STEPS

SCIENCE, TECHNOLOGY, ENGINEERING, AND POLICY STUDIES

ISSUE 2, 2014-2015

Robert Hummel, PhD
Editor-in-Chief

IN THIS ISSUE

POTOMAC INSTITUTE PRESS

STEPS is published by Potomac Institute Press of the Potomac Institute for Policy Studies.

Thank you to the following Potomac Institute individuals for their contributions to this issue: Unnati Mehta, Richard Pera, Mia Ramesh, Stephen Lompado, Patrick Cheetham.

Access to this journal is available free online at: www.potomacinstitute.org/steps.

Cover image: "Sextant" by Alex Taliesen.

The Potomac Institute's Navigator Awards recognize individuals who have sought bold solutions to national challenges. These leaders – hailing from Congress, the Administration, and the private sector – have striven to improve science and technology (S&T) policy throughout their careers. Recipients of a Navigator Award have demonstrated remarkable leadership, audacity, and patriotism. These policy leaders have each made meaningful and enduring contributions to solving national S&T challenges.

STEPS (Print) ISSN 2158-3854
STEPS (Online) ISSN 2153-3679

Printed in the United States.

About *STEPS*

STEPS stands for Science, Technology and Engineering Policy Studies. *STEPS* is the technical publication of the Potomac Institute for Policy Studies, where scholarly articles of broad interest are published for the policy studies communities. We welcome original article submissions including, but not limited to: discussions of policies that either promote or impede S&T research; articles that address implications and/or consequences of S&T advances on national or international policies and governance; articles that introduce or review topics in science, technology, or engineering, including considerations of potential societal impacts and influences; and non-partisan opinion pieces concerning policies relevant to S&T, to include S&T research trends; S&T policy event highlights; editorials; letters to the editor; book reviews; and similar contributions.

The Potomac Institute for Policy Studies defines policy and policy studies as a two-way street with respect to science, technology, and engineering. Policies are necessary to advance scientific research toward achieving common good, appropriate use of human and material resources, and significant and favorable impacts on societal needs. At the same time, the creation of effective policy depends on decision makers being well-informed by science.

Societal changes arising from technological advances have often been surprises to mainstream thinking – both within technical communities and the general public. *STEPS* encourages articles that introduce a bold and innovative idea in technology development, or that discuss policy implications in response to technology developments. These articles can include more controversial "outside-the-box," thought provoking contributions intended to 1) encourage discussions concerning science, technology, and engineering developments and related policies, 2) stimulate new research and development or policy actions, and/or 3) stimulate scientist, engineers, and policymakers to support relevant activities. Articles published in *STEPS* will include contributions that consider potential advances that might otherwise be suppressed by reviewers as being too unlikely or "too far out there."

Impressum

Editorial and Production Staff

Editor-in-Chief
Robert Hummel, PhD
Email: rhummel@potomacinstitute.org

Associate Editor
Kathy Goodson, PhD
Email: kgoodson@potomacinstitute.org

Website + Imaging
Alex Taliesen
Email: ataliesen@potomacinstitute.org

Design + Editorial
Sherry Loveless
Email: sloveless@potomacinstitute.org


20 Years
POTOMAC INSTITUTE FOR POLICY STUDIES
of Bold Ideas
and S&T Innovation

POTOMAC INSTITUTE FOR POLICY STUDIES

STEPS

SCIENCE, TECHNOLOGY, ENGINEERING, AND POLICY STUDIES

CONTENTS

ARTICLES

VIEWS IN BRIEF

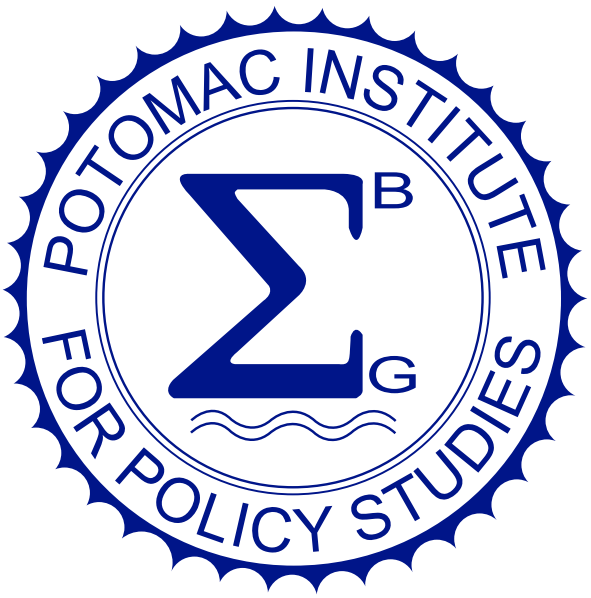
About the Potomac Institute for Policy Studies

The Potomac Institute for Policy Studies is an independent, 501(c)(3), not-for-profit public policy research institute. The Institute identifies and aggressively shepherds discussion on key science, technology, and national security issues facing our society. The Institute remains fiercely objective, owning no special allegiance to any single political party or private concern. With over nearly two decades of work on science and technology policy issues, the Potomac Institute has remained a leader in providing meaningful policy options for science and technology, national security, defense initiatives, and S&T forecasting. The Institute hosts centers to study related policy issues through research, discussions, and forums. From these discussions and forums, we develop meaningful policy options and ensure their implementation at the intersection of business and government.

These Centers include:

- Center for Revolutionary Scientific Thought, focusing on S&T futures forecasting;
- Center for Adaptation and Innovation, chaired by General Al Gray, focusing on military strategy and concept development;
- Center for Neurotechnology Studies, focusing on S&T policy related to emerging neurotechnologies;
- Center for Regulatory Science and Engineering, a resource center for regulatory policy; and
- International Center for Terrorism Studies, an internationally recognized center of expertise in the study of terrorism led by Professor Yonah Alexander.

The Potomac Institute's mission as a not-for-profit is to serve the public interest by addressing new areas in science and technology and national security policy. These centers lead discussions and develop new thinking in these areas. From this work the Potomac Institute develops policy and strategy for their government customers in national security. A core principle of the Institute is to be a "Think and Do Tank." Rather than just conduct studies that will sit on the shelf, the Institute is committed to implementing solutions.



From the CEO

Michael S. Swetnam

The Potomac Institute for Policy Studies is pleased to present this issue of *STEPS: Science, Technology, Engineering and Policy Studies*. With this issue, *STEPS* becomes an important outlet for scholarly works by the Institute and our many friends in the science and technology policy arena. The articles in this issue continue the tradition wherein the Potomac Institute addresses the hardest issues of our time, involving the interaction of science and technology developments with policies that determine how we live and work.

When the government procures systems, whether the Department of Defense or any other department or agency, they must follow the laws and regulations governing government acquisition. We've long known that the Federal Acquisition Rules, and the procedures around them, have grown overly cumbersome and even counterproductive to the good of society.

This past year, there has been yet another attempt at "acquisition reform." The Potomac Institute for Policy Studies has participated by helping to provide guidance and policy recommendations to those most responsible for spearheading the reform effort. The need for reform is far greater than the need for any organization to take credit for the ideas or the benefits. Our only goal is that our contributions will make a difference.

Alas this year's effort, like so many efforts in the past, has so far failed to yield results. The most likely outcome is that the reform effort will be tabled for consideration at a later date. If the conference committee manages to pass a National Defense Authorization Act, which has not happened as I write this, then certain aspects of acquisition reform may be addressed in the coming year.

The featured article by Alden Munson asks the pointed question "Why can't we get acquisitions right?" He diagnoses the central problem as a "conspiracy of hope." With technology moving faster than ever, and new products and capabilities popping up with a frequency that exceeds the government's ability to react, it is important that the government develop new policies that enable our national security and economic prosperity to benefit from cutting edge developments. Most importantly, Munson provides a broad set of recommendations, which together with recommendations from other articles in this issue, point to criteria that will be needed in a comprehensive acquisition enterprise for not only the Department of Defense, but for the Federal government as well.

We hope and expect that *STEPS* fosters discussions on key science, technology, and national security issues facing our society. Solving the most difficult problems requires boldness and courage of a few who dare to believe that they can make the vital difference and communicate it to the world. We welcome continuing discussions and seek to inform and influence vital debates, and provide input into policy discussions at high levels. We are able to observe and learn from science and technology changes throughout the world that directly impact us, and to communicate those findings through our symposia and writings. At the Potomac Institute, we aspire to be a continuous voice for meaningful and sound policies that impact, or are impacted by, our rapid developments in science and technology.

Editor's Notes

Robert Hummel, PhD

Although this is the second formal issue of *STEPS*, it is a most special edition. The publication coincides with this year's Navigator Awards Dinner, which is the premier event for Science and Technology Policy leaders in Washington DC. The Navigator Awards, presented to The Honorable Mac Thornberry, the Honorable Alan Shaffer, and Dr. David Brin on October 8, 2015, honor leaders who have worked to improve science and technology policy throughout their careers. The Navigator article by Richard Pera describes the awards and awardees in more detail.

This issue is also special, as it contains a set of articles concerning acquisition policies. Efforts at reforming the US acquisition system, and particularly acquisition of complex technical systems as well as science and technology support, date back decades, and have largely failed to accomplish anything but add to the regulations and the complexity of the enterprise. Like the tax code, the Federal Acquisition Rules and the International Traffic in Arms Regulations have metastasized into intolerable messes. This year, renewed efforts at acquisition reform in the Department of Defense have been pursued (in part, by Congressman Mac Thornberry in his role as chairman of the House Armed Services Committee), while the need for reform has grown due to the continual threat of sequestration from the Budget Control Act. This issue of *STEPS* includes articles – highlighted by the article of the former acquisition chief of the intelligence community, Alden Munson – on systemic problems with the acquisition system, together with some observations on possible remedies. Ken Hamilton looks at the stresses caused by the budget woes, and my own article with Richard Pera and Charles Meuller discusses the ITAR enterprise run amuck. The recommendations in these thoughtful articles deserve to be taken seriously and acted upon in both policy and legislation.

We include a pair of viewpoint articles, one taking us into space, and the other to the seas bordering coastal regions. Both suggest that our current policies are outdated and need to be changed. *STEPS* is glad to publish bold ideas: Ideas such as reversing our position on international space treaties, to seek cooperation, and seemingly crazy ideas, such as building infrastructure of coastal cities on floating pontoons.

The next issue of *STEPS* is already being planned, and should appear before the end of 2015. If you have an idea for an article or viewpoint, talk to me or send an email proposal. If the article is already written, we gladly accept contributions. *STEPS* articles are intended to be eclectic, topical, and thought provoking. They will often be controversial, and would thus have trouble mustering support in a peer review process without being watered down excessively. Articles will be critically reviewed for their logic and scholarship, but *STEPS* is not afraid to be bold or provocative. As a non-partisan scholarly publication on science, technology, engineering policy studies (*STEPS*), we seek to promote effective policies that support healthy science and technology research, and policies that are based on sound, established, science and technology.

Robert Hummel, PhD
STEPS Editor-in-Chief
rhummel@potomacinstitute.org

From the CReST Blog

The Center for Revolutionary Scientific Thought (CReST) blog features timely discussions addressing key societal, national, and international science and technology issues. CReST addresses Bold Ideas, current events, and policy recommendations. The CReST Blog is one of CReST's forums for discussion of science and technology futures from both an academic and policy perspective. These blog entries are available online at: *www.potomacinstituteceo.wordpress.com*.

JENN LATO
Cyberizing Covert Action

How will covert action continue in the digital age and what is its relationship to cyber security?

CHARLES MUELLER, PHD
"Who Are We Becoming?"

Science and technology has allowed us to shape the evolution of humanity, let's make sure we guide ourselves in the right direction.

CReST
CENTER FOR REVOLUTIONARY SCIENTIFIC THOUGHT

STEPS Policy News

Certain Neonicotinoids May Be Dangerous to Bees

The European Food Safety Authority (EFSA) has performed studies revealing that three neonicotinoid pesticides: clothianidin, imidacloprid, and thiamethoxam, may be harmful for bees when sprayed on plant leaves. Bees are essential for pollination and have a significant impact on agricultural yield, and protecting the species is therefore a major concern. While a two-year ban is currently in place, environmental groups are appealing to the European Union to extend this ban. The EFSA plans to reassess the risks posed by the three chemicals and will determine the extent of their impact on bees. See: *http://cen.acs.org/articles/93/web/2015/08/EU-Agency-Says-Neonicotinoids-Pose.html*.

Nuclear Waste Disposal Under Scrutiny

US nuclear waste managers are facing a challenging job when asked to dispose of radioactive waste as per government legislation. Various waste management groups are now urging the Nuclear Regulatory Commission (NRC) to change the limitations to US nuclear waste classifications by simplifying them and following an international model. The National Council on Radiation Protection and Measurements states that the confusion stems from unclear, inconsistent definitions of the existing nuclear waste classifications. The Council proposes that the US establish three classes of waste: exempt waste, low-level waste, and high-level waste. These classes would be based on chemical, physical, and radioactive properties, to ensure that risk to human health and the environment is minimized and that waste can be stored with the proper amount of containment. While these recommendations may take years to turn into legislation, one positive point to note is that the United States has used its experience in the nuclear field to simplify waste classifications for countries recently emerging with nuclear capabilities. See: *http://cen.acs.org/articles/93/i34/Nuclear-Waste-Long-History-Confusing.html*.

2015 the Hottest Year to Date as Earth's Average Temperature Continues to Rise

The US National Oceanic and Atmospheric Administration (NOAA) found that July 2015 was the warmest month in the hottest year the Earth has ever recorded. In addition, there has been an increase in the frequency and intensity of heat waves, especially in Europe and the Middle East. The El Niño phenomenon, which brings warm water to the surface of the ocean, reemerged in June and is likely to continue into spring 2016. This contributes to the rise in average temperature. Compared to the 20th century average temperatures, 2015's temperatures were 0.85° C warmer. At the end of 2015, diplomats will negotiate a climate agreement in Paris that will limit temperature increases to less than 2° C by 2100. *http://cen.acs.org/articles/93/web/2015/08/Earths-Average-Temperature-Continues-Rise.html*.

Biomedical Research on Chimpanzees in the US May Halt

This year, no labs have applied for the required permits to conduct invasive research on chimpanzees in the US. It is not clear whether this hiatus in biomedical research with chimpanzees is temporary or permanent. In 2013, the National Institutes of Health (NIH) announced that it would slowly halt government-funded research using chimpanzees and transfer most of them to sanctuaries. Since then, invasive research on the animals has decreased. Researchers fear that NIH's decision will have adverse impacts on biomedical research, as many disease-related experiments have been delayed or canceled. In addition, researchers worry that this may impact labs that perform solely behavioral research on chimpanzees. Though a permit is not required for this, any stress the animals face, even snipping hair, may introduce the requirement of a permit. Robert Lanford, the director of the South National Primate Research Center (SNPRC), believes that something will be negotiated in the future to allow invasive research to continue. In the meantime, labs are debating on where the chimpanzees should live. See: *http://www.sciencemag.org/content/349/6250/777.summary*.

If No Action is Taken, Annual Deaths Due to Air Pollution Could Double by 2050

According to the World Health Organization, there are about 3.5 million premature deaths annually due to air pollution. A study published in Nature states that if measures are not taken to control and decrease current air pollution levels, this number could double to almost 6.8 million premature deaths. This study marked progress towards identifying how major sources of air pollution play a role in this global issue; this could prove useful for policymakers as they shape regulations according to these issues. Conventional perception of air pollution involves industry and automobile emissions. However, other major pollutants include agricultural activities and residential energy use, which is in fact the deadliest source of pollution. The greatest numbers of deaths are likely to occur in India and China, where it has been more difficult to regulate clean energy technologies. The findings of the study are conditional, however. This projection is accurate assuming that all air pollution particles have the same relative toxicity. In addition, the particles could impact some diseases differently than others, potentially altering the outcome. However, based on the most updated epidemiological equations, premature deaths due to air pollution will skyrocket if policymakers do not effectively control emissions. See: *http://news.sciencemag.org/environment/2015/09/unless-nations-act-air-pollution-deaths-will-double-2050-study-concludes.*

U.S. Navy Agrees to Reduce Sonar Testing in Biologically Significant Areas

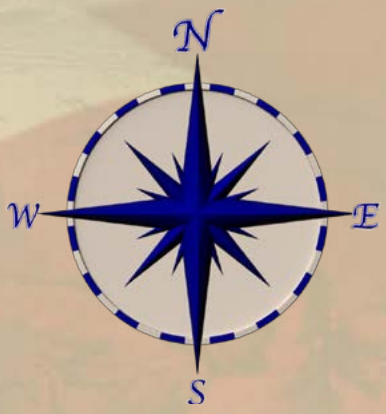
A federal court ruling earlier this year stated that certain Navy exercises are illegally harming populations of whales, dolphins, and other marine mammals. As a result, the U.S. Navy has reached a settlement with two environmentalist groups in which it has agreed to limit sonar testing that unintentionally harm these populations. The National Marine Fisheries Service (NMFS), the federal agency responsible for protecting marine life, has been in dispute about sonar testing with the Navy for quite some time. The Navy will no longer train in specified areas near Hawaii and southern California. Ships deploy sonar blasts to find submarines; the sound waves released by those blasts can disrupt communication and feeding as well as cause internal and external bleeding in marine mammals. Many whales were found beached and dying in the Bahamas, and related investigations pointed undisputedly to sonar. The Navy agrees that some of their training practices are unintentionally harmful, and has its own Marine Species Modeling Team to calculate the likely injury to marine mammals resulting from training exercises. The current agreement lasts until 2018, after which it will have to be renewed. See: *http://news.sciencemag.org/scientific-community/2015/09/u-s-navy-limit-sonar-testing-protect-whales*

Debate on Gene Editing As Research Technique Continues

Many researchers believe that genetic editing of human embryos is very valuable to understanding early human development and the functionalities of some diseases. The Hinxton Group, an organization composed of members from eight countries, believes that some gene editing is ethically justifiable. This Group was formed to discuss stem cells, ethics, and the respective policy implications. After a group of Chinese researchers published a study that used genome editing, controversy and criticism arose in the scientific community regarding the subject. The Hixton Group met on September 13 and 14, and released a statement highlighting that, while use of these technologies is premature, gene editing in the lab is important to determine which techniques work. Essentially, the Group propounds that policymakers should not restrict scientific research unless there is a concrete need to do so. See: *http://news.sciencemag.org/biology/2015/09/research-gene-editing-embryos-justified-group-says.*

NAVIGATOR AWARDS

Image:
Sextant.
Alex Taliesen



The Navigator Awards

Richard Pera

As a non-profit successor to the congressional Office of Technology Assessment, the Potomac Institute for Policy Studies has sought to shepherd meaningful discussion of science and technology (S&T) by operating at the intersection of business and government. Its leadership possessed the foresight to recognize the potency of certain fields – including neurotechnology, nanotechnology, robotics, terrorism, and amphibious warfare – and has actively worked to promote smart policy that supported each.

Within the past two decades, new threats emerged during an unprecedented period of American hegemony. Concurrently, scientific and technological capabilities burgeoned at an unprecedented rate. The increasing speed and accessibility of the Internet, along with e-mail, presented new opportunities in human communication, as well as challenges in government awareness. Global positioning satellites became fully operational, impacting everything from armed conflict to transportation. Animals were first cloned, raising serious questions about bioethics. Construction of the International Space Station established a permanent human presence beyond Earth's atmosphere. Additionally, groundbreaking research on DNA had a revolutionary effect on the criminal justice system. Citizens were well aware of these remarkable developments, but few were concerned with the policy that shaped them. It was in this frenetic world of technology development that the Potomac Institute for Policy Studies was born.

In its nascent years, the Institute became accustomed to exercising its independence. It aspired to identify new ways to highlight the growing need for shrewd and perceptive policy. At the turn of the millennium, the Institute's founders believed that there ought to be an "Academy Awards" event for S&T and national security.

"At the time, there was not enough appreciation for science and technology policy that addressed the rapidly evolving challenges of our time," said longtime Institute CEO and Chairman, Mike Swetnam. "We concluded that if the US is going to be the leader in S&T, then someone should recognize individuals who boldly champion their advancement. Additionally, honoring these bold innovators would raise awareness of the Potomac Institute's unique mission as a non-partisan, non-profit think tank."

Fifteen years and ten banquets later, the Navigator Awards have become a treasured and respected event in influential circles around Washington, DC. Most classes comprise at least one awardee from the legislative branch, one from the executive, and another from the private sector. Past honorees represent a remarkable range of contributions to S&T policy: of over 30 recipients, ten have been sitting Members of Congress; ten have headed federal departments or agencies; and four have been general or flag officers in the military. They include leaders in industry, from a founder of a defense-contracting firm to a pioneer in unmanned aviation. One past awardee is even a former editor-in-chief of a popular scientific publication.

Among the distinguished honorees over the years, awards have gone to the 29th Commandant of the US Marine Corps, General Alfred Gray, Jr. (2000); former Director of the National Security Agency, General Keith Alexander, USA (2006); former Science Adviser to the President and Director of the Office of Science and Technology Policy, John Marburger; CEO of Space Exploration Technologies (SpaceX) and CEO of Tesla Motors, Elon Musk (2010); and the current Director of National Intelligence, James Clapper (2012).

Since the inaugural event in 2000, the Navigator Awards have been held in the ballroom of the famous Willard Inter-Continental hotel on Pennsylvania Avenue. A black tie affair, it is attended by over 250 leading figures in industry and government. The honorees' acceptance speeches usually prove stimulating, as they highlight the reciprocal, complementary, and mutually dependent relationship of S&T and national policy. Guests then engage in hearty conversation over dinner.

Dr. Jim Richardson, a Senior Fellow at the Institute, says that "…the uniqueness of this award is that it looks across all of science, technology, government, and industry. It is a much more holistic look at accomplishments." This is in distinction to the fact that "The recognition of work done in science and technology is often channeled by scientific area."

The physical award is a representation of the recipient's achievements in leadership. One of the earliest, most foundational inventions in human history is timekeeping, upon which so much of society is based: from ancient agriculture to the functioning of our contemporary world. As such, the Navigator Award is a ship's gimbaled clock – a device that allowed, in addition to timekeeping, for celestial navigation. The gadget's creation revolutionized travel and commerce by allowing mankind to venture well beyond its familiar shores.

