee Chair

NOVEMBER 2022 UPDATE

Committee Roster

Chair: Mr. Steven B. Lipner (NAE), SAFECode **

Vice Chair: **Dr. Mark Lowenthal,** Intelligence & Security Academy, LLC **

<u>Committee Members</u>

Mr. Hans Robert Davies, Toffler Associates **

Mr. Chip Elliott, BBN Technologies

Mr. Glenn S. Gerstell, Center for Strategic & International Studies

Dr. Nadia Heninger, University of California, San Diego **

Dr. Seny Kamara, Brown University

Mr. Paul Carl Kocher (NAE)

Dr. Brian LaMacchia, Microsoft Research

Dr. Butler Lampson (NAS, NAE), Microsoft Research

Dr. Rafail Ostrovsky, University of California, Los Angeles

Ms. Elizabeth Rindskopf Parker, State Bar of California (retired)

Mr. Peter Swire, Georgia Institute of Technology

Dr. Peter J. Weinberger, Google Inc.

** Today's presenters

Statement of Task Summary

- Identify potential scenarios over the next 10 to 20 years for the balance between encryption and decryption.
- Assess the national security and intelligence implications of the scenarios the committee deems most relevant and significant.
- Identify and assess options for responding to the scenarios, assess implications for future IC investments.

Report Outline

- Summary
- Introduction
- Introduction to Encryption
- Scenario Methodology
- Drivers
  - Scientific Advances
  - Society and Governance
  - Systems
- Scenarios
- Implications for U.S. Intelligence
- Findings

In addition to scenarios, report presents findings that are important across all future scenarios

About Encryption

- Cryptography: science of transforming information using algorithm and key – algorithm widely known; information unreadable as long as (decryption) key protected
  - Secret-key/symmetric cryptography: used for bulk encryption
  - Public-key cryptography: used for key exchange/negotiation and authentication

- Applications
  - Encryption: Protect confidentiality of communications and data at rest
  - Authentication: Verify authenticity of data, people, or code
  - Emerging technologies: Computing on encrypted data, zero-knowledge proofs...

Creating Scenarios

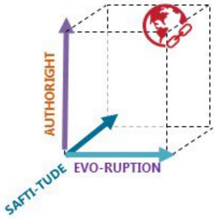
For the purposes of the study, the committee is using scenario planning to design the worlds

RESEARCH

Scan the environment, collect multi-dimensional information

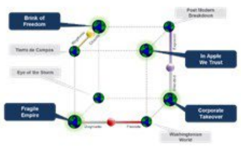
ANALYSIS

Identify the drivers causing and contributing to change, deeper than trends



SYNTHESIS

The intersections of drivers identify worlds defined by future scenarios



STORYTELLING & ROLE-PLAY

"Living in the worlds" with future-focused personas creates robust understanding

Brink of Freedom
In Apple We Trust
Fragile Empire
Corporate Takeover
Low
High

EVALUATION & PLANNING

Take the worlds we find most relevant to the sponsor's question(s) and explore the risks and opportunities. Ultimate outcomes include tangible and actionable recommendations for implementation.

Drivers of the Future of Encryption

Committee's briefings from technical and policy experts, and members' experience point to these three orthogonal drivers of the future

Scientific Advances

PREDICTABLE — DISRUPTIVE

The rate at which scientific discovery and application has advanced encryption and related technologies

Society and Governance

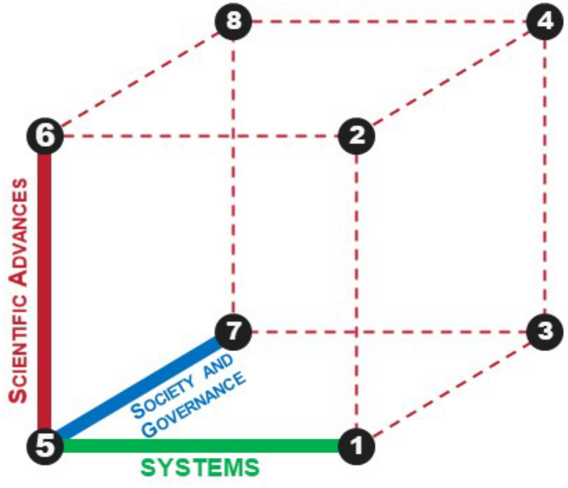
FRAGMENTED — GLOBAL

How nation states and individuals perceive risks and benefits of encryption and have designed standards, laws, and policies to address them

Systems

CHAOTIC — MATURE

The manner in which encryption technologies are implemented



NATIONAL ACADEMIES *Sciences Engineering Medicine*

Driver Details: Scientific Advances

Predictable

- Quantum computers do not threaten current cryptography
- Refined suite of quantum-resistant encryption algorithms
- Specialized deployments of advanced techniques

Disruptive

- Unforeseen improvements in quantum computers
- Significant cryptanalytic breakthroughs threaten deployed cryptography
- Unexpected new applications of cryptography cause frenzy of attention

