Weekly Media Report – Feb. 2 - 8, 2021

TECHNOLOGICAL LEADERSHIP:

1. Technological Leadership: Combing Research and Education for Advantage at Sea

(USNI Feb 21) ... NPS President retired Vice Adm. Ann E. Rondeau, US Navy

We stand at a critical inflection point. U.S. national security must contend with increasing great power competition (GPC), which is fundamentally an innovation race—one well contested by our near-peer rivals. While technological change is inevitable, the rapidly emerging integration of computational power with its human masters, the so-called Cognitive Age is poised to create unprecedented national security challenges, and at a pace measured in months and not years.

RESEARCH:

2. Xerox and Naval Postgraduate School Announce Collaboration to Advance Solutions with 3D Printing Research

(NPS.edu 3 Feb 21) ... NPS Office of University Communications
(Navy.mil 3 Feb 21) ... NPS Office of University Communications
(Business Wire 3 Feb 21)
(Odessa America 3 Feb 21)
(TCT Magazine 3 Feb 21) ... Sam Davies
(3D Printing Media 4 Feb 21) ... Davide Sher
(Metal AM 4 Feb 21)
(ExecutiveBiz 4 Feb 21) ... Nichols Martin
(West Fair Online 5 Feb 21) ... Phil Hall

Xerox and the Naval Postgraduate School (NPS) announced today a strategic collaboration focused on advancing additive manufacturing research, specifically 3D printing, which has the potential to dramatically transform the way the military supplies its forward-deployed forces.

3. This huge Xerox printer can create metal parts for the US Navy

(Popular Science 3 Feb 21) ... Rob Verger

Xerox's new printer is 9 feet wide, 7 feet tall, and reaches an internal temperature of more than 1,500 degrees Fahrenheit. It's not an inkjet, of course—it's a 3D printer that can produce bespoke metal components. The Naval Postgraduate School, a grad institution for Naval officers and others, is the first place to put one of these massive Xerox machines into service.

4. NPS-Led Research Reveals Greater Abundance of Life Under Arctic Ice Than Previously Thought

(NPS.edu 2 Feb 21) … Rebecca Hoag
(Navy.mil 2 Feb 21) … Rebecca Hoag

For the longest time, scientists have written off there being much life below the Arctic sea ice. Surely not enough sunlight would be able to get through the snow and ice to sustain an abundance of life. Additionally, satellites can't see through the ice, and it was difficult for scientists interested in investigating this further to get out to the Arctic during the winter and spring – when the percent of Arctic ocean iced over was the highest – because most Arctic expeditions wait until there's thinner ice so icebreakers can move through.

5. Technology Sector Update: SNE,XRX,SMCI,GOOG,GOOGL

(Nasdaq 3 Feb 21) … MT News Wires

Technology stocks was hanging on for a narrow increase, giving back earlier gains led by Google parent company Alphabet (GOOG,GOOGL) reaching a new record high after reporting Q4 earnings and revenue topping analyst estimates. At last look, the SPDR Technology Select Sector ETF was rising 0.1% although the Philadelphia Semiconductor Index was sinking 1.6% this afternoon…Xerox (XRX) climbed 4.4% after Wednesday announcing a strategic collaboration agreement with the **Naval Postgraduate School** to work on 3-D printing and manufacturing research. As part of the deal, Xerox in December installed one of its first ElemX liquid-metal printer at the Monterey, Calif., campus, providing students and faculty with hands-on experience with on-demand 3D printing of metal parts and equipment.

6. GSA: taking advantage of industry with its ML & AI RFIs

(Spend Matters 5 Feb 21) … Nancy Cinton

Based on a **Naval Postgraduate** report from March 2019, companies spend over 1400 hours each year replying to government RFIs. If you do the calculation, even the most basic labor rates, and the annual economic cost of this transfer of effort approaches one million dollars. As a former contracting officer, Frank McNally of Public Spend Forum has mixed feelings about RFIs. On one hand, companies that want to win lucrative contracts should expect some degree of effort, and RFIs can be an effective tool for both parties. On the other hand, it's expensive to bid on government contracts and when we transfer the market research effort to contractors, we're adding overhead that just gets passed back to government. Market research is a time-consuming chore, hunting down supplier info on myriad public sector databases isn't how anyone wants to spend their time. So Frank explains how they created GovShop to consolidate all those sites and provide government contracting professionals with a "high resolution view" of a supplier's capability and key demographic data.

GREAT POWER COMPETITION:

7. Former Strategic Command, Pacific Fleet Commander Talks Great Power Competition in Guest Lecture

(Navy.mil 2 Feb 21) … Mass Communication Specialist 2nd Class Taylor Vencill
(Defence Connect 4 Feb 21) … Stephen Kuper

Naval Postgraduate School (NPS) distinguished alumnus retired U.S. Navy Adm. Cecil D. Haney, former Commander, U.S. Strategic Command, spoke virtually to Naval Postgraduate School (NPS) faculty, staff and students on the topic of "Great Power Competition (GPC) in the Cognitive Age" during the latest edition of the Secretary of the Navy Guest Lecture (SGL) series, Jan. 26.

EDUCATION:

8. NPS Regional Security Program Prepares Deploying Forces, Surpasses Milestone

(NPS.edu 5 Feb 21) … Mass Communication Specialist 3rd Class James Norket
(Navy.mil 5 Feb 21) … Mass Communication Specialist 3rd Class James Norket

For more than two decades, the Naval Postgraduate School's (NPS) Regional Security Education Program (RSEP) has provided leading subject matter experts to deploying forces in transit delivering on-site, graduate-level briefings on regional issues and challenges, historical and security context, and cultural sensitivities in Combatant Commanders Areas of Responsibility (AOR's) and regions where our forces will operate. From carrier strike groups

to SEAL teams, the RSEP program has delivered briefings and critical lectures to more than 500,000 Department of Defense participants worldwide as well as international allies and partners operating with our deployed Naval Forces.

CYBERSECURITY:

9. The U.S. Spent $2.2 Million on a Cybersecurity System That Wasn't Implemented and Might Have Stopped a Major Hack

(Spend Matters 2 Feb 21) … Peter Elkind and Jack Gillum

As America struggles to assess the damage from the devastating SolarWinds cyberattack discovered in December, ProPublica has learned of a promising defense that could shore up the vulnerability the hackers exploited: a system the federal government funded but has never required its vendors to use…

n-toto's system has supporters among experts in the government and corporations. When ProPublica asked Robert Beverly, who oversees in-toto's federal grant as a program director at the National Science Foundation, whether using in-toto could have saved the government from the hack, he replied, "Absolutely. There seems to be some strong evidence that had some of the, or all of the, in-toto technologies been in place, this would have been mitigated to some extent." Beverly, whose NSF responsibilities include "cybersecurity innovation for cyberinfrastructure" and who is on leave from his post as a computer science professor at the **Naval Postgraduate School,** added that it's impossible to know for sure what impact in-toto would have had, and that the system remains at an early stage of adoption. "Unfortunately," said Beverly, "it often takes some of these kinds of events to convince people to use these kinds of technologies."

10. We can make software secure, but not at a price you'd be willing to pay

(Tech Beacon 2 Feb 21)

The recent compromise of SolarWinds' Orion software has led to lots of largely ineffective hand-wringing. I've seen more time spent on talking about whom should be blamed for the incident than on how to mitigate the damage that it caused or to reduce the chances of a similar incident happening in the future… Modern software is probably the most complex thing ever created by man. Getting something that complex to work is hard. Try understanding the build process for your typical enterprise software these days and you'll be surprised that we can even get the stuff to work at all. Getting something that complex to work correctly is even harder. Getting something that complex to work securely may be so hard that it might be impossible in many cases. A study done by the **Naval Postgraduate School** nicely summed up the situation:

FACULTY:

11. Peter Denning: Award Recipient

(IEEE Computer Society)

Naval Postgraduate School Distinguished Professor Dr. Peter Denning was fascinated with science from an early age and began building electronic circuits as a teenager. His algebraic computer built from pinball machine parts won the science fair in 1959, launching him into the new field of computing. A decade later, at MIT's Project MAC for his doctorate, he took on the gnarly performance problem of the nascent virtual memory technology. Instabilities with thrashing and replacement algorithms threatened to scuttle that technology. He invented the Working Set Model, which immunized operating systems to thrashing and maximized system throughput. His solutions to these problems are widely used today in operating systems from desktops to smartphones. He is widely known as a virtual memory and computer systems performance pioneer.

12. US Foreign Policy and Great Power Politics

(BollyInside 2 Feb 21)

(The Diplomat 2 Feb 21) … Mercy A. Kuo

Trans-Pacific View author Mercy Kuo regularly engages subject-matter experts, policy practitioners, and strategic thinkers across the globe for their diverse insights into U.S. Asia policy. This conversation with **Zachary Shore – professor of history at the Naval Postgraduate School**, a senior fellow at UC Berkeley's Institute of European Studies, and a National Security Visiting Fellow of Stanford's Hoover Institution – is the 257th in "The Trans-Pacific View Insight Series." The opinions expressed in this interview belong to the speaker alone and do not necessarily reflect the official policy or position of the Naval Postgraduate School or any other governmental entity.

13. Lab publishes fourth 'Strategic Latency Unleashed' book

(Mirage News 3 Feb 21)
(Lawrence Livermore National Laboratory 3 Feb 21)

The Lawrence Livermore National Laboratory's (LLNL) Center for Global Security Research (CGSR) has published the fourth book in its Strategic Latency series — "Strategic Latency Unleashed: The Role of Technology in a Revisionist Global Order and the Implications for Special Operations Forces."… **Zachary Davis, a senior fellow at CGSR and research professor at the Naval Postgraduate School** (NPS) in the department dedicated to SOF, combined scientists and analysts from national labs, think tanks and universities, with experienced special operators to examine the ways that emerging technologies can assist or threaten SOF in future conflicts.

14. upGrad Creates UK Board with four prominent figures in global education

(Hindustan Times 4 Feb 21)
(Big News Network 4 Feb 21)
(LiveMint 4 Feb 21)
(PR Newswire 4 Feb 21)

upGrad, India's largest higher edtech company announced the appointment of a four-member independent board to build their UK-based operations and accelerate expansion. The board comprises distinguished leaders such as Professor Sir Deian Hopkin, Julie Mercer, Dr. Kishore Sengupta, and Ashwin Assomull.

Sir Deian is currently Principal Advisor at Wells Advisory and Associate Partner Anderson Quigley. Sir Deian was previously Vice-Chancellor and Chief Executive at London South Bank University (2001-2009) and Expert Adviser, First Minister of Wales (2012-2020). Also on the board is Julie Mercer, who was Global Industry lead for Deloitte's Education Practice over her 20 years there and is currently a partner at Cairneagle Associates. Another seasoned professional on the board is **Dr. Kishore Sengupta, who has been associated with INSEAD and Naval Postgraduate School**, California in the past and is now Reader in Operations at Judge Business School, University of Cambridge. Rounding up this quad of illustrious leaders is Ashwin Assomull who is currently a partner at LEK Consulting, and a former Partner and Member of the Emerging Market's Leadership Team at the Parthenon Group.

15. Dino Pick returns home after work in Washington D.C. to clean up 'ethical lapses' in U.S. Special Operations

(Monterey County Now 3 Feb 21) … Asaf Shalev

As he watched the Capitol insurrection unfold from the Pentagon, Dino Pick says he worried only about potential injury and destruction of property. "I was never concerned that the violence would ultimately succeed in conquering the Congress or derailing the electoral process. I continue to have deep faith in the pillars of our democracy because, Lord knows, they've been challenged." … Pick is now back home. He resigned from his Del Rey Oaks job for a new assignment, running international graduate programs for the **Naval Postgraduate School**.

