Report of the National Commission for the Review of the Research and Development Programs of the United States Intelligence Community

National Commission for the Review of the Research and Development Programs • United States Intelligence Community •

E PLURIBUS UNUM

SPECIAL TOPIC WHITE PAPER: THE IC'S ROLE WITHIN U.S. CYBER R&D

Preface

CO-CHAIRS:

Mr. Maurice Sonnenberg
Samantha Ravich, PhD

COMMISSIONERS:

Sen. Dan Coats
Rep. Mike Conaway
Rep. Rush Holt
Hon. Shirley Ann Jackson, PhD
Mr. Gilman Louie
Mr. Kevin Meiners
Hon. Stephanie O'Sullivan
Mr. Troy Wade
Sen. Mark Warner
Hon. John J. Young, Jr.

EXECUTIVE DIRECTOR:

David A. Bray, PhD

National Commission for Review of the Research and Development Programs • United States Intelligence Community

Since Congress created the modern Intelligence Community (IC) with the passage of the National Security Act of 1947, the IC has existed to serve one overarching goal—to provide timely and accurate intelligence to inform, warn, and act on behalf of U.S. decisionmakers to ensure our continued national security. The National Commission for the Review of the Research and Development Programs of the United States Intelligence Community was established by Public Law 107-306, as amended by Public Law 111-259, to review the R&D programs of the IC and to ensure that this goal is being, and will continue to be, met.

In the legislation establishing the Commission, Congress noted that for the foreseeable future, the IC "must operate in a dynamic, highly-challenging environment against a growing number of hostile, technically-sophisticated threats." Aided by their growing national commitments to R&D, current and potential adversaries of U.S. interests have easy access to advanced sensors, social media tools, a variety of communication networks, precision weapons and home-made devices, analytical software, and many other capabilities for undermining our national advantage. IC R&D programs are critical to ensure that the United States advances and maintains "technological capabilities to detect, characterize, assess, and ultimately counter the full range of threats to the national security of the United States."

The Commission conducted a thorough review of the IC R&D enterprise, including its relationship with the broader U.S. R&D base and the U.S. R&D talent pool. The Commission held individual sessions with R&D leaders and national security experts from the IC, Department of Defense, Executive Office of the President, academia, and private industry and also reviewed policies and programs aimed at enhancing the nation's science, technology, engineering, and mathematics (STEM) workforce. Several IC-wide data calls were conducted to gain information about current IC R&D budgets as well as R&D priorities. The Commission also reviewed five IC R&D topics to consider illustrative areas of high interest in more detail.

There are two key challenges that Congress and the IC must address to ensure U.S. national security. First, the global diffusion of R&D efforts is accelerating, posing increasing risk to the essential capabilities of the IC and to national security. Second, the ever-increasing sophistication of our adversaries—coupled with the growing volume and complexity of the data collected—is testing the ability of the IC R&D enterprise to succeed in its mission absent greater Community-wide integration and leadership. To address these challenges, Congress and IC leadership must ensure that R&D is recognized as a critical and strategic component of the IC's missions—and empower the IC R&D enterprise to act accordingly.

We echo previous congressional commissions and prominent studies as we stress that complementing our above concerns is the need for Congress to better protect and prepare the broader U.S. industrial base through legislation focused on improving STEM education, creating skills-based immigration policies, securing the supply chains of critical materials and technologies, and countering cyber theft and foreign espionage.

Like traditional national security issues, these R&D issues transcend partisanship, and, for the good of our nation, Congress should act to address these concerns.

Summary of Main Report Findings and Recommendations

Broaden Scientific and Technical Intelligence

Finding 1: The Commission found a limited effort by the IC to discern and exploit the strategic R&D—especially non-military R&D—intentions and capabilities of our adversaries, and to counter our adversaries' theft or purchase of U.S. technology.

Recommendation 1: Conduct comprehensive strategic collection and analysis of scientific and technical intelligence (S&TI); use it for IC R&D planning and resource allocation.

Enhance Integrated Intelligence

Finding 2: The Commission found that while the traditional ways and means of collecting and analyzing intelligence remain useful and necessary, emerging and future threats cannot be addressed without Enhanced Integrated Intelligence capabilities that enable shared, discoverable data for analysis and shared, discoverable information for decisionmakers.

Recommendation 2: Focus advanced IC R&D on Enhanced Integrated Intelligence approaches—methods that integrate diverse sources and expertise and that employ automated capabilities to tag, discover, access, and aggregate both data and analyzed information.

Empower R&D Leadership

Finding 3: The Commission found that there is inadequate IC R&D strategic planning and inadequate awareness of IC R&D investment plans and programs.