Driver Details: Society and Governance

Fragmented

- Governments demand local data storage and access, and limit privacy
- Local technologies are the norm
- Citizen mistrust poses internal and external challenges for IC

Global

- Markets preserve a unified Internet protected by strong encryption
- International standards rule the Internet
- Citizen trust enables solutions for IC mission while preserving privacy

Driver Details: Systems

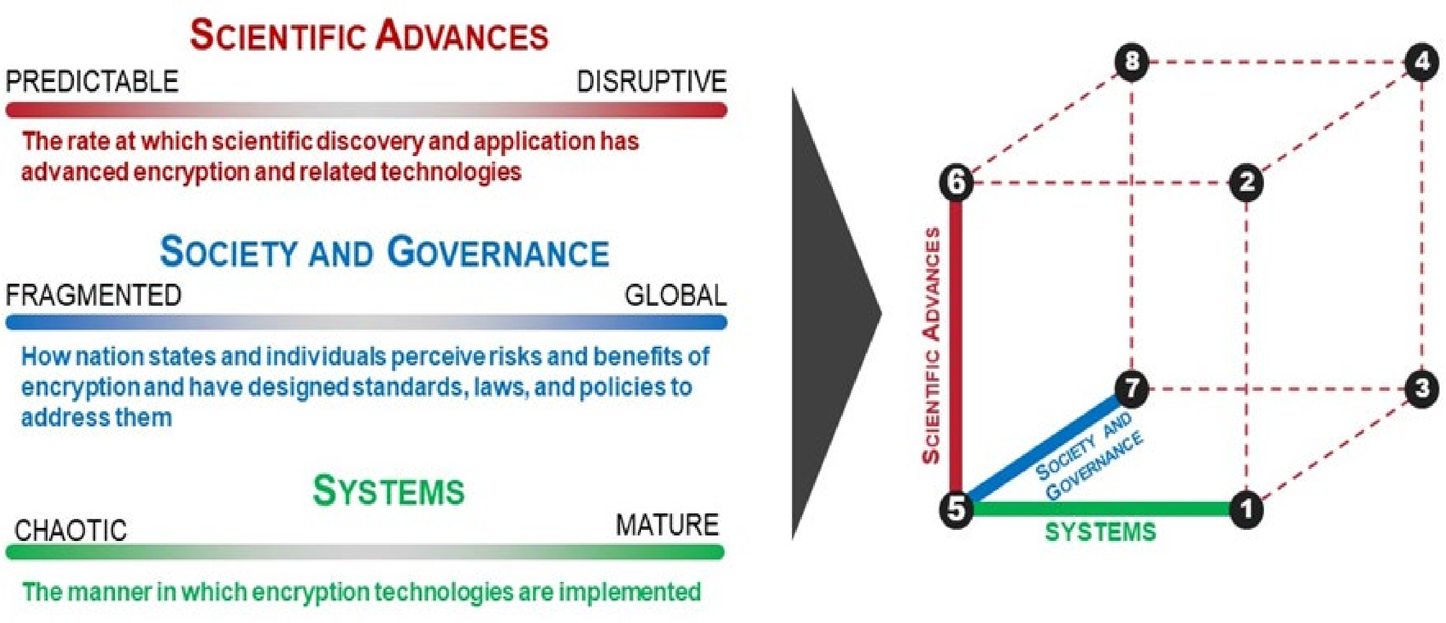
Chaotic

- Customers cope with the security they're delivered
- Vendors deliver features and performance
- Slow progress in security tools and processes
- Security is a niche specialty for engineering and IT

Mature

- Customers demand secure products and services
- Vendors view security as a must-have attribute
- Market demand leads to significant progress
- Security knowledge and expertise are both broad and deep

Potential Worlds



Scientific Advances

PREDICTABLE — DISRUPTIVE

The rate at which scientific discovery and application has advanced encryption and related technologies

Society and Governance

FRAGMENTED — GLOBAL

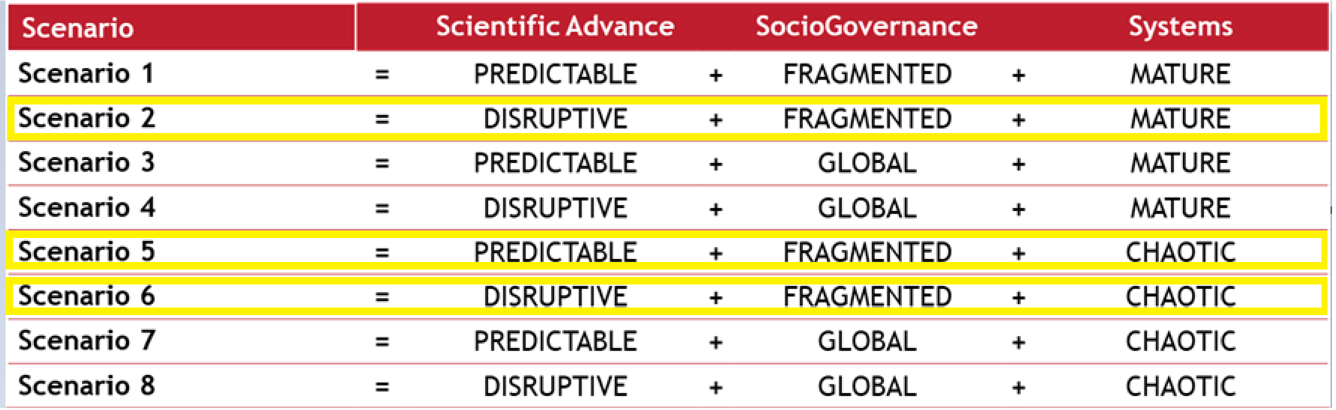
How nation states and individuals perceive risks and benefits of encryption and have designed standards, laws, and policies to address them