Like ships' captains of old, recipients of a Navigator Award have demonstrated remarkable leadership, audacity, and patriotism. The Institute, now celebrating its 20th anniversary, has worked alongside these titans of policy to produce meaningful and enduring solutions to national S&T challenges.

The S&T developments of the late 1990s seem distant and insignificant compared to today's concerns. The haste and power of the Internet has grown exponentially, as its access now reaches across every continent and country, available to friend and foe alike. Ethical apprehensions have evolved from cloning to the implications of detailed genetic engineering. Research and development of exascale computing provides convincing evidence that singular machine intelligence is within our grasp. Neuroscientists continue to unlock the human brain's intricate complexities, expanding technological possibilities in fields as diverse as medicine, economics, and defense.

Not only do breakthroughs in any of these areas carry the potential to revolutionize society, but they also raise questions regarding the very nature of human identity. In this context, the Navigator Awards distinguish those who have intrepidly met these challenges and who have striven to improve our nation's policies to cope with the demands of the future from a position of confidence and strength.

The Institute is pleased to announce the 2015 Class of Navigator Awardees.

CONGRESSMAN MAC THORNBERRY

Congressman Mac Thornberry[1] has represented Texas' 13th District since 1995, and currently serves as Chairman of the House Committee on Armed Services (HASC). Before his election to Congress, Thornberry worked on the personal staffs of two Texas Congressmen, and later at the Department of State during the Reagan Administration. After practicing law in Amarillo for several years, he decided to run for federal office.

Since his days as a staffer, Thornberry has been a fervent guardian of our national security and a diligent student of military applications of S&T. His expertise on matters in defense, intelligence, and foreign affairs is extensive and respected. Thornberry has previously

served on the House Permanent Select Committee on Intelligence, as well as the Select Committee on Homeland Security. Additionally, the Congressman chaired the Congressional Task Force on Cyber Security in 2011 and 2012.

As Chairman of HASC, Thornberry has directed a comprehensive defense policy reform effort. Though it has yet to be enacted, the Fiscal Year 2016 National Defense Authorization Act will address a wide array of issues, including healthcare, pay, and retirement – most of which have achieved bipartisan accord. Most importantly, though, the Chairman is committed to addressing an outdated and obsolete defense acquisition process that hampers our warfighters and severely limits federal research and development. His leadership on acquisition reform is critical to developing an agile and lethal force over the next several decades.

It is a credit to his diplomatic disposition that acquisition reform has moved forward in Congress. Indeed, Thornberry consulted all actors in the acquisition process: defense contractors, civilian and uniformed program managers, military customers, and battlefield operators of the technology.[2] Of note, the Chairman has also requested recommendations from the think tank community and academia, ensuring that research and development concerns are fully addressed. In an era of crippling partisan polarization, the Chairman has worked closely with colleagues from across the aisle to achieve consensus-driven solutions.

Thornberry has enthusiastically supported S&T matters for three decades on Capitol Hill. His acquisition reform efforts are especially emblematic of his intrepid nature and reflect a steadfast commitment to maintaining America's strategic advantage and technological edge in a dynamic world.

MR. ALAN SHAFFER

Alan Shaffer[3] currently serves as Director of the NATO Collaboration Support Office in France, where he is responsible for coordinating and synchronizing S&T between the alliance's member states and partner nations. His NATO network comprises of more than 3,000 scientists.

Shaffer has served his country for over four decades, starting with the Reserve Officer Training Corps during undergraduate study. His 24-year career in the US Air Force included assignments in command, meteorology, intelligence, and acquisition oversight in locations across the US and overseas, including direct support of an Army unit during Operation DESERT STORM.

After leaving the military, Shaffer was appointed to the Senior Executive Service, filling positions in the Office of the Secretary of Defense. Prior to accepting his current position with NATO just months ago, he was the Principal Deputy Assistant Secretary of Defense for Research and Engineering (ASD(R&E)) for eight years, beginning in 2007. Six of those eight years were spent as Acting ASD(R&E). During that time, Shaffer oversaw $25 billion per year in the DoD's Research, Development, Test, and Evaluation programs. Additionally, he directed several task forces, including those on energy security and appraisal of select facilities in the 2005 Base Realignment and Closure.

However, Shaffer's proudest accomplishment is the development of the Mine Resistant Ambush Protection (MRAP) vehicle, for which he served as director of its task force from 2007 to 2012. In a four-year span, 27,000 MRAPs were delivered to the battlefield, providing unprecedented security for warfighters.

"I do not know how many lives we saved," said Shaffer in a seminar at the Institute in May. "I would say that the biggest highlights of my career have been when a service member or a parent have come up to me and said, "Thank you, your MRAP saved my life," or "Thank you, your MRAP saved my child's life." We all worked pretty long days during that time, but when you are saving lives, it is important."[4]

Throughout his distinguished career, Shaffer has demonstrated proficiency and familiarity with a broad collection of technologies that are vital to national security. His unquestioned leadership and commitment to S&T advancements have significantly contributed to our military's current and future preparedness.

DR. DAVID BRIN

One of the most eclectic individuals one could ever encounter, Dr. David Brin[5] has based his entire career around cultivating his passions for creativity and curiosity. A scientist by training, Brin holds a PhD in astrophysics from the University of California at San Diego, where he studied under a Nobel Prize recipient. He was a postdoctoral fellow at the California Space Institute and the Jet Propulsion Laboratory.

Brin is best known for his novels, of which several have been *New York Times* best sellers and winners of a variety of awards. At least a dozen have been translated

into more than twenty languages. As a futurist, Brin's books often construct unconventional settings and raise serious questions about the nature of humanity, the fate of Earth, and other cosmic considerations. His works, which date to the 1980s, have eerily and perceptively foreshadowed topics like climate change, the Internet, and cyber security in the digital age.

"Change is the core attribute of our era," Brin said at a seminar at the Institute in 2013. "I deal with it daily, wearing both my 'hat' as a science fiction author and in my work as a scientist and technology pundit. Instability can be both exciting and unnerving. We are riding – surfing – upon a tsunami of changes, and it does little good to peer myopically just one year ahead…the future is coming, and the future's future after that! It will best be dealt with in clear-eyed calm and courage."[6]

Brin serves on a diverse assortment of advisory committees concerning issues such as national security, nanotechnology, astronomy, calculated prediction, space exploration, and the search for extra-terrestrial intelligence. His ongoing scientific projects engage with everything from astronautics to optics to human evolution, and his patents involve improving human communication over the Internet. Additionally, Brin served as an "Oracle" in a six-month US Air Force program that sought insight into future force structure, logistics, emerging threats, and combat.

For decades, Brin has fostered his brilliance, ingenuity, and imagination – all with a dose of endearing humor – sparking meaningful discussion of S&T issues. His novels challenge the reader to imagine the trepidations and opportunities of the future, forcing consideration of how to best prepare for them in the present. A fascinating mixture of art and science, his works – both fiction and non-fiction – have made a profound impact upon his nation and its government's policies.

Congratulations and many thanks to this year's awardees.

NOTES

1. US Congressman Mac Thornberry official biography.
2. Armed Services Committee, Thornberry/Smith Introduce DOD Acquisition Reform Bill. Mar 25 2015.
3. Mr. Alan Shaffer biography, S&T Organization Collaboration Support Office.
4. CReST Bold Ideas Seminar: "Lessons Learned from the Office of the Secretary of Defense."
5. David Brin website, biography.
6. CReST Bold Ideas Seminar: "Featuring David Brin."

Photo credit: Potomac Institute for Policy Studies.

FEATURE ARTICLE

Why Can't We Get Acquisitions Right?

How the Conspiracy of Hope Undermines Acquisition Performance

Alden Munson

Acquisition of the major technical systems that are so central to the security of the US is a major responsibility of the Intelligence Community and the Department of Defense. While the successes of this process are many, there have been, increasingly, notable failures of the process to deliver systems at all, or failure to deliver systems with the balance of cost, schedule and benefit that was promised at the time the programs were initiated. The acquisition system has been studied many times over the last 20 years or so with the intent to implement systematic reforms, and many changes have been made. The most obvious result of these reform initiatives is that the acquisition system has gotten successively more bureaucratic, even sclerotic. This article posits that the intense political environment in which the acquisition system is immersed, the arcane nature of most technical defense and intelligence procurements, the challenges faced by the acquisition priorities in competing with "mission" and a Conspiracy of Hope across government and industry have combined to thwart the most well-meaning of reform initiatives. The article offers an unvarnished assessment of causes for the decline of acquisition system performance. The author provides specific recommendations aimed at stemming the decline.

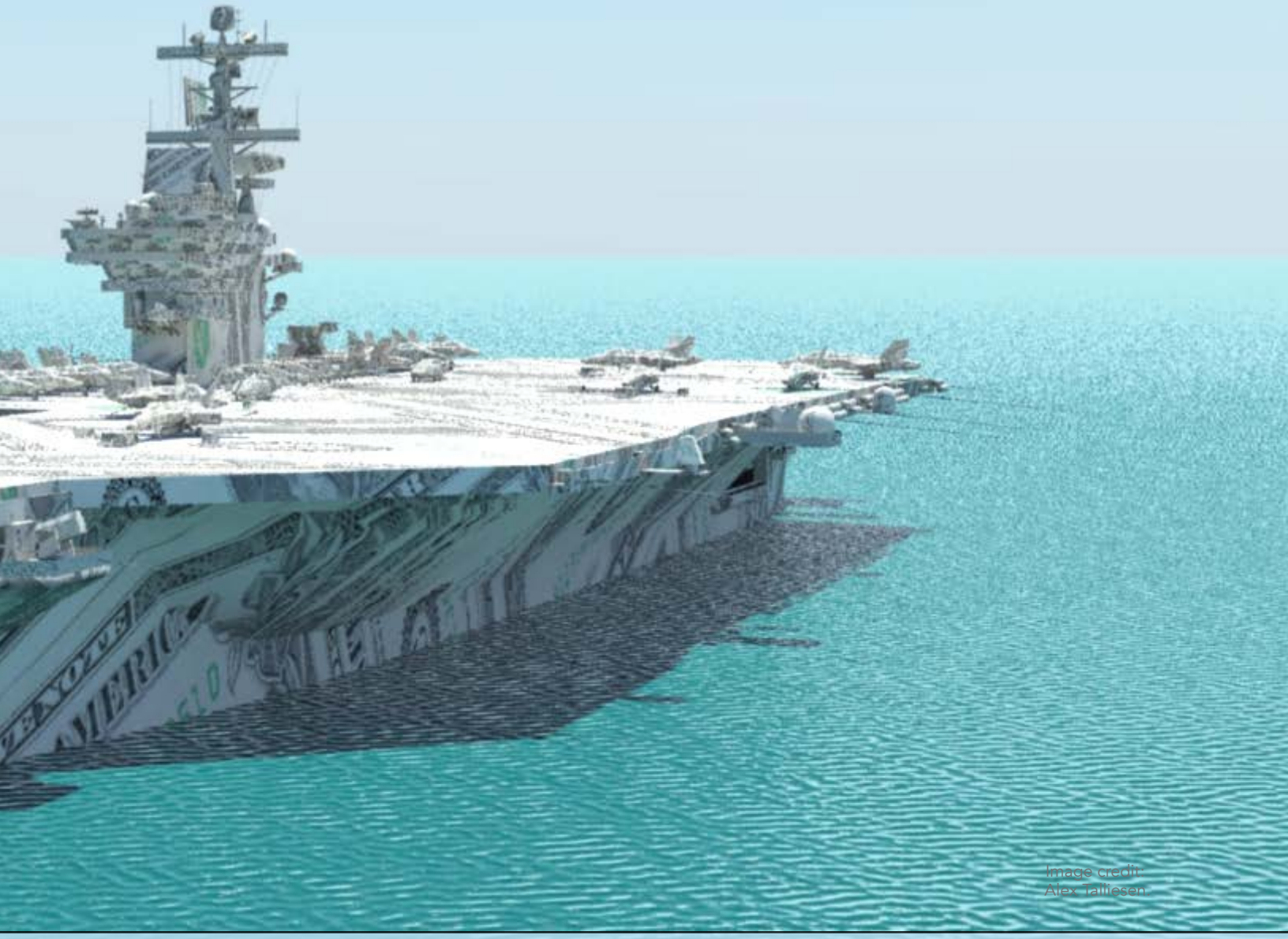


Image credit: Alex Tallisen

BACKGROUND

A fundamental underpinning of a strong, modern military force, and, therefore, essential to the security of any modern nation, is a system to acquire the physical materials and services to be employed by that military force in defense of the nation. And, with the caveat that we're talking about a modern military force, this system must be able to acquire elements that are not readily available in everyday commercial markets and may involve extremely ambitious technology components – think of intelligence satellites, aircraft carriers, fighter aircraft, armored combat vehicles, myriad special electronic equipment, etc. This is not to say that a military force doesn't require elements commonly available in commercial markets; of course they do. These commercial purchases are acquired through the formal acquisition system, but they do not drive the peculiar, stressing requirements that have led to the complex, comprehensive acquisition system in the use by the US Department of Defense (and the US Intelligence Community) today. It is the requirements for very specific national

security mission related equipment and systems cited above that are the drivers. Within this acquisition system, provision must be made for:

- Conducting basic and applied research to create the technologies and innovations on which to base specific advanced national security systems;
- Turning those technologies and innovations into achievable, producible designs for said systems;
- Developing, manufacturing and testing for these systems and for support of these systems in operations;
- Building specialized facilities in which the above tasks and subsequent operational support for these systems can be accomplished; and
- Contracting for services in support of all phases and elements.

Much of this acquisition, or purchasing, activity occurs on the leading edge of technology or innovation; because of inherent risk, pundits sometimes call it the "bleeding" edge. Therefore, it has become commonplace that much RDT&E (research, development, test and evaluation) work is contracted with industry under cost reimbursable type contracting. Under this model, all legitimate direct and indirect costs associated with accomplishing the required effort for producing the required products are reimbursed, and an appropriate profit on the work is also provided to industry. For these high risk development efforts, with essentially no broader markets in which the resulting systems and products can be offered, the premise is that industry cannot be expected to bear the risk of development without being fully compensated; the government customer bears the development risk. The cost reimbursed contracting model is contrasted with fixed price contracting, with which we are familiar in our everyday lives as we purchase a house, a car, household items, clothing, food, etc. For programs that begin with a challenging RDT&E phase, presumably to be followed with a production phase, such as the ongoing F-35 program and so many other past and current weapons systems programs, it is common for the RDT&E phase to be contracted on a cost reimbursable basis with the production items (e.g. individual or groups of aircraft) to be acquired on a fixed price basis. Most of our well known weapons systems are acquired in this mixed procurement model. For systems with no large production runs, such as most of our space systems (with relatively small production runs) and nearly all of our advanced data systems (in which production involves creating computer software which is replicated with de minimis incurred cost), an entire program may be procured under the cost reimbursable model. Cost reimbursable procurements are initiated through a request for proposal conveying the acquisition requirements and terms under which the program is to be conducted. A significant element of a responsive proposal is the so-called "Cost Volume," in which all the reasonable costs expected to be incurred in conduct of the program are presented in excruciating detail. Evaluation of the cost proposal is a major element of the source selection process. Since no absolute criteria exist for what constitutes "reasonable costs" for a particular new development program, the evaluation of a cost proposal for "reasonableness and credibility" is largely a matter of judgment; lower is frequently judged "better." Since the proposed cost is generally a significant factor in the source selection process, suppliers are highly incentivized to make their proposed cost as low as possible, while endeavoring to make that cost appear credible.

All of the acquisition or procurement activities outlined above are governed by the Federal Acquisition Regulations (FAR). For the DoD and the IC, additional specific regulations are promulgated in DoD 5000 and ICD 801, respectively, as modified over the years.

As specified in the FAR and in all more specific acquisition regulations, and as strongly embedded in the American system and values, competition among aspiring suppliers is the Gold Standard for acquiring the systems, material and services required for the national defense.

THE PROBLEM

It is relatively straight forward for the average US citizen to go into the competitive US auto market and come home with a car that satisfies his/her driving needs and with reasonable certainty that s/he paid a fair price for that car. No such straight forward process, that the average US citizen could execute or even comprehend, exists for the acquisition of complex military systems. To begin, for advanced military systems, there is no catalog, no accepted fair price, no ability to test drive, nor demonstrated performance. Instead, the formal DoD acquisition system must be invoked, and it is becoming decreasingly effective in many dimensions.

The aforementioned acquisition regulations have steadily gotten more thicket-like over the years, as

successive generations of acquisition officials have sought to insure that the most recent "failure" of the acquisition system "never happens again." Additionally, the FAR has become a vehicle to promote national objectives such as competition, diversity, promotion of small and/or disadvantaged businesses, and a propensity to "buy American." And, these continually expanding acquisition regulations are employed by legions of government acquisition professionals (assisted by more legions of supporting professionals from industry) to acquire the required national security capabilities from a rich diversity of sophisticated and capable industrial suppliers, all constituting the US "military/industrial complex" (per retiring President Eisenhower's characterization in 1960).

The unintended consequences when this arcane process fails to deliver on its objectives, too frequently make the press, cause investigations, waste taxpayer monies and underserve our war fighters and policy makers. Even when the process does not "run off the rails" or cause some onerous harm, even when it is being executed "properly," it can decreasingly be executed in a timely or efficient manner. Ambitious, paradigm busting space systems that the US fielded early in the space age in 5 years, would likely take 8, 10, or more years today. When faced with the deadly impacts of IEDs (Improvised Explosive Device) in Iraq (which by 2006 constituted 80% of the casualties), the DoD abandoned the formal acquisition process and created the JIEDDO (Joint Improvised Explosive Device Defeat Office) to develop and deploy defenses. They also employed a special task force to acquire the MRAP vehicle. Quoting from former SecDef Gates' memoir, *Duty* (p. 126): "The hidebound and unresponsive bureaucratic process that the department uses to acquire equipment performs poorly in peacetime. As I saw it, it did so horribly in wartime."

The Intelligence Community (IC) has long had the ability to execute an efficient, streamlined acquisition process when imperatives required a rapid response, and these authorities have been a significant factor in many extraordinarily successful IC acquisitions.

When the formal acquisition process does "run off the rails" the impacts can be staggering. The Intelligence Community's most notorious failure, the FIA (Future Imagery Architecture) program, cost billions in the process of failing and more billions to reestablish US capability in this critical mission area. In about the same time period, the DoD/USAF Space Based Infrared Reconnaissance System (SBIRS) program was overrun by billions and years late, although it finally did achieve its mission objectives without the need to start over. These two programs represent manifest failures of the acquisition system to accomplish its primary objectives:

1. Select a supplier (team) with the proven capability to execute the program.

2. Get on contract with that supplier at an achievable cost, performance and schedule baseline.

3. Execute the program to achieve the required results within that baseline.

Note that unless 1 and 2 above are achieved, 3 is clearly unachievable. 1 and 2 are addressed in the competition/selection process and constitute the most critical elements of the overall acquisition process. This is where the basis for an executable program is established. And, this is where the current acquisition system frequently comes up short, although there are still opportunities for a properly constructed program to run off the rails in 3. More on all of this below.

The two major acquisition failures noted above were on space programs. There are numerous other examples. The author has current, reasonably close exposure to two ground data system programs that will exceed their original cost and schedule targets by wide margins, but which will most probably produce the required capabilities eventually, without a major restructuring or restart. (These 2 programs, plus a third with which the author has lesser intimacy, are not named herein because they are currently on journeys through the acquisition "valley of the shadow of death"[see below] and don't need gratuitous attention at this point, journalistic standards notwithstanding.) The Army's Future Combat System (FCS) mega-program is generally seen as a failure because it was terminated after having expended fairly substantial monies, but not because it crashed and burned. The failure of FCS presents an opportunity to discuss another facet of the acquisition system wherein acquisition difficulties can originate.

Acquisition professionals refer to the Little "a" and the Big "A." The Little "a" is where the nuts and bolts work of acquisition occurs. The source selection occurs and the program is executed in the Little "a." The Little "a" is conducted in the context of the Big "A," the larger world of the stakeholders of a program: the requirements sponsors; operators, users; operational test and evaluation folks; operational customers of a program; the executive management of the DoD, the IC, etc.; the

programming planning and budgeting functions; and the political system, including the congress (and by extension, the effects of lobbying from private industry, regional governments, and others). Failures in the Big "A" can prevent the right conditions for a successful program from solidifying, as happened on FCS (and was detected reasonably early in the program execution), and can lead more or less directly to an acquisition program failing to deliver acceptably, as happened with SBIRS and FIA. The fact that the DoD did not choose to restructure and restart FCS presents the prima fascia case that the program was not supported in the Big "A," and, perhaps should never have been undertaken. Even heroic execution in the Little "a" is rarely able to overcome serious issues in the Big "A." Having said all of this, we need to dig deeper into the proximate causes of acquisition failure resulting in these general domains.

But first, a short digression into a slightly more ethereal view of our acquisition challenges. I had the privilege to participate in the 2005 Defense Acquisition Performance Assessment (DAPA), led by Lt. Gen. Ronald Kadish, USAF (Ret.), former Commander of the Missile Defense Agency. I offered in that study that acquisition programs are perennially cursed by a Conspiracy of Hope. Lt. Gen. Kadish adopted this phrase to punctuate his study; I have subsequently used it in Op-Ed pieces on acquisition challenges. The Conspiracy of Hope pervades all elements of the acquisition system in both government and industry. In this paradigm, participants across the Big "A" and the Little "a" see the possibility for important benefits to their organizations, their missions, their careers, or their business prospects tied to the success of a particular program. Without ever having a conspiratorial conversation, the players "hope" that:

- The money will be found for the program even if it's not in the budget;
- The requirements are achievable and accurately represent operational needs;
- The technical risks can be manageable;
- "I can win the competition";
- The selected contractor will have the required domain knowledge and will find the right people;
- "If I'm overrunning (both Gov't and industry program managers), I can find a way to survive and not get cancelled";
- "The execution difficulties we're encountering will be resolved soon";
- The acquisition staff is competent and experienced enough to manage the program;
- And more.