Recommendation 3: Empower IC R&D leadership to develop a comprehensive R&D strategy and oversee R&D resource allocation.

Leverage People/Talent

Finding 4: The Commission found substantial interest within the IC to take advantage of talent and innovation in both the domestic and international private sectors, as well as within the IC itself, but the IC must evolve its business and personnel practices to leverage and exploit the STEM personnel marketplace.

Recommendation 4: Assess longer-term workforce needs within the context of a more competitive private sector and global marketplace and develop procedures to recruit and keep needed talent. Increase and augment IC R&D talent by emphasizing approaches to innovation sharing within the public and private sectors, universities, and research and national labs, and by developing an IC strategy and approach for creating R&D opportunities for non-U.S. citizens.

Special Topic:
The IC's Role within U.S. Cyber R&D

The growing cyber threat

The national security of the United States requires that our public and private enterprises be safe from cyber exploitation and cyber espionage. The United States is witnessing a dramatic increase in cyber-related risks as both the numbers and the magnitude of attacks rise, affecting critical infrastructure, public and private institutions, financial and communication systems, national defense elements, and the economic security of every citizen. Both U.S. companies and individual Americans must do more to protect themselves than simply practicing good cyber hygiene and best information technology (IT) practices.

The most worrisome cyber attacks are believed to be state-sponsored, and some of them may include the use of proxies. Cyber attacks can be designed to deny access to critical services, reduce the reliability and trust of U.S.-based institutions, cause failure in the nation's critical infrastructure, or steal intellectual property, financial resources, and identities. Other attacks are intended to extort, blackmail, or probe for vulnerabilities in preparation for a larger attack.

Distributed denial of service (DDoS) attacks may target entire industries, as demonstrated by recent attacks against U.S. financial institutions. In milliseconds, DDoS cyber attacks—with loads measured in hundreds of gigabits per second—can overwhelm the bandwidth of Internet-based services of even large enterprises. When DDoS attacks overwhelm the defenses of a target, they can degrade quality of service, cause localized outages, or mask other attacks.

Attacks more sophisticated than DDoS also have been observed. These attacks modify their behavior in near real time in response to the defenses they encounter. Furthermore, attacks of types not yet known may have been executed, or may be ready to be launched at a future time.

The Intelligence Community and the Department of Defense, because of both their capabilities and their missions, are at the forefront of understanding, assessing, and countering this growing threat.

The need for a new approach for U.S. cyber R&D

On the basis of information provided to the Commission, we conclude that there are several urgent needs regarding U.S. cyber R&D investment. The nation must carefully examine and clarify the roles of individual government agencies with respect to cyber R&D. The government also should design a process for collaborating that makes private enterprises more comfortable about cooperating with government agencies and each other. The United States must leverage cyber expertise in private industry and academia—and look to parts of the IC that are already investing successfully in the people and technology to confront these growing threats—when considering how to align cyber R&D resources.

Important R&D focus areas include, but are not limited to, the following:

- Deterring, detecting, defeating, and attributing cyber attacks during their planning, deployment, or operations phases, using cyber and other means
- Identifying behavioral signatures of different human actors or groups
- Modeling the behaviors, decisions, and strategy of human actors involved in a cyber attack
- Improving IC analytical capabilities to characterize, stop, or mitigate major classes of coordinated attacks against U.S. interests in real time, using cyber and other means
- Collaborating with industry on capabilities to exchange real-time information relevant to IC interests, while also protecting privacy
- Developing trusted devices and software
- Developing new techniques and mathematics to replace public-key infrastructure (PKI)
- Creating transparent and multifactor authentication
- Establishing methods to use Big Data analytics for threat correlation and threat containment

Framework for U.S. cyber R&D investment

Three principles should guide U.S. investment in cyber R&D.

Cyber R&D must be informed by full threat and vulnerability assessments. Comprehensive knowledge of the threats and vulnerabilities of both our systems and those of our adversaries is fundamental to formulating a national cyber R&D strategy. This is why scientific and technological intelligence is important, and why threat and vulnerability knowledge today possessed by the IC must be part of the cyber R&D strategy.

A cyber R&D framework must respect privacy and civil liberties. A cyber R&D framework must develop capabilities that protect U.S. systems, while adhering to U.S. policies and laws governing privacy, security, and liability.

Cyber R&D must be informed by information exchange. The federal government should partner with governments, industry, and academia to exchange knowledge of cyber exploitation mechanisms and successful defense tactics.