16. Nord Stream 2: Implications and Outcomes for US-German Relations and the Nato Alliance

(News 247 World Press 2 Feb 21)

A white paper produced by members of the NATO Science and Technology Organization's Systems Analysis and Studies (SAS)-163, "Energy Security in the Era of Hybrid Warfare."
Margarita Assenova, Senior Fellow, Jamestown Foundation
John R. Deni, PhD, Research Professor, Strategic Studies Institute, US Army War College
David R. Dorondo, D.Phil., Associate Professor, Western Carolina University
Arnold C. Dupuy, PhD, Chair, SAS-163; Senior Analyst, SAIC
Ion Iftimie, PhD, Researcher, Central European University, Vienna, Austria
Daniel Nussbaum, PhD, Mentor, SAS-163; Director, Energy Academic Group, Naval Post-graduate School
Paul Michael Wihbey, Director, George Washington University/Institute on the Geopolitics of Energy

17. The Right Response to SolarWinds

(The Council on Foreign Relations 8 Feb 21) … **Dr. Scott Jasper, Naval Postgraduate School Lecturer**

In a formal joint statement, four U.S. agencies in charge of intelligence and cybersecurity affirmed that an advanced hacking group, "likely Russian in origin," is responsible for the SolarWinds Orion software compromise. President Biden has ordered a sweeping review of American intelligence on Russia's role in the breach and reportedly told Putin that "that the days of the United States rolling over in the face of Russia's aggressive

actions — interfering with our elections, cyberattacks, poisoning its citizens — are over." Taking a more assertive tone toward Moscow may be the easiest part of the White House's reaction to the SolarWinds hack. Finding the right balance of effective offensive and defensive actions will be more difficult.

ALUMNI:

18. Chiefs of the Monterey Peninsula Welcome New CPOs to the Mess

(DVIDS 2 Feb 21) … Chief Cryptologic Technician (Interpretive) Demian Ford

Information Warfare Training Command (IWTC) Monterey and **Naval Postgraduate School** pinned three new chief petty officers (CPO) at the Naval Postgraduate School, Jan. 29.

19. Colorado State University alumna tapped to lead FEMA

(Coloradoan 3 Feb 21) … Molly Bohannon

President Joe Biden nominated Deanne Criswell, a Colorado State University alumna, to lead the Federal Emergency Management Administration.

Criswell went to CSU for her undergraduate education; she received a bachelor's degree in technology education. She later earned master's degrees in public administration and security studies from University of Colorado Denver and the **Naval Postgraduate School**, respectively.

20. City Workers Graduate from Highly Competitive Naval Postgraduate School Emergence Program and Executive Leaders Program

(NOLA 4 Feb 21)

The Naval Postgraduate School Center for Homeland Defense and Security (CHDS) will be highlighting two NOHSEP employees for being two of very few who are accepted into this highly competitive program.

21. Plurilock Adds Adm Jan Tighe to Advisory Board

(Yahoo Finance 4 Feb 21)

Retired Vice Admiral has held numerous executive roles in the U.S. Navy and National Security Agency and currently serves on the board of Goldman Sachs… **Dr. Tighe was commissioned as a cryptologist who graduated from the Naval Postgraduate School**, Monterey, California, with a Master of Science in Applied Mathematics and a Doctorate in Electrical Engineering.

22. Wrap Technologies Inc. [WRAP] is 48.24% higher this YTD. Is it still time to buy?

(DBT News 5 Feb 21) … Annabelle Farmer

Wrap Technologies Inc. [NASDAQ: WRAP] price surged by 16.99 percent to reach at $1.04. The company report on January 11, 2021 that Former Police Chiefs Kathleen O'Toole and Sylvia Moir Join WRAP as Senior Advisors… Chief Moir holds a Bachelor of Science in Criminal Justice from California State University, Sacramento, a Master of Arts in Organizational Management, and a Master of Science degree from the **Naval Postgraduate School.**

23. Black History Month Feature: Blacks Walking in Space Victor Glover walks in space this week

(Pride Publishing Group 5 Feb 21) … Cass Teague

In November 2020, NASA astronaut Victor Glover launched on his first spaceflight, becoming the first Black astronaut to live on the International Space Station as part of a long-duration mission. Glover is the first African American ISS Expedition crewmember to live on the ISS, not just visit the ISS for a short stay like on the Space Shuttle as an ISS assembly astronaut, as have most of the 14 other Black Americans NASA has sent to space out of a total of more than 300 NASA astronauts… Glover has three Master of Science degrees: Master of Science in Flight test engineering, Air University (United States Air Force) (USAF TPS), Edwards Air Force Base, California, 2007; Master of Science in Systems Engineering (PD-21), **Naval Postgraduate School**, 2009; and Master of Military Operational Art and Science, Air University (United States Air Force), Montgomery, Alabama, 2010. Glover also completed a Space Systems Certificate from the **Naval Postgraduate School** whilst on deployment, and a Certificate in Legislative Studies at Georgetown University whilst serving as a Legislative Fellow.

TRAINING:

24. Monterey naval installation conducting security drills

(Monterey Herald 5 Feb 21) … Dennis L. Taylor

If anyone in Monterey or Del Rey Oaks has recently seen or heard police sirens entering a naval annex: don't worry, this is just a drill.

Naval Support Activity Monterey this week and next is conducting an annual active shooter training drill at one of its annex locations in Del Rey Oaks. The drill is taking place from its Monterey installation where the **Naval Postgraduate School** is located out to the U.S. Navy's Fleet Numerical Meteorology and Oceanography Center in Del Rey Oaks.

UPCOMING NEWS & EVENTS:

February 9: NWSI Brief on the Tri-Service Strategy and the CNO's NAVPLAN
February 15: Presidents Day
February 16: V-SGL with Dr. William D. Phillips: A New Measure: Quantum Reform of the Metric System

EDUCATION FOR SEAPOWER

SEAPOWER CONVERSATION

Discussing trends, technologies, and tactics that shape modern Seapower

NAVAL WARFARE STUDIES INSTITUTE

Tri-Service Maritime Strategy
"Advantage at Sea"

9 February 2021

1500-1630 PST

The Naval Warfare Studies Institute of the Naval Postgraduate School presents a virtual discussion on the recently issued maritime strategy, *Advantage at Sea*. Hear from U.S. Navy, Marine Corps, and Coast Guard leaders directly involved in the creation of this tri-service strategy that "provides strategic guidance on how the sea services will prevail in day-to-day competition, crisis, and conflict over the next decade". A short discussion will be held followed by audience Q&A.

Speakers:
CAPT Matthew Culp - Naval Strategy OPNAV N7 (USN)
Col Robb Sucher - Plans & Strategy, PP&O, HQMC (USMC)
CDR Kate Higgins-Bloom - Office of Emerging Policy (USCG)

Moderated by:
Col Randy Pugh – NWSI Deputy Director (USMC)
CAPT Dan Sunvold –NWSI Deputy Director (USN)

NPS livestream link: www.nps.edu/web/video

For more information and to submit discussion questions contact Capt Spencer Hayashi – spencer.hayashi@nps.edu

The Naval Postgraduate School proudly presents

THE SECRETARY OF THE NAVY GUEST LECTURE SERIES

In Collaboration With the Naval Education Enterprise

Dr. William D. Phillips

"A New Measure: Quantum Reform of the Metric System"

16 FEBRUARY 1500 (PST)

1997 Nobel Prize in Physics recipient Dr. William D. Phillips is a pioneer and leading researcher in laser cooling and trapping of atoms at the National Institute of Standards and Technology. His fundamental studies were used to develop applications for new kinds of physics measurements and processes such as high resolution spectroscopy, atomic clocks, atomic collisions, atom optics, bio-molecular interactions, and atomic-scale and nano-scale fabrication. Dr. Phillip's research was fund-ed in part by the Office of Naval Research and has yielded many relevant Naval applications, in particular precision timekeep-ing, navigation and quantum information. His current research includes Laser Cooling and Trapping of Neutral Atoms, Atomic-Gas Bose-Einstein Condensates and Quantum Information with Single-Atom Qubits. Read more about Dr. Phillips' Nobel Prize here.

V-SGL series page
www.nps.edu/sgls

Viewing link
www.nps.edu/web/video

NPS
PRAESTANTIA PER SCIENTIAM
1909

TECHNOLOGICAL LEADERSHIP:

Technological Leadership: Combing Research and Education for Advantage at Sea

(USNI Feb 21) ... NPS President retired Vice Adm. Ann E. Rondeau, US Navy

We stand at a critical inflection point. U.S. national security must contend with increasing great power competition (GPC), which is fundamentally an innovation race—one well contested by our near-peer rivals. While technological change is inevitable, the rapidly emerging integration of computational power with its human masters, the so-called Cognitive Age is poised to create unprecedented national security challenges, and at a pace measured in months and not years.

More than just a strategic shift to global hegemonic powers, naval forces must be prepared to compete in the cognitive and conventional arenas: to outthink, outmaneuver, and outfight. To prevail, we must quickly secure technology advantages, as well as the cognitive agility to employ them effectively. This is technological leadership.

Falling behind is an existential risk. Preparing naval leaders for a maritime battlespace rapidly increasing in technical complexity requires integrating the latest science and technology (S&T) research quickly into naval S&T education to simultaneously accelerate solutions and develop leaders with the knowhow to use them. Developing intellectual capital is a critical component of the GPC innovation race.

Education is as vital to seapower as platforms and weapons systems. This was the conclusion of the *Education for Seapower* report published in December 2018, which remains a solid foundation on which to build. The new tri-service maritime strategy, *Advantage at Sea*, goes further, calling on the Navy, Marine Corps, and Coast Guard to prioritize training and education as the first of six lines of effort to create an integrated, all-domain naval force.

For its part, the Department of the Navy (DoN) launched the U.S. Naval Community College, revised Navy and Marine Corps personnel evaluation systems to include education as a promotion criterion, and gave OPNAV N7 oversight of a new Naval Education Enterprise (NEE). The DoN has already taken significant steps to align education and research for seapower within the NEE. These successes must not be end points, but rather building blocks toward a more agile and adaptive tri-service maritime fighting force.

How then do we continue this vital work of accelerating our technological and intellectual advantage at sea? The answer is to fully synchronize advanced naval science, technology, engineering, and math (STEM) education with research in emerging technologies. Tighter coupling of naval research with graduate education will focus, enhance, and accelerate development and delivery of technology applications—from management to warfighting—shaping the future while enhancing the ability of our warriors to use these technologies across the all-domain maritime battlespace.

Naval research and education each temper the other's steel—together they forge superior technology and intellectual prowess to create the cutting edge of decisive capability.

Research + Education = Capability

The bottom line is simple: whoever innovates effectively the fastest wins. This is a technical and intellectual race.

Already, the Naval Research Enterprise (NRE), led by the Office of Naval Research (ONR), is demonstrating ever greater agility by accelerating the transformation of research programs to operational results. Reseach enables technology and provides a hedge against uncertainty.

Yet, technology alone does not assure victory. Superior technology must be combined with the critical thinking of well-educated officers at every echelon to explore new concepts and employ technology to create the decisive edge. Education enables leaders to identify and navigate uncertainty.

Prevailing in great power competition requires the full integration of research and education for advantage at sea. The fact that the Naval Postgraduate School (NPS) is now a chartered member of the Naval R&D Establishment (NR&DE) is testimony to the importance of this partnership. Building on our

history of collaboration in *research* and *education* will accelerate naval innovation and *capability*: **R + E = C**.

Naval Education: Our Cognitive Advantage

Opportunities for innovation abound in every age of acceleration. However, new technology without the intellectual pursuit of education to recognize, analyze, and employ research solutions is the equivalent of a technological edge without a cognitive whetstone.

Take the case of Lieutenant William Sims, a mid-career officer who, at the turn of nineteenth century, designed and introduced continuous-aim firing for naval guns using gears and telescopic sights to compensate for a ship's roll, thus increasing accuracy by 3,000 percent. Decisive as that may sound, Sims' reports were repeatedly disregarded by the Navy's Bureau of Ordnance, citing the technology as "unnecessarily disruptive to the social order of a ship." Without a pathway to cultivating new ideas, skills, and knowledge inside the Navy, Sims' innovation went underutilized and largely ignored.

Exasperated, Sims wrote to President Theodore Roosevelt, who in 1902 circumvented Navy bureaucracy, appointing Sims Inspector of Target Practice to commission and test new gunnery, instilling continuous-aim technology. Sims ultimately retired at the rank of admiral and historian Samuel Eliot Morison credited him as the "the man who taught us how to shoot."

Just a few years later, in June 1909, the record-setting world cruise of the Great White Fleet, which exhibited Sims' technology, provided the strongest evidence yet that science and engineering prowess were of critical importance to naval strength. To sharpen the blade of technological advance, Secretary of the Navy George von L. Meyer signed General Order No. 27 that same year, establishing a graduate-level school of marine engineering at Annapolis, which would later become NPS. Meyer broadened NPS' role in officer graduate studies by directing that ordnance and gunnery electrical engineering, radio telegraphy, naval construction, and civil engineering be added to the curriculum, laying the foundation for NPS to become an innovation hub where officers apply the tools of academic rigor to developing technology solutions.