The *Conspiracy of Hope*, leads to a slew of distortions.

- Contracts are sometimes let at a small fraction of an independent cost estimate for the programs,
- Contractors are selected without evidencing the required domain knowledge or experience,
- Leadership personnel are cycled through a challenging program like interchangeable parts of some machine,
- Success is assumed in a critical technology development without commitment of monies and time for its maturation,
- Growing execution shortcomings are allowed to linger without being specifically addressed,
- Increasing cost overruns and schedule erosions are played down,
- Program is not staffed as indicated by independent estimates, and so on.

The conspiratorial component in all of this is that the various program participants are sometimes reluctant to call a foul on their correspondents because they fear that the program will suffer, and then none of their collective hopes for success will be realized. Not all of these sins occur in all programs, but I have seen episodic evidence of some of them in all programs, especially in poorly performing and failed programs. This is the stuff of failed acquisition programs.

When acquisition programs fail outright, or fail to deliver the required performance or are significantly delayed, the impacts are manifest. The worst and most obvious impact is that our national security forces are deprived of critical capabilities. The aforementioned

work-a-rounds to address the IED threats in Iraq and Afghanistan were to avoid just such a disastrous outcome; lives of our military personnel were at stake because the formal acquisition system could not respond effectively. FIA's failure required that a closed production capability be reactivated to produce interim capability (at significant expense!) to gain the time to put a replacement program in place. The cost of the FIA failure has been variously estimated to approach $15B. Fortunately, our space assets have evolved to performance levels and on-orbit lifetimes such that the Nation suffered no serious shortfalls in capability during this regrettable episode. For SBIRS, the government/contractor team just plowed ahead and eventually achieved an acceptable performance capability, although at costs and on schedules that beggar the imagination. Again, long lived surviving assets protected the Nation from exposure to extreme risk during the delay.

the GAO report (with only occaisional dips between the lines) in the context of program execution difficulties as enumerated herein, a clear picture of a program deep in its journey through the "valley of the shadow of death" emerges; contractor staffing and performance issues, technology challenges, falling productivity in later more difficult program phases, consumption of contract reserves to resolve early issues, and so on. Much of the nuanced wording in the reporting seems calculated to avoid the obvious conclusion that the original contract was awarded based on an aggressively optimistic bid from a supplier not fully qualified to deliver on that bid.

In recent years, an additional area of acquisition challenge has arisen. Most well-known acquisition programs result in tangible deliveries: airplanes, ships, satellites, communications and data systems, etc. It is commonplace to contract for expert staffing in many areas of the US defense and intelligence establishment.

"...The conspiratorial component in all of this is that the various program participants are sometimes reluctant to call a foul on their correspondents because they fear that the program will suffer, and then none of their collective hopes for success will be realized."

But, in both of these cases, there was another insidious cost of the poor execution. The trust and confidence among the senior leadership in the executive branch and in the Congress towards the government and industry acquisition participants was seriously compromised. When I joined the Office of the Director of National Intelligence (ODNI) as the first Deputy Director of National Intelligence for Acquisition and Technology I found that the IC's acquisition reputation and credibility had seriously declined. The Congressional oversight committees and the senior administration leadership expressed a near total lack of confidence in the IC's ability to execute its acquisition programs. Indeed, this lack of confidence had played into the reorganization of the ODNI in 2007 to bring focus to the IC's major acquisition programs.

While this article focuses primarily on DoD and IC acquisitions, over the years, NASA has had its share of acquisition issues as well. The James Web Space Telescope program (JWST) is years and billions beyond its original plans. Recent GAO reports[1] cite the Space Network Ground Segment Sustainment program (SGSS) for substantial cost and schedule overruns. If one reads

These experts from industry, working on contract, assist the government in mission and technical analyses, operations, maintenance, and myriad other tasks. And, in some of today's critical fields – many areas of information and electronics technology – the required skills are also in very high demand in commercial markets. The evaluation of the experience and skills being proposed in response to a government solicitation for sophisticated technical performance is proving to be an extremely difficult task for government source selection teams. When coupled with the extreme competition for high level skills in both government and commercial markets and increasing cost pressures in competing in the government marketplace, the government is increasingly being faced with selected contractors unable to provide staffing with the required skill and experience levels at the costs promised in the bids. I have seen cases wherein competing suppliers, seeking to displace an incumbent in such a service paradigm, have proposed prices 40% below the cost currently being incurred. Contract costs in such an application are almost totally dominated by the salaries of high demand individuals, and it is inconceivable that the

required performance levels could be achieved at the implied salary rates. Just as the failure of a development program for an airplane or a satellite can harm the US defense or IC capability, so too can a failure to achieve the required skills, experience and staffing levels on service contracts in support of critical US capabilities.

The litany above could suggest that the US is totally incapable of conducting complex national security development programs successfully; this is clearly not so. The US currently has underway a wide spectrum of space, air, maritime and ground development programs with every reasonable expectation that they will eventually meet their performance objectives and go on to satisfy their US national security missions. What does seem clear, as a seminal assertion of this article, is that few of these programs were procured competitively and went on to success without the painful journey through "the valley of the shadow of death." The hope is that they go through a vigorous, cost reimbursable competitive process and transition from that process into smoothly executing programs, meeting the cost, schedule and performance projections that were the bases for their roles in the US national security architecture and their source selection decisions. Instead, experience over the last 20 or so years would seem to prove that we no longer have the ability to achieve this result. If so, this indicates a serious systemic flaw in our acquisition system, seriously needing to be remediated.

The Defense Science Board has addressed acquisition challenges in the DoD several times over the years. Two recent reports are "DoD Policies and Procedures for Aquisition of IT," March 2009 and "Creating a DoD Strategic Acquisition Platform." April 2009.[2,3]

CAUSES OF ACQUISITION FAILURES

While the NRO and industry were roundly criticized for the FIA failure as a failure in the Little "a," it was most certainly a failure in the Big "A," exacerbated by poor execution in the Little "a." While many of the specifics remain classified, an article by Phil Taubman in the *New York Times* laid out the very convincing case for this assessment.[4] There was Congressional interaction on the program (some might call it meddling) and many "agendas" were being worked in the context of the program. The NRO failed in the first two of the three primary objectives of an acquisition outlined above: it failed to select a team with demonstrated capability to produce the required systems (although the team was comprised of fine companies with demonstrated performance in other areas) and, it failed to issue a contract at a credible price – the contracted price was perhaps a factor of two below a credible cost estimate for the program. After selecting a contractor team with a long, expensive learning curve ahead of it and a non-credible cost/schedule baseline, additional requirements added to the program with inadequate additional funding or schedule accommodation, and the Congress stepped in to reduce the NRO's flexibility to manage the program by capping the total expenditures. From the Taubman article in *The New York Times*:

> *"FIA was grossly underfunded,"*
> *"This train wreck was predetermined on day 1,"*
> *A. Thomas Young, former senior defense industry executive and chairman of a FIA failure review panel.*

> *"The FIA contract was technically flawed and un-executable the day it was signed."*
> *Robert J. Herman, former Director of the NRO.*

> *"I shouldn't have allowed it to go forward."*
> *Keith Hall, former Director of the NRO, commenting in hindsight after the congressionally directed funding cap was imposed on FIA.*

Without accurate cost and schedule baselines, credible cost and schedule planning and management is impossible. If the Conspiracy of Hope then "intrudes" (as it inevitably does), both the contractor and various elements the government may worry that if these issues receive the harsh light of objective scrutiny, the viability of the program will be questioned. To keep projected costs from soaring out of sight, the program is staffed and managed as if the contracted cost and schedule accurately represent the program that needs to be executed. This means that many tasks that must ultimately be accomplished in a successful program are understaffed (or not staffed at all). Before too long, evidence of the mismatch between the contracted cost and schedule and actual cost and schedule accomplishments and plans begins to emerge. Frequently, the mismatch is initially explained or hope'd away. Eventually, everyone acknowledges the problem and efforts to address the mismatch

begin. Occasionally, (contrary to the fervent hopes of the participants) a program is terminated at this point as not having sufficient mission value to be worth more than the contracted cost; the program would be scored as a failed acquisition at this point, but the damage might be manageable. More frequently, the contractor is asked for a proposal to address the additional work that will be required. That proposal is presented to the government amid promises that the cost and schedule baselines are now correct. Frequently they are not; the insidious Conspiracy of Hope intervenes to constrain the new cost and schedule estimates to levels perceived to be below those which might precipitate immediate cancellation. Large, complex programs can sometimes go through several such evolutions, each accompanied by promises that the new cost and schedule estimates are correct. A couple of new factors emerge. First, as time proceeds with tasks being undone (or underdone), a bow-wave of additional work accumulates that will be needed to correct errors in incomplete or poorly done earlier work and to accomplish work not yet done at all; the costs for this additional work are only slowly realized. Second, with poor cost, schedule and technical performance on the contract and a continuing stream of broken promises, working relationships among program participants degenerate; leaders are replaced, questions from Congress are generated, independent reviews – or even IG investigations – are spawned. I refer to this period wherein there is no credible cost or schedule baseline for the program, program performance is poor, relationships and trust erode, etc., as the journey through the "valley of the shadow of death" for a program. Some don't survive this journey – FIA did not. Some do – SBIRS has, but it has not shed the taint of its painful development journey. Some even go on to be judged as extraordinarily successful programs, as memories of the pain of the development period fade amid excellent or even just acceptable mission performance.

An important factor in achieving the acquisition objectives is related to the quality, consistency and constancy of the government's acquisition management team. As important as the absolute imperative to get a competent contractor team on board, is the need for the government acquisition office to be staffed with trained, experienced acquisition professionals in assignments of responsibility and duration commensurate with the program being acquired. Most complex national security programs take many years to complete, even if we restrict ourselves to the primary RDT&E phase. For space and major weapons systems programs, this phase is commonly 8-10 years, or more. This issue was addressed in a pair of OpEd pieces I did a few years ago.[5]

Consider a salient assertion in Malcolm Gladwell's book *Outliers*: It takes 10,000 hours to become truly an expert in some field.[6] Gladwell points out that even the Beatles put in their 10,000 hours playing nonstop engagements in Hamburg, Germany before any of us in the US had ever heard of them. In "Talent is Overrated," Geoff Colvin[7] argues that 10 years of "deliberate practice" involving a "well defined set of activities" pursued "diligently" with regular "feedback" is required to achieve excellence. Notwithstanding the compelling arguments supporting the requirement for acquisition program leadership assignments of substantive durations, the Government program manager on a program to which I was recently exposed, reported that he had been cursed with a 250% rotation rate among his senior subordinates during his first 12 months at the head of the program. On another program, a program manager was parachuted in for 18 months (and then moved on to another assignment) while the program was deep in its journey through "the valley of the shadow of death."

I offer the following assessment relative to the acquisition workforce:

1. The acquisition workforce is growing less experienced and less well trained as more experienced acquisition professionals retire or seek positions closer to "mission" as a protection in a downsizing.

2. Positions in acquisition are sometimes filled by generalists as "broadening assignments," and short tour rotations are common, especially in the services, a point made forcefully in the Space News pieces cited herein.

3. Acquisition, as a "skills, knowledge and experience" based profession, is not universally recognized or respected, relative to professions closer to "mission." This is particularly problematic given that over 60% of the IC's budget, for example, is expended through the acquisition system.

4. The less qualified government acquisition workforce is poorly matched against industry's longer serving professionals, meaning that in the contest of competing interests involved in major programs, the government's interests are sometimes poorly served.

5. This less qualified workforce is also tempted to treat acquisition regulations as "chiseled in stone" and to follow the most conservative direction/guidance of the compliance oriented members of the acquisition community (contracting offices and attorneys) to avoid personal career risk. Such conservatism is a major causative factor in our inability to operate with the flexibility and agility that many insist is permitted by the FAR and other policies.

This assessment (along with others discussed throughout this article) is echoed in a recently unpublished study on acquisitions in the IC.

The second of the primary objectives of an acquisition system enumerated earlier – getting on contract with a credible supplier at an achievable cost, schedule and performance baseline – presents the domain wherein almost limitless difficulty can occur. As noted earlier, the RDT&E phases of most significant national security systems are conducted under cost reimbursable contract models. And, since the costs actually incurred in conduct of a program will be reimbursed, even if they exceed the originally proposed cost by a wide margin, the disincentive to submitting an incredible, low cost bid are weak, especially if the program is critical to the offeror's business. To wit: perhaps the most respected industry executive of our recent past is widely quoted as declaring that "there is no excuse to lose a cost reimbursable competition on cost." To the extent that this attitude and the resulting practices are shared across industry (and they are!), cost proposals on cost reimbursable procurements cannot be assumed to be reasonable and credible representations of what the government and the taxpayers should expect to pay for a particular national security system. The disastrous execution trajectories for SBIRS and FIA and many other programs before and after them began with non-credible cost (sometimes called "low ball") proposals. This issue is perhaps the most insidious flaw in the US acquisition system currently, and, exacerbated by the Conspiracy of Hope across government and industry, has been stubbornly resistant to resolution. Lest the reader conclude that this problem is squarely and solely the fault of industry, it must be observed that industry is responding to the Government's inability to accurately assess complex cost proposals and to award at other than a "low" price.

Another factor that can cause acquisition failures involves the advanced technology that is frequently required for ambitious national security programs; significantly, many, but not all, involve space programs. If elements of advanced technology are required for a particular program and if sufficient time, monies and rigor are not applied to the development and maturation of those technologies, they can stall program progress, frequently at the time when the program is staffed at its maximum level and spending at its maximum rate. And, maturity of critical technology is yet another area where the Conspiracy of Hope is frequently a factor with corrosive impact on program execution. When President John F. Kennedy committed the US to the Moon Mission, the technology challenges were daunting – even overwhelming. But, instead of just hoping that these challenges would be overcome in a timely manner, a well-funded and rigorously managed program, with parallel paths and options was undertaken to assure that the required technologies were ready when they were required. And that model has been followed in others of our most ambitious programs in space and elsewhere. Unfortunately, it has not been applied everywhere it was needed, and has contributed to acquisition difficulties and outright acquisition failures; both FIA and SBIRS were impacted by technology challenges that were not rigorously addressed in the development process, and "hope" proved to be an insufficient substitute.

An additional factor not always associated with outright acquisition failure but an increasing factor in the unresponsiveness of the acquisition system, is that of Bid Protests. In short, if a competitor feels that he has been treated unfairly in a source selection process, several venues are open to seek redress. In the early days of our modern acquisition system, bid protests were extremely rare, and success in causing a source selection decision to be overturned were even much rarer. Today, a major focus in the government's preparation to conduct a competitive procurement is around actions to take (or not take) to decrease that chance


Image credit: DoD photo by Master Sgt Ken Hammond, U.S. Air Force.

that the eventual decision will be protested by a loser in the competition. This emphasis on avoiding protests is having a stultifying effect on the competitive process. To avoid the risk of communicating more richly with one or another competitor, the government has reduced the periods within the competitive process wherein communication with potential competitors can occur and has reduced the quality of those communications. This has the effect of reducing the clarity and increasing the ambiguity in the bidders' understanding of the government's needs, and therefore, in the responsiveness of the bids to those needs. An insidious impact on an acquisition is that any such ambiguity or lack of clarity is invariably turned into optimistic assumptions, leading to an overly optimistic (read: unrealistic) cost proposal, with the obvious implications as discussed elsewhere in this article. If a bid decision is protested, the program can be delayed years while the issues are resolved. The Air Force Tanker competition is a telling recent example.

Another impact of the ever present threat of bid protests is that the government is more frequently using (or misusing) LPTA (Low Price, Technically Acceptable) and IDIQ (Indefinite Delivery, Indefinite Quantity) procurement vehicles. These vehicles both have appropriate uses in acquisition; the former, to procure commodity like products or services; the latter, to procure variable quantities of differing products or services. Neither of these vehicles is likely to serve the Nation or the war fighters well when they are employed by relatively inexperienced acquisition personnel, primarily because they are thought to be less vulnerable to bid protest, in acquisition of highly complex, highly differentiated systems or services.

In any gathering of government and/or industry acquisition professionals, bid protests are bemoaned for their corrosive impacts on the acquisition process, generally. However, in a recent gathering of industry acquisition officials, a suggestion that industry might offer a moratorium on bid protests as an incentive to stimulate discussion around alternatives to decrease

protests, was summarily rejected. The assertion was offered that bid protests are now a more or less routine element of business strategy in industry instead of an extraordinary mechanism, to be used sparingly in only the rarest of circumstances. On the other side, if the government eschews true professionalization of acquisition, it can expect that its decreasingly domain knowledgeable, trained and experienced acquisition staff will conduct increasingly ambiguous competitions and increasingly subject its acquisition decisions to bid protests.

Before we go on to suggested remedies, let's summarize those causes of acquisition difficulty or failure that we've touch on – with a little paraphrasing:

1. Lack of a contract based on a credible cost, schedule and performance baseline;

2. Selection of a contractor without the requisite experience, domain knowledge and capability to perform;

3. Inexperienced government acquisition workforce, lacking in training, skills, domain knowledge and experience and/or assigned on short tours in acquisition programs;

4. Dependence on immature technologies without the requisite time, funding and process rigor to provide a high confidence of timely success;

5. Instability in requirements and/or funding;

6. Gyrations in the Big "A" perturbing the program and/or limiting the options of program management;

7. "Conspiracy of Hope," with impacts on funding; contractor selection; technology maturity; government acquisition office capabilities; program cost, schedule and performance progress and risk assessments and projections; and

8. Bid Protests.

WHAT TO DO?

Let's now consider possible remedies to the underlying causes of acquisition failures:

1. Contractual Baseline: Given that overly optimistic, and therefore unachievable, bids in competitive cost reimbursable contracts have become virtually the standard, we must conclude that the costs and schedules submitted in such competitions are no longer dependable factors for selection decisions. This may sound like heresy, but the recent track record in competitions across the DoD and the IC is undeniable. In a 2011 letter to the then DoD Undersecretary for Acquisition, Technology and Logistics, Dr. Ashton Carter, I proposed that contracts should be awarded at or near the Government determined "should cost/schedule" as the "target cost/schedule," essentially independent of what cost/schedule was proposed. This implies that the selection decision is based on so-called technical, management and past performance factors with cost (and schedule) considered lightly or not at all. Such contracts should be structured to pay fee only on the costs that were bid and to provide positive/negative fee incentives for underrunning or overrunning the target cost and schedule. This is essentially what happens on programs with large overruns, but with my proposed approach, the contractor begins working immediately to the correct cost and schedule baseline and avoids for the government and himself the painful journey through "the valley of the shadow of death" and the costs of redoing poorly done work in the always futile attempt to forestall the inevitable. Since the letter to Dr. Carter, an additional contract provision to discourage overly optimistic bids has emerged. A major factor in a decision to submit an overly optimistic bid is that all costs, including indirect costs, are reimbursed even if the contract is massively overrun. If a bidder sees an attractive long term business opportunity flowing from a program competition, having only to forego the profit (generally a few percentage points of costs incurred) on the amount of an instant contract overrun may be a good trade

off. Therefore, it is recommended that only a fraction of the indirect costs be reimbursed on the overrun amount. In particular, it would seem only fair and reasonable that the IRAD (independent research and development) and B&P (bid and propose) allocations not be reimbursed on the overrun costs. In any case the government must work to avoid issuing a contract at some non-credible cost and schedule.

2. Selection of a qualified supplier: While competition is a bedrock principle of the American economic system, it does not work in some circumstances without serious, unintended consequences. Such circumstances are common in the very specialized world of DoD and IC procurement. Especially after the major consolidation of the industrial base following the end of the Cold War, there are market segments wherein there is only one credible supplier; aircraft carriers provide a well-known example, and there are many others. If there is only one truly competent supplier for a particular capability, running a competition risks getting a disastrous outcome (such as FIA) or a manifestly suboptimal outcome, wherein an industrial team with no credible chance of winning is induced to spend government reimbursed research and bidding monies and company funds that could have been applied elsewhere for greater National benefit. A cruelly ironic factor in a bid by a nonqualified competitor is that his labor cost estimate should be higher than that of a qualified competitor to account for the inevitable learning that must occur. But, since he doesn't know what he doesn't know, his lack of experience will drive his labor bid even lower! It is this factor that has led to the worst of our acquisition disasters. The government "should-cost/schedule" for a program referred to above, generally assumes that a competent supplier will be doing the work. If through some vagary of the competition process, a supplier of lesser capability is selected, the should-cost/schedule must be increased to account for the need to develop (read: for the government to pay to develop) the required capabilities to execute the program. In a market without true competitors, the interests of the warfighters and the taxpayers are better served if the government simply selects the qualified supplier and then jointly works with that supplier to define the required capability and the cost and schedule to develop that capability and contracts accordingly. Many of our most exquisite DoD and IC systems have been procured in this manner for decades. If for political or other reasons competition is mandated, the government must spend time and money (for large, complex systems – years and billions) to "create" a competition.

3. Professional, qualified government acquisition staff: As outlined in the above referenced 2014 IC acquisition study, acquisition management is a skills, training, and experience based profession. Acquisition is not the domain of generalists or short serving specialists from other domains on career broadening rotations. Acquisition must be recognized as the professional career field that it is. Its professionals must be led, trained and rewarded appropriately and must include not just the program managers and contracting officers, but systems engineers, costing and scheduling experts and other specialties as needed. In the previously referenced Op-Ed pieces on USAF staffing of space system acquisition assignments, there is the thinly veiled implication that, if frequent assignment rotations are mandated by the "big" Air Force, then perhaps the Air Force needs to commit to a civilian acquisition core so that it can get the sustained high level performance required by today's complex acquisition programs. In the IC's civilian agencies, acquisition professionals must be recognized and rewarded comparably with the professionals who serve "closer" to critical missions.

4. Technology maturity: When an acquisition program has the need of one or more advanced technologies, the risks, costs and time inherent in bringing the required technology through the maturation process must be acknowledged and accommodated in the program plans from the very beginning. The costs and schedules

must be worked into the baseline, and, if indicated by objective measures of risk (such as Technology Readiness Level), separate initiatives and parallel approaches pursued.

