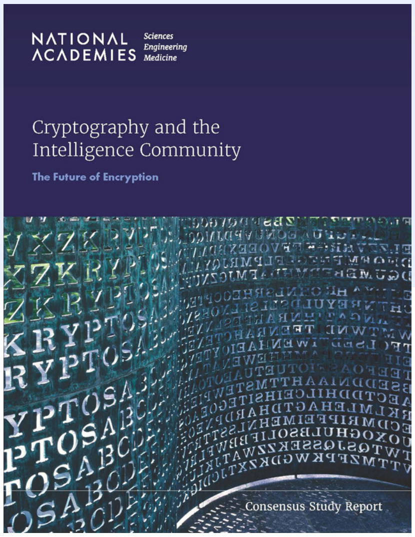
NATIONAL ACADEMIES Sciences Engineering Medicine

Consensus Study Report
Highlights

Cryptography and the Intelligence Community: The Future of Encryption


NATIONAL ACADEMIES Sciences Engineering Medicine
Cryptography and the Intelligence Community
The Future of Encryption
Consensus Study Report

Cryptography plays a significant role in the intelligence community's mission to both protect sensitive information from disclosure and collect intelligence about the activities of governments and others who pose potential threats to the nation's interests. In an increasingly digital world, more data are encrypted. At the same time, efforts to attack or disrupt encrypted systems—government, personal, and private sector—have also increased.

The Office of the Director of National Interest (ODNI) requested the National Academies establish a committee to identify potential scenarios that explore the range of possible developments in cryptography and their implications over the next 10 to 20 years. This report assesses the national security and intelligence implications of a subset of those scenarios, chosen for the challenges that they present.

Looking forward, one of the key concerns in cryptography is the potential development of quantum computers programmed to defeat almost all public key encryption and digital signature systems that are used on the Internet. However, the intelligence community will also need to address the impact of other trends in technology, policy, and society. *Cryptography and the Intelligence Community: The Future of Encryption* examines these issues and ways to address them. This document highlights some of the committee's findings. The complete report and findings can be read or downloaded at https://nap.nationalacademies.org/catalog/26168.

EXPLORING SCENARIOS FOR THE FUTURE

The committee identifies scenarios for the future of encryption and potential areas of technology surprise. The scenarios result from combinations of technical and non-technical "drivers" that influence the direction of technology as well as the decisions and actions of individuals and governments.

The report considers three major drivers the committee believes will greatly influence the future of encryption over the next 10 to 20 years: theoretical breakthroughs or technological advances, such as large-scale quantum computers; changes in society and digital governance, including policies, politics, and points of view; and the products and technology that implement, embed, or support encryption. The committee identified what would define the extremes of each of the three drivers. Those extremes were then used to construct scenarios. For example, the two endpoints of scientific advances are predictable or disruptive. See the figure below for more detail.

Using these drivers and their endpoints, the report identifies eight possible scenarios for the future of encryption and focuses on three of the scenarios for in-depth exploration, based on the objectives of covering plausible futures and exploring scenarios that result in illustrative challenges and opportunities. The scenarios were chosen because they offered the chance to explore the most interesting resulting worlds, not because they necessarily were presumed to be likely. The table below shows the eight possibilities, with the three scenarios that the committee explored highlighted.

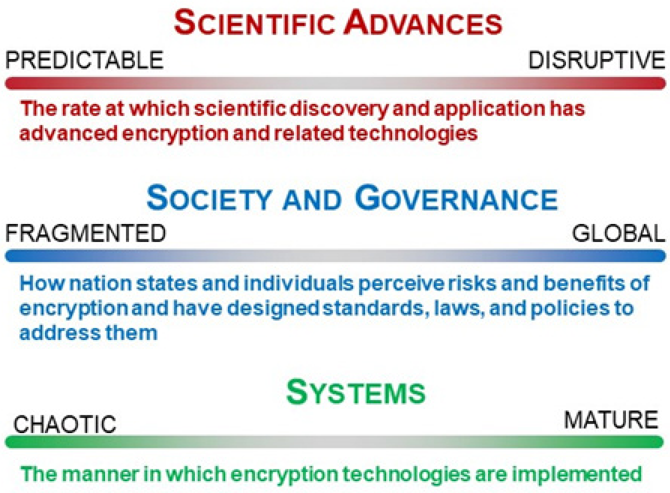

SCIENTIFIC ADVANCES
PREDICTABLE
DISRUPTIVE
The rate at which scientific discovery and application has advanced encryption and related technologies
SOCIETY AND GOVERNANCE
FRAGMENTED
GLOBAL
How nation states and individuals perceive risks and benefits of encryption and have designed standards, laws, and policies to address them
SYSTEMS
CHAOTIC
MATURE
The manner in which encryption technologies are implemented

FIGURE Visual representation of space defined by drivers.

TABLE
Endpoints That Define the Eight Possible Scenarios

SCENARIO	SCIENTIFIC ADVANCE	SOCIETY AND GOVERNANCE	SYSTEMS
1	Predictable	Fragmented	Mature
2	Disruptive	Fragmented	Mature
3	Predictable	Global	Mature
4	Disruptive	Global	Mature
5	Predictable	Fragmented	Chaotic
6	Disruptive	Fragmented	Chaotic
7	Predictable	Global	Chaotic
8	Disruptive	Global	Chaotic

THE CHOSEN SCENARIOS

The following paragraphs give a summary of each of the three chosen scenarios.

A Brave and Expensive New World

This scenario posits that a breakthrough in quantum computing is offset by an orderly transition to post-quantum encryption and other emerging cryptographic techniques because of investments in systems and cybersecurity. Overall, the balance now favors defense. However, the global political picture remains fragmented. The bottom line for the intelligence community is that offensive cryptography efforts have become more difficult, and the alliance structure that is a major plus for U.S. intelligence is less reliable and more fluid.