Naval Research: Cradle of our Technological Advantage

Research and education are two sides of the same capability coin. Smart people conduct research. Application of research develops new technologies to solve problems. The Naval Research Laboratory (NRL) was established in 1923 after the urging of America's greatest inventor, Thomas Edison, who applied his considerable talent during World War I to naval technology, most of which never got past the prototype stage.

Frustrated, but never one to give up, Edison firmly believed in the necessity of a federal research laboratory to produce new ideas and inventions to improve the military. "The Government should maintain a great research laboratory. . . In this could be developed all the technique of military and Naval progression without any vast expense," he remarked in a *New York Times* interview.

NRL played a pivotol role in breakthrough technologies that enabled victory in World War II. After that war, and with the Cold War on the horizon, Congress established the ONR in 1946 to ensure naval leadership in national research and to maintain naval superiority. ONR investments in promising ideas and talented people today convert potential into seapower at NRL, NPS, naval warfare centers across the NR&DE, and at thousands of partner universities, small businesses, and industry connecting the sea services to the energy, creativity, and innovation of the U.S. economy. This connectivity must be leveraged to maximum capacity.

At NPS, naval research and education are uniquely catalyzed in a deliberately diverse military environment combining operational insight, applied research, and interdisciplinary curricula to develop relevant solutions, while advancing mid-career officers' technical proficiency, critical thinking, and leadership ability.

Securing Our Technological Leadership

In this era joining the Cognitive Age and great power competition, peer adversaries have nearly equaled our access to emerging technologies; arguably more as they can reach into U.S. research universities, think tanks, and tech incubators without our reciprocal access.

Research and education at NPS are inseparable—and secure. Every master's student is required to complete an applied research thesis or capstone project to graduate, some classified. Through research conducted alongside expert faculty, their operational experience delivers informed solutions. With proximity to Silicon Valley, and the recently added Central Coast Tech Bridge, NPS also provides officer-students with greater opportunity to enhance their research with the latest technology from civilian industry.

Recognizing its potential to help solve key operational problems, the NPS mission has been revised to reflect this new emphasis and increasing need:

> *"To provide defense-focused graduate education, including classified studies and interdisciplinary research, to advance the operational effectiveness, technological leadership and warfighting advantage of the Naval service."*

The key words "technological leadership" reflect renewed commitment to deliver both research solutions and solution leaders. Put another way, the best translator of operational need to the naval research community is an NPS-educated operator. Students at NPS, a continually refreshed resource, know what matters, and they want to make a difference—for them its personal.

To execute this revised mission, NPS will leverage it strengths: *responsive*, *interdisciplinary*, *applied*, *innovative*, *classified*, and *secure*, to deliver "technological leadership" through three lines of effort:

- First, complex multidisciplinary problems require interdisciplinary solutions. Establishing the Naval Warfare Studies Institute (NWSI) provides a front door to access NPS and coordinates the university's interdisciplinary response to warfighting needs. NWSI is a new and vital link between naval forces, the NR&DE, industry, and the academic/research centers at NPS to conduct concept development, wargaming, experimentation, and analysis as well as rapid prototyping of emerging technology applications—from warfighting to the business of defense.
- Second, innovation at NPS is accelerated by operational insight. As a member of both the NEE and NR&DE, the university will leverage this advantage guiding student-faculty applied research to solve key operational problems. This accelerates DoN competitiveness and returns to the naval forces technology-savvy graduates qualified to employ and advocate for emerging technologies and capabilities.
- Third, STEM-based education at NPS delivers needed future talent. Direct input from end-user students and warfare sponsors continually guides curricula development. NPS will increase our accessibility by leveraging technologies and innovative methods in education and classified capabilities on our secure campus. Already, the faculty are working to enhance distance learning options, create new hybrid, low-residency programs, and offer more professional certificates to advance our military and civilian STEM workforce.

Securing our technological leadership is accelerated through stronger partnerships, such as those between NPS and ONR where there is natural common ground: NPS is education with research, while ONR, as the naval STEM Executive, is research with education.

Research and education are not competing priorities. They are complementary and interdependent at NPS. Only NPS synchronizes graduate education and applied research with student operational experience and faculty expertise to deliver twice the return on education investment: today's innovative solutions, and tomorrow's innovation leaders.

Technological Leadership: A Call to Action

Our maritime advantage is at risk. *Advantage at Sea* will enhance interoperability across the sea services, and education must play an increasing and key role in generating unity of effort.

Critical technologies are within the reach of our competitors. To prevail for good in this Cogntive Age of great power competition, we must set the innovation pace, foster agility, and be a principal partner in the national innovation ecosystem. Compared with the Cold War era, the Cognitive Age is more about capability over capacity.

The advantage in this race will go to whomever is first-to-field; yet, technological leadership is more than being first in technology. Bold thinking and innovative leaders with mastery, commitment, and courage are essential.

Our decisive edge requires long-term investment and support for naval research and high-quality STEM education of our officers and workforce. NPS is the catalyst for this ciritical fusion and is a competitive advantage for our Naval forces and nation. When fully optimized as DoN's graduate university for applied research, NPS offers a winning formula to accelerate our advantage at sea: **R + E = C**.

Research drives technological advantage. Education drives intellectual dominance. Together they deliver technological leadership for a decisive, integrated, all-domain naval force.

https://www.usni.org/magazines/proceedings/2021/february/technological-leadership-combining-research-and-education

Return to Index

RESEARCH:

Xerox and Naval Postgraduate School Announce Collaboration to Advance Solutions with 3D Printing Research

(NPS.edu 3 Feb 21) ... NPS Office of University Communications
(Navy.mil 3 Feb 21) ... NPS Office of University Communications
(Business Wire 3 Feb 21)
(Odessa America 3 Feb 21)
(TCT Magazine 3 Feb 21) ... Sam Davies
(Popular Science 3 Feb 21) ... Rob Verger
(3D Printing Media 4 Feb 21) ... Davide Sher
(Metal AM 4 Feb 21)
(ExecutiveBiz 4 Feb 21) ... Nichols Martin
(West Fair Online 5 Feb 21) ... Phil Hall

Xerox and the Naval Postgraduate School (NPS) announced today a strategic collaboration focused on advancing additive manufacturing research, specifically 3D printing, which has the potential to dramatically transform the way the military supplies its forward-deployed forces.

As part of a Collaborative Research and Development Agreement (CRADA), NPS was the first to receive an installation of the Xerox ElemX™ Liquid Metal Printer on the university campus in December. The Xerox solution will provide NPS faculty and students with hands-on exploration of new ways the technology can deliver on-demand 3D printing of metal parts and equipment.

"The military supply chain is among the most complex in the world, and NPS understands first-hand the challenges manufacturers must address," said Xerox Chief Technology Officer Naresh Shanker. "This collaboration will aid NPS in pushing adoption of 3D printing throughout the U.S. Navy, and will provide Xerox valuable information to help deliver supply chain flexibility and resiliency to future customers."

With access to the latest additive manufacturing equipment, NPS faculty and students will use the ElemX printer to conduct thesis research to develop new capabilities for the Navy and Marine Corps.

"As the Department of the Navy's applied research university, NPS combines student operational experience with education and research to deliver innovative capabilities and develop innovative leaders with the knowhow to use them," said NPS President retired Vice Adm. Ann Rondeau. "This collaborative research effort with Xerox and the use of their 3D printing innovations is a great example of how NPS

uniquely prepares our military students to examine novel approaches to create, make, prototype and manufacture capability wherever they are."

"From the age of sail to the nuclear era, sailors have been fixing things at sea so they can complete the mission," she continued. "This partnership is about the strategic ability of the Navy to have sailors on ships with the capability through creativity and technology to advance their operations at sea. Through collaboration, NPS and Xerox are helping build a Navy for the 21st Century."

The Xerox ElemX printer uses cost-effective aluminum wire to fabricate end-use parts that can withstand the rigors of operational demands. This ability to produce reliable replacement parts on-demand reduces the dependency on complex global supply chains for deployed forces and also addresses the hidden costs of traditional manufacturing.

"The NPS Alumni Association and Foundation supported bringing the ElemX liquid metal printer to NPS because it will enable soldiers, sailors, airmen, and marines to solve their problems where they are, when problems occur," noted retired U.S. Marine Corps Col. Todd Lyons, vice president of the NPS Alumni Association and Foundation. "By providing the right digital tools and the liquid metal printer, all of a sudden we've helped transform not just the supply chain, but how the Department of Defense (DoD) thinks operationally about supplying war."

"This is one way to bend the cost curve so that the DoD is not spending a thousand dollars for every dollar that a peer competitor spends," he added.

"Global supply chains leave industries like aerospace, automotive, heavy equipment, and oil and gas vulnerable to external risks," said Tali Rosman, vice president and general manager, 3D Printing, Xerox. "Our goal is to integrate localized 3D printing into their operations, and the real-time feedback from NPS gives us actionable data to continuously improve the ElemX."

The Collaborative Research and Development Agreement (CRADA) does not imply endorsement of Xerox or its products by the Naval Postgraduate School, the Department of the Navy, or the Department of Defense.

Mission of the Naval Postgraduate School

The Naval Postgraduate School provides defense-focused graduate education, including classified studies and interdisciplinary research, to advance the operational effectiveness, technological leadership and warfighting advantage of the Naval service. For additional information, visit the university online at http://www.nps.edu.

https://nps.edu/-/xerox-nps-announce-collaboration-to-advance-solutions-with-3d-printing-research

https://www.navy.mil/Press-Office/News-Stories/Article/2491871/xerox-nps-announce-collaboration-to-advance-solutions-with-3d-printing-research/

Xerox and Naval Postgraduate School Announce Collaboration to Advance Solutions with 3D Printing Research | Business Wire

Xerox and Naval Postgraduate School Announce Collaboration to Advance Solutions with 3D Printing Research - Odessa American: Business (oaoa.com)

Xerox ElemX Liquid Metal Printer to be used by Naval Postgraduate School in US military research efforts - TCT Magazine

ElemX, Xerox's liquid metal 3D printer now has a name » 3dpbm (3dprintingmedia.network)

Xerox installs first ElemX Liquid Metal Additive Manufacturing machine (metal-am.com)

Xerox 3D Printer to Support Manufacturing Research at Naval Postgraduate School | ExecutiveBiz

Xerox partners with U.S. Navy on military-focused 3D printing research - Westfair Communications (westfaironline.com)

Return to Index

This huge Xerox printer can create metal parts for the US Navy

(Popular Science 3 Feb 21) ... Rob Verger

Xerox's new printer is 9 feet wide, 7 feet tall, and reaches an internal temperature of more than 1,500 degrees Fahrenheit. It's not an inkjet, of course—it's a 3D printer that can produce bespoke metal components. The Naval Postgraduate School, a grad institution for Naval officers and others, is the first place to put one of these massive Xerox machines into service.

Aluminum wire is the base material that the printer, the ElemX, uses to create metal parts. It's like a tiny aluminum foundry in a machine that might someday find a home on a ship out at sea, where the ability to create a custom aluminum part that's strong and light could come in handy. "Aluminum is very resistant to oxidation and corrosion," explains I. Emre Gunduz, an associate professor of mechanical and aerospace engineering department at the Naval Postgraduate School. "In maritime environments, that's a very significant factor."

While the Navy clearly couldn't use it for large jobs—it won't print a torpedo any time soon—it may be a good solution for small problems that need a durable part. "There are many bits and pieces on a ship and a submarine," Gunduz adds.

The liquid metal printer works by starting with a spool of aluminum wire. "We melt the wire, and then, in the liquid form, we jet droplets of aluminum, drop by drop, layer by layer, building the part," explains Tali Rosman, vice president and general manager for 3D printing at Xerox.

Most commercial 3D metal printing requires powders, which can pose an "explosion risk," Rosman says. That means that the common aluminum wire required for the Xerox contraption is a better, safer fit for a Naval ship. Plus, metal powders also can present a "breathing hazard," Gunduz points out. In the tight environments of a ship or sub, wire makes more sense.

Right now, the printer is on land at the Naval Postgraduate School in Monterey, California, and Gunduz says they need to do further research before a machine like it would be deployed at sea. "There are certain considerations, like vibrations, and shaking, and things like that—those are the things that we need to evaluate before we can put it on a ship," he says.

The widgets and gizmos it prints can have a volume of about 12 inches by 12 inches by 5 inches, and the length of time it takes to produce a metal piece varies. The printer may need about 3 to 4 hours for a "nice-size part," Rosman says, but littler items "would be much faster."