5. Requirements and funding stability: It is axiomatic that if you don't have a firm baseline on what you are to build and can't count on the funds to build it, you won't have a successful acquisition program. It is naïve to expect, given today's rapidly evolving technologies and threats, that complex multiyear DoD and IC development programs should enjoy unchanging requirements baselines. And, the US employs yearly budgeting, notwithstanding the compelling cases made over and over again for the cost saving achievable through multi-year funding. But, recognizing these realities doesn't mean that disciplined management of the requirements baseline and driving for the maximum possible funding stability shouldn't be in the top priorities of an acquisition management staff – they must be! Temptations to go after that last new capability or accommodate a newly emerging customer must be carefully managed. Bigger changes must be accommodated through block strategies for programs to avoid harmful perturbation in the often high risk initial development phase. And, agencies with multiple, simultaneous acquisition programs must be unsentimental about triage in the face of budget instability, instead of just "butter spreading" cuts across all programs.

6. Gyrations in the "Big A": Many actions in the "Big A" are inherently part of US system of governance: checks and balances, redress of grievance, petition to the Government, advocacy of one's interest, etc. and the legitimate actions of the "customers" of the acquisition system to hold it accountable. Changes in these domains invariably require legislative action and are problematic because they involve these fundamental "rights." They also require that acquisition oversight and decision rights in the executive and legislative branches of the government be addressed – never an easy proposition. The "…hidebound and bureaucratic process…" to which former SECDEF Gates referred is an immutable result of the efforts of the various holders of budget authority and decision rights to defend, or even expand, those authorities and rights relative to acquisitions. The recent Better Buying Power (BBP) initiatives of the DoD represent thoughtful attempts to address some of these issues, and others. BBP1 included strong support for fixed price (FP) contracts. Of course, FP contracting should be used whenever it is appropriate. But, to use FP contracting for national security programs with high RDT&E content invites financial disaster for industry and unmet requirements for the intelligence professionals and the war fighters. The poster child and legacy of an ill-conceived initiative to remedy acquisition problems in the 1980s through FP contracting, was the Navy's failed A-12 aircraft development program, which recently exited a 20 year journey through the courts. The recently released BBP3 includes some of the acquisition remedies proposed in this article.

7. Conspiracy of Hope: Given that "hope" is among the most enduring and empowering of the human emotions, it is unreasonable to expect that it can be completely purged from the acquisition system. However, replacement of hope with commitment to the disciplines of good acquisition management: objectivity, rigor, risk assessment, cleared eyed judgment, solid financial projections, etc., can substantially improve the performance of the acquisition system. Imposition of discipline in acquisitions is the purview of the acquisition oversight bodies and they can make a difference if they, themselves, adhere to those same disciplines. The acquisition overseers must be willing to "throw the flag" consistently when they encounter lack of discipline in any element or phase of the acquisition system. As foretold above, the actions to mitigate the Conspiracy of Hope include the following:

   a. Do not begin acquisition programs that are not affordable.

b. Do not award contracts (for both end item development and services) at other than the cost and schedule captured in a credible government "should cost" for the program.

c. Do not run competitions for a major development programs unless there are at least two fully qualified candidate suppliers.

d. Depend only on mature technology (high TRL – technology readiness level) for major programs, or commit to rigorous technology maturation programs.

e. Professionalize the government acquisition workforce and make acquisition personnel decisions consistent with the expected challenges and durations of all programs.

f. Rigorously manage program requirements and fund the program to those requirements.

g. Conduct regular rigorous, objective reviews on all development programs.

8. Bid Protests: The government must strive to reduce the vulnerability of its acquisition decisions to bid protests. The first line of action must be that the acquisition process be put in the hands of domain knowledgeable, trained and experienced acquisition professionals; no amount of half measures involving increasingly bureaucratic, stultifying "rules" implemented by amateurs or generalists will do the job, while enhancing the responsiveness of the acquisition process to the needs of the Nation. Not only is this action likely to reduce the probability that decisions will be protested, it will increase the government's ability to defend forcefully and competently its award decisions. And, acquisition oversight officials must assure that the appropriate contracting vehicle is used for each acquisition. Discouraging industry's use of protests except in the most obvious and consequential cases is a harder problem, and legislation might be needed. However, once the government has demonstrated its commitment and ability to conduct protest resistant procurements and to defend vigorously and successfully its decisions, industry's recent protest aggressiveness might well decline. Joint industry/government dialog on the subject of protests might also be helpful.

IN CLOSING

As evidenced by the steady stream of acquisition reform initiatives over the years, most having relatively little positive impact, the acquisition system has proven itself remarkably resistant to systemic reform. I am tempted to conclude (as have others before me) that this is so because the participants in the system have found ways to advance their particular interests under the existing system and do not desire that it be changed in any fundamental ways. Accepting this reality, I have proposed specifically focused proscriptions that could be implemented under the direction of DoD and IC agency heads and acquisition oversight authorities that would avoid the worst of the acquisition shortfalls of the present and recent past.

NOTES

1. "NASA: Assessments of Selected Large-Scale Projects," GAO Report 15-320P, March 2015.
2. "Department of Defense Policies and Procedures for the Aquisition of Information Technology." Report of the Defense Science Board Task Force. March 2009.
3. "Creating a DOD Strategic Acquisition Platform," Report of the Defense Science Board, April 2009.
4. Philip Taubmean, "In Death of a Spy Satellite Program, Lofty Plans and Unrealistic Bids," *New York Times* 11 November, 2007.
5. I wrote about staffing issues in national space programs in a pair of Op-Ed pieces in *Space News*: "Can the Air Force Fill Space Acquisition Assignments?," November 23, 2010 (See more at: http://spacenews.com/guest-blog-can-air-force-fill-space-acquisition-assignments/#sthash.E77nMT8p.dpuf) and "Air Force Staffing of Space Acquisition Assignments – Revisited," April 4, 2011 (See more at: http://spacenews.com/guest-blog-air-force-staffing-space-acquisition-assignments-revisited/#sthash.P4fyPNns.dpuf).
6. Malcolm Gladwell, *Outliers: The Story of Success* (Little, Brown and Company: New York, 2008).
7. Geoff Colvin, *Talent is Overrated: What Really Separates World-Class Performers from Everybody Else* (Penguin Publishing Group: New York, 2008).

Stress Fractures

Ken Hamilton

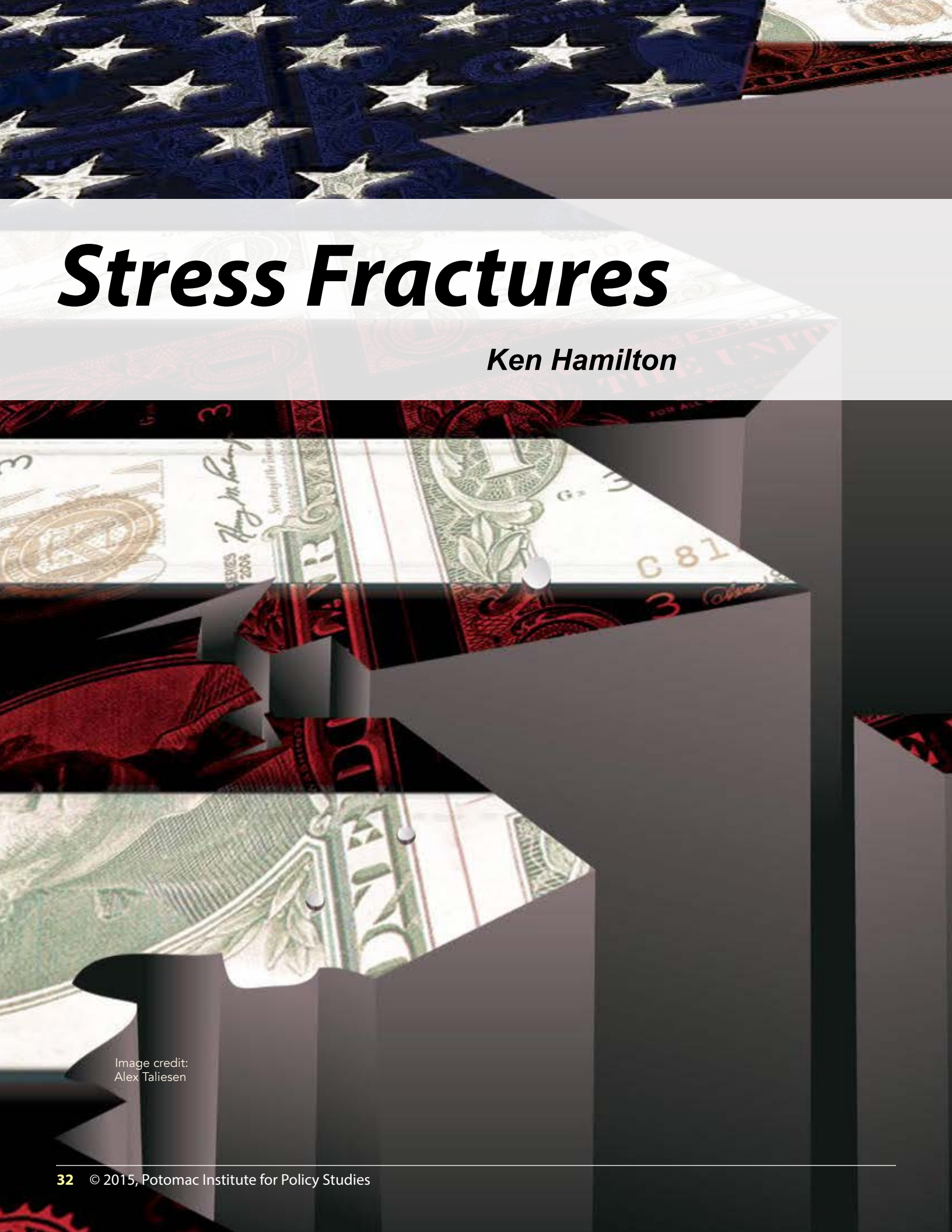
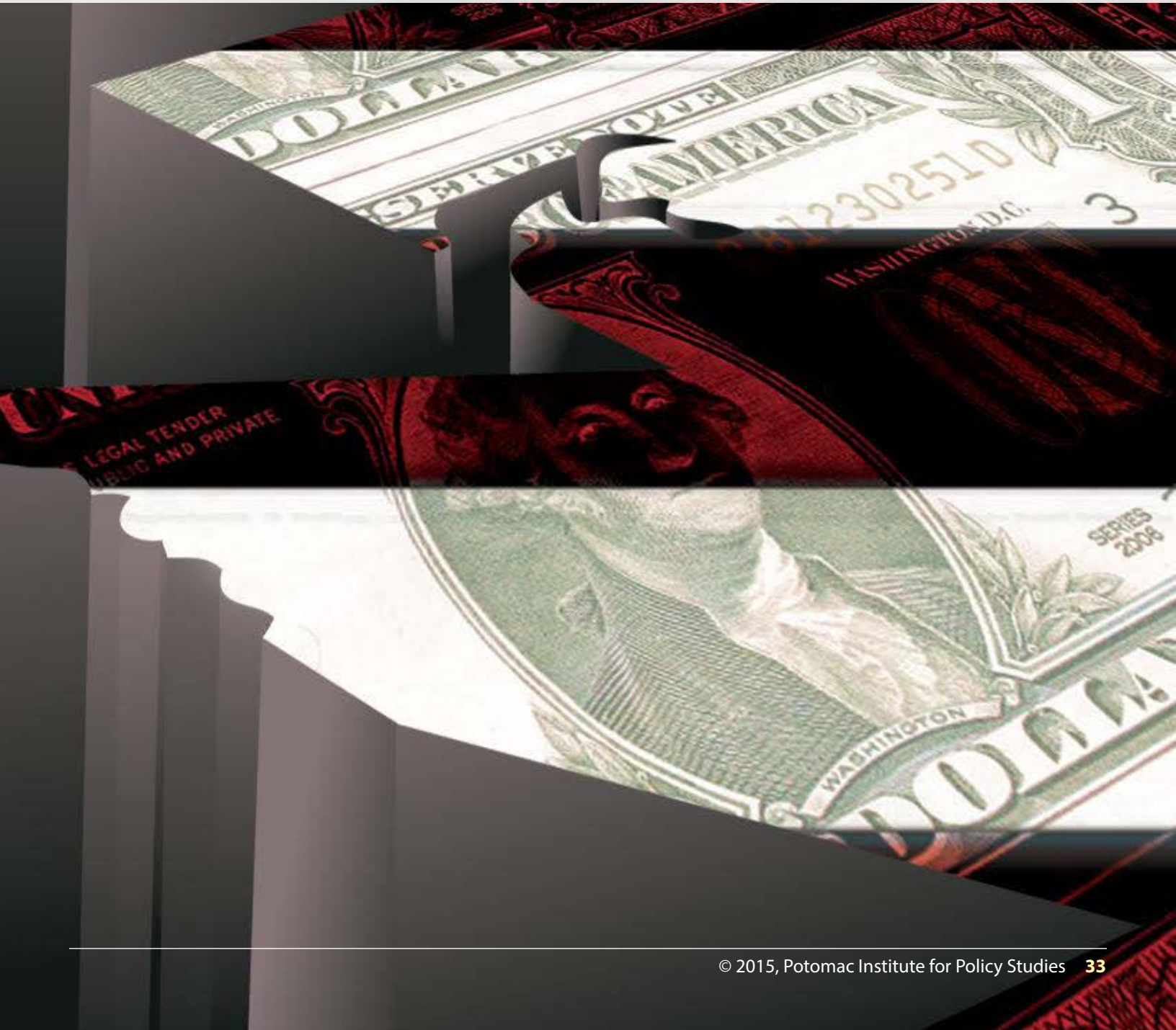


Image credit:
Alex Taliesen

Most who have been involved in the early stages of research and development, commonly referred to as science and technology (S&T), would agree that it is the basis for a long-range vision. It is the mechanism by which the innovative thought of some clever individual or group of individuals is allowed to begin the process of manifesting itself as a useful product. In the majority of cases this sort of innovation is born in small businesses and in many cases, it is actually a single individual who is the visionary or champion. Nearsighted fiscal and contracting policies have caused stress fractures in the incentives and business of S&T research.



Funding for S&T efforts in the DoD has been a hotly debated topic for decades. Policies come and go with all of their attendant "adjustments" in both the planning and execution arenas. The long-range vision of the innovative, entrepreneurial people and companies are often severely affected by these adjustments. Recently, some new policies in the execution arena of contracting have raised eyebrows and given pause to both Government and contractor personnel in virtually all sectors of the military industrial complex. The National Defense Industrial Association wrote a detailed complaint to DoD on some of the new policies.[1]

Although the policy pendulum swings regularly and sometimes wildly in the budgeting and contracting arenas, the latest "jihad" basically began with the Budget Control Act and sequestration.[2] From a policy perspective, sequestration is a classical paradox because everyone understands how and why it happened and yet no one truly understands it. Nor does anyone understand its full impact. Suffice it to say that because no one could agree on necessary budget cuts, almost everything was cut. The purpose of this article is not to analyze the sequestration decision process, but rather to discuss what I consider to be some secondary or tertiary effects of the process used to implement those decisions on the S&T enterprise, and show how they are likely to have a profound effect on how we will do business for the foreseeable future. I would submit that they will have far reaching unintended negative consequences for the whole military industrial complex, S&T specialists included.

Budget cuts happen all the time and Program Managers on both sides of the fence understand them. This is not new. Science and technology projects, like all others are always subject to having their budgets cut. For all of the traditional reasons, the major acquisition programs, by and large, were protected in the latest round of budgetary gymnastics. The focus for major reductions was, as usual, on proposed new starts and services. Both are realms where S&T often resides.

One specific budget-reducing tactic was to establish new caps on the amount that the Government would pay for any given labor category. The caps became fondly known as "tripwires." (See examples of Navy Tripwire Guidance in notes 3 and 4 of this article.[3,4]) The concept, by itself, was not particularly bothersome. Caps already existed, for the most part – they were just lowered. Some could legitimately argue that it was a logical, "common sense" approach to budget reduction, although many might argue with the wisdom upon which the limits were determined. S&T labor can, after all, be quite expensive compared to other categories due to the level of seniority and specialization that is often involved, but let us set that argument aside for the moment. If the new tripwire limits had been applied to all future contracts, then the issue would be simply whether the new values were reasonable. Some might not like it, but there would be no real substantive argument against new values, other than whether contracts could be negotiated that could fulfill the needs. The new limits could also have been applied to the exercise of options under current contracts, since the exercise of an option is an open invitation for negotiations under the contract from both sides. Again, folks might not like it, but the provisions for these kinds of changes have long been in place under the FAR. However, whereas both of these approaches were utilized, the Government also unilaterally changed many contracts in the middle of an execution year with what amounted to a "take it or leave it" attitude.[5] This, in my opinion, was a foul ball.

The first order effects of such a policy are obvious. There is an almost instantaneous unplanned and un-negotiated reduction in revenue on a contract that is currently being executed. The number of options for the contractor are fairly limited. Among the first to surface were:

a. **Forfeiture of the contract.** The message sent to many contractors was that they basically had to accept the changes or the Government would cancel the contract all together "for convenience." Some of the large businesses opted to forfeit immediately and the Government "mysteriously" found a way to exempt their contracts from the tripwire policy because they couldn't afford to lose the support. Funny how that works, but they had the horsepower to play that card. Few small businesses enjoy the luxury of being able to simply walk away from a contract when the Government misbehaves. Of course, those small businesses whose portfolios are entirely in the services category were particularly vulnerable and forfeiture of the contract was tantamount to closing their doors.

b. **Absorb the loss.** This is another choice that is really only available to large businesses and/or those who have particularly large

cash reserves. However, in an environment where service providers are being beaten down to margins in the 6% realm as opposed to typical commercial margins in the 30% realm, even the large businesses were loath to even consider such a thing. Large cash reserves in a 6% profit environment for anybody are not common.

c. **Reduce salaries.** This choice quickly becomes very complex and has first, second and third order effects of its own that will vary from one company to the next, but the overall impact on the services community and the Government is negative. First of all, many of the employees in question are operating under an employment contract which may have been violated by this unilateral decision unless provisions for these sorts of unexpected changes had been provided for in advance, which was not likely. In the case of senior level personnel, who are the most likely to be affected by this policy, salary reductions on the order of 40% occurred and were common. Ordinary negotiations on changes of this magnitude may not even be reasonable or possible. The employee may have no choice but to take his expertise elsewhere. Of course, the second order effect is that the contractor may not be able to perform under his contract without that expertise. The Government loses access to the expertise. The work stops. This is forfeiture of the contract by another name. It's just slower and more painful. To my surprise, some small businesses were actually able to reduce salaries and maintain their staff and hold onto their contracts. The budgeteers probably claimed a major victory in those cases. My opinion is that the full spectrum of impacts are yet to be fully realized.

There are at least three (and almost assuredly many more) second order effects of this policy implementation that, in my opinion, have done serious long term damage to the military industrial complex and require some measure of corrective action. Sooner would be better than later.

The first is the impact on the way cash is managed in support of DoD contracts. The "fiscal gymnastics" that causes money to flow from a Congressional appropriation to a contract vehicle is fraught with just about every sort of risk imaginable. Contrary to the Planning, Programming, and Budgeting System (PPBS) doctrine, there is absolutely nothing that gives a Government Program Manager (PM) any guarantee that the funds he needs to execute his program will be at the right place at the right time. After more than 30 years as a so-called Acquisition Management Professional, I think a more honest description would be that we are professionals in "hope management" when it comes to a budget. At the end of the day, you do your best to execute with what you're given and that amount may not bear any resemblance to what you painstakingly estimated and requested. That said, after the funds reach the contract vehicle, the process for managing those funds in the execution of the work is very well defined, fairly predictable, and reasonably effective and efficient. Funds are allocated to a contract vehicle that is fully negotiated and executed. The fact that this action is called an "obligation" is germane. The Government is committed to distribute those funds based upon the fully negotiated and executed terms of the contract. It is important to note that these terms are the product of a bilateral agreement between the Government and the contractor. The subtle but critically important issue here is that this "signed Government contract" has become some of the best collateral available to the banking industry.

Everyone knows that the Government is not always on time when it comes to paying invoices. The process has improved dramatically in recent years, but there are still any number of factors that can cause delays in payment and funds may not be available to the contractor to pay for salaries or other expenses when he needs them. That said, there is very little doubt that the invoice will be paid – eventually – because, after all, it's a "signed Government contract." You may just have to wait longer than you would like. For this reason, the cultural norm is to operate with a pre-approved line of credit from a bank. The terms upon which these lines of credit are based are now very well established by the banking industry. The military industrial complex has created an entire financial sector or subculture that is the fundamental enabler for businesses both large and small to provide products and services to the Government in spite of the schedule risks associated with the payment system.

For all its faults, the system actually works pretty well and it is at least reasonably predictable, so business

and Government PMs can have a relatively high degree of confidence that the work can get done. But what should be becoming obvious at this point is that it is based entirely upon the perceived value of the "signed Government contract" in the eyes of the banker. The banker has nearly 100% confidence that any valid invoice under the contract will be paid, so his risk is very small. When the Government unilaterally decides that the terms of the contract, and particularly the amount that will be paid under the contract, are going to be changed, the banker's confidence plummets. In effect, the Government has demonstrated that its word is no good. The term "obligation" loses its meaning. Some small businesses lost as much as 40% of the authorizations under their lines of credit overnight which, for all intents and purposes, shut them down.

Again, the major issue was not the fact that less money was being paid. The problem was in how the policy was implemented. In "normal" adjustments due to budget cuts, the Government and the contractor enter into some sort of negotiation. The Government PM is given the authority and latitude to decide how the cuts would be distributed across his area of responsibility and contracts are modified based upon a bilateral negotiation. Options may be to reduce the scope of the contract, terminate it early, defer some work to a later date, etc., but the point is that the PM and the contractor both get a vote and the sanctity of the Government's "obligation" is preserved. The modified contract still carries the full weight of the Government's commitment. Even if a contract is cancelled all together "for convenience of the Government" because funds are no longer available, this clause is almost always included in a Government contract and that risk is known to both the contractor and the banker, but the invoices that are outstanding at the time the contract is cancelled are still paid according to the agreed upon terms and the banker's confidence in the "signed Government contract" is intact. The contractor loses business, but the banker loses no money. However, in this case, neither the PM nor the contractor were given a vote. The decision as to how the cuts were to be applied was basically made by the budgeteers at the Service Secretary level (some might argue at the Congressional level) and imposed upon the rest of the community without regard for the impact on a program let alone the impact on the health and welfare of the military industrial complex or its foundational business norms. Comptrollers and contracting officers were left to make up their own rules in an almost desperate attempt to comply with the fiscal direction on very short notice. Predictably, the result was a well-intended but extremely short sighted attempt at implementation of bad policy.

