The Stuff of Movies: DARPA, Innovation, and National Security

December 2020

Nadya T. Bliss, PhD
1. Myth-busting national security research
2. DARPA: What is it and where did it come from?
3. The American innovation ecosystem and its role in national security
4. What’s on deck? The national security challenges of the next decade
5. Conclusion
Discussion:

What do you think of when you hear the term national security research?
Some government-funded gadgets

First known human climbing of a glass wall using climbing devices inspired by geckos. The historic ascent involved a 218-pound climber ascending and descending 25 feet of glass, while also carrying an additional 50-pound load in one trial, with no climbing equipment other than a pair of hand-held, gecko-inspired paddles. (source: DARPA, https://www.darpa.mil/news-events/2014-06-05)


Through advances in medical devices and synthetic biology, a program aims to develop a travel adapter for the human body. The integrated system will be designed to entrain the sleep cycle – either to a new time zone or back to a normal sleep pattern after night missions – and eliminate bacteria that cause traveler’s diarrhea after ingestion of contaminated food and water. (source: DARPA, https://www.darpa.mil/news-events/2020-04-06)
DARPA: What is it and where did it come from?
A galvanizing breakthrough

• Sputnik: the first artificial satellite, launched by the Soviet Union in October 1957

• Marked the start of the space age and the US/USSR space race

• Sparked a period of fear and anxiety in the U.S. about a perceived technological gap between the U.S. and its Cold War rival, the USSR

*Credit: NASA*
American response to Sputnik

Within a year of Sputnik’s launch, the U.S. government:

- Created NASA
- Greatly expanded federal funding for STEM education
- Established the first federal student-loan program
- And, created ARPA (later renamed DARPA) to advance military technology
DARPA’s charge and core tenets

• Make **pivotal investments** in breakthrough technology for national security

• Be the **initiator and not the victim** of strategic technological surprise

• Reach for **transformational change** instead of incremental advances

• Accept and value failure that comes from **taking big risks** that promise big returns
The origins of the internet

THE EVOLUTION OF ARPANET

1969
First four nodes of the ARPANET
- University of California, Santa Barbara
- University of California, Los Angeles
- University of Utah
- Stanford Research Institute (SRI)

1970
Multiple geographically dispersed nodes

1977
Switch to Transmission Control Protocol (TCP) and the Internet Protocol (IP) (TCP/IP)

1983
Significant expansion across U.S. military bases, government labs, and universities

1989
ARPANET Ended

Some other high-profile successes

Global Positioning System (GPS)  Stealth planes  Endurance unmanned aerial vehicles

Computer mouse  Radar mapping  First weather balloon  Speech recognition

Source: A selected history of DARPA innovation, DARPA: https://www.darpa.mil/Timeline/index
Results of the American response

• Established the U.S. Government as a main driver of significant technological advancement over the next few decades
  o Essentially every aspect of information technology on which we rely today bears the stamp of U.S. Govt. support
  o Drove key innovations decades ago
  o U.S. Government support of early-stage scientific research was critical
    ▪ Often took 15 years or more before research translated into a product in the market
    ▪ Developments in one sector often enabled advances in others, sometimes serendipitously
    ▪ Led to the creation of significant business sectors
What Makes the iPhone so Smart?

Figure 13 from The Entrepreneurial State: debunking public vs. private sector myths (2015, p. 116)
The American innovation ecosystem and its role in national security
Innovation ecosystem

From the Computing Community Consortium's 'Catalyzing I.T.'s Virtuous Cycle' slide
Government must foster that ecosystem

Where we are: In 1960s, U.S. Govt. accounted for nearly twice as much R&D funding as industry. Today, industry funds nearly twice as much R&D as U.S. govt.*

What’s needed: “A federal government that coordinate(s) and provide(s) direction to private actors when formulating and implementing policies that address societal challenges through innovation.” **

<table>
<thead>
<tr>
<th>Industry Priorities</th>
<th>Government Priorities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Broad functionality</td>
<td>Mission-specific functionality</td>
</tr>
<tr>
<td>Convenience</td>
<td>Security</td>
</tr>
<tr>
<td>Speed to market</td>
<td>Transformational advances</td>
</tr>
<tr>
<td>Access to global markets</td>
<td>Technological superiority over geopolitical competitors</td>
</tr>
<tr>
<td>Capability</td>
<td>Size, weight, power efficiency</td>
</tr>
<tr>
<td></td>
<td>Explainability</td>
</tr>
</tbody>
</table>

* Congressional Research Service: U.S. Research and Development Funding and Performance: Fact sheet, June 29, 2018
The U.S. is among a small group of countries with declining public R&D investment.

Technological innovation no longer driven by governments

• In the Internet age, the government’s role in technological innovation has diminished

• Industry is now the main innovator, and governments are one customer among many (and often not the most important or influential)

• This shift has led to rapid dispersion of new technologies and a focus on accessibility and ease of use

• National security no longer a primary concern when developing a new technology
U.S. Government’s current role in sample defense challenges

<table>
<thead>
<tr>
<th>Driver</th>
<th>One customer among many</th>
<th>Bystander</th>
<th>Last to know</th>
</tr>
</thead>
<tbody>
<tr>
<td>Force projection</td>
<td>Infrastructure resilience</td>
<td>Biodefense</td>
<td>Algorithmic exploitation</td>
</tr>
<tr>
<td>Nuclear forces</td>
<td></td>
<td></td>
<td>Combating disinformation</td>
</tr>
<tr>
<td>Space capabilities</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Missile defense</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
• The U.S. Govt. is the *driver* in hard power areas: military might and traditional warfighting capabilities.