This huge Xerox printer can create metal parts for the US Navy | Popular Science (popsci.com)

Return to Index

NPS-Led Research Reveals Greater Abundance of Life Under Arctic Ice Than Previously Thought

(NPS.edu 2 Feb 21) … Rebecca Hoag
(Navy.mil 2 Feb 21) … Rebecca Hoag

For the longest time, scientists have written off there being much life below the Arctic sea ice. Surely not enough sunlight would be able to get through the snow and ice to sustain an abundance of life. Additionally, satellites can't see through the ice, and it was difficult for scientists interested in investigating this further to get out to the Arctic during the winter and spring – when the percent of Arctic ocean iced over was the highest – because most Arctic expeditions wait until there's thinner ice so icebreakers can move through.

According to the Department of the Navy's recently-published Arctic Strategy, "Progress is not possible without pushing the boundaries of science and technology." And an innovative research effort funded by the National Science Foundation and U.S. Dept. of Energy, led by researchers at the Naval Postgraduate School (NPS), is definitely pushing the boundaries of those long-held assumptions about just how much life is under the Arctic ice.

Researchers at NPS have a long history of innovative research in the Arctic and Antarctic regions. University faculty were direct contributors to the Navy's Arctic Road Map released in 2014, students are

frequent participants in the Navy's ICEX exercise, and several faculty have partnered with the Office of Naval Research on a wide range of research projects.

Employing innovation and advanced computer modeling techniques, an NPS research team led by Oceanography Professors Jaclyn Clement Kinney and Wieslaw Maslowski modeled Arctic under-ice primary production from 1980 to 2018. The results of their effort showed a greater abundance of life under Arctic ice than previously thought, mostly in the form of single-cell plants (or phytoplankton) called diatoms. Their findings were published in the *Journal of Geophysical Research - Oceans* in August 2020.

The team, including NPS professor Younjoo Lee, former NPS post-doc Marina Frants, and several outside collaborators, modeled what is most likely under the ice bio-physical environment. They then compared their model's results with actual data provided by the few excursions who did get samples. (Scientists estimate phytoplankton based on the level of chlorophyll-*a* in the water.)

"It's really quite a simple idea and sometimes, I think, the best science ideas are simple and straightforward," Kinney says.

The idea might have been simple, but the implementation was anything but. It took a multi-institutional team and years of research time to develop, evaluate and tune the model, the Regional Arctic System Model (RASM). RASM has been designed and used to simulate "the physical and biogeochemical environments at high-resolution over multi-decadal time scales," according to Maslowski.

Among its many applications, the model has been used to replicate phytoplankton blooms under the ice, and how these blooms have changed seasonally and interannually. Such a research program required large allotments of high-performance computing resources, which were competitively secured through the DOD's High-Performance Computing Modernization Program (HPCMP).

Their model's results matched well with limited data collected in different parts of the Arctic … There is more life tingling under the ice than previously thought. The study found the majority of Arctic pelagic primary production takes place in areas at least half covered with ice. Unsurprisingly, the plankton population is at its peak during the summer when the Arctic experiences the most sunlight and nutrients are still abundant.

The model also found that under-ice primary productivity has increased over the past decades. Kinney concludes this is most likely the result of an increase in the photosynthetically active radiation in the water driven by changes in surface reflectivity from the thinning ice and melting of snow on the ice.

Scientists are also interested in the bountifulness of these microscopic plants because ocean phytoplankton are the base of the food chain and make up about half of the Earth's natural carbon drawdown (how much carbon dioxide the planet can store).

"We need to understand the rate of carbon uptake and its total budget in the Arctic to diagnose its change and trends, as well as its contribution to and impact on global warming," Maslowski explains.

The team hopes this research could lead to more predictive capabilities into the Arctic's biogeochemical and physical environments, including prediction of snow and sea ice melt and open water phytoplankton blooms.

https://nps.edu/-/nps-led-research-reveals-greater-abundance-of-life-under-arctic-ice-than-previously-thought

https://www.navy.mil/Press-Office/News-Stories/Article/2494170/nps-led-research-reveals-greater-abundance-of-life-under-arctic-ice-than-previo/

Return to Index

Technology Sector Update: SNE,XRX,SMCI,GOOG,GOOGL

(Nasdaq 3 Feb 21) … MT News Wires

Technology stocks was hanging on for a narrow increase, giving back earlier gains led by Google parent company Alphabet (GOOG,GOOGL) reaching a new record high after reporting Q4 earnings and

revenue topping analyst estimates. At last look, the SPDR Technology Select Sector ETF was rising 0.1% although the Philadelphia Semiconductor Index was sinking 1.6% this afternoon.

In company news, Sony (SNE) Wednesday hit its best share price in 21 years, topping out with a more than 11% gain at $110.60 after the consumer electronics giant reported fiscal Q3 results exceeding Wall Street expectations and also raised its FY21 revenue forecast. It is now projecting JPY8.8 trillion in sales and operating revenue for the 12 months ending March 31, up from its prior outlook expecting JPY8.5 trillion and beating the Capital IQ consensus looking for JPY8.667 trillion in FY21 sales.

Xerox (XRX) climbed 4.4% after Wednesday announcing a strategic collaboration agreement with the **Naval Postgraduate School** to work on 3-D printing and manufacturing research. As part of the deal, Xerox in December installed one of its first ElemX liquid-metal printer at the Monterey, Calif., campus, providing students and faculty with hands-on experience with on-demand 3D printing of metal parts and equipment.

Super Micro Computer (SMCI) rose 4.2% after reporting better-than-expected results for its fiscal Q2 ended Dec. 31 and projected non-GAAP net income and revenue for the current quarter also topping analyst estimates in addition to authorizing a new, $200 million stock buyback program running through July 2022. The storage and server technology company late Tuesday also promoted chief compliance officer David Weigand to succeed Kevin Bauer as chief financial officer after steps down on Feb. 28.

Technology Sector Update for 02/03/2021: SNE,XRX,SMCI,GOOG,GOOGL | Nasdaq

Return to Index

GSA: taking advantage of industry with its ML & AI RFIs

(Spend Matters 5 Feb 21) … Nancy Cinton

Based on a **Naval Postgraduate** report from March 2019, companies spend over 1400 hours each year replying to government RFIs. If you do the calculation, even the most basic labor rates, and the annual economic cost of this transfer of effort approaches one million dollars. As a former contracting officer, Frank McNally of Public Spend Forum has mixed feelings about RFIs. On one hand, companies that want to win lucrative contracts should expect some degree of effort, and RFIs can be an effective tool for both parties. On the other hand, it's expensive to bid on government contracts and when we transfer the market research effort to contractors, we're adding overhead that just gets passed back to government. Market research is a time-consuming chore, hunting down supplier info on myriad public sector databases isn't how anyone wants to spend their time. So Frank explains how they created GovShop to consolidate all those sites and provide government contracting professionals with a "high resolution view" of a supplier's capability and key demographic data.

Public Spend Forum: ML & AI RFIs and Ravens on Mars (spendmatters.com)

Return to Index

GREAT POWER COMPETITION:

Former Strategic Command, Pacific Fleet Commander Talks Great Power Competition in Guest Lecture

(Defence Connect 4 Feb 21) … Stephen Kuper

(Navy.mil 2 Feb 21) … Mass Communication Specialist 2nd Class Taylor Vencill

Naval Postgraduate School (NPS) distinguished alumnus retired U.S. Navy Adm. Cecil D. Haney, former Commander, U.S. Strategic Command, spoke virtually to Naval Postgraduate School (NPS) faculty, staff and students on the topic of "Great Power Competition (GPC) in the Cognitive Age" during the latest edition of the Secretary of the Navy Guest Lecture (SGL) series, Jan. 26.

Naval Postgraduate School (NPS) distinguished alumnus retired U.S. Navy Adm. Cecil D. Haney, former Commander, U.S. Strategic Command, spoke virtually to Naval Postgraduate School (NPS)

faculty, staff and students on the topic of "Great Power Competition (GPC) in the Cognitive Age" during the latest edition of the Secretary of the Navy Guest Lecture (SGL) series, Jan. 26.

Haney explored the strategic objectives of China and Russia – peer competitors of the U.S.– and why there must be a continued emphasis on strategic deterrence. Due to the recently published Tri-Service Maritime Strategy, which aligns the U.S. Navy, Marine Corps and Coast Guard to achieve an "advantage at sea" over China and Russia, Haney's guest lecture is another example of NPS fostering cognitive and intellectual advantage by discussing the strategies, problem sets and potential solutions associated with Great Power Competition.

"The global security environment today is more complex, dynamic and volatile than at any other time in our history," noted Haney. "We must take advantage of the Naval Postgraduate School environment to expand your knowledge of the competitor nations, their culture, their perspective, their ideology, and their objectives, holistically. The dangers presented by this unpredictable security environment are compounded by the continued propagation of asymmetric methods, unprecedented proliferation of advancing technologies, and the dual use nature of the acceleration of technical development outside normal national security channels in the commercial and academic circles."

"Now Russia and China are investing in long term military modernization programs that could pose an existential threat to the United States," continued Haney. "Russia seeks to reassert itself as a great power and at the cost of its neighbors and regional stability. Even with its strained economy, Russia continues to modernize its triad of nuclear forces while China is pursuing regional dominance in the East and South China Seas and also continues to make significant military investments to its nuclear and conventional capabilities."

With these existential threats in mind, Haney stressed the familiar concept of deterrence. He suggested that we master deterrence to ensure no adversary is able to escalate their way out of a failed conflict and they understand that we can and will, if necessary, respond in a time, place and manner of our choosing.

"Deterrence is fundamentally a human endeavor, firmly rooted in psychology and social behavior," said Haney. "The first is an aggressor's recognition that unacceptable costs may be imposed for taking an action, and recognition that foregoing this action may result in lesser costs. The second is an aggressor's belief that the contemplated action will not produce its perceived benefit, or that not acting will produce a greater benefit."

Put another way, deterrence is creating a risk to our adversaries that is not worth any potential gain by aggressive actions.

"Today, as we craft meaningful strategic and operational plans and carry out strategic operations, the key to deterrence is maximizing leadership decision space, particularly that of the President of the United States," said Haney.

He went on to explain that this requires timely intelligence, command and control to move information to decision makers, synthesis of dedicated sensors, and a robust combination of missile defense, conventional forces, cyberspace architecture and credible nuclear weapons that inform polices, treaties and plans that link and knit organizations and capabilities together that provide leaders with options.

"Taken together this deterrent capability must ensure that even in crisis, strategic stability will remain intact and ensure that any adversary understands they will not get the benefits they seek and the cost will be too much to bear if they employ nuclear weapons."

After his prepared remarks, Haney spent time answering a series of questions from NPS students from the Navy, Marine Corps and Air Force – who asked about increasing partnerships at strategic choke points, adversaries weaponizing information on a strategic scale, and using artificial intelligence to augment sensors.

The cognitive aptitude of the students did not disappoint Haney.

"The Naval Postgraduate School and advanced education is so important now, and in the future," said Haney. "[NPS] develops the critical thinkers in so many areas, and develops new concept of operations and capabilities to address the threats in this 21st century in a collaborative and free-thinking way."

Following the lecture, Haney joined NPS President retired Vice Adm. Ann Rondeau to induct retired Vice Adm. Edward Moore Jr. into the university's prestigious Hall of Fame (HOF) during a virtual induction ceremony. Moore was a trailblazer who at the time of his retirement in 2001 was the highest-ranking black officer in the Navy.

"What a remarkable individual," Haney said of Moore. "He is just so deserving of this Hall of Fame recognition. It's just great to know such a remarkable individual that paved the way for so many others."

For more discussion on Great Power Competition (GPC), tune in to the latest episode of the NPS' video series – Listen, Learn, Lead – with university President retired Vice Adm. Ann E. Rondeau. In the episode, GPC experts Drs. Robert Tomlinson and Jim Wirtz hold a robust discussion on key factors leading to peer power competition, and discuss GPC in the context of the new Tri-Service Maritime Strategy.

The university has also launched a number of GPC-focused educational initiatives, including a seminar course and multiple graduate certificate programs, with more planned offerings in development.