So why does the banker care? If a new policy requiring lower rates to be paid is applied to new contracts, the banker simply sees a smaller number on a contract and adjusts his commitment accordingly. Authorizations under the lines of credit are usually expressed as a percentage of the invoice, so nothing changes the banker's confidence in the signed Government contract. However, when the Government basically says it's just not going to honor the contract as negotiated and signed, its value as collateral is reduced dramatically. The banker not only sees that the Government has decided not uphold its end of a bargain for which his money is at risk, but he also sees that his client, the small business, is now at serious risk of not being able to perform on the contract which only portends more heartache in the future. Many banks have already changed their policies regarding Government contracts to guard against this new risk. In some cases, the amount they will lend has been reduced from 90% to 50% of an invoice. If the small business could afford to carry 50% of the Government's payment obligation for a period of ninety days or so, they probably would not need the line of credit in the first place. The net effect is a loss in production capacity due to a loss of confidence in the Government's integrity in the eyes of the financial community. This is ground that is now lost that will not be regained in the near future.

Another second order effect is caused by the Government's contradictions of itself. There are many examples, but one that stands out is the fact that minimum standards for salary and fringe benefits are in existence; they are called "Wage Determinations." They are developed and promulgated by the US Department of Labor in accordance with Public Law. Nearly every Government contract that buys labor is subject to these minimum standards. The DoD is not excepted.[6] In some cases, the tripwires that were established by the budgeteers turned out to be lower than the established wage determinations for a given labor category. There were some small businesses who noted this discrepancy and brought this fact to the attention of their contracting officers, pointing out that their contracts required them to ensure that they met these minimum standards. In some cases, the contracting officer imposed the lower rate anyway in direct violation of the Department of Labor standards. In other cases, contracting officers "compensated" by lowering the

fee that was to be paid on the overall contract, which is another commitment in the "signed Government contract" that the Government unilaterally decided not to honor. Both approaches were wrong, in my opinion, and I'm amazed that we don't have a ten year backlog of lawsuits over it. Of course, when a small business is faced with the choice of "sucking it up" or closing the doors, the law of self-preservation usually prevails. Aside from the obvious administrative confusion that this sort of contradiction causes, the more sinister long term effect is the additional erosion of confidence in the integrity of the Government as a whole.

Both of these effects contribute to a third effect: the impact all this confusion will have on future DCAA audits. The DCAA backlog is so severe that they are currently auditing books that were created in 2008 or earlier. A phenomenon that is already haunting DoD contractors due to this backlog is the fact that today's auditors have no idea what the prevailing policies were seven years ago. Decisions made seven or more years ago were based on policies and conditions that are often much different than they are today. In fact, personnel turnover, recollection abilities, and other effects due to the elapsed time means that the audits are strained and difficult. This problem will be greatly exacerbated when today's books are audited, perhaps a decade from now, assuming the companies survive that long. The culture associated with this process is already difficult, because any failure to comply with an auditor's individual perception of what policy implementation should be is viewed as being tantamount to criminal intent. This of course makes for an adversarial relationship with the auditor from the outset. To the extent that contractors seek "innovative" ways to accommodate a poorly implemented policy, they will almost certainly run afoul of future auditors. Failure to comply with wage determination requirements is a good example. Of course, this will almost certainly cost the contractor some money, but because of the magnitude of the policy deviations involved, the amount of money at stake could be enough to drive otherwise healthy companies out of business a decade from now. But perhaps the greatest impact will be that future auditors will look at the erratic and sometimes desperate entries in today's books and feel compelled to make new policy to ensure that the Government's interests are protected. This will result in bad policy being based upon bad performance which was driven by bad policy – a cycle that can only produce bad results. These secondary and tertiary effects will permeate the entire defense industry, but will be particularly dire for companies providing services in the science, engineering, and technical assistance area, and for those performing S&T research.

Science and technology is supposed to be our investment in the future. It is therefore, by definition, the basis of a long range endeavor. In order for it to produce the desired results, it must be nurtured by a fiscal and contracting process that is at least stable. The near sighted fiscal and contracting policies we've seen implemented recently have produced stress fractures in the very foundation of how not only the S&T community, but the entire military industrial complex conducts business. Any structural engineer will tell you that the problem with stress fractures is their propensity to propagate, particularly in the presence of continuous stress. If they are detected, they can in some cases be repaired, but the structure will never be as strong as its original self. The fiscal stress we have endured in recent years is likely to continue for at least the next couple of budget cycles and maybe longer. The question is whether we have even noticed that the stress fractures have occurred. Failure to recognize the negative second and third order effects of our short term vision is to fail to recognize that the stress fractures exist. Without the acknowledgement that they exist, it is a near certainty that they will continue to propagate.

NOTES

1. NDIA Letter to the Honorable Frank Kendall dated 30 November, 2012. Accessed Aug 14, 2015.
2. Public Law 112–25–Aug. 2, 2011, Budget Control Act of 2011.
3. Naval Air Systems Command Instruction 4200.58, dated June 08, 2012.
4. Naval Space and Naval Warfare Systems Command Tripwire Implementation Guidance dated 23 October, 2012.
5. Alan Chvotkin. "Navy trips over acquisition tripwires." May 3, 2012.
6. Federal Acquisition Regulations Subpart 22.10-Service Contract Labor Standards.

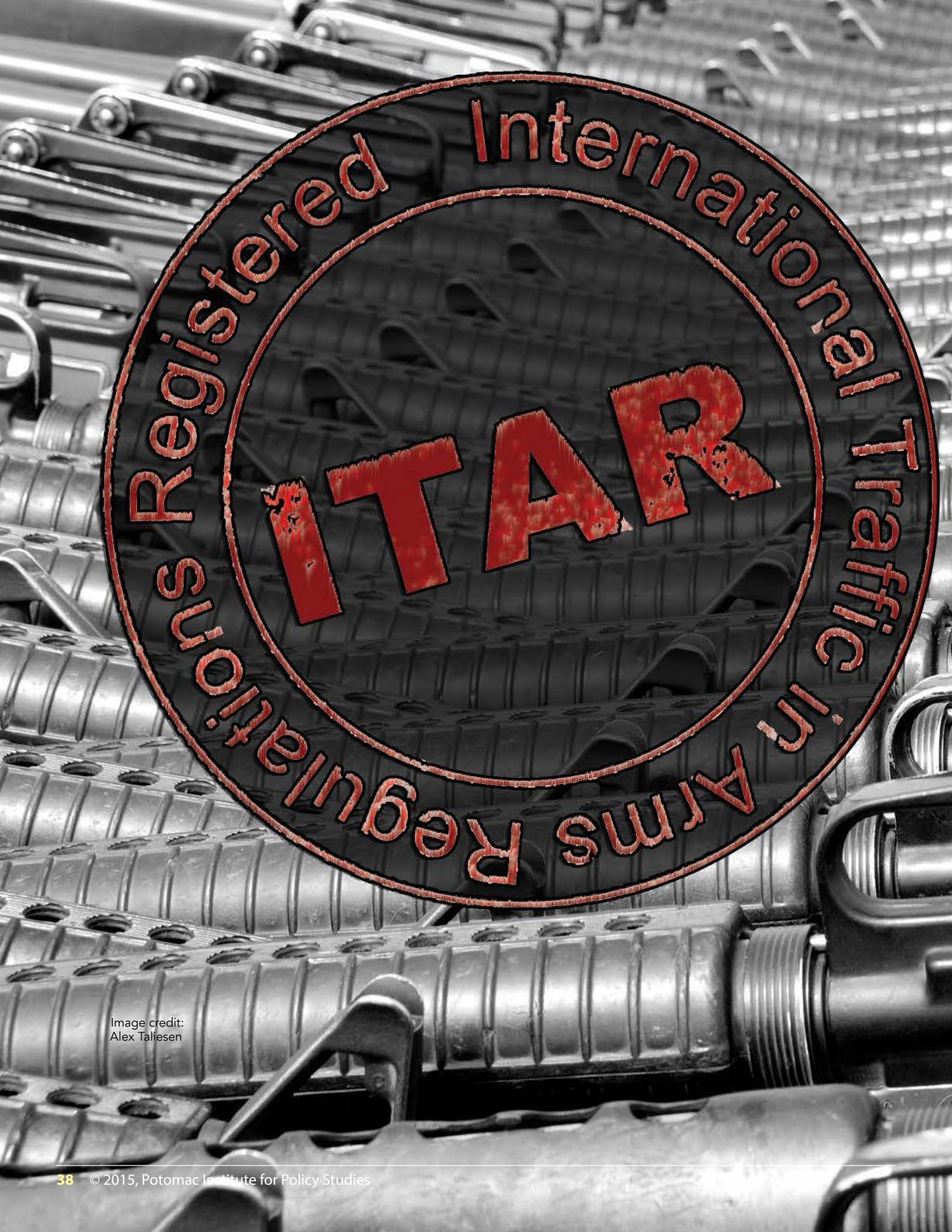


Image credit:
Alex Taliesen

The Decline and Fall of the ITAR Empire

Robert Hummel, PhD, Richard Pera, and Charles Mueller, PhD

The authors take on ITAR, the International Traffic in Arms Regulations. ITAR places burdens on researchers, to avoid export of information about a large range of technical topics that can relate to military systems. Since an export can amount to nothing more than showing a viewgraph at a domestic conference, or sending an email to a colleague, ITAR casts a dark shadow over US research. While reform efforts are moving slowly, this article dares to make an obvious conclusion: That ITAR must be completely rescinded. The case is made that ITAR, by virtue of restricting information, is more harmful than good, and that other mechanisms and laws exist to protect secrets and systems for national security purposes.

INTRODUCTION

The International Traffic in Arms Regulations (ITAR) is collapsing from excessive bureaucracy. Beginning in 1976 as a heavy-handed attempt to restrict both transfer of physical munitions and disclosure of information about munitions, the subsequent introduction of thousands of amendments turned ITAR into a monstrosity of complexity that typifies regulation gone amuck. Not only is it collapsing because it is unwieldy, it is also outmoded in its attempts to restrict the flow of information.

The original purpose of the export control system, of which ITAR is a major component, is to "promote our national security interests and foreign policy objectives."[1] As a result of the system, anyone wishing to export any product, item, idea, or to disclose information, to any foreign person whether in the US or abroad, must be concerned with the potential need for an export license, or whether the item is subject to export control.

The main lists that describe "articles" to be restricted are the United States Munitions List (USML) and the

Commerce Control List (CCL). ITAR deals with the USML. Administered by the State Department, the Department of Defense is particularly concerned with the USML, through the Defense Technology Security Administration (DSTA).[2] A history of ITAR's evolution and convoluted association with multiple federal agencies can be found in an MIT open access paper.[3]

There are complex regulatory processes whereby restrictions are updated and lists are examined and modified. Congress regularly passes laws calling for updates to the regulations, which are then assembled in amendments. In 2010, an interagency review determined that the overall export control system in the US is, to put it politely, a mess.[4] Reportedly, the review said that the current system is "overly complicated," redundant, and "in trying to protect too much, diminishes our ability to focus our efforts on the most critical national security priorities."[5] Secretary Robert Gates said that the system is a "byzantine amalgam of authorities, roles, and missions scattered around different parts of the federal government."[6] Accordingly, the President's administration announced an Export Control Reform Initiative in 2011.[7] The result has been a flurry of Federal Register notices and ongoing reviews of each of the 21 categories of the USML.[8] Reform of each category is subject to public comment, and categories and other reforms are being addressed incrementally, as documented by the government's export.gov website.[9]

Reforms are being pursued slowly and methodically, with incremental updates to the current structure of the ITAR Empire. Commenting on the initiative, the US Chamber of Commerce observes that the "the US export controls regime has long covered too many products that lack a significant military application or are readily available from other countries. The United States should eliminate controls that serve no real security purpose."[10] That does not seem to be happening. Instead, some categories are being updated, and lists are being consolidated and made easier to access. However, information in 21 categories will still be restricted.[11] The well-meaning reform initiative, which has plodded along for six years at this point, has devolved into tweaking of vague descriptions of poorly understood technologies that support a grotesque framework of patched-together regulations and misguided directives.

This framework is based on many complex definitions, bureaucratic insertions, and amendments. For example, ITAR makes a distinction between a "US person" and a "non-US person." A "US person" involves a convoluted definition that includes US citizens, many people with "US permanent residency," and certain corporations that are predominantly located in the US (Yes, a US person is not necessarily a person.) There are further complications involving "dual nationals" and "third country nationals," for so-called "third party transfers."[12] The law makes a distinction among different classes of weapons, including "Significant Military Equipment" (SME), and the Missile Technology Control Regime Annex (MTCR),[13] along with the Department of Defense Military Critical Technologies List (MCTL) and the Developing Science and Technologies List (DSTL).[14] The 21st category in the USML is titled "Miscellaneous Articles," which includes "any article not specifically enumerated in the other categories" with military applicability designed for military purposes, or technical data or services related to such an article.[15] Finally, there are different categories of foreign people, which need to be accounted in terms of a potential transfer. For example, a university can disclose ITAR technical data to a foreign person who is a full-time employee (e.g., postdocs), providing certain procedures are followed and that the employee is not from a country to which the United States observes an arms embargo, which includes China.[16] A similar complication arises with respect to dual nationals who are employees of an

"The fact that economic interests might be in conflict with national security concerns is a seed of anxiety."

end-use company that has been approved for an export of a product or technical data.

It is easy to complain about the many bureaucratic layers that are embedded in ITAR. The complexity is such that observance of ITAR is rarely based on observation of its provisions, but rather out of fear of prosecution from inadvertent transfers. Further, its outdated provisions undermine its credibility as an effective tool for export control. The reform initiative will not change that reality.

DEFENSE ARTICLES AND INFORMATION

Our main interest in this article is with the restrictions that ITAR imposes on the transfer of information. The convergence of systems and information is such that ITAR's primary effect is to restrict the free flow of information; the export of actual defense systems is typically regulated by treaties, agreements, and other export control provisions.

ITAR prohibits the export of defense articles and defense services, as carefully defined in Part 120. Defense articles include technical data concerning items on the USML. Technical data includes "information…required for the design, development, production, manufacture, assembly, operation, repair, testing, maintenance or modification of defense articles. This includes information in the form of blueprints, drawings, photographs, plans, instructions, or documentation."[17]

Technical data is thus explicitly information. This can manifest in viewgraphs, verbal presentations, or digital data on an accessible server or in an email message. Note that the original definition predates the Internet age, before information is easily sent across borders and among colleagues digitally. Whereas the regulations envisioned the transport of hard documents and physical presentation of information, now an email can be considered a defense article.

ITAR explicitly does not apply to basic knowledge taught in schools. As written in the regulations, however, this exception would not apply to research that discovers new knowledge. Thus ITAR inhibits research at universities that might otherwise apply to defense systems, when foreign graduate students might be involved.

ITAR further restricts defense services, which include "the furnishing to foreign person of any technical data controlled under this subchapter…whether in the United States or abroad."[18]

Accordingly, an email sent to a colleague across the hall, who happens to be a foreign person, can be a prohibited defense service. Release of technology within the borders of the US is called a "domestic export," or, as defined by the Department of Commerce, a "deemed export."[19] In its current incarnation, a violation of ITAR need not be an intentional service to a foreign entity, but rather a simple and potentially unwitting transfer of information.[20] Further, once an article (whether a system or information) is subject to ITAR, it is restricted from further export no matter where it is – re-export requires a license.[21] ITAR has global reach.

ITAR TECHNICAL INFORMATION

The genesis of ITAR, and of the related Export Administration Regulations (EAR), go back to the Arms Export Control Act (AECA) of 1976,[22] which builds upon a series of Export Control Acts dating back to 1940.[23] The 1976 act gives the executive branch the authority to control exports of "defense articles and services." This responsibility was subsequently assigned to the Department of State. The intent of the legislation, developed amidst the Cold War, was to restrict sales and "trafficking" in military equipment and services so as to lessen the likelihood of regional conflicts. It was designed to help promote US economic interests, which include assurance of military equipment sales to friendly nations. The fact that economic interests might be in conflict with national security concerns is a seed of anxiety.

The AECA actually seeks to promote cooperation among friendly nations for mutual defense, including sharing of defense information and research results.[24] While the original legislation does not provide definitions for "defense articles" and "defense services," enabling regulations and subsequent amendments make clear that definitions can be found in Section 644(d) and (f) of the Foreign Assistance Act of 1961 (22 U.S.C. 2403). Defense services include information that is transmitted for the deliberate purpose of providing military assistance. Information, according to the act, is defined as follows.

The U.S. Code states: "'Defense information' includes any document, writing, sketch, photograph, plan, model, specification, design, prototype, or other recorded or oral information relating to any defense article or defense service, but shall not include Restricted Data as defined by the Atomic Energy Act of 1954, as amended [42 U.S.C. 2011 et seq.], and data removed from the Restricted Data category under section 142d of that Act [42 U.S.C. 2162(d)]."[25]

Thus, when we speak of ITAR technical information, we mean "defense information" that relates to an article restricted by ITAR (i.e., related to an article on the USML). ITAR prohibits providing technical information to a foreign national, whether in the US or abroad, based on an assumption that the information will knowingly provide military assistance.

The news media and those subject to its restrictions often ridicule the fact that defense articles include technical information, such as the inclusion of software and encryption technology on the USML.[26] Non-military systems that contain USML components themselves become ITAR restricted, which induces foreign manufacturers to use non-US components in order to advertise their systems as "ITAR-free."[27] This encourages US companies to avoid participating in defense work for fear of tainting their products with the ITAR label.[28]

Systems and information are increasingly equivalent, as information to make a munition becomes tantamount to the ability to acquire that weapon. Since nearly any system can be reverse-engineered given sufficient diligence, possessing a weapon system amounts to having the information about that system. Thus ITAR became strongly restrictive of the export of technical information. Effectively, the migration from controlling the export of physical articles to controlling the disclosure of information was necessary, as information became the dominant source for acquiring systems.

There remains an underlying assumption in ITAR concerning information about USML articles, that the US maintains technical dominance in each area. It makes no sense to protect information when adversaries have superior products and thus superior information. Historically, the United States excelled in areas of technology, such that the USML exclusively contained articles for which the United States was the world's leader. Although the USML is updated from time to time (and is so mandated in the original legislation), it is not maintained with sufficient technical understanding of the international landscape. Indeed, ITAR is a powerful incentive to foreign friends and adversaries alike to develop their own military technology research programs. Further, certain communities have complained that by restricting their sales market, ITAR has impeded their technological development for subsequent generations. Examples include the fields of satellites[29,30] and high energy lasers,[31] potentially causing the United States to fall behind competitors.

Nevertheless, we maintain that there is often a need to restrict the transfer of information. It is one thing to sell a missile to an adversary such that it might be used in a conflict against us, but it is quite another to provide the information needed to manufacture, sell, and utilize thousands of missiles. Since digital information is so easily shared, and with the coming possibility of providing files of data that permit the near-instant manufacture, via 3-D printing, of true defense articles, it becomes more urgent than ever to ensure that information pertaining to munitions, weapons, and national security be kept truly secure. The current lists (the USML and CCL) do not, however, appropriately differentiate between what needs to be protected, and what can be safely made open source.

There are proposed changes to the definitions of ITAR "technical data" that would strengthen legal sanctions against sharing design files, such as 3-D printable guns.[32] These changes would attempt to systematize the differentiation between information that should be kept secure versus what can be posted. However, because the onus of interpretation is left to the person possessing the information, enforcement is likely to be capricious and post-facto.

As a result, our current treatment of technical information is haphazard and irrational. We attempt to protect "Sensitive But Unclassified" design data for the F-35, only to discover that Chinese cyber warriors pillage the networks for intelligence to speedily develop their own jet fighter.[33] We actively collaborate with the Chinese on advanced thorium-based molten-salt cooled nuclear power plant development, which will help modernize its navy.[34] We decry Chinese censorship

of the Internet, and yet we expect US researchers to self-censor their postings of research results.[35]

At issue is whether ITAR is the appropriate discriminant of information that should be secured. If so, at what cost?

THE BURDENS OF SECURING ITAR TECHNICAL INFORMATION

ITAR places the burden on the developer, researcher, or person possessing information. Essentially, every US person is expected to know and understand the USML in order to prevent transfer of ITAR technical information to a non-US person. Since an export occurs with a mere email message or verbal communication, ITAR expects total familiarity with the USML, and for researchers in certain fields to exercise great restraint in scholarly communications.[36]

There are recurring concerns over the constitutionality of the implied prior restraint on free speech imposed by ITAR.[37] These concerns have only been heightened by recent reform efforts.[38] While the First Amendment does not protect speech that divulges classified information, as early as 1981, the Department of Justice warned that technical data disseminated by someone "unconnected with any foreign enterprise" to a foreign person, even when it is known that the information may be used in the manufacture or use of arms, is protected free speech.[39] Because ITAR is enforced through prosecutions[40] and threat of prosecutions, it denies rights guaranteed by the Constitution when it inhibits speech that poses no grave and immediate threat to national security.

Further, every industry, small business, and university lab that engages in defense research work, together with all people in those organizations, must track the "US-person" status of every staff member and every visitor.[41] Conferences and presentations concerning defense research will often need to restrict attendance, and must again be cognizant of the status of each attendee. Universities with foreign graduate students and postdocs, many of whom are awaiting green cards, must carefully consider whether they will accept contracts and grants that sponsor research related to defense technologies, for fear of inadvertent violations based on domestic export of unclassified information.

This might not be such a burden if the USML were clear and concise, and if the distinction between defense work and commercial research were well-articulated. But the increasing globalization and convergence of technology research with multi-use objectives makes discernment with the USML impossible. The lack of US-personhood identity cards means that the regulations are dependent on foreign persons declaring that they are foreign. As a result, compliance is based on guesswork. And if the US lead in technical areas of the USML were still as commanding as it once was, then protecting the information from disclosure would still make sense. But we are now largely protecting outdated information.