Systems

CHAOTIC — MATURE

The manner in which encryption technologies are implemented

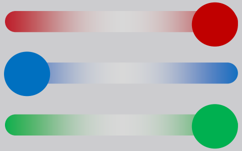
Selected Scenarios



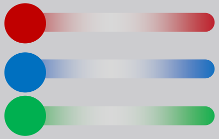
Scenario		Scientific Advance		SocioGovernance		Systems
Scenario 1	=	PREDICTABLE	+	FRAGMENTED	+	MATURE
Scenario 2	=	DISRUPTIVE	+	FRAGMENTED	+	MATURE
Scenario 3	=	PREDICTABLE	+	GLOBAL	+	MATURE
Scenario 4	=	DISRUPTIVE	+	GLOBAL	+	MATURE
Scenario 5	=	PREDICTABLE	+	FRAGMENTED	+	CHAOTIC
Scenario 6	=	DISRUPTIVE	+	FRAGMENTED	+	CHAOTIC
Scenario 7	=	PREDICTABLE	+	GLOBAL	+	CHAOTIC
Scenario 8	=	DISRUPTIVE	+	GLOBAL	+	CHAOTIC

- Fragmented scenarios maximize stress, possibly most realistic
- Variations in Scientific Advances and Sytems expose a range of future events

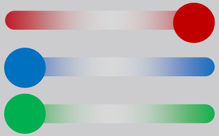
2: A Brave and Expensive New World

Driver Endpoints	Highlights
 Disruptive Fragmented Mature	- A breakthrough in quantum computing is balanced with more secure systems and software and an orderly transition to post-quantum encryption. - International relations dominated by a few major power blocs each with its own preferred encryption standards - Defense has the advantage in this scenario, making human intelligence sources a priority

5. The Known World, Only More So

Driver Endpoints	Highlights
 Predictable Fragmented Chaotic	• With no major breakthroughs and a continued lack of focus on systems and security, breaches remain common; meanwhile, the slow pace of technology change has allowed emerging competitors the chance to "catch up." • Attacks on systems are the province of governments and private actors, large and small • Offense has the advantage and all parties face a continuing stream of successful attacks

6. Colony Collapse

Driver Endpoints	Highlights
 Disruptive Fragmented Chaotic	- A breakthrough in factoring and a lack of focus on cryptographic systems and security puts information at risk. - Despite advances in computing on encrypted data, public trust remains low. - Fragmented standards and government limitations on encryption help lead to offensive advantage and all parties face a continuing stream of successful attacks

Key Finding Summaries

- Chaotic systems are likely to undermine the security of encryption
- Fragmented society and governance are likely to degrade the security of systems and organizations that rely on encryption
- Addressing the challenges posed by encryption requires technical talent that is in short supply
- A mathematical breakthrough could threaten current encryption algorithms
- Computing on encrypted data has the potential to improve security and privacy for individuals and organizations

Implications for U.S. Intelligence

- Encryption will be a significant factor across all aspects of the work of the Intelligence Community
- There will be a premium on early, accurate detection of trends
  - Given the challenges of such detection, the IC may need to concurrently plan for alternate outcomes
- It is incumbent on the Intelligence Community to make clear to policy makers what is at stake
- Key Finding: With more adversary nations (especially China) seeking and making advances in encryption and as academic researchers (especially in Europe) continue to invest in cryptography, the advantage of the Intelligence Community will diminish if not disappear.
- It may be necessary to adapt personnel policies to accommodate short-term employees or external consultants to gain access to needed expertise and external contacts.

Questions and Answers

E = mc²
There is grandeur
in this view of life,
with its several powers,
having been originally breathed
into a few forms or into one;
and that, whilst this planet
has gone cycling on
according to the fixed
law of gravity,
from so simple a beginning
endless forms most beautiful
and most wonderful have been,
and are being, evolved.

Society and Governance Talking Points

- This driver is really orthogonal to the other two drivers which are much more technical
- It focuses on the human, non-technical, and “messy” aspects that influence the use and effectiveness of encryption
- Including cultural elements of privacy and trust as well as broader geopolitics
- Of particular note is that fragmented governance may lead to fragmented technology including systems, networks, and encryption
- And fragmented society may lead to challenges with the trust in people that has to underlie secure encryption and other technologies