Former Strategic Command, Pacific Fleet Commander Talks Great Power Competition in Guest Lecture > United States Navy > News-Stories

Former US STRATCOM, Pacific Fleet commander details challenges of Great Power competition - Defence Connect

Return to Index

EDUCATION:

NPS Regional Security Program Prepares Deploying Forces, Surpasses Milestone

(NPS.edu 5 Feb 21) … Mass Communication Specialist 3rd Class James Norket
(Navy.mil 5 Feb 21) … Mass Communication Specialist 3rd Class James Norket

For more than two decades, the Naval Postgraduate School's (NPS) Regional Security Education Program (RSEP) has provided leading subject matter experts to deploying forces in transit delivering on-site, graduate-level briefings on regional issues and challenges, historical and security context, and cultural sensitivities in Combatant Commanders Areas of Responsibility (AOR's) and regions where our forces will operate. From carrier strike groups to SEAL teams, the RSEP program has delivered briefings and critical lectures to more than 500,000 Department of Defense participants worldwide as well as international allies and partners operating with our deployed Naval Forces.

The program was created in the aftermath of the events on Oct. 12, 2000 – a date that many Sailors will never forget. On that day, the USS Cole (DDG 67) docked in Aden, Yemen for a routine fuel stop. Not long after mooring, a small fiberglass boat carrying C4 struck the side of the ship, creating a 40-by-60-foot gash in the hull, killing 17 Sailors and wounding 37 others. The attackers were later identified as part of the terrorist organization al-Qaeda.

Then Chief of Naval Operations (CNO) Adm. Vern Clark asked all of his flag officers in the fleet how they could prevent anything like this from ever happening again. The Naval Postgraduate School had an answer: RSEP.

"When we first started the program in 2001, almost nobody could even spell al-Qaeda," said retired Rear Adm. Steve Loeffler, fleet operations director for RSEP. "Now it is the life's work of our professors and subject matter experts to be well informed on every issue, challenge and threat imaginable in their areas of expertise and deliver that knowledge to our deploying forces."

As for today's era, the recently published Tri-Service Maritime Strategy, which aligns the U.S. Navy, Marine Corps and Coast Guard to achieve "advantage at sea," and the recently announced CNO NAVPLAN, calls for the Navy to contribute to regional security, and operate interchangeably with key allies and partners, are both necessary to attaining that advantage at sea.

Supporting these strategies, NPS has a network of 350 subject matter experts from across the country who specialize in different regions of the world. Dr. Wade Huntley, academic director for RSEP, is responsible for assembling the right group of people to brief deploying units.

"The program is there to support the interest of deploying Naval forces," said Huntley. "Regardless of where the unit is heading, we will have a team ready to tell them everything they need to know about their area of operations."

For example, RSEP has become a mainstay of "Academic Week" for deploying SEAL Teams. Whether teams need briefings on ISIS/al-Qaeda operations and other terror networks in the Middle East and North Africa, or Great Power Competition between nations in certain regions, or U.S. bilateral agreements in Southeast Asia and the South Pacific, RSEP will focus the discussion on where each force element will deploy.

"This is what we do," said Huntley. "We create briefs about potential threats and regional challenges in areas of operations and provide them to anyone who will listen. We want our fleet to be prepared for anything."

In a pre-COVID environment, the RSEP team would create dozens of briefs and then travel with deploying units and inform senior enlisted and officers on regional issues and challenges in the area of operations during their deployments.

"When we go aboard a ship, we might have a list of between 25-40 briefs that we offer and then we try to give all of those briefs over the course of their transits," Loeffler explained. "During that course of time we would have given literally each of the lectures probably 5-10 times. We want to make sure they are prepared to accomplish the mission at hand."

COVID-19 has certainly had an impact on how RSEP accomplishes its mission. While unable to travel with deploying units due to COVID-19, the team now prepares dozens of briefings and pre-recorded lecture videos that they send out and let the commanders, Sailors and Marines aboard organize the briefs. Recent feedback from deployed strike groups, cruisers, destroyers and amphibious ships has been very positive as they use RSEP DVD's to educate and train Sailors and Marines of all paygrades. Similarly, symmetric briefs via collaboration tools with Selective Reserve units from around the fleet have resulted in comments such as, "Best drill weekend in years!"

"RSEP is the greatest and largest outreach program that NPS has ever had," Loeffler noted. "Not only are we educating the fleet, but we are getting the word out about how important NPS really is to the Navy and Marine Corps."

https://nps.edu/-/nps-regional-security-program-prepares-deploying-forces-surpasses-milestone
https://www.navy.mil/Press-Office/News-Stories/Article/2495818/nps-regional-security-program-prepares-deploying-forces-surpasses-milestone/

Return to Index

CYBERSECURITY:

The U.S. Spent $2.2 Million on a Cybersecurity System That Wasn't Implemented and Might Have Stopped a Major Hack

(Spend Matters 2 Feb 21) … Peter Elkind and Jack Gillum

As America struggles to assess the damage from the devastating SolarWinds cyberattack discovered in December, ProPublica has learned of a promising defense that could shore up the vulnerability the hackers exploited: a system the federal government funded but has never required its vendors to use.

The massive breach, which U.S. intelligence agencies say was "likely Russian in origin," penetrated the computer systems of critical federal agencies, including the Department of Homeland Security, the Treasury Department, the National Institutes of Health and the Department of Justice, as well as a number of Fortune 500 corporations. The hackers remained undetected, free to forage, for

Bottom of Form

The hackers infiltrated the systems by inserting malware into routine software updates that SolarWinds sent to customers to install on its products, which are used to monitor internal computer networks. Software updates customarily add new features, remove bugs and boost security. But in this instance, the hackers commandeered the process by slipping in malicious code, creating secret portals (called "back doors") that granted them access to an untold bounty of government and company secrets.

The incursion became the latest — and, it appears, by far the worst — in a string of hacks targeting the software supply chain. Cybersecurity experts have voiced concern for years that existing defenses, which focus on attacks against individual end users, fail to spot malware planted in downloads from trusted software suppliers. Such attacks are especially worrisome because of their ability to rapidly distribute malicious computer code to tens of thousands of unwitting customers.

This problem spurred development of a new approach, backed by $2.2 million in federal grants and available for free, aimed at providing end-to-end protection for the entire software supply pipeline. Named in-toto (Latin for "as a whole"), it is the work of a team of academics led by Justin Cappos, an associate computer science and engineering professor at New York University. Cappos, 43, has made securing the software supply chain his life's work. In 2013, Popular Science named him as one of its "Brilliant Ten" scientists under 40.

Cappos and his colleagues believe that the in-toto system, if widely deployed, could have blocked or minimized the damage from the SolarWinds attack. But that didn't happen: The federal government has taken no steps to require its software vendors, such as SolarWinds, to adopt it. Indeed, no government agency has even inquired about it, according to Cappos.

"In security, you almost never go from making something possible to impossible," Cappos told ProPublica, during two video interviews from Shanghai, where he is teaching. "You go from making it easy to making it hard. We would have made it much harder for the [SolarWinds] attackers, and most likely would have stopped the attack." Although the SolarWinds breach was a "really sneaky" approach, Cappos said, "in-toto definitely can protect against this. It's very possible to catch it."

In-toto's system has supporters among experts in the government and corporations. When ProPublica asked Robert Beverly, who oversees in-toto's federal grant as a program director at the National Science Foundation, whether using in-toto could have saved the government from the hack, he replied, "Absolutely. There seems to be some strong evidence that had some of the, or all of the, in-toto technologies been in place, this would have been mitigated to some extent." Beverly, whose NSF responsibilities include "cybersecurity innovation for cyberinfrastructure" and who is on leave from his post as a computer science professor at the **Naval Postgraduate School,** added that it's impossible to know for sure what impact in-toto would have had, and that the system remains at an early stage of adoption. "Unfortunately," said Beverly, "it often takes some of these kinds of events to convince people to use these kinds of technologies."

Some companies have embraced in-toto, and others, like Microsoft, have expressed interest. "I am a big fan of in-toto," Kay Williams, head of Microsoft's initiatives in open source and supply-chain security, said in an email to ProPublica. A second Microsoft program manager, Ralph Squillace, praised in-toto in a recent NYU press release for applying "precisely to the problems of supply chain confidence the community expects distributed applications to have in the real world." (After Williams' initial response, Microsoft declined to comment further.)

One senator blasted the government's failure to use a system it paid for. "The U.S. government invested millions of dollars in developing technology that can protect against this threat, and while several large technology companies have already adopted it, they are the exception," said Sen. Ron Wyden, D-Ore., a member of the Senate Intelligence Committee. "The government can speed up industry adoption of this best practice by requiring every government contractor to implement the best available technology to protect their supply chains."

The in-toto system requires software vendors to map out their process for assembling computer code that will be sent to customers, and it records what's done at each step along the way. It then verifies electronically that no hacker has inserted something in between steps. Immediately before installation, a pre-installed tool automatically runs a final check to make sure that what the customer received matches

the final product the software vendor generated for delivery, confirming that it wasn't tampered with in transit.

Cappos and a team of colleagues have worked to develop the in-toto approach for years. It's been up and running since 2018. The project received a three-year grant from the National Science Foundation that year, aimed at promoting "widespread practical use" of in-toto. (Later in 2018, President Donald Trump signed the Federal Acquisition Supply Chain Security Act, aimed at protecting government secrets from software supply-chain threats.)

In-toto could block and reveal countless cyberattacks that currently go undetected, according to Cappos, whose team includes Santiago Torres-Arias, an assistant electrical and computer engineering professor at Purdue University, and Reza Curtmola, co-director of the New Jersey Institute of Technology's Cybersecurity Research Center. In an August 2019 paper and presentation to the USENIX computer conference, titled "in-toto: Providing farm-to-table guarantees for bits and bytes," Cappos' team reported studying 30 major supply-chain breaches dating back to 2010. In-toto, they concluded, would have prevented between 83% and 100% of those attacks.

"It's available to everyone for free, paid for by the government, and should be used by everyone," said Cappos. "People may still be able to break in and try to hack around it. But this is a necessary first step and will catch a ton of these things." The slow pace of adoption is "really disappointing," Cappos added. "In the long game, we'll win. I just don't know that we want to go through the pain that it'll take for everyone to wise up."

One of in-toto's earliest adopters, starting in 2018, was Datadog, a SolarWinds competitor that provides monitoring software for internet cloud applications. Now a publicly traded company with 2020 revenues of nearly $600 million, its customers include Nasdaq, Whole Foods and Samsung. Datadog uses in-toto to protect the security of its software updates. In an NYU press release, Datadog staff security engineer Trishank Kuppusamy, who worked on the program's design and implementation, said that what distinguishes in-toto is that it "has been designed against a very strong threat model that includes nation-state attackers." (Datadog did not reply to ProPublica's requests for comment.)

The General Services Administration, which provides access to software for federal government agencies, still lists SolarWinds products available for purchase. But it said in a statement that "compromised versions" of SolarWinds programs identified by DHS are no longer available.

SolarWinds itself declined to weigh in on whether its hack could have been prevented. "We are not going to speculate on in-toto and its capabilities," a spokesman said in an emailed statement. "We are focused on protecting our customers, hardening our security and collaborating with the industry to understand the attack and prevent similar attacks in the future."

Previously little known to the general public, SolarWinds is a public company based in Austin, Texas, with projected 2020 revenues of just over $1 billion. It boasts of providing software to 320,000 customers in 199 countries, including 499 of the Fortune 500 companies. In a recent SEC filing, the company said its flagship Orion products, the vehicle for the cyberattack, provide about 45% of its revenues. A SolarWinds slogan: "We make IT look easy."

After the hack was discovered, SolarWinds' stock plunged, and it is now facing shareholder lawsuits. The company has shifted aggressively into damage-control mode, hiring CrowdStrike, a top cybersecurity firm; elite Washington lobbyists; a crisis-communications advisor; and the newly formed consulting team of Christopher Krebs, the former director of the Cybersecurity and Infrastructure Security Agency (who was famously fired for contradicting Trump's claims of mass voting fraud) and Alex Stamos, former security chief at Facebook.

News of what's now known as the SolarWinds attack first came on Dec. 8. That's when FireEye, perhaps the nation's preeminent hack-hunter, announced that it had itself fallen victim to a "highly sophisticated state-sponsored adversary" that had broken into its servers and stolen its "Red Team tools," which FireEye uses to try to hack into the computer networks of its clients as a test of their cyber-defenses. FireEye soon discovered the attackers had gained access through corrupted updates to the SolarWinds Orion network-monitoring software that it used.