The costs of ITAR are not just the encumbrances of compliance, nor the opportunity costs of the work that might be done in place of compliance efforts, but also the missed opportunities caused by behaviors undertaken to avoid being covered by the law.

Both domestic and foreign industries avoid purchasing American components in order to develop versions of their products that are "ITAR-free."[42] US multinationals have been establishing research centers abroad, in part to enable research by non-US persons in directions that might be subject to ITAR if performed domestically by US employees.[43] ITAR not only suppresses commerce by restricting foreign sales, bust also erodes America's technological dominance by inhibiting our best scientists and researchers from collaborating on a myriad of technical areas.

The costs of ITAR information restrictions would be justified if it truly protected information that needs to be kept secret. The Department of State views the restrictions as a "classified lite" system, with less onerous control mechanisms compared to the security apparatus that implements our classification system. The security laws, however, are very clear: if the material is classified, it must be handled in specific ways. There is a high degree of confidence (and empirical evidence) that it will not be transferred to those ineligible to receive it. Only those dealing with classified information must be concerned with the rules for handling classified information, and the decision as to what is classified is up to original classification authorities. ITAR information, on the other hand, is of concern to everyone who

comes into contact with information that might relate to any of a long list of systems and technologies with military applicability. The burden of dealing with ITAR may be only one-fourth of the burden of dealing with, say, information classified at the confidential level per person. But the burden may fall on a hundred times as many people, and thus cost society many times more than simply classifying the information.

A WAY FORWARD

Reform of ITAR and the export control system is laudable, but happening at a pace that is slower than the pace of technology. The reform initiative has already failed.

ITAR is outdated. By trying to control information dissemination in addition to the export of physical systems, it has failed to adapt to an environment where technology changes rapidly, is nearly always of multiple use, and has near-instantaneous reach anywhere on Earth.

To control the export of physical systems, the legislation, treaties, and authorities that fund the development of the systems (i.e., the Department of Defense) can readily ensure that weapons do not fall into the wrong hands.

In order to control information flow, there is an existing system. The existing system actually works, as opposed to a poorly contrived ITAR system that attempts to limit the flow but in fact may facilitate theft or adversarial development of information. The system that works is based on the security law of 1947 and its implementing regulations.[44] When information is classified, it is generally kept within channels for a long time, and works to protect the information. ITAR restrictions, on the other hand, most likely offer no protection at all.

Indeed, when we secure ITAR information on unclassified systems that are bundled and marked as ITAR, there is a sense in which we have enticed others by affixing a "steal me here" label.

Security laws include a level of classification called "Confidential," which is defined as material that would damage national security if disclosed. These laws also acknowledge other forms of restrictions, such as "Controlled Unclassified Information," "Restricted," and "For Official Use Only." Major defense acquisition projects have "program protection plans" that include protocols to protect design information. It would seem that security laws have sufficient mechanisms to protect information, if only that information were assessed and labeled at its creation. ITAR provides an excuse to forego appropriate classification of technical information, which results in the lack of protection to a substantial amount of data that should be protected using the classification system.

If we classify technical data that is currently labeled as ITAR, then only those with appropriate security clearances will be able to access and work on the technology. Right now, a US security clearance is only available to US citizens, and not US persons. (However, the background check required for a position of "Public Trust" might suffice for non-citizens.) Further, material can only be classified if its disclosure will cause harm to US national security. Whether these are the appropriate criteria to ensure security is a matter for the security apparatus. Central to this argument is that there already exist constitutional and effective means of protecting information without a burdensome and cumbersome ITAR.

Of course, the best defense is one where we possess the best weapons and best technology, and maintain dominance by adapting, updating, developing, adopting, and integrating new technologies faster and more efficiently than any other nation. Rather than facilitating our dominance, ITAR has become a burden to our advancement.

We should classify at appropriate levels that information that should be protected, and permit open and widespread collaboration on topics where it benefits us to stay current.

CONCLUSION

The conclusion is that ITAR must be completely rescinded. Reforming ITAR will not fix its flaws. Its categories and lists cannot be kept current at the rate required to be rational. By confounding systems and information, ITAR has become an impediment to the development of technology, thereby threatening to upend US dominance in technical areas that are relevant to national security. By attempting to protect information from communication – even in lectures and email correspondence – ITAR has allowed information that should be classified to remain unclassified. Furthermore, through intimidation it restrains legitimate research and collaboration, including among US persons, which are vital to our economic and security future.

To truly control the trafficking in arms, we need to pass and enforce laws that control foreign arms sales, based on specific systems. When component technology needs to be protected, the information required to make that component should be classified. Thus export of systems with sensitive component technology should be controlled by means of security laws. When information needs to be protected from disclosure because it could harm our national security, that information should be classified at the appropriate level.

These are common-sense steps that would greatly benefit our national security and economic prosperity. The decline and fall of the ITAR Empire is well underway and inevitable; let us not allow its obsolescence to crumble our country, too.

NOTES

1. US Department of State, "Overview of U.S. Export Control System."
2. Office of the Secretary of Defense, "DTSA Mission."
3. Morgan Dwyer, Gwen Gettliffe, Whitney Lohmeyer, Annie Marinan, Erik Stockham, Annalisa Weigel, and Kerri Cahoy, "The Global Impact of ITAR on the For-Profit and Non-Profit Space Communities." International Astronautical Federation, 2012.
4. Export.gov, "About Export Control Reform."
5. Leigh T. Hansson, ESQ. and Michael J. Lowell, ESQ., "Top Ten Things to Know About Export Control Reform," Association of Corporate Counsel, June 01, 2011.
6. "Robert M. Gates' Speech Before the Business Executives for National Security, April 20, 2010."
7. Export.gov, "About Export Control Reform."
8. US Department of State "Export Control Reform."
9. Export.gov, "Export Control Reform News."
10. US Chamber of Commerce, "Modernize Export Controls," last modified May 19, 2015.
11. The unofficial updated USML is maintained at "Electronic Code of Federal Regulations." The unofficial CCL is maintained by the Bureau of Industry and Security, US Department of Commerce at "Export Administration Regulation Downloadable Files." The official list is the annual baseline publication together with all amendments in the Federal Register.
12. US Department of State,"Third Party Transfer Process and Documentation."
13. See Part 121.1(b) and (c): "The International Traffic in Arms Regulations (ITAR)."
14. "Funding Cut, Military's List of Critical Defense Technologies Languishes," *The Security Ledger*, January 25, 2013.
15. Part 121.1, Category XXI, "Miscellaneous Articles."
16. 22 CFR Part 125.4 (10), referencing 22 CFR Part 126.1, (a): "The International Traffic in Arms Regulations (ITAR) Part 125."
17. "(ITAR) Part 120.10."
18. "*Ibid*, Part 120.9."
19. Refer to §734.2(2)(ii): "Export Administration Regulation §734"
20. Zlatko Hadzismajlovic, "Foreign Nationals and Defense Hiring: The Most Delicate of Decisions," *New York Law Journal*, August 6, 2012.
21. Bureau of Industry and Security, US Dept of Commerce, "Guidance on Reexports."
22. US Department of State, "The Arms Export Control Act"
23. "This Day in History: July 5th, 1940: United States passes Export Control Act." History, A&E Networks.
24. See 22 U.S.C. § 2751 "…facilitate the common defense by entering into international arrangements with friendly countries which further the objective of applying agreed resources of each country o programs and projects of cooperative exchange of data, research, development, production, procurement, and logistics support to achieve specific national defense requirements and objectives of mutual concern."
25. 22 U.S.C. § 2403(e)
26. Dan Froomkin and Amy Branson, "Deciphering Encryption." *Washington Post*, May 8, 1998.
27. Steven Brotherton and Karen Server, "Beyond reach? How to develop ITAR-free systems." *World ECR* 1 (2011): 16-19.
28. "ITAR Amendments Undermine Key DOD Acquisition Goal." *Defense Trade Law Blog*, March 18, 2015.
29. Ryan J. Zelnio, "Determining the Effects of ITAR Regulation on Commercial Space Manufacturing." Paper presented at the Interdisciplinary Graduate Student Conference: Science and Technology in Society March 31-April 1, 2007.
30. Richard Kusiolek, "ITAR Dilemma: Finding The Balance Between Regulation And Profit." *Via Satellite*, July 1, 2008.
31. Martin Seifert and Anthony Rallo, "Market Insights: U.S. military high-energy laser development hindered by ITAR regulations." *Laser Focus World*, June 1, 2015.
32. Brian Krassenstein, "US Government Proposes ITAR Amendments to Choke Off Distribution of 3D Printable Gun Models." *3DPrint.com*, June 8, 2015.
33. David Alexander, "Theft of F-35 design data is helping U.S. adversaries-Pentagon." *Reuters*, June 19, 2013.
34. Mark Halper, "The U.S. is helping China build a novel, superior nuclear reactor." *Fortune*, February 2, 2015.
35. Sharon Weinberger, "Export-control laws worry academics," *Nature* 461 (2009): 156.
36. Beginning in the 1990s, this was a major concern for number theorists working on encryption algorithms. A court case based on infringement of first amendment free speech resulted in changes to the export administration regulations; See Daniel J. Bernstein v. U.S. Department of Commerce, et al. Second Supplemental Complaint.
37. "ITAR Control of Public Speech." *Defense Trade Law Blog*, June 3, 2015.
38. Andy Greenberg, "3-D Printed Gun Starts The War Between Arms Control and Free Speech," *Wired*, May 6, 2015.
39. Constitutionality of Proposed Revisions of the Export Administration Regulations.
40. Thaddeus McBride and Reid Whitten, "Prison Time and Export Control: University Professor's Case Illustrates Dangers of Ignoring Export Compliance." *Government Contracts, Investigations & International Trade Blog*, Shepard Mullin, October 24, 2011.
41. See section on "Criticism of the Current Rule" in John M. Hynes, "New ITAR Rule on Transfer of Defense Articles to Dual and Third-Country Nationals Creates Substantial New Compliance Obligations," *Government Contracts, Investigations & International Trade Blog*, Shepard Mullin, June 16, 2011.
42. Richard Kusiolek, "ITAR Dilemma: Finding The Balance Between Regulation And Profit." *Via Satellite*, July 1, 2008.
43. See section on "The Growth of Foreign Research Centers of U.S. Multinationals" in Wessner, Charles W. and Alan Wm. Wolff, eds., *Rising to the Challenge: U.S. Innovation Policy for the Global Economy*. (Washington, D.C.: The National Academies Press, 2012).
44. Stephen A. Cambone, "The National Security Act of 1947– 26 July 1947." A New Structure for National Security Policy Planning. Washington, D.C.: CSIS, 1998. 228-32.

The Cost of Access

Jennifer McArdle, Brian Barnett, and Kathy Goodson, PhD

The Internet has become a platform of societal interaction: an information repository, communication tool, commercial-space, and a location for self-brand promotion. Internet web platforms provide users with petabytes of data at their fingertips, and thus provide opportunities for commerce, research, and societal interaction, all at what appears to be no cost. However, access is not free. When an individual accesses their email, a web search platform, online banking, or any other Internet service, the cost of access is the collateral divulging of data – data that has immense value.

DATA HAS VALUE

Global digital data is doubling yearly, and individual consumers create the majority of that data, producing in essence, digital footprints. These individual digital footprints – downloads, e-mails, cell-phone readings, "likes," tweets, clicks, and purchases – on their own provide relatively esoteric indicators of a particular individual. However, big data, by fusing information flows with insights derived from behavioral science, allows advertisers, search engines, and social media platforms to predict and model human behavior.

As data begins to reveal more information about individuals, its value and impact on individuals will increase. Indeed, the value derived from data has already been compared to 18th century commodities, such as oil[1] or 17th century power derived through land.[2] Data is the 21st century equivalent of oil or land – an asset that corporations and governments alike are trying to tap.

Privacy Fix, an app developed by the security software company AVG, has attempted to estimate how much a specific individual's data may be worth to some of the Internet's largest tech giants. In 2014, the company estimated that the most valuable Facebook users generate about $37.98 in revenue per year, while an average Google user is worth about $223 in revenue per year.[3] Multiply those figures by Facebook and Google's nearly 700 million and 1.7 billion users respectively, and it becomes exceedingly clear that personalized data has immense value.

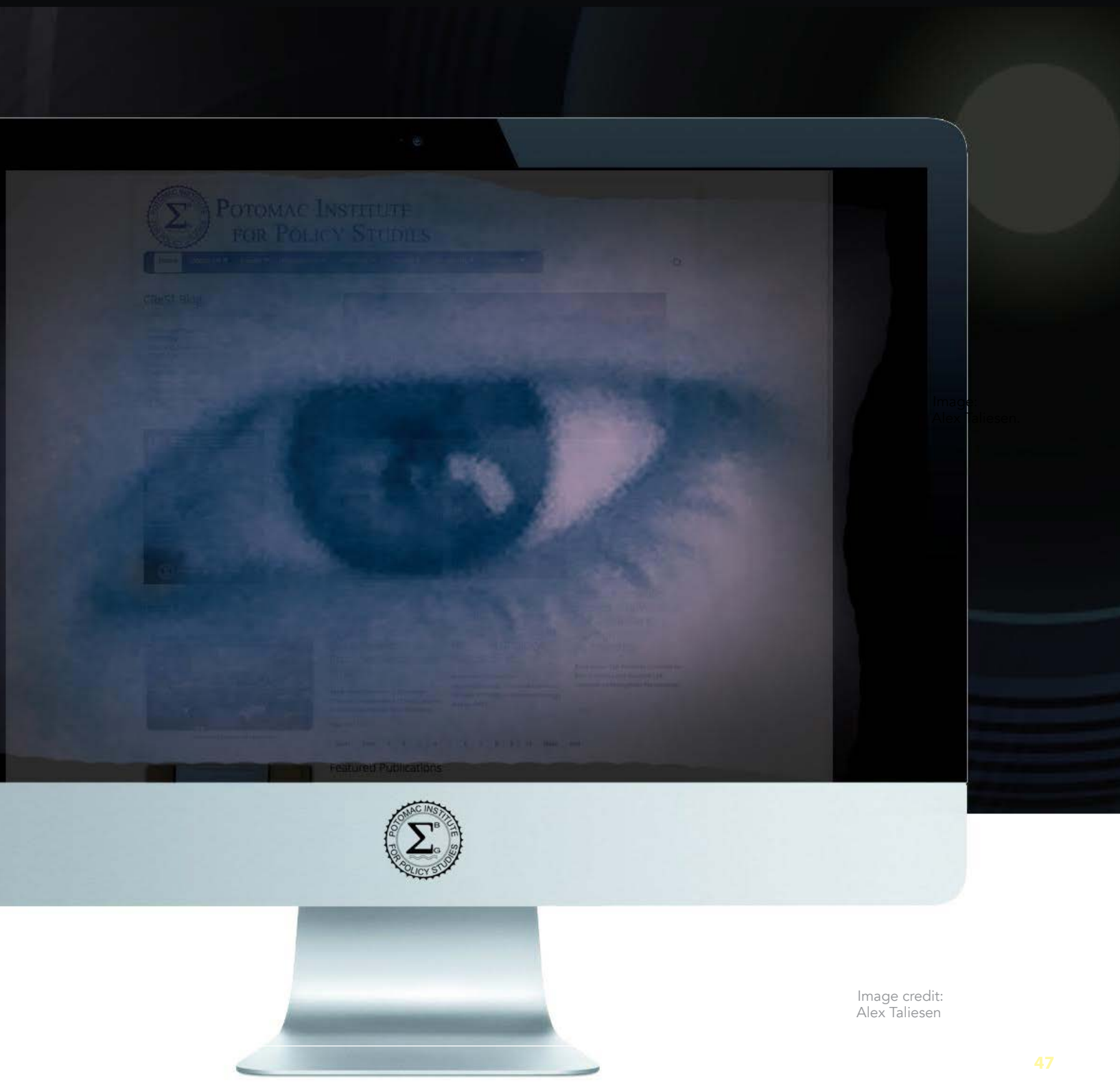


Image credit:
Alex Taliesen

THE COST OF ACCESS

While the sharing of data has facilitated healthier living, smarter cities, more effective disease control and prediction, and any number of other benefits,[4] there is a cost – a dark underbelly to the collection and sharing of personalized data.

In a 2014 World Privacy Forum report,[5] Pam Dixon and Robert Gellman indicate that data brokers, analytical firms, and retailers utilize personal data to create hundreds of inaccessible consumer scores, ranking individuals based on their perceived health risk, the likelihood that they will keep their job, and their alleged propensity to commit fraud. Data brokers have been known to use data to sort individuals into marketable categories: potential inheritor, diabetic, senior needs, low credit, etc. Companies such as InfoUSA have sold lists of "gullible seniors." Others, such as Teletrack – which was later fined by the FTC – sold lists of people who applied for nontraditional credit, such as payday loans, to companies who wanted to target high-risk consumers for poor financial deals. The use of secret consumer scores and data profiles can cast an indelible stain on individuals, and are becoming sources of classification, profiling, and discrimination."[6]

For example, in 2011, Google described how consumers with "high value profiles" received bids by corporations for targeted advertisements to their profiles.[7] Concurrently, consumers with "low-value profiles," often received no bids at all. Jeff Rosen of George Washington Law warns that this will essentially eliminate a free and open marketplace; as consumers will no longer "haggle" with sellers on equal terms, while being unaware of what discounts and prices other preselected individuals are being offered.[8] Even more problematic is the fact that these consumer scores could affect an individual's eligibility for a new job, a loan, credit, or affordable insurance. In short, one could see the emergence of a class of "digitally disenfranchised" individuals, whose prospects and ambitions are limited or denied due to the existence of "digital scarlet letters."

Perhaps more troubling than the profiling itself, is that these profiles are often wrong. Indeed, the Economist ran a blog on the increasing backlash against big data, noting three mainstream criticisms of big data.[9] While big data criticism is not an attack on the data itself, it is a critique on the numerous perceived

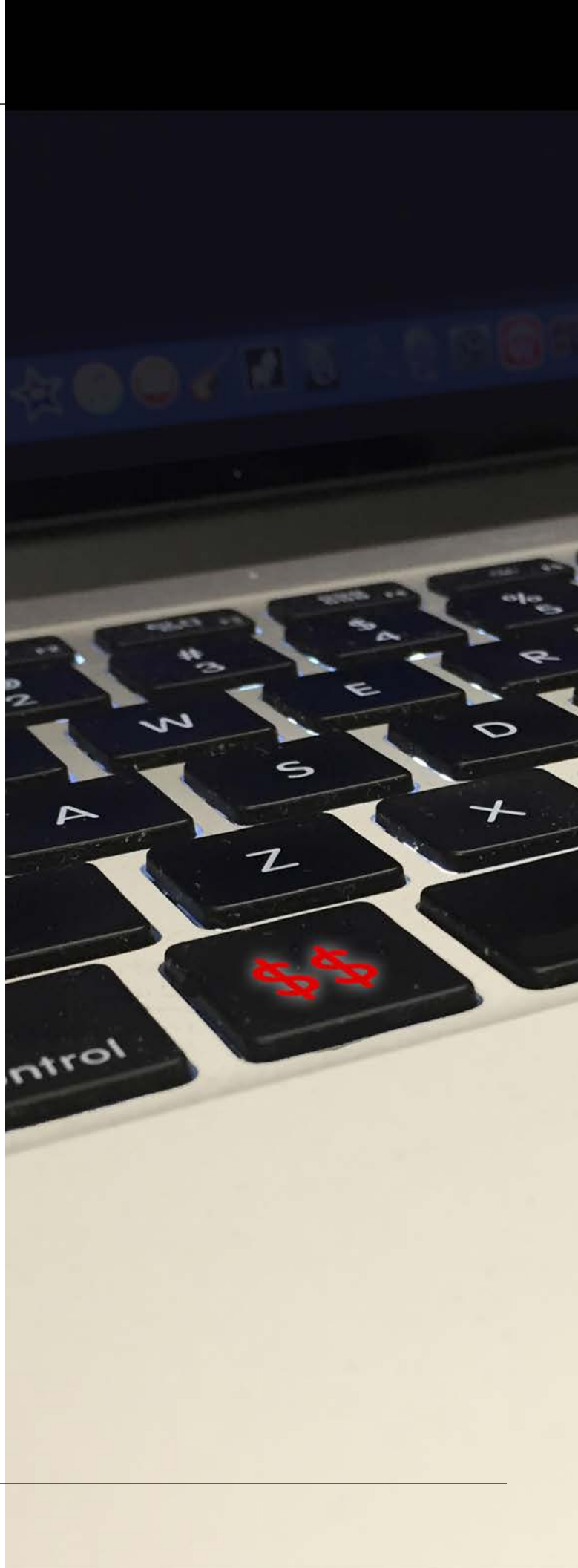


Image credit: Alex Taliesen

"The devices, software, hardware, and networks by which people access Internet platforms are inherently insecure, and this insecurity puts data at significant risk."

deficiencies of data analytics. Data analysis can come to erroneous conclusions and correlations. In a conversation with an insider from a data aggregation and profiling site, the person revealed that the company's labeling is correct only 40% of time.[10] While an accuracy rate of only 40% may not seem like a big deal when Amazon is using individual data to tailor-make book recommendations, a 60% error rate looks a whole lot more disturbing when that same data is then used to determine job eligibility and proclivity to commit crime.

THE COST OF DATA INSECURITY

However, it is not just the misuse or profiling of individuals through their data that come at a cost, the storage of that data also poses significant risk.

In 1998 a group of hackers called LOpht warned Congress that "if you are looking for security, then the Internet is not the place to be"[11] – computer software, hardware, and networks had not been designed with security in mind. Seventeen years later, not much has changed. Melissa Hathaway, the former acting director for cyberspace at the National Security Council, and John Stuart, Senior Vice President of Cisco, notes that there are currently "no standards – much less enforceable ones – for devices connecting to the Internet, aside from those inconsistently created by network operators. In addition, entire industries are building connectable devices with little to no experience or history in building (secure, resilient, well-engineered) connectable devices."[12] The devices, software, hardware, and networks by which people access Internet platforms are inherently insecure, and this insecurity puts data at significant risk.