Recommended cyber R&D actions

I. Establish a national cyber R&D agenda

Adversaries already employ a full range of social, technical, and economic capabilities against U.S. computing and communications resources. Increasingly, cyber means are used to access, influence, or disrupt not just computer networks but also more traditional targets. Future cyber R&D must incorporate work from numerous disciplines—for example, biological sciences, behavioral sciences, social network science, and quantum science. New approaches might include economic intelligence, motivation-based modeling, and predictive models characterizing the attacker, not just the attack. At the same time, cyber R&D should inform cyber policymakers about what is possible and its cost.

II. Determine what cyber R&D is being done now

Current U.S. government cyber R&D activities are spread over a large number of agencies with little apparent coordination. There needs to be a comprehensive accounting of cyber R&D programs and budgets. This evaluation should included assessments of cyber R&D also being pursued by other nations and industries.

III. Examine and evaluate approaches to public–private partnerships for cyber R&D

(i) At present, no one knows the ideal form that cyber security cooperation and sharing within and between the government and the private sector should take. To determine appropriate cyber R&D approaches for partnerships and real-time information exchange within the government and with the private sector, there must be experimentation and pilot programs incorporating the concepts discussed above and other examples.

(ii) Key to addressing the vulnerability of important private-sector systems is the adoption of security standards that raise the cost of attacking critical systems. In partnership with industry, the U.S. government must develop such standards, practices, and requirements.

Possible models for U.S. cyber R&D investment activity

There are a number of examples on which we can draw in organizing collaborative R&D and information exchange beyond just a government-led effort, including the following:

- *Enduring Security Framework (ESF)*. The National Security Agency (NSA) serves as the executive agent for a groundbreaking public–private cyber R&D effort. The NSA, partnering with the National Institute of Standards and Technology (NIST), brings together leading private-sector actors across the IT industry and the defense industrial base to reduce U.S. exposure to important classes of threats. The ESF incorporates activities across the full range of leadership and staff, from periodic strategic discussions at the level of CEOs and government agency heads to continuous, detailed planning and concrete action at the level of technical experts. Other countries are pursuing similar arrangements. For example, the Australian National Cyber Center plans to start up at the end of 2013, and in the United Kingdom, GCHQ (Government Communications Headquarters) and the Security Service (MI-5) have a public–private partnership with industry for the exchange of information on cyber threats.
- *Cyber business clusters.* There are several cyber business clusters developing in the United States in regions including the San Francisco Bay Area, Boston, Raleigh/Durham, Austin, and Northern Virginia. Such clusters are centers of excellence that typically grow up around leading universities with strong engineering, mathematics, and computer science departments; world-class research labs (public and private); and interconnected technology businesses, suppliers, and service providers. A sizable population of technical talent, skilled labor, and entrepreneurs

naturally assembles in this environment. Such clusters exhibit positive feedback: commercial contributions enable universities to strengthen their computing programs, a development that leads to an even stronger research program and generates the high-caliber talent needed to strengthen the industrial base.

- *Sector-specific consortia including industry and academia—such as for banking, energy, financial services, telecommunications, and defense—which exchange information and set research directions*

  (i) In 1987, 14 U.S.-based semiconductor manufacturers and the U.S. government came together to solve common manufacturing problems by leveraging resources and sharing risks as part of the SEMATECH (Semiconductor Manufacturing Technology) consortium. SEMATECH focuses on improving industry infrastructure and working with a wide variety of actors to improve capabilities, foster technology innovation, and accelerate the commercialization of new materials and nanostructures. SEMATECH also supports applied research in universities.

  (ii) The In-Q-Tel Lab 41 program involves teams from industry and academia who collaborate to solve complex problems involving Big Data. A similar kind of effort could be effective in addressing certain classes of cyber security problems.

- *FinTech Innovation Lab.* FinTech Innovation Lab is an annual program run by the New York City Investment Fund and Accenture for early- and growth-stage companies that have developed cutting-edge technology products targeted at financial services customers. Through a competitive process, the chief technology officers of the world's leading financial services firms determine which proposals are accepted for further development and deployment. Winners get the chance to refine and beta test their financial technology products in New York City in partnership with these firms.

- *The Oak Ridge National Laboratory.* The Oak Ridge National Laboratory is partnering with the National Nuclear Security Administration to establish a cyber test range at the Nevada National Security Site (formerly the Nevada Test Site). The range involves two major substations in area 25 at NNSS, the site that now houses the now-defunct Yucca Mountain project. The Extreme Cyber Test Range would utilize these two substations, with independent power supplies, to do offensive and defensive testing of network designs coming from Oak Ridge National Laboratory.

National Commission for the Review of the Research and Development Programs • United States Intelligence Community •

E PLURIBUS UNUM