On the evening of Dec. 13, CISA issued an emergency directive, identifying SolarWinds as ground zero for the hack and alerting federal agencies using Orion products to disconnect them immediately.

Over the following weeks, investigators discovered that SolarWinds had been targeted back in early September 2019, when hackers started testing their ability to inject code into its software updates. After remaining undetected for months, they inserted malware in new updates between February and June 2020. SolarWinds estimated these infected updates affected "fewer than 18,000 of its customers."

Precisely what the hackers saw, and stole, has yet to be determined and is under investigation. But the full impact of the breach is becoming clearer, as we now know it touches several tech companies, including Microsoft. The software giant has also labored to limit the damage by helping seize an internet domain in the U.S. that the hackers used to siphon data from some SolarWinds customers.

Stamos told the Financial Times, in an interview after being hired to help SolarWinds, that he believed the attackers had embedded hidden code that would continue to give them access to companies and government agencies for years. He compared the situation to Belgian and French farmers going out into their fields where two world wars were fought and discovering an "iron harvest" of unexploded ordnance each spring.

Dmitri Alperovitch, who co-founded CrowdStrike (the cybersecurity firm SolarWinds has hired to investigate the hack) before leaving last year to start a nonprofit policy group, said he thinks that, in theory, the in-toto system could work. But he warned that software is so complex, with many products and companies in the supply chain, that no one defense is a panacea. Still, he agrees that in-toto could provide protection, and said "it's always a good thing to have more protection for supply chains."

Russian intelligence services have clearly identified supply-chain attacks "as a much better way to get in," offering "a much bigger set of targets," Alperovitch said. "This is an indictment of the entire cybersecurity industry, as well as the intelligence community, that they were able to orchestrate such a broad, sweeping attack right under our noses."

https://www.propublica.org/article/solarwinds-cybersecurity-system

Return to Index

We can make software secure, but not at a price you'd be willing to pay

(Tech Beacon 2 Feb 21)

The recent compromise of SolarWinds' Orion software has led to lots of largely ineffective hand-wringing. I've seen more time spent on talking about whom should be blamed for the incident than on how to mitigate the damage that it caused or to reduce the chances of a similar incident happening in the future.

But it has motivated the creation of lots of new initiatives to increase the security of software by adding all sorts of additional processes and oversight to software engineering organizations. These efforts might provide some small, incremental gains in the security of software, but they are probably doomed to do little more than that.

Security of code simply isn't a priority for some developers, and it's going to be very hard to change that for much of the software currently in use. And it's probably the case that even the most careful and thorough software security engineering practices are not going to produce secure commercial software. Here's why.

The problem with FOSS

Free and open-source software (FOSS) is here to stay. Although most FOSS projects don't go anywhere, those that do can end up making a huge difference. Lots of the Internet now runs on the FOSS LAMP stack—the Linux operating system, the Apache web server, the MySQL database, and the PHP programming language. Commercial alternatives for each of these exist, but they have yet to gain the level of acceptance and use that their FOSS competitors have. Similarly, FOSS components are part of essentially all commercial software these days.

It isn't easy for software companies to get their developers to take software security seriously. My experience has been that it takes a significant effort backed by the highest levels of management to get this to happen. But it has happened in some places, and the quality of software has dramatically increased in many cases because of these efforts.

But it seems to be much harder to get FOSS contributors to take security seriously. The Linux Foundation's recent 2020 FOSS Contributor Survey suggests that FOSS programmers just aren't that interested in security. Instead, things such as learning new things and gaining the respect of their peers motivate them. They spend less than 3% of their time responding to security issues. And some of their responses to the survey suggest that it's going to be very hard to get them to take security more seriously.

Text responses indicated that many respondents had no interest in increasing time and effort on security; it was not simply that they wanted to be proactive. One respondent said, "I find the enterprise of security a soul-withering chore and a subject best left for the lawyers and process freaks. I am an application developer." Another said, "I find security an insufferably boring procedural hindrance."

So with a significant amount of software that's being used today using FOSS in some way, it seems likely that we'll be dealing with the security issues that come with it for the foreseeable future.

The problem with software

But the security issues with software aren't limited to FOSS. Those related to FOSS are probably just harder to manage (and FOSS programmers may be more honest about how they feel about security).

I routinely do things that definitely qualify as insufferably boring procedural hindrances, but I do them because it's part of my job. I can't just decide to not do them because I don't feel like doing them, but that's an option that FOSS developers have, and some seem to take advantage of this.

It's hard to fault them. If I wasn't getting paid to do my job, I'd be avoiding insufferable procedural hindrances, too. Unfortunately, it looks as if security might be getting less attention than some people might like it to because of that.

But it may be impossible to make any form of software reasonably secure, at least in a commercially acceptable way.

Modern software is probably the most complex thing ever created by man. Getting something that complex to work is hard. Try understanding the build process for your typical enterprise software these days and you'll be surprised that we can even get the stuff to work at all. Getting something that complex to work correctly is even harder. Getting something that complex to work securely may be so hard that it might be impossible in many cases. A study done by the **Naval Postgraduate School** nicely summed up the situation:

The problem with system security is that it is easy to find flaws, but it is difficult to find all flaws. Thus, if post-development flaw discovery and remediation is chosen as the path to achieving a secure system, then it is difficult to make a statement regarding the completeness of the security mechanism. Similarly, security functions that are added to a pre-existing system require analysis to ensure that they will perform with the level of trustworthiness intended. This analysis will extend to all elements depending on or upon which the security addition depends, as well as all resources shared by the addition, e.g. global data. Furthermore, unless the system has already been rigorously developed, the security analysis is likely to become so complex that starting anew would be more effective.

In other words, it's probably impossible to make a system secure unless you carefully design it to be secure from the beginning. But commercial systems aren't made that way. It's simply too expensive.

NASA's experience suggests that it is indeed possible to create very reliable and secure software, but it will end up costing more. Way more. Maybe a factor of 20 or so more. So if you think enterprise software is expensive now, imagine how much more expensive it would be if it were developed using the robust system security engineering methodology that NASA uses.

An unfortunate reality

So we know how to make secure software. We just don't know how to make secure software that's cheap enough to be sold. And because of that, it seems likely that we'll be living with software that's merely expensive instead of prohibitively expensive and that we'll also be living with the many security issues that will come with that software.

That's the unfortunate reality of the software business. We can make it better, but we can't make it perfect. At least not for a price that you'd be willing to pay.

https://techbeacon.com/security/we-can-make-software-secure-not-price-youd-be-willing-pay

Return to Index

FACULTY:

Peter Denning: Award Recipient

(IEEE Computer Society 2 Feb 21)

Naval Postgraduate School Distinguished Professor Dr. Peter Denning was fascinated with science from an early age and began building electronic circuits as a teenager. His algebraic computer built from pinball machine parts won the science fair in 1959, launching him into the new field of computing. A decade later, at MIT's Project MAC for his doctorate, he took on the gnarly performance problem of the nascent virtual memory technology. Instabilities with thrashing and replacement algorithms threatened to scuttle that technology. He invented the Working Set Model, which immunized operating systems to thrashing and maximized system throughput. His solutions to these problems are widely used today in operating systems from desktops to smartphones. He is widely known as a virtual memory and computer systems performance pioneer.

He became an educator and taught computer science at Princeton, Purdue, NASA-Ames, George Mason University, and Naval Postgraduate School. At NASA-Ames, he established RIACS as one of the nation's leading centers in computation science, working on high performance computing, telescience, and neural networks. In the early 2000s, he established the Great Principles of Computing Project, which seeded a major reform of computing education. He co-founded the CSNET, the first community network to use the Internet technology, leading the transition to the modern Internet.

At NASA-Ames he became keenly interested in technology transfer and adoption. He went on to develop a way of teaching innovation leadership for adoption, co-author a book (innovators-way.com) and found an Innovation Leadership program at the Naval Postgraduate school.

Dr Denning has been recognized for his contributions with 33 awards for technical contribution, education, and professional service. These include his 1959 grand award for building a linear-equation solving computer, his international award for co-founding CSNET, his Hall of Fame award for his early work in operating systems, and his outstanding educator and teaching awards.

Since 1965, Dr Denning was an active contributor to the Association for Computing Machinery (ACM). He edited four journals including Communications. He chaired three boards including the Publications Board, where he led the development of the ACM's digital library, the first full online library offered by a professional society. He served as an officer, council member, and President.

https://www.computer.org/profiles/peter-denning

Return to Index

US Foreign Policy and Great Power Politics

(BollyInside 2 Feb 21)

(The Diplomat 2 Feb 21) … Mercy A. Kuo

Trans-Pacific View author Mercy Kuo regularly engages subject-matter experts, policy practitioners, and strategic thinkers across the globe for their diverse insights into U.S. Asia policy. This conversation with **Zachary Shore – professor of history at the Naval Postgraduate School**, a senior fellow at UC Berkeley's Institute of European Studies, and a National Security Visiting Fellow of Stanford's Hoover Institution – is the 257th in "The Trans-Pacific View Insight Series." The opinions expressed in this interview belong to the speaker alone and do not necessarily reflect the official policy or position of the Naval Postgraduate School or any other governmental entity.

Identify key characteristics of great power politics in the Trump era.

The most significant shift involved U.S.-China relations. China changed by adopting a far more aggressive foreign policy, antagonizing its neighbors from India to Mongolia to Vietnam and other Southeast Asian states. China even managed to rouse the ire of Australians and Canadians. Beijing under President Xi Jinping appears to have no interest in a charm offensive. Through the provocative maneuvers of its fighter jets and warships, China has stoked genuine concerns in Japan and Taiwan.

While China became more aggressive, America under Trump changed from viewing China as a peer competitor to seeing it as an outright threat. Trump also upended long-standing American policies through his near indifference to human rights abuses, his interpretation of the national interest that lessened the utility of traditional alliances, and his extreme undervaluing of diplomacy as a key tool in foreign affairs. He also made America more susceptible to being played by rivals, from the Taliban to Pakistan to North Korea.

Meanwhile, Vladimir Putin steadily sought to expand Russian influence beyond its near abroad by exerting force in the Middle East and by increasing cyber campaigns in Western states and possibly in Asian democracies as well.

On the whole, the Trump era saw a striking uptick in great power competition.

How might the evolution of great power rivalry unfold in the post-Trump era?

There is a logic to international relations. Actions trigger reactions. Wise leaders grasp the balance of power. Bismarck understood that as strong as Germany was, it could not afford to alienate all of its neighbors, lest they align against it. As China's power grows, wise leaders will rein in their ambitions and cultivate cooperation. Unwise leaders will overestimate their power and trigger a coalition of states aligned against them.

If China continues to antagonize other states, the U.S. will lead a tightening alliance of those who feel threatened and bullied by Beijing. This in turn will heighten China's fear of encirclement, which risks the loss of vital resources abroad, resources on which China desperately depends.

Sanctions and trade wars will continue unless the leaders of China, Russia, and the U.S. break the cycle of tit-for-tat retaliation. If states seek to avoid military confrontations, we can expect Russian, Chinese, and American cyber operations to increase. If these are not managed through international agreements, we could see attacks on state's energy grids, with devastating consequences for innocent civilians.

Assess the assumptions shaping leaders' perceptions and calculus.

Leaders must also be sensitive to what is sometimes called "window logic," the idea that states have windows of opportunity, which open and close based on conditions beyond their control. Some suspect that China's aggressiveness stems from the perception that time is actually against it, given its aging population, water and soil pollution, dearth of arable land, and other factors. Combined with their perception that the West is declining, Chinese leaders may grow increasingly opportunistic, engaging in provocative actions, particularly in China's borderlands.

All of this assumes that current trends will continue. There is always the chance of "Black Swan" events, remote possibilities which, when they occur, have dramatic effects. Putin's corruption and brutality could trigger his downfall. A more contagious variant of COVID-19 could sweep through China, leaving the government bereft of an effective vaccine. The United States could reverse its current woes by controlling the pandemic and reviving its economic dynamism. If any of these should occur, then the competition would look very different.

Analyze how the Biden administration might recalibrate U.S. foreign policy.

President Biden, like most Democrats before him, will return to internationalism by strengthening traditional alliances. This is one of America's great advantages over China and Russia: It has a robust network of powerful allies, which China sorely lacks. China's aggressive behavior has also presented new openings for America to expand and increase its alliances, particularly its military and economic ties to India. Out of necessity, Vietnam will likely continue balancing between the two great powers, but, if the U.S. handles it deftly, Vietnam might tilt slightly more toward some American aims in the region.