Indeed, in the past six months, nearly 91 million consumer social security numbers were compromised through the corporate breaches to Premera Blue Cross and Anthem. However, that pales in comparison to the EBay and Home Depot 2014 breaches that compromised 145 million and 109 million consumers respectively.[13] In 2013, the number of breached records grew by 350%, resulting in over half of the US population's personal information being exposed.[14] The Center for Strategic and International Studies estimates that the annual cost to the global economy from cybercrime is more than $400 billion.[15] Data breach and cybercrime can have wide reaching implications for individuals, resulting in financial loss, identity theft, intellectual property (IP) loss, and the erosion of consumer confidence and trust.

Moreover, as the recent Office of Personnel Management (OPM) hack highlights, governments' stores of personal information are not immune to breach. The OPM breach, which could affect up to 32 million Americans, and likely involves at least 4 million government clearance application (SF-86) forms, has been labeled by some as "worse than the Snowden affair."[16] The personal nature of information in the SF-86 – foreign contacts, past employment and residencies, credit history, drug-use, travel, among other information – makes the documents the "crown jewels" of intelligence.[17] They reveal an individual's vulnerability to blackmail or recruitment. Moreover, sensitive details about an individual's interaction with foreign nationals could be used against those nationals in their own country. While the breach of this data inevitably is a cost to government, it is also of significant cost to those individuals and foreign nationals whose privacy was violated.

As government, industry, and academia shift toward digitizing, marketing, and selling information, they have passed the cost of access to the consumer. Although online accessibility is presented to the consumer as a convenience, the consumer incurs the cost and associated risk of practice.

THE COGNITIVE ASPECTS OF "FREE" PRODUCTS

In light of these costs, it is problematic that people are not wired to rationalize the potential downsides that arise from using these services and platforms.

A study by Kristina Shampanier, et al. shows that people offered a choice between a 1-cent Hershey's or a 26-cent Ferrero chocolate will generally prefer the Hershey's, but that when they are offered a choice between a free Hershey's and a 25-cent Ferrero, there is a significant increase in their preference for the Hershey's.[18] While the actual monetary value of both types of chocolate decreased at the same rate, the participants' behavior indicated that they perceived additional value in the free Hershey's. Even when the Hershey's price is held constant at zero, and the Ferrero price is reduced by a significant amount, people still prefer the free chocolate. This effect was replicated across a wider range of products with heftier prices as well. The reduction of a price to zero has a more powerful effect on behavior than a significant price reduction for another item that still has a positive price.

While the study of consumer choice with Hershey's chocolate may appear to be vastly different from individual access to Internet platforms and services, it does provide insight into consumer behavior when a product or service appears to be free. The fact that these Internet services appear to be free is disproportionately affecting individuals behavior and choices. Individuals need to be conditioned to realize that access to Internet platforms and services do come at a cost.

A WAY FORWARD?

While the Internet and its associated platforms yield immense societal and economic benefits, access does come at a cost. The onus is on individuals, corporations, and governments to mitigate the risks. The following are suggestions for each stakeholder.

Government:

- *Regulating for Corporate Notification of Data Sale:* Governments should pass regulations that require corporate notification and permission to sell individual data to third party data-brokers. This would provide individuals some transparency into the location and use of their personal data, particularly data that was not exchanged for access.

- *Regulating Against Data Profiling:* Government regulation should be put in place that protects individuals from opaque corporate profiling. Similarly to a credit score, individuals should be able to access and contest their "big data scores."

- *Secure System Accountability:* Congress and the Executive should move quickly to hold accountable agencies that do not secure their systems. Personal information on former employees should have an expiration date, whereby that data is deleted from government databases. It may be wise for the government to rethink what data they digitize, in an era where most information in accessible and "hackable," perhaps some information should remain off of computer servers.

Corporations:

- *Develop an Underwriters Laboratory for Internet Connected Devices:* Corporations could be incentivized to create an independent group, or tech-equivalent to an Underwriters Laboratory for Internet connected devices.[19] The first underwriter's laboratory was created in 1894 by William Merrill to ensure the safety of electrical devices. Today the underwriters laboratories provide safety related certification, validation, testing, and inspection to seven business areas, prior to providing their stamp of approval on a given product. An Underwriters Laboratory for Internet connected devices could incentivize corporations to manufacture products for security versus marketability.

Individuals:

- *Educating for Data Risk:* Individuals need to approach Internet access with cost in mind. While Internet users should not cease use, users should become more informed about their data and associated risks to that data. Educating oneself is the first step in protecting one's data.

- *Practice Adequate "Cyber Hygiene":* From a data profiling perspective, individuals should refrain from taking online quizzes that ask personal information in exchange for "free services" or games. Individuals that use social media platforms should be aware that they might be relinquishing ownership of their data. At the very least, individuals on these platforms should be cautious of their privacy settings. Search platforms such as DuckDuckGo do not collect data on personal searches and can be used as a mechanism to prevent corporate surveillance and data accrual.

- *Secure (to the best of your ability) Your Digital Assets:* From a data security perspective, most states offer quarterly credit score checks for free, individuals that use online banking or credit cards should track their credit carefully for early warning of identity theft. Credit cards have better protections than debit cards and therefore individuals should be cautious of using their debit cards for online transactions.

While these suggestions are certainly not meant to be exhaustive, their implementation could provide a framework for consumer protection moving forward. Today, consumer risk and digital access are intermingled, and cannot be viewed as separate entities. In the future, as the "Internet of Things" becomes a ubiquitous reality – and more of our critical services are connected to the Internet – consumers (and their data) will be increasingly at the mercy of those devices and platforms. There will always be a cost incurred for the benefits afforded by connecting our lives and our things to a digital universe of seemingly free access. The real question, moving forward, should be at how steep of a price?

Image credit: Alex Taliesen

NOTES

1. Joris Toonders notes, "Like oil, for those who see data's fundamental value and learn to extract and use it there will be huge rewards." See: Joris Toonders, "Data is the New Oil of the Digital Economy," *Wired* (July 2014).
2. Jennifer McArdle draws a comparison between the determining element of power in 17th century pre-industrial England, land, and data in the 21st century. See: Jennifer McArdle, "Rethinking Property in the Digital Era," *National Interest* (May 2014).
3. Cotton Delo, "How Much Are Your Really Worth to Facebook and Google?" *Advertising Age* (May 7, 2014).
4. For more information, see: Alex Petland, *Social Physics: How Good Ideas Spread–The Lessons from a New Science* (New York, New York: The Penguin Press, 2014).
5. Pam Dixon and Bob Gellman, "The Scoring of America: How Secret Consumer Scores Threaten Your Privacy and Your Future," *World Privacy Forum* (December 2014).
6. Bruce Schneier, *Data and Goliath* (New York, NY: W.W. Norton & Company, Inc: 2015) p.52.
7. IAB, Google, and Forrester, "The Arrival of Real Time Bidding," *Slideshare* (June 16, 2011).
8. Jeff Rosen, "Who Do Online Advertisers Think You Are?" *The New York Times* (November 30, 2012).
9. The Economist identifies three criticisms that are "not intrinsic to data…but endemic to data analysis." The first, "are biases inherent to data…Second, some proponents of big data have claimed that theory (i.e. generalizable models about how the world works) is obsolete. In fact, subject-area knowledge remains necessary even when dealing with large data sets. Third, the risk of spurious correlations–associations that are statistically robust but only happen by chance–increases with more data." See: "The Backlash against big data," *The Economist* (April 14, 2014).
10. Author interview with data insider (April 2014).
11. Craig Timber, "A Disaster Foretold–And Ignored," *The Washington Post* (June 22, 2015).
12. Melissa Hathaway and John Stuart, "Taking Control of Our Cyber Future," *Georgetown Journal of International Affairs* (July 25, 2014).
13. Keith Collins, "A Quick Guide to the Worst Corporate Hacks," *Bloomberg* (March 18, 2015).
14. "2013 Cost of Data Breach Study: Global Analysis," *Ponemon Institute* (May 2013).
15. Center for Strategic and International Studies, "Net Losses: Estimating the Global Cost of Cybercrime," *Economic Impact of Cybercrime McAfee* (June 2014).
16. Ryan Evans, "Why the latest government hack is worse than the Snowden affair," *The Washington Post* (June 17, 2015).
17. *Ibid.*
18. Kristina Shampanier, Nina Mazar, Dan Ariely, "Zero as a Special Price: The True Value of Free Products," *Marketing Science* 26.6 (November-December 2007) 742-757.
19. See: Melissa Hathaway and John Stewart, "Taking Control of Our Cyber Future," *Georgetown Journal of International Affairs* (July 25, 2014) and Craig Timber, "A Disaster Foretold–And Ignored," *The Washington Post* (June 22, 2015).

VIEWS IN BRIEF

Image credit.
www.shutterstock.com.

Space to Breathe: The Argument for a New Outer Space Treaty

Joshua Hampson

Since the beginning of the space race, military space policy has been pursued in an environment with little international consensus. The force-enhancement capabilities provided by military space assets have been tied into the overall deterrence structure of the US, and because of this, American policymakers have resisted international efforts to regulate military actions in space. Given growing complexities in the space environment, however, and an increase in the number of space-faring nations, it would be wise for the US to reconsider its approach to space policy. The pursuit of a new international space treaty, along with changes to American space policy, could create needed stability, protect space infrastructure, and strengthen US deterrence capabilities.

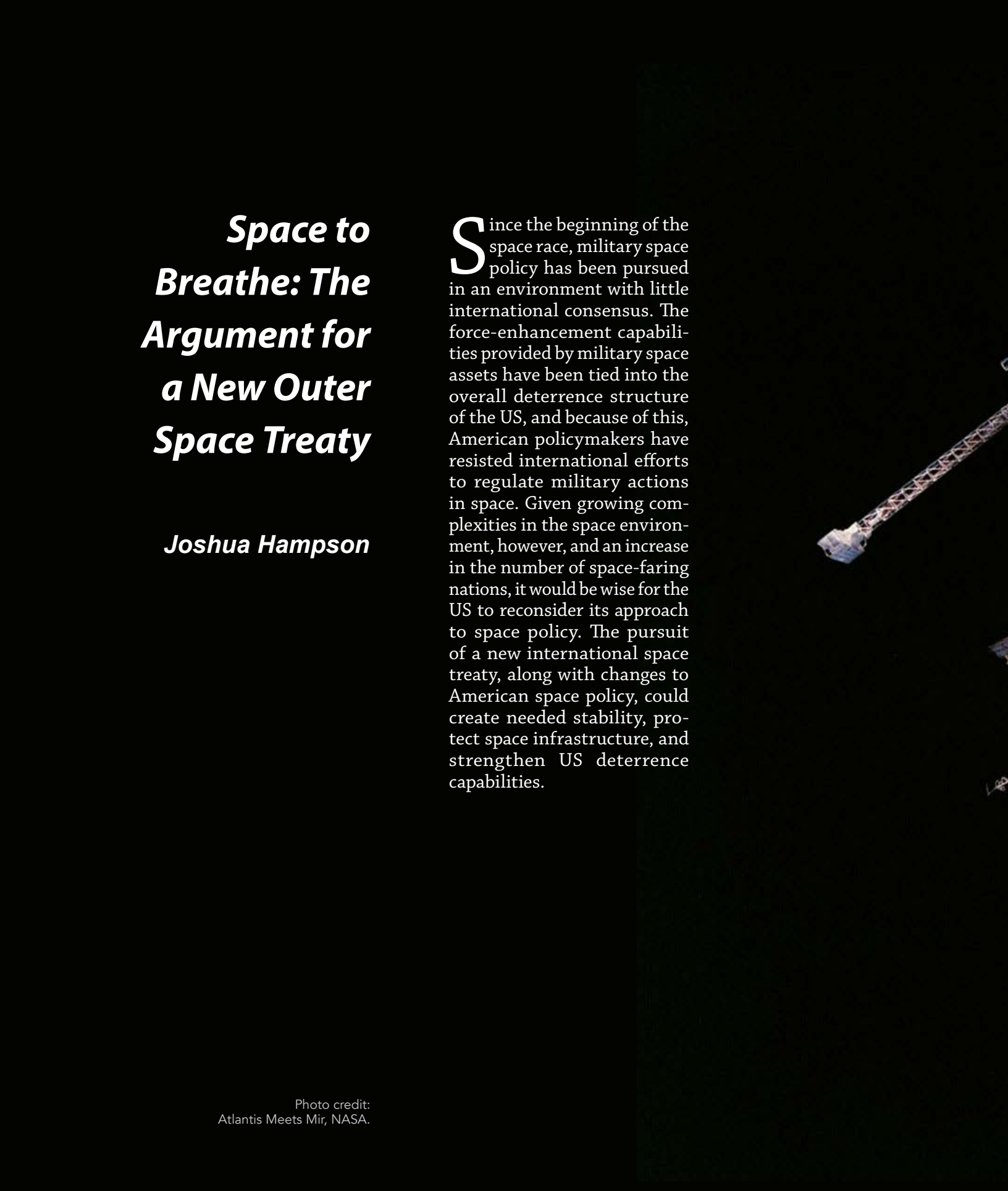
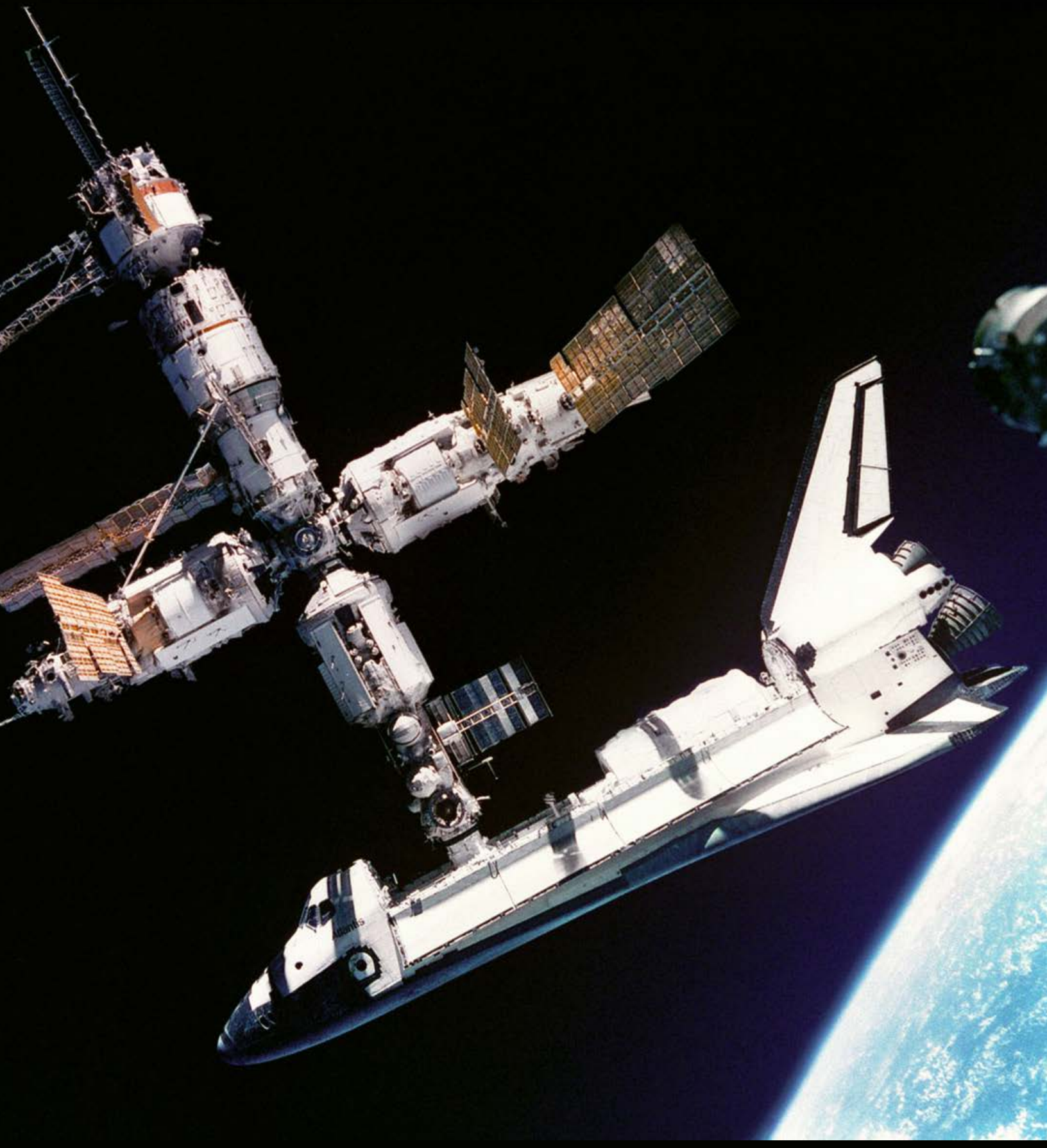


Photo credit:
Atlantis Meets Mir, NASA.



The past few decades have seen international actors internalize outer space as a theater for economic, scientific, and military operations. The use of space has not only revolutionized technology, but has also led to dramatic changes in organizational arrangements and strategy. Space infrastructure is frequently used in support of civilian and military operations.

The US military in particular has come to rely on space power. As the most space-dependent country in the world, the US predicts that its use of space will only deepen in the future.[1] In particular, space infrastructure has provided key force-enhancement capabilities, and these capabilities are couched within the language of deterrence.

> *"By being exceptionally powerful in all dimensions … the United States is a factor in the calculations of many rogues, aggressors, and patriots who do not need to receive personal American messages of discouragement addressed to them by name, place and issue."*[2]

It is therefore important to examine how the development of the space environment interplays with American deterrence. While complex military space capability has certainly benefited the force-enhancement side of American deterrence, the world is slowly entering a new stage of space exploitation. So far, there has been little pressing need for a strong international treaty involving space, but it may benefit the US to pursue a new international space treaty in the near future.

The benefits of military space infrastructure are well known. Satellites provide an impressive line-of-sight view, and facilitate communications to and from battlefield operations. These force-multiplying benefits provide the US with large increases in accuracy, agility, range, and effectiveness. Space assets have effectively altered the "nature of war."[3] Space infrastructure allows for smaller, more efficient military units to wield the same level of power projection as erstwhile larger forces. The growth of external commitments, bilateral treaties, multipolar concerns, and international influence post-Cold War has meant that conflict demands lighter, more flexible units whose strength rests on knowledge, not necessarily size. As such, space infrastructure has become a significant tool for information dominance and therefore deterrence.

Space infrastructure is also crucial for drone operations, which in turn increases power projection while limiting human exposure to risk.[4] While drones themselves are not spacefaring, they would not be so effective or ubiquitous without their satellite links and satellite-guided munitions.

The United States has thus sought to protect its ability to exploit space independent of international oversight. Within the current mindset, it is intolerable to cede potential capabilities to global veto. Thus the United States has not supported UN efforts to ban weapons in space and to prevent an outer space arms race.[5] A list of recent actions include:

- In 2014, The United States voted against a UN "no first placement of weapons in outer space" draft resolution.
- In 2008, The United States argued in the UN that it is impossible to define space-based weapons, and that an effective agreement on banning terrestrial-based anti-satellite systems is also impossible.[6]
- In 2005, The United States voted against an attempt in the UN to stipulate that the legal regime in outer space needed enhancement to prevent an arms race.[7]

The era of unconstrained American exploitation of space is passing, however, regardless of a potential treaty. There are new technological and developmental trends that will force a new American approach to space.

The first trend ties into the increasing use of space and the inherent low level of survivability of space infrastructure. Shrapnel fields, for example, prove incredibly disruptive to space operations. In 2007, China demonstrated its capability to destroy space infrastructure in a test that generated thousands of highly dangerous shrapnel fragments.[8] The anti-satellite test demonstrated that potential challengers to the global order are pursuing means to deny American space services[9] through asymmetric exploitation of American vulnerabilities in space.[10]

The United States recognizes that space infrastructure will likely be a future target. War games organized by the US Army have demonstrated American vulnerability and dependency on space.[11] Yet deterring an attack against its space infrastructure is difficult.

Few comparative threats can be leveled against a non-space-integrated military when American space infrastructure is threatened.

American allies have also pursued a greater space presence, increasing the complexity of the space environment.[12] An equally demanding problem is the growing crowdedness of space as private enterprise enters the space arena. In all, it is becoming difficult for any single power to keep track of what exactly is up there.

The shift in the international environment of space – growth of rival powers, asymmetric balancing, and the growing complexity of maneuvering within space itself – must lead to a shift in the American approach to international space policy. When international involvement was limited it was easier to reject draft treaties, but as exploitation of space has progressed, the lack of a comprehensive structure could prove dangerous. There are, however, steps that could be taken.

The United States should pursue a treaty on our own terms. First, the treaty should seek operational coordination. Space is getting crowded, and the growing number of satellites and pieces of junk in orbit will threaten military, economic, and scientific use of space. The international community needs to create a framework for public and private sector use of space and much clearer measures of liability for incidents in space. Built-in deorbiting measures should also be an international norm.

Second, The United States should lead a discussion on space code of conduct. It has been American policy to avoid altering the 1967 Space Treaty, but the usefulness of that treaty has long since expired. The international community needs to ban ASAT tests, even with claims that it is an unenforceable ban. The lack of testing would constrain ASAT utility during times of conflict. A ban would help protect American space assets and provide a moral argument for moving aggressively if space assets are attacked.

The treaty could codify an international response to violations. The sabotage of another country's space assets could, for example, lead to a ban from using international space constellations. The response could also incorporate economic sanctions. In this regard, the 1967 Space Treaty is too vague, and allows different space-faring countries to interpret the terms with great fluidity. For example, it explicitly forbids weapons of mass destruction in space, but little else. If damaging space assets results in coordinated punishment, The United States will be able to more confidently rely on its space assets to support power projection and deterrence.

The United States currently relies on its own military and scientific prowess to prevent damage to its space assets. That might not be enough in the future, and so The United States should establish space norms while it is still the dominant actor. Creating an international regime that would ease concerns about the safety of space infrastructure would allow The United States to more confidently use its military power for terrestrial deterrence.