The Known World, Only More So

In this scenario there are no major breakthroughs regarding a quantum computer, and there is a continued lack of focus on systems and security. Therefore, system breaches remain common. Also, the slow pace of technology change has allowed emerging competitors the chance to catch up. The overall balance continues to favor offense. A key issue for U.S. intelligence is the broadening of the threat. Already the world is one in which many states and a growing number of non-state actors pose threats to U.S. and allied interests. These threats will likely increase in number and severity in this scenario, potentially compounded by the weakening of traditional alliances and partnerships. At the same time, a world of this sort remains a target rich environment for U.S. intelligence collection efforts. The constantly growing Internet of Things also adds to this threat and to the opportunity.

Colony Collapse

This scenario posits a breakthrough in the form of a new classical factoring algorithm. Such a breakthrough would render current public key encryption algorithms more easily attacked with much less effort than today, including by use of conventional computers. There would be much less need for a quantum computer; a roomful of powerful servers might be sufficient. Compared to a quantum computing breakthrough, a factoring breakthrough would probably have less advance notice, be easier to keep secret, and be attainable by more countries. In addition, a lack of focus on systems and security puts information at risk in this scenario. Despite advances in computing on encrypted data, trust remains low. This suggests, overall, a much more chaotic world combined with, as in the other scenarios, a more fragmented world politically that complicates the challenges for the intelligence community. Like the second scenario, the balance favors offense.

ESTABLISHING COMMON TRENDS AND KEY FINDINGS

The report looks at trends that are common across some or all of the scenarios and associated risks, opportunities, and actions. After examining these trends and overarching considerations that span most or all of the scenarios, the committee identified several key findings to help the intelligence community and other elements of the U.S. government, as well as the private sector, prepare for the future, recognize emerging threats and developments, and respond appropriately.

Immature systems are likely to undermine the security of encryption. The wide dependence of governments, companies, and individuals on commercial information technology products amplifies the importance of those products' implementation and applications of encryption. Vulnerabilities, bugs, and other errors can enable attackers to bypass or undermine encryption and compromise systems.

Fragmented society and governance are likely to degrade the security of systems and organizations that rely on encryption. The committee found that society and governance characterized by distrust among nations and individuals and the breakdown of national alliances will lead to wider use of cryptography, less sharing of information, and the proliferation of a variety of exclusive, national, post-quantum encryption standards.

Addressing the challenges posed by encryption requires technical talent that is in short supply. Despite initiatives aimed at enlarging the pool of cybersecurity talent, there remain unmet needs for security competence among software developers and information technology staff, for the more highly trained populations of engineers who create security software and systems, and for researchers who develop and analyze new encryption algorithms and protocols.

A mathematical breakthrough could threaten current encryption algorithms. While much of the current concern about the future of encryption is motivated by the potential development of working, large-scale, quantum computers, the report highlights that a disruptive breakthrough in mathematics could also pose a threat. Mathematics that would improve the performance of conventional computers on specific problems relevant to decryption, such as factoring and discrete logarithms, could provide an offensive advantage.

The lead of the intelligence community in encryption is diminishing. The United States and its intelligence community have long been leaders in encryption and related areas. The report notes that this advantage is shrinking as other countries invest and make advances in the theory and practice of encryption.

Computing applied to encrypted data has the potential to improve security and privacy for individuals and organizations. In recent years, there have been significant advances in algorithms that enable some kinds of processing of information without requiring that the information be decrypted. The research community continues to make improvements in the technology of computation on encrypted data. Such improvements can be expected to enable new ways of securely sharing information.

MOVING FORWARD

Regardless of which scenario envisioned by this study develops, the committee notes that encryption will change in fundamental ways that will pose challenges across all aspects of intelligence.

COMMITTEE ON THE FUTURE OF ENCRYPTION **STEVEN B. LIPNER (NAE)** (*Chair*), SAFECode/Carnegie Mellon University; **MARK LOWENTHAL** (*Vice Chair*), Intelligence & Security Academy, LLC; **HANS ROBERT DAVIES,** Toffler Associates; **CHIP ELLIOTT,** BBN Technologies; **GLENN S. GERSTELL,** Center for Strategic & International Studies; **NADIA HENINGER,** University of California, San Diego; **SENY KAMARA,** Brown University; **PAUL CARL KOCHER** (NAE), American Cryptographer; **BRIAN LAMACCHIA,** Microsoft Research; **BUTLER W. LAMPSON** (NAS /NAE), Microsoft Research; **RAFAIL OSTROVSKY,** University of California, Los Angeles; **ELIZABETH RINDSKOPF PARKER,** State Bar of California (Retired); **PETER SWIRE,** Georgia Institute of Technology; **PETER J. WEINBERGER,** Google, Inc.

STAFF **CARYN A. LESLIE,** Director, Intelligence Community Studies Board; **JON EISENBERG,** Director, Computer Science and Telecommunications Board; **LYNETTE MILLETT,** Senior Program Officer; **MARGUERITE SCHNEIDER,** Administrative Coordinator

FOR MORE INFORMATION

This Report Highlights was prepared by the National Academies' Intelligence Community Studies Board based on the report *Cryptography and the Intelligence Community: The Future of Encryption* (2022).

The study was sponsored by the Office of the Director of National intelligence. Any opinions, findings, conclusions, or recommendations expressed in this publication do not necessarily reflect the views of the sponsors.

This Consensus Study Report is available from the National Academies Press (800) 624-6242 | http://www.nap.edu | http://www.nationalacademies.org

Division on Engineering and Physical Sciences

NATIONAL ACADEMIES *Sciences Engineering Medicine*