Biden will also re-emphasize human rights. He will cooperate with the EU to take a much tougher stance on Russia, while still seeking arms control agreements.

What should be top priorities for the articulation and implementation of U.S. foreign policy under the Biden administration regarding transpacific and transatlantic relations?

In normal times, it would be enough to reinvigorate America's Asian and European alliances as the best move in great power competition. However, these are not normal times, and two domestic matters have become crucial to foreign policy success.

First, the pandemic has exposed how poorly educated many Americans have become, as evidenced by mass movements of citizens who are anti-mask-wearing, anti-vaccination, anti-science, and anti-democracy. In the late 1950s, President Eisenhower signed the National Defense Education Act (NDEA), investing in education from primary school to post-doctoral research. The benefits were enormous. Americans learned science, math, engineering, civics, foreign languages, and overall elevated their income-earning potential. Investing in education is an investment in the American economy. China's power has stemmed from its rising wealth. American wealth (as measured in its share of global output) is declining relative to other countries. Biden should dedicate some of the pandemic relief funds for a new NDEA. America's military is dominant, but the best safeguard of the national interest is a robust economy driven by an educated populace.

Second, Biden must find ways to forge a bipartisan consensus on foreign policy. The endless policy reversals that accompany each new administration undercut the national interest. Republicans and Democrats share concerns about China, some share concerns about Russia, and nearly all view Iran, North Korea, and Islamist extremism as dangers. Building consensus for a consistent foreign policy, as the U.S. exhibited to a large extent toward communism during the Cold War, is essential to America's long-term success.

US Foreign Policy and Great Power Politics – The Diplomat

American Foreign Policy and the Politics of the Great Powers - The Diplomat - Political Bollyinside

Return to Index

Lab publishes fourth 'Strategic Latency Unleashed' book

(Mirage News 3 Feb 21)
(Lawrence Livermore National Laboratory 3 Feb 21)

The Lawrence Livermore National Laboratory's (LLNL) Center for Global Security Research (CGSR) has published the fourth book in its Strategic Latency series — "Strategic Latency Unleashed: The Role of Technology in a Revisionist Global Order and the Implications for Special Operations Forces."

Previous volumes in the Latency series have examined the effects of emerging technologies on national and international security from the perspective of the intelligence community and the defense department.

The recent volume, which has 40 chapters and includes more than 60 authors, examines the implications of emerging technologies from the perspective of America's special operations forces (SOF).

The book's sponsor, U.S. Special Operations Command (USSOCOM), asked principal investigator and project lead Zachary Davis to assemble a group of experts to explore how emerging technologies are shaping the operational environment for future SOF.

Zachary Davis, a senior fellow at CGSR and research professor at the Naval Postgraduate School (NPS) in the department dedicated to SOF, combined scientists and analysts from national labs, think tanks and universities, with experienced special operators to examine the ways that emerging technologies can assist or threaten SOF in future conflicts.

Speaking about the nearly 600-page book, Davis said: "Projects of this scope and magnitude that cross so many disciplinary boundaries and involve so many experts from multiple agencies can be challenging, but also rewarding in terms of intellectual payback."

Asked if he is ready to begin another book, Davis said that several prospective sponsors have expressed interest, but he's in no rush. As for next steps, CGSR will host a workshop in April on Strategic Latency for SOF.

In line with CGSR's core mission, the volume brought together outstanding contributors from the scientific, technical and national security communities within LLNL.

CGSR Director Brad Roberts wrote about SOF contributions to strategic deterrence and Z Program manager Brad Hart and Forensic Science Center expert Brian Souza contributed a chapter on new

forensic techniques. Davis wrote chapters on SOF counterproliferation futures and about the geopolitical trends that are remaking global security. Chris Rager of Z Program was the chief editor.

The book is divided into six sections that explore trends in geopolitics, biology, materials science, cyber tools, business practices and the multi-domain operational environment.

In many chapters, SOF operators collaborated with scientists to ensure relevance for the SOF community, including current and former NPS students and faculty.

The growing relationship between LLNL and NPS was enshrined in a recent memorandum of understanding signed by both institutions that supports this type of collaboration. Many of Davis' NPS students have conducted thesis research with LLNL scientists who benefit from their operational experience.

The book is receiving praise from the SOF, defense and intelligence communities for both its breadth and depth of content as well as its readability for both the expert community and newcomers to the field.

Along with the book, "Strategic Latency Unleashed" has a multimedia web page that contains videos for the chapters and additional resources recommended by the authors. The password is Beyond;20.

"Strategic Latency Unleashed" and previous volumes in the Strategic Latency series are available on the CGSR website.

Lab publishes fourth 'Strategic Latency Unleashed' book | Lawrence Livermore National Laboratory (llnl.gov)

Lab publishes fourth 'Strategic Latency Unleashed' book | Mirage News

Return to Index

upGrad Creates UK Board with four prominent figures in global education

(Hindustan Times 4 Feb 21)
(Big News Network 4 Feb 21)
(LiveMint 4 Feb 21)
(PR Newswire 4 Feb 21)

upGrad, India's largest higher edtech company announced the appointment of a four-member independent board to build their UK-based operations and accelerate expansion. The board comprises distinguished leaders such as Professor Sir Deian Hopkin, Julie Mercer, Dr. Kishore Sengupta, and Ashwin Assomull.

Sir Deian is currently Principal Advisor at Wells Advisory and Associate Partner Anderson Quigley. Sir Deian was previously Vice-Chancellor and Chief Executive at London South Bank University (2001-2009) and Expert Adviser, First Minister of Wales (2012-2020). Also on the board is Julie Mercer, who was Global Industry lead for Deloitte's Education Practice over her 20 years there and is currently a partner at Cairneagle Associates. Another seasoned professional on the board is **Dr. Kishore Sengupta, who has been associated with INSEAD and Naval Postgraduate School**, California in the past and is now Reader in Operations at Judge Business School, University of Cambridge. Rounding up this quad of illustrious leaders is Ashwin Assomull who is currently a partner at LEK Consulting, and a former Partner and Member of the Emerging Market's Leadership Team at the Parthenon Group.

Phalgun Kompalli, Co-founder, upGrad commented, "We are excited to work with our board to help us achieve our global aspirations. The appointment of this board signals our commitment to moving aggressively ahead with our international expansion strategy."

The edtech company aims to build a strong UK-based business operation to help expand in the region and undertake development plans in the global markets. The board comes with vast experience and myriad skillsets, well-equipped to attract, and build meaningful partnerships, understand the market and its ever-evolving requirements, and build credibility for the brand.

"One clear consequence of the restrictions imposed by the pandemic has been to widen the search for new ways of delivering high quality higher education. upGrad is a highly successful innovator in the delivery of online learning. Building on its excellent track record of achievement, working in partnership

with key universities and major technology enterprises, it is now poised to expand its provision globally and help to transform the future workplace," said Sir Hopkin.

Julie Mercer added, "I am excited to be working with upGrad to support their plan to bring their offer to the UK. There has never been a better time to bring a digital-first, student-centered approach to higher education and upskilling and reskilling as we work to rebuild and reshape our economy. Working with university partners and experienced career coaches with a focus on employment outcomes, I believe that upGrad will play an important role in supporting students learn online in partnership with some of the best universities in the world."

Appointment of the illustrious board members comes within a month of the onboarding of Zubin Gandevia as CEO, Asia-Pacific. In 2020, upGrad had also announced an appointment of Saranjit Sangar taking over as the CEO, UK & EMEA. By strengthening its leadership team, upGrad is all set to expand its penetration into the international markets.

About upGrad

upGrad is an international higher edtech leader, offering 100+ courses in Data, Technology, Management, Arts, etc., in collaboration with universities like Deakin Business School (Australia), Duke CE (US), LJMU (UK), IIT Madras (India), etc. upGrad is India's #1 startup (LinkedIn's Top Startups 2020) and is amongst GSV Global EdTech 50 List.

upGrad creates UK Board with four prominent figures in global education (prnewswire.com)
upGrad creates UK board with four prominent figures in global education (livemint.com)
upGrad creates UK Board with four prominent figures (bignewsnetwork.com)
upGrad creates UK board with four prominent figures in global education | Hindustan Times

Return to Index

Dino Pick returns home after work in Washington D.C. to clean up 'ethical lapses' in U.S. Special Operations

(Monterey County Now 3 Feb 21) … Asaf Shalev

As he watched the Capitol insurrection unfold from the Pentagon, Dino Pick says he worried only about potential injury and destruction of property. "I was never concerned that the violence would ultimately succeed in conquering the Congress or derailing the electoral process. I continue to have deep faith in the pillars of our democracy because, Lord knows, they've been challenged."

In one week last September, Danial "Dino" Pick went from managing the $4 million budget of the city of Del Rey Oaks to shaping the $13.2 billion budget for Special Operations in the United States military.

He had been recruited for a temporary assignment that brought him within the top echelon of the Pentagon. The news of his leave, an ascension so sudden and meteoric, caught the community by surprise – his former job commanding the Defense Language Institute didn't seem a sufficient prerequisite. People who knew him more closely sung of his top-secret past and described him as a real-life Jack Ryan. He served in Special Forces groups twice as an intelligence officer, once in the Asia-Pacific region and once in Iraq in 2003, during the initial U.S. invasion.

Pick is now back home. He resigned from his Del Rey Oaks job for a new assignment, running international graduate programs for the **Naval Postgraduate School**.

Weekly: Minus the classified part, what you were brought in for?

Pick: There was bipartisan support for the creation of a senior civilian leader that would oversee the Special Operations community and strengthen the civilian oversight over U.S. Special Operations Command.

The reason was a fast growth over the previous 15 years, since 9/11, in the size of the Special Operations enterprise without a strengthening of civilian oversight. The result has been discipline problems, ethical lapses, acquisition missteps and, more recently, a general sense that the Special Operations enterprise was overly focused on counterterrorism rather than on great power competition.

You're saying a lot here. Can you talk about what ethical issues?

Those issues are fairly high-profile and easy to find on the internet. They involved the SEAL Chief [Eddie] Gallagher. They involve the murder of a Green Beret at the hands of SEALs on deployment in Africa, as well as other high-profile cases.

How do you prevent such things from happening?

It will take resources and it will take a return to a certain mode of oversight by commanders with a focus on professional education and leadership, and less deployed time and more time in garrison to build institutional strengths back. There is a lot more work to do.

What does "focusing on great power competition" mean?

We're not going to take our eye off al Qaeda or ISIS. But as we are methodically reducing our footprints overseas, we will also be orienting our Special Operations community on great power competition. That means addressing Russian expansionist activities, Chinese efforts in the South China Sea and the Asia Pacific region, and actions by states such as Iran and North Korea.

You have a military background, then you went on to serve in local government. How does that lead to a top job at the Pentagon?

I don't know exactly why I was recruited. I was not privy to that decision. But the fact of the matter is, I spent a lifetime in uniform in national security, and had a network of peers and colleagues that serve in various national security positions.

I was contacted by a colleague that I had served with, and went through the vetting and interview process.

What was Jan. 6 like at the Pentagon?

I experienced the beginning of the day as most other days in the Pentagon. Then we were watching the newsfeeds on large-screen televisions that we have in our workspaces with growing concern. We were directed to send personnel home to comply with a curfew imposed by the mayor of Washington, D.C. We eventually all got home and watched with horror at what unfolded.

When you are near the top of federal decision-making, does managing Del Rey Oaks feel less significant in context?

Not at all. The only reason the federal government exists is to set the conditions for cities, counties and states to have thriving communities. The beauty of our system is that the federal government doesn't run it all. The vast majority of what affects local day-to-day life involves local jurisdictions, paving roads, making sure the sewer works, water runs, signage is clear, school districts are functioning businesses are allowed to be licensed and operate safely.

Dino Pick returns home after work in Washington, D.C. to clean up 'ethical lapses' in U.S. Special Operations. | Face to Face | montereycountyweekly.com

Return to Index

Nord Stream 2: Implications and Outcomes for US-German Relations and the Nato Alliance

(News 247 World Press 2 Feb 21)

A white paper produced by members of the NATO Science and Technology Organization's Systems Analysis and Studies (SAS)-163, "Energy Security in the Era of Hybrid Warfare."