NOTES

1. C. Robert Kehler, "Shaping the Joint Fight in Air, Space, and Cyberspace," National Defense University, 2008, p. 34.
2. Colin Gray, *Maintaining Effective Deterrence*, Strategic Studies Institute, US Army War College, 2003. p. 30.
3. See: US Army Space and Missile Defense Command, "Rendezvous in Space: Looking in on Military Space Power," *Army Space Journal* 2010.
4. Christian Enemark, "Drones over Pakistan," National Security College, 2011. p. 228.
5. United Nations Meetings Coverage, "Disarmament Committee Approves Drafts on No First Placement of Arms in Outer Space, Ban on New Types of Mass Destruction Weapons," Oct. 30, 2014. Accessed 20 August 2015.
6. United Nations Meeting Coverage, "Preventing Outer Space Arms Race…" Oct. 20, 2008. Accessed 25 August 2015.
7. United Nations Meetings Coverage, "*Preventing Outer Space Arms Race…*" Oct., 25, 2005. Accessed 25 August 2015.
8. Ashley Tellis, "China's Military Space Strategy." *Survival: Global Politics and Strategy*, 49 no. 3 (2007): 41.
9. "Shaping the Joint Fight in Air, Space, and Cyberspace," p. 35.
10. James Lewis, "China as a Military Space Competitor." Center for Strategic and International Studies, 2004.
11. Benjamin Lambeth, *Mastering the Ultimate High Ground*. (Santa Monica, CA: RAND, Project Air Force, 2003). p. 100.
12. Frank Slijper, "From Venus to Mars," Compagnetegen Wapenhandel, 2007. p. 36.

Joshua Hampson studied International Relations and Economics at the University of St. Andrews, Scotland, and graduated in 2013 with a First Class MA degree. He has since worked as a political risk analyst, a foreign policy fellow in the US House of Representatives, and an international relations forecaster. He is currently a macroeconomic and international strategy analyst for Wikistrat.

Water on the Rise: Policies for Coastal Plains

Christopher A. Wilson

A potential sea level rise in coastal areas such as Miami, Norfolk, and New York City threatens the population's economic and social status quo. Engineers, policymakers, and emergency managers, are encouraged to rethink their approach to mitigating the risk from hurricanes, storm surge, and the potential of elevated sea levels. The state of Louisiana, in general, is one of the regional economic hubs for energy production, infrastructure distribution and international and domestic trade; nevertheless, the loss of land over time due to sea level rise and hurricanes is threatening infrastructure in this coastal area.

Image credit: Alex Taliesen

Engineers can use the environment and technology to adapt to changes in the environment. The author promotes the idea to build floating cities, which would use solar energy to produce electricity and recyclable seawater to produce freshwater. Funding for such projects would come from public-private partnerships utilizing limited recourse or non-recourse financing. Investing in a floating city concept would save the money that would have been invested in levee systems upgrades, protecting the city from flooding, and creating larger ports that encompass greater services to assist with the distribution system. Therefore, implementation of the floating city project can put the coastal people and the infrastructure out of danger, and hence, ensure social and economic stability.

INTRODUCTION

Sea levels are rising throughout the world, in different amounts in different regions. Coastal communities are vulnerable to social, security and economic issues; the consequential flooding, hurricanes and storm surges endanger their lives and property. There is a need to protect coastal communities from the devastating effects such as those seen during Katrina, which is still struggling to recover a decade later. The rise in the sea level is driven by a variety of factors; the first is melting of glaciers, which is assessed by determining the height of the water as measured along the coast relative to a point on land. Other factors include tectonic factors that change the profile of ocean basins, storms, tides and climate change which influences the density and amount of ocean water.

The changing heights of land (subsidence or uplift) and ocean have caused an irregular change in the sea level. The sea level is rising faster in some locations, like in New Orleans, than the global average while, in other regions, such as Alaska, it may be falling. Estimating present and future local rates of relative sea level change for specific areas based on observations and projections of global sea level rise allows coastal engineers and policy makers to study and strategize for the impacts for efficient mitigation.[1] Subsequently, land use decisions should consider lessons learned from the mitigation efforts employed in vulnerable areas.

The study of sea level rise is a large field. We state many facts and statistics as reported by our references.

COASTAL IMPACTS

After the 1927's Great Flood in Louisiana, the United States Army Corp of Engineers built levees to protect communities living in the delta of the Mississippi River. Historically, in the case of New Orleans, wetlands, barrier islands, and dunes have played a significant role in protecting coastal wetlands. But salt water from the ocean moving into fresh water wetlands has degraded the defense to coastal areas. As a result, many coastal areas along Southern Louisiana Coastline are vulnerable to storm surge and future hurricanes. Today the region faces new challenges, both outside the levee walls from rising seas and inside from land subsidence and regular flooding.[2] Many other coastal communities such as Miami, Florida, Norfolk, Virginia, New York City, and New Jersey, face a similar threat.

Norfolk is residence to the United States chief naval facility, but is facing multiple threats from storm surge, coastal inner city flooding, and elevated sea levels. The land is still sinking in connection with the Chesapeake Bay Impact Crater that was left over from an asteroid impact 35 million years ago.[3] The total tally of flooding occurrences in Norfolk have tripled every year since the 1970s while tidal flooding happened approximately once per month. The predicted sea level rise at Norfolk is six inches by 2030. By then, the city could have 40 tidal flooding events per year.[4] In addition to tidal flooding, many tunnels and roads are closed when high tide occurs, impacting emergency evacuation routes.[5] Nevertheless, Norfolk is in partnership with the Rockefeller Foundation to build elevated roads, tide gates, floodwalls, and pumping stations. The cost is expected to exceed $1 billion. Miami has a similar problem.

In Miami, a majority of citizens live in flood plain areas. Most of the existing land does not accommodate future sea level rise or storm surge. Currently, the geology of Miami is made up of Limestone soil, equated by engineers to Swiss cheese, which has caused salt water from the ocean to destroy fresh water aquifers. The cost of keeping seawater off the streets in Miami is expected to cost $400 million over the next 20 years.[6] New Orleans has an even bigger problem.

In New Orleans, drainage pipes become overwhelmed with inner-city flooding caused by heavy rainfall. New Orleans and areas along the Southern Louisiana coastline are fighting the epic battle of subsidence. According to Waggoner & Ball Architects,[7] subsidence is the sinking of ground that damages infrastructure like roads, pipes, and buildings. Subsidence will cost the state of Louisiana an estimated $2.2 billion dollars for repairs to infrastructure over the next 50 years. In a report by Marshall,[8] it is noted that 60 percent of the residents of the metropolitan area live on land lower than the lake's surface. Despite investment of millions of dollars in levees, the city is still sinking. New methods are needed to protect New Orleans and other coastal communities.

NEW SOLUTION FOR PROTECTING COASTAL COMMUNITIES

Engineers and architects have a new vision that embraces living with rising water. Instead of fighting

the very threat that many coastal communities face, coastal communities should adapt and make use of the environment. According to Paul Lewis of Princeton University, every house that is located near water can be viewed as a waterfront house.[9] Guy Nordenson, also at Princeton, rejects the notion of a dividing line between land and sea. His approach calls for amphibious suburbs with landscape that could sustain periodic flooding. In addition to the amphibious suburbs, Nordenson is encouraging a reconsideration of the FEMA flood zone boundaries that ultimately determine insurance rates and building code requirements. Geographical areas that are prone to flood risk should be assessed on the outcomes and probabilities of diverse storm events, not the protection afforded by artificial levees that can be overtopped by high storm surges.[10]

Nordenson further calls for revitalizing natural wetlands and beach dunes. This approach has the potential to reduce the impact of waves, improve water quality, and allow for recreational areas to be created along coastal communities. And then there is the concept of floating the city of New Orleans. Environmental engineers and architects have produced computer simulations, but no one has yet tested the concept.

In general, the idea is to quit fighting the rising sea, but rather to build communities that can adapt to it.

Accordingly, a 21st Century concept for adaptation involves building infrastructure on top of floating platforms near coastlines. This fanciful idea is more practical than one might think. Of course, the underlying infrastructure would be costly. However, compared to fighting the rising sea with barriers and pumps and overbuilt drainage systems, the concept might be considered affordable. The state of Louisiana estimates a price tag of $9 billion dollars to build a floating city equivalent to the Dutch approach in Amsterdam.[11]

One possibility for financing the development of floating infrastruction would be to use public/private partnerships. "Public Private Partnerships" is a funding concept being embraced by state and local communities. The Public Private Partnership Infrastructure Resource Center defines them as government instruments to acquire and implement public services or infrastructure using the knowledge, resources and skills from the private sector.[12] A partnership with the private sector can assist with innovation by providing new finance opportunities.[13]

Each city would need to execute an economic development strategy adapted to the unique city's experience according to the type and extent of sea level rise. Plans would be adapted to the risk of future events, both catastrophic and gradual, and thus "buy-down" risk. The plans would take into account expected sea-level-rise, restoration of surface water, and hydrology, and the need to lessen the danger of salt water intrusion.

OBSTACLE OR CHALLENGES COASTAL COMMUNITIES MAY FACE TO BECOMING RESILIENT

A floating city can have homes, schools, businesses, roads, infrastructure, sewage systems, etc., just like any other city. The difference is that floodwaters from rain and storm surge are no longer great threats. The floating city will have to worry about maintenance and corrosion, but is no different from land-based cities. Accrued cost savings from the comparison with post-disaster recovery and flooding cleanup can be 4 to 10 times more expensive than the mitigation efforts for the same hazards before they occur.[14] Those mitigation efforts, in turn, are as expensive or more expensive than building floating cities with more resilient designs.

There could be legal issues if floating cities cause deterioration of adjacent shores due to erosion or other causes.[15,16] The main obstacle, however, is the need to finance prevention as opposed to crisis response that might come decades later. Accordingly, realistic projections and insurance costs can help motivate resilience measures; there are indications that federally financed flood insurance rates have given home owners a poor warning of the actual risks of living by the sea.[17] Better projections require good science, with good estimates of the uncertainties.

CONCLUSION

The impact of coastal sea level rise is a gradual threat that may transpire over decades. But as engineers, policy makers, and emergency managers have learned from the past, action now can protect the future. Coastal communities such as Norfolk, Miami, New York, and the Jersey shore are already being impacted by high tides, storm surge, and elevated sea levels. Fighting

against the mounting threat using new designs and new technologies, including the concept of floating cities, will enable coastal communities and businesses to continue to thrive economically and socially in a more resilient way.

NOTES

1. Harvey Ruvin, et al. Miami-Dade Sea Level Rise Task Force Report and Recommendations. July 1, 2014.
2. Waggonner & Ball Architects. Greater New Orleans Urban Water Plan. (2013).
3. Climate Central. "Facts and findings: Sea level rise and storm surge threats for Virginia," (2014) and "Surging Seas" by Climate Central (accessed Sept 24, 2015).
4. Union of Concerned Scientists. "Encroaching tides: How sea level rise and tidal flooding threaten U.S. East and Gulf Coast communities over the next 30 years," Authored by Spanger-Siegfried, E., M.F. Fitzpatrick, and K. Dahl. Cambridge, MA: Union of Concerned Scientists Oct 2014, Accessed Sept 24, 2015.
5. *Ibid*, p 44.
6. Christina Veiga, "Miami Beach to spend up to $400 million to deal with flooding issues,"*Miami Herald*. Feb 12, 2014.
7. Waggonner & Ball Architects.
8. Bob Marshall, "Special report: How New Orleans is making a 'serious problem' worse with its levees, pumping stations," March 1, 2015, in *The New Orleans Advocate*, (Retrieved 13 April 2015.)
9. Molly Sharlach, RESILIENT SHORES: After Sandy, climate scientists and architects explore how to co-exist with rising tides. (Nov 14, 2014,) News at Princeton, Retrieved April 15, 2015.
10. Catherine Zandonella, "After Hurricane Sandy, climate scientists and architects explore how to co- exist with rising tides," in Phys. Org, (Jan 6, 2015).
11. Bob Marshall, "Special report."
12. World Bank. "What are Public Private Partnerships? Public Private Partnerships Resource Center," Aug 2015. Accessed Sept 24, 2015.
13. World Bank. "Main Financing Mechanisms for Infrastructure Projects," (May 2015). Public Private Partnership in Infrastructure Resource Center.
14. Susanne C. Moser, S. Jeffress Williams, and Donald F. Boesch, "Wicked challenges at land's end: Managing coastal vulnerability under climate change," in *Annual Review of Environment and Resources* 2012. 37:51–78.
15. Siders, A.. "Managed coastal retreat: A legal handbook on shifting development away from vulnerable areas," © New York, NY: Columbia Center for Climate Change Law, Columbia Law School. Oct. 2013. Accessed Sept 24, 2015.
16. Wes Shaw, "Storm Smart fact sheet 2: No adverse impact and the legal framework of coastal management," Boston, MA: Massachusetts Office of Coastal Zone Management. April 2008, Accessed Sept 24, 2015.
17. Union of Concerned Scientists. "Overwhelming Risk: Rethinking Flood Insurance in a World of Rising Seas," August, 2013. (Accessed December 23, 2013.) Report authored by Rachel Cleetus.

Christopher Wilson joined the Department of Homeland Security in July 2011 as a management program analyst and has served as an adjunct online instructor at Georgia Military College.

Image credit: Alex Taliesen

Featured Authors

Robert Hummel, PhD

STEPS, Editor-in-Chief

Dr. Robert Hummel serves as the Chief Scientist of the Potomac Institute for Policy Studies in the Science and Technology Policy Division and is a member of the Center for Revolutionary Scientific Thought. He is the author of the recent Potomac Institute book on "Alternative Futures for Corrosion and Degradation Research," and is also serving customers in DARPA and OSD. He is the principle author of the Institute's forthcoming book on machine intelligence. Prior to joining the Potomac Institute, he served as a program manager at DARPA for nearly nine years, managing and initiating projects in information exploitation, computer science, and sensor design. Prior to joining DARPA, he was a tenured faculty member at NYU's Courant Institute of Mathematical Sciences in the Computer Science Department, where he did research in computer vision and artificial intelligence. Dr. Hummel's PhD is from the University of Minnesota in mathematics, and he holds a B.A. from the University of Chicago, also in mathematics.

Kathy Goodson, PhD

STEPS, Associate Editor

Dr. Kathy Goodson is the Director of Communications at the Potomac Institute for Policy Studies. Dr. Goodson leads outreach and communications components of a joint Potomac Institute and Office of Corrosion Policy and Oversight effort. Prior to joining the Potomac Institute, Dr. Goodson was an Assistant Professor of Biological and Physical Sciences at the College of Southern Maryland. She completed her studies for a doctorate in biochemistry from the University of Maryland, College Park, Department of Chemistry & Biochemistry in 2012. Her dissertation research focused on spectroscopic determination of protein-DNA complex conformations using organic dye molecules. Her areas of graduate research study included biochemistry, physical chemistry, biophysical chemistry, and molecular biology. Dr. Goodson received her B.S. in Chemistry from Virginia State University. Dr. Goodson is a member of the American Chemical Society and the National Organization for the Professional Advancement of Black Chemists and Chemical Engineers (NOBCChE).

Brian Barnett

Brian Barnett is a Research Assistant at the Potomac Institute for Policy Studies in the CEO's Office. Brian Barnett currently provides research and analytic support to guide discovery of innovative, non-traditional solutions and develop technology assessments for the Rapid Reaction Technology Office (RRTO) in its mission to enable new, affordable capabilities. He also performs research for the Center for Neurotechnology Studies (CNS), where he creates analyses and policy recommendations for leveraging the benefits of neuroscience. Brian organizes events, conferences, and discussions for both RRTO and CNS at the Institute and at other venues, by interfacing and coordinating with government officials, venture capitalists, commercial leaders and academics. He obtained his B.S. in Neurobiology & Physiology at the University of Maryland, College Park, where he completed an undergraduate thesis investigating the behavioral and neural components of an animal model of ADHD. He also contributed to publications on the valuation and representation of reward within the rat fronto-striatal circuit.

Ken Hamilton

Ken Hamilton, a Senior Research Fellow at the Potomac Institute, has had a distinguished career as a naval officer and as an expert in DoD acquisition management. He is the founder of KTMG, an engineering management-consulting firm supporting major DoD Acquisition Programs and industry clients. He has served as the principle strategic management advisor to ACAT I acquisition programs, and is a founding member for OSD's Systems of Systems Center of Excellence. Mr. Hamilton is the co-founder of Mission Technology Systems LLC, a manufacturer of small tactical unmanned aerial systems. Previously, he specialized in rapid acquisition for the US Navy SEALs and for the Joint Special Operations Forces (SOF), including serving as the senior advisor to the Commander, USSOCOM, and program management of NRO and ONR projects. CAPT Hamilton's military career includes 30 years of active and reserve service following graduation from the US Naval Academy.

Jennifer Lato

Jennifer Lato is a former intern and current Research Assistant in the Science and Technology Policy Division of the Potomac Institute for Policy Studies. Jennifer first joined the Institute in 2013, and provides analytic and research support for the Corrosion Policy and Oversight (CPO) and Defense Microelectronics Activity (DMEA) efforts. Jennifer also provides editorial assistance for Potomac Institute publications such as "U.S. Health Policy: An Insider's Perspective" (2014). Jennifer has a B.A.in History and Spanish from SUNY Geneseo as well as a M.A. in International Affairs from the George Washington Universities Elliott School of International Affairs. Jennifer brings an interdisciplinary perspective to policy analysis. Prior to joining the Potomac Institute, Jennifer worked in the Department of Treasury's Office of Financial Assets Control, where she assisted sanctions investigators as part of a as part of an executive order to combat transnational criminal entities. Additionally, Jennifer held a short-term post at the Bureau of Intelligence of Research (INR) at the State Department. In this position, Jennifer coordinated the review of strategic signals intelligence requirements with INR analysts.

Jennifer McArdle

Jennifer McArdle is a Research Associate and Fellow in the Center for Revolutionary Scientific Thought at the Potomac Institute for Policy Studies. Ms. McArdle joined the Potomac Institute for Policy Studies in March of 2014. Ms. McArdle provides strategic planning guidance on cyber hardware and supply chain security for the Defense Microelectronics Activity and additionally works for the Cyber Readiness Index team building out a cyber readiness index that assess 125 states cyber readiness across 7 different indices. Prior to joining the Potomac Institute, Ms. McArdle worked at the American Association for the Advancement of Science (AAAS) in the Center for Science, Technology, and Security Policy on Indo-US science of cyber diplomacy. Ms. McArdle joined AAAS after serving as a Visiting Fellow from the U.S. National Defense University at two think tanks in New Delhi, India: the Observer Research Foundation and the Institute for Defense Studies and Analyses. Ms. McArdle received MPhil in Politics with honors from the University of Cambridge and a BA in Political Science from the University of New Hampshire, summa cum laude. Ms. McArdle's work has featured in Real Clear World, the National Interest, the Pacific Standard, FierceGovernmentIT, GovInfo Security, among others. She is currently the chair of the Young Professionals in Foreign Policy (YPFP) cyber discussion group and has previously been selected by YPFP as one of the 99 most influential individuals under 33 in foreign policy. Jennifer is a PhD candidate at Kings College London, Department of War Studies. Her academic research focuses on national perspectives of information warfare.

Charles Mueller, PhD

Dr. Mueller works on identifying important S&T regulatory issues and developing sound regulatory policy solutions founded in the best available science. Additionally, Dr. Mueller is the lead on a project with the Office of Corrosion Policy and Oversight within the Department of Defense (DoD) that is attempting to optimize the DoD's current Corrosion Prevention and Control strategies by applying regulatory science & engineering principles. Prior to joining the Potomac Institute, Dr. Mueller obtained his doctorate in biochemistry from the University of Maryland's Chemistry and Biochemistry Department in 2014. His dissertation involved the characterization of two putative DNA metabolizing enzymes in the bacterium Deinococcus radiodurans and required a combination of molecular biology, cell biology, microscopy, and biochemical analyses. Before obtaining his doctorate he obtained a B.A. in Chemistry from Elon University and then worked at the National Cancer Institute at the National Institutes of Health studying the effects of selenium on cancer using both live mouse models and tissue cultures. Dr. Mueller is a member of the American Association for the Advancement of Science (AAAS).

Alden V. Munson, Jr.

Mr. Munson is a Senior Fellow and Member, Board of Regents at Potomac Institute for Policy Studies, has served on the Defense Science Board and is an advisor to government and industry in defense and intelligence matters. He was the Deputy Director of National Intelligence for Acquisition from May 2007 until July 2009. Previously he was a consultant in defense, space, and intelligence and was associated with the investment banking firm Windsor Group. He was Senior Vice President and Group Executive of the Litton Information Systems Group, leading information technology, command and control, and intelligence businesses for defense, intelligence, civil, commercial, and international customers. Mr. Munson was Vice President at TRW, in the System Integration Group, the Space and Electronics Group, and the Information Systems Group (the former TRW Credit Business). In these assignments, he led numerous space, intelligence, and information technology organizations and activities. He began his career at the Aerospace Corporation, where he provided system engineering support to many space and intelligence programs. Mr. Munson received a bachelor's degree in mechanical engineering from San Jose State University (SJSU) and a master's degree in mechanical engineering from the University of California, Berkeley.

Richard Pera

Richard Pera serves as Legislative Assistant at the Potomac Institute for Policy Studies, updating the CEO's Office on various developments on Capitol Hill. Pera brings policy and legislative experience to the Institute, including stints in several Members' offices in the US House of Representatives. In 2014, Pera worked on the staff of a US Senate campaign in Alaska, directly advising the candidate on policy matters. Before that, he served on the policy and communications team at the British Consulate-General in Chicago, reporting political and economic developments to UK officials in Washington, DC and London. Pera also worked at the Department of State, where he evaluated a program enabling diplomats to locate and assist US citizens abroad. Though a native Washingtonian, Pera's upbringing in a military family included overseas tours in Paris, France and Gaeta, Italy. He also studied European politics in Freiburg, Germany. Pera earned a B.A. in Political Science from Kenyon College in Gambier, Ohio.

STEPS (Print) **ISSN 2158-3854**
STEPS (Online) **ISSN 2153-3679**

POTOMAC INSTITUTE PRESS