• But *last to know* in areas where adversaries can exploit existing technologies to attack weaknesses in political system.
U.S. Government’s role in technology innovation and challenges – past and future

**1960s – 1970s**
Early AI, internet, computer architecture, software technologies, etc.

**2000 to current**
Social media, spread of disinformation, algorithmic bias and vulnerabilities

**2020 and beyond**
Al, quantum computing, Mission-driven resilient information networks
What’s on deck?
The national security challenges of the next decade
Artificial intelligence at an inflection point

### Current national security challenges in cybersecurity
- Cybercrime
- Vulnerable critical infrastructure
- Disinformation/influence operations
- Leaks/security of information
- Large threat surface
- Skilled technical workforce
- Speed of adoption of new technology to keep pace with evolving threats

### Potential national security challenges in AI
- Algorithmic hacking
- Systemic error at scale
- More sophisticated/widespread disinformation operations
- AI arms race
- Adversarial AI
- Skilled technical workforce
- Speed of adoption of new technology to keep pace with evolving threats

DATA
COMPUTATIONAL ADVANCES
DEMOCRATIZATION OF TECH

AI ON THE CUSP OF WIDESPREAD ADOPTION

MASSIVE IMPLICATIONS FOR NATIONAL SECURITY
## Disinformation research and development: disciplinary elements

<table>
<thead>
<tr>
<th>Misinformation (no intent)</th>
<th>Disinformation (intent)</th>
</tr>
</thead>
</table>

### Intent

<table>
<thead>
<tr>
<th>Small Scale</th>
<th>IMPACT</th>
<th>Large Scale</th>
</tr>
</thead>
<tbody>
<tr>
<td>o Computational journalism</td>
<td>o Automated fact-checking</td>
<td>o Network analytics</td>
</tr>
<tr>
<td>o Automated fact-checking</td>
<td>o Media literacy training</td>
<td>o High performance computing</td>
</tr>
<tr>
<td>o Media literacy training</td>
<td>o Narrative influence</td>
<td>o Anomaly detection</td>
</tr>
<tr>
<td>o Narrative influence</td>
<td>o Network analysis</td>
<td>o Multi-media data analysis</td>
</tr>
<tr>
<td>o Network analysis</td>
<td>o Information propagation</td>
<td>o Network analytics</td>
</tr>
<tr>
<td>o Information propagation</td>
<td>o Psychological science</td>
<td>o Early detection</td>
</tr>
<tr>
<td>o Psychological science</td>
<td>o Decision support systems</td>
<td>o International relations</td>
</tr>
</tbody>
</table>

Disciplines needed include computer science, law, political science, psychology, journalism, sociology, anthropology, international relations, and others.
An effective strategy to reduce the national and global burden of pandemics must:

- Detect timing and location of occurrence, taking into account the many interdependent driving factors.

- Anticipate public reaction to an outbreak, including panic behaviors that obstruct responders and spread contagion.

- Develop actionable policies that enable targeted and effective responses.

Climate security

Climate change is impacting national security by contributing to increased resource scarcity, refugee flows, and threats to critical infrastructure, among other issues. A research agenda will need to include:

• How human activities and changing climate affect each other;

• New technologies to decrease the negative effects of human activity, like carbon emissions;

• Developing new systems to improve the resiliency of critical infrastructure.
Interdisciplinary approaches to understanding technology’s impact on society

Instilling a values-driven approach to technological development that takes into account the full racial, socioeconomic, gendered and political diversity of the society with which it will interact requires:

- Mechanisms for transdisciplinary work.
- Evaluation and assessment.
- Education and training.
- Community building across disciplines.

New challenges from advances in quantum computing

Advances in quantum computing promise new opportunities for scientific advancement, but also pose a clear threat to foundational components of today’s digital security and privacy.

• Awareness, education and planning are key to prepare for the eventual transition to post-quantum cryptographic algorithms

New approaches to wicked problems

- They do not have a definitive formulation.
- They do not have a “stopping rule.” In other words, these problems lack an inherent logic that signals when they are solved.
- Their solutions are not true or false, only good or bad.
- There is no way to test the solution to a wicked problem.
- They cannot be studied through trial and error, because every trial counts.
- There is no end to the number of solutions or approaches to a wicked problem.
- All wicked problems are essentially unique.
- Wicked problems can always be described as the symptom of other problems.
- The way a wicked problem is described determines its possible solutions.
- Planners, that is those who present solutions to these problems, have no right to be wrong. Unlike mathematicians, “planners are liable for the consequences of the solutions they generate; the effects can matter a great deal to the people who are touched by those actions.”

Conclusion
The face of national security is changing
Q next?

Q/played by

Ben Whishaw
James Bond

Desmond Llewelyn
James Bond

John Cleese
Die Another...

Peter Burton
Dr. No

Alec McCowen
Never Say ...

Geoffrey Bayldon
Casino Roy...
Further reading

• 2014 Quadrennial Defense Review
• 2018 National Defense Strategy
• 2019 Worldwide Threat Assessment of the U.S. Intelligence Community
• The Entrepreneurial State: debunking public vs. private sector myths: Mariana Mazzucato
• Loonshots: How to Nurture the Crazy Ideas That Win Wars, Cure Diseases, and Transform Industries: Safi Bahcall
• The Pentagon's Brain: An Uncensored History of DARPA, America's Top-Secret Military Research Agency: Annie Jacobsen
• Dilemmas in a general theory of planning: Horst W. J. Rittel & Melvin M. Webber, June 1973