Margarita Assenova, Senior Fellow, Jamestown Foundation
John R. Deni, PhD, Research Professor, Strategic Studies Institute, US Army War College
David R. Dorondo, D.Phil., Associate Professor, Western Carolina University
Arnold C. Dupuy, PhD, Chair, SAS-163; Senior Analyst, SAIC
Ion Iftimie, PhD, Researcher, Central European University, Vienna, Austria
Daniel Nussbaum, PhD, Mentor, SAS-163; Director, Energy Academic Group, Naval Post-graduate School
Paul Michael Wihbey, Director, George Washington University/Institute on the Geopolitics of Energy

Abstract[1]: Resolving the areas of contention between Germany and the United States is of the utmost importance early in President Joe Biden's term. One of these disputes is the ongoing

disagreements on the Nord Stream 2 undersea natural gas pipeline. This issue comes at a difficult time as Berlin is in a precarious position regarding its energy security outlook. To meet economic and environmental obligations after the shutdown of its nuclear power plants, Germany will depend on steady imports of natural gas; and Nord Stream 2 will secure additional volumes from Russia. Ironically, this will also increase Russia's political and economic leverage over Ukraine as well as several Central and Eastern European Allies dependent on Russian gas. The US has voiced strong opposition to Nord Stream 2, but Germany is determined to proceed with its construction, further complicating efforts to normalize relations between the two nations. This position paper provides three potential scenarios on Nord Stream 2, discussing the implications of each for US-German relations, as well as for the NATO Alliance. Ultimately, careful diplomacy and compromise solutions from Washington and Berlin offer the best potential for ameliorating trans-Atlantic relations during a fraught election year in Germany.

Introduction

Berlin's commitment to shut down its nuclear power plants by 2022[2] and cease coal-fired electricity generation by 2038,[3] has placed the Federal Republic of Germany in a challenging energy security environment. Through its Energiewende (Energy Transition), Chancellor Angela Merkel's government is committed to carbon-free energy generation by 2050.[4] However, with a raft of regional and national elections in 2021, and important economic, environmental and geostrategic considerations, the government also remains committed to completion of the Nord Stream 2 (NS 2) pipeline from Russia. In its pursuit of Russian gas, Berlin is at odds with the United States and/or other NATO/EU member that argue that NS 2: 1) fails to diversify gas supply sources to Europe; 2) as a diversionary pipeline does not provide new volumes of Russian natural gas; 3) leaves Ukraine vulnerable to further Russian aggression; 4) fails to "safeguard the security of gas supply" to the Baltic States and Poland (as directed by EU Regulation 2017/1938); and 5) obstructs developing "a truly interconnected internal energy market with multiple entry points and reverse flows [by] completing the North-South and Southern Gas corridors".[1] While much has been written about the pipeline politics in Europe, this paper outlines three potential scenarios regarding NS 2, while discussing the implications to US-German relations and the NATO Alliance.

Revision or Status Quo: Pipeline Politics in Europe

Background

According to the European Energy Security Strategy, in 2013 the EU imported 66% of the natural gas it consumed, and the Russian Federation accounted for 39% of the gas imported by the EU.[2] By 2019, EU net gas imports amounted to 82.6 % of total gas consumption, while Russia accounted for 46% of the natural gas imported by the EU.[3] These figures demonstrate the EU's increasing dependence on Russian gas.

From the proponents' perspective, [4] NS 2 is "purely economic and purely commercial," based on expected increases in gas demand and diminishing natural gas production in Europe.

NS 2 opponents claim it is a diversionary pipeline that would not bring new gas to Europe but would divert Russian gas from Ukrainian pipelines. Therefore, it is a Russian political venture to control the European energy market and exert dominance over Eastern European countries, notably Ukraine, Poland and the Baltic States.

Key EU-Russia Energy Co-dependencies: National and Regional Perspectives

As Germany is the main consumer of Russian natural gas within the EU,[1] the energy codependency implications to the NATO Alliance must be addressed. Our paper recognizes the perspectives of key NS 2 stakeholders, notably the European Union, Germany, Russia, the United States, other member states in Central and Eastern Europe, Ukraine and NATO.

Germany

Natural gas is perceived as a 'bridge' fuel taking Germany to full reliance on renewables, bio-gas, hydrogen, and/or fusion.[2]Therefore, from the German perspective, increased levels of natural gas must be imported for domestic consumption and transshipment to other countries. The questions become, with

COVID-19-induced budgetary pressures, from where will the gas be imported and at what cost? From Germany's view, completion of NS 2 is of vital importance, and impacts the 2021 regional and federal elections, as well as Berlin's ambitions as a regional hub for natural gas[3] and hydrogen.[4]

Other considerations include whether Germany doubles down on Energiewende, and the impact on local, regional and global energy prices and competitiveness? Would Germany support other pipeline projects in North Africa or elsewhere, or the possibility to source non-Russian gas? Finally, there is the option to invest in liquified natural gas (LNG) facilities and import from US, Qatar and Australia.

Russia

As a result of the 2006 and 2009 gas crises, Russia declares Ukraine as an unreliable transit country and views NS 2 as a vital national interest and economic priority, thereby justifying the Kremlin's push for the pipeline's completion. From a political perspective, increasing Germany's dependency on Russian natural gas also 1) undermines EU energy security strategy; 2) provides Russia with military freedom of maneuver in eastern Ukraine, and 3) weakens NATO's cohesion.

United States

These benefits to Moscow are not lost on Germany's allies, particularly in the United States. The Obama, Trump, and now the Biden, Administrations have opposed NS 2, and Senators Ted Cruz (R-TX) and Jeanne Shaheen (D-NH) co-authored the 2020 sanctions packages aimed at the project. The 2021 National Defense Authorization Act (NDAA) imposes even stronger sanctions, notably on financial institutions, insurers, port facilities, and certifying companies. This is in addition to the 2019 sanctions, which targeted pipelaying companies. In July 2020 the State Department also lifted restrictions on NS2 under the Countering America's Adversaries

https://news247worldpressuk.com/2021/02/01/nord-stream-2-implications-and-outcomes-for-us-german-relations-and-the-nato-alliance/

Return to Index

The Right Response to SolarWinds

(The Council on Foreign Relations 8 Feb 21) … **Dr. Scott Jasper, Naval Postgraduate School Lecturer**

In a formal joint statement, four U.S. agencies in charge of intelligence and cybersecurity affirmed that an advanced hacking group, "likely Russian in origin," is responsible for the SolarWinds Orion software compromise. President Biden has ordered a sweeping review of American intelligence on Russia's role in the breach and reportedly told Putin that "that the days of the United States rolling over in the face of Russia's aggressive actions — interfering with our elections, cyberattacks, poisoning its citizens — are over." Taking a more assertive tone toward Moscow may be the easiest part of the White House's reaction to the SolarWinds hack. Finding the right balance of effective offensive and defensive actions will be more difficult.

While the president has publicly vowed to make Russia "pay a price" for this significant cyber incident, his aides have reportedly cautioned him that because, at least for now, the operation appears to be an intelligence gathering effort, U.S. options for responding directly are limited. There is no express prohibition on cyber espionage in international law *per se*—and all nations, including the United States, do it. The Computer Fraud and Abuse Act (CFAA) could be used to indict Russian state hackers for trespassing in government computers or obtaining national security information. The latter section of the U.S. legal code is infrequently used, partly because national security information is often classified and thus protected from exposure. Nonetheless, a 2001 case, *United States v. Ivanov*, shows that there is precedent and intent for CFAA applying extraterritorially to foreign hackers.

Sanctioning or indicting Russian state actors for cyber espionage, however, could set a dangerous precedent to be used against individual NSA or CIA hackers. Previously, the U.S. government has used sanctions in response to destabilizing activities by the Russian military,

including election interference and destructive cyberattacks, such as the NotPetya attack. Indictments have been issued against Chinese military personnel for breaching the networks of U.S. companies and stealing trade secrets. If the United States sanctions or indicts for cyber espionage, others could do the same.

If Director of National Intelligence Avril Haines finds the SolarWinds operation was not limited to espionage, retaliatory cyber operations against Russian infrastructure could be another option. Back doors could have been inserted into compromised systems, allowing Russian hackers to alter data or shut down networks. Leveraging these in the future to produce destructive effects would be a violation of sovereignty per international law and justify countermeasures. Moscow appears to recognize this possibility and has issued a security alert to Russian businesses, warning of a possible retaliatory cyberattack by the United States.

However, direct retaliation is not without its own risks. Momentarily turning off the power in Moscow, which would certainly constitute "an appropriately strong response," is also likely to cause unintended escalation. Moreover, Russia would quickly patch the vulnerabilities that allowed for such a visible attack, possibly burning access and eliminating the means to conduct an attack when it really counts, like in a major conflict.

A more suitable approach than retorsion would be degrading the Kremlin's ability to repeat similar intrusions. Previous hunt forward operations in Europe to find Russian malware on allied networks by U.S. Cyber Command could serve as a model for mass malware inoculation. Through this process, Cyber Command teams have discovered malware on networks in Macedonia, Montenegro, and other countries and then publicly released the code to the cybersecurity community to help others avoid falling victim to it. The U.S. government has stepped up its malware inoculation efforts since the 2018 U.S. midterm elections by publishing technical details on previously undisclosed malware used by Russian military intelligence, thereby making it harder for them to avoid detection.

The United States should also improve its cyber defenses. Erica Borghard shows that a resilience-based approach assumes some compromises are impossible to prevent. What matters is how organizations respond after they occur and combat post-compromise activity inside their networks. Most current security measures are insufficient to defeat a highly evasive attacker that uses multiple techniques to obscure their activity.

However, new cloud-centric solutions that leverage data correlation technologies for threat detection, investigation, and response promise better defense and increased resilience. These tools stop advanced threats with machine learning and behavioral analysis while providing an understanding of attack causality. They would also address supply chain attacks that download malware in software updates by detecting subsequent misuse of legitimate tools and command lines. Furthermore, by deploying these tools, victim organizations would be able to remedy cyber breaches without disrupting their operations. However, these emerging capabilities are admittedly expensive, and only those with large budgets can currently afford them.

The Biden administration says that it intends to take steps to hold Russia accountable for malign activities, including the SolarWinds incident, at a time and manner of their choosing. They believe imposing costs and consequences will have an effect on Russia's behavior. A strongly worded message has been sent to Moscow, but a forcible response that changes minds is elusive, especially in response to cyber espionage. With limited means to induce fear of reprisal or failure, a formidable commitment to U.S. cyber defenses is warranted to stop the next breach before harm is done.

https://www.cfr.org/blog/right-response-solarwinds

Return to Index

ALUMNI:

Chiefs of the Monterey Peninsula Welcome New CPOs to the Mess

(DVIDS 2 Feb 21) … Chief Cryptologic Technician (Interpretive) Demian Ford

Information Warfare Training Command (IWTC) Monterey and **Naval Postgraduate School** pinned three new chief petty officers (CPO) at the Naval Postgraduate School, Jan. 29.

Roughly 30 Navy servicemembers, mostly CPOs, gathered, physically-distanced in King Hall Auditorium, a venue meant to accommodate 1,300 personnel. At center stage stood three Sailors – Chief Yeoman Crystal Bowyer, Chief Cryptologic Technician (Networks) Charles Heinen and Chief Information Systems Technician Hector Rosario – looking somewhat tired, but full of pride and determination while wearing their khakis for the first time.

Advancement to the rank of CPO is one of the most significant milestones in any enlisted person's career, and chief pinning is the culmination of weeks of intense training that begins when selection results are released. Initiation, or "Chief Season" consists of formal training in a classroom setting, physical training, morale, heritage, and community service events.

"Chief Season is about introducing new chiefs to the Mess and to the values of the Mess," shared Chief Cryptologic Technician (Interpretive) Amos Hoover, a Navy military training instructor at IWTC Monterey. "We delve deeply into the Navy's Core Values, Core Attributes, and our Guiding Principles. We explore what it means to be cognizant of and to employ the increased authority and inherited trust that come with the anchors. The crux of the season, however, is establishing the relationships that are the strength of the Mess. We are brothers and sisters, ready to help each other at a word, but also ready to hold each other accountable to a high standard."

This year's Chief Season has been different than most. Normally held in the months of August and September, delays in promotion selections due to COVID-19 mitigation efforts postponed this year's results until the end of November. As a consequence, Chief Season took place throughout December and January. That's not the only way season was affected. Navy policy and local regulations restricted the number of chiefs and selects that could be gathered in one place and restricted the type of contact they could have. This year's planners had to make significant revisions to the script, scrapping some time-honored traditions, and perhaps beginning new ones.

"The job of making new chiefs is too important not to accomplish," added Hover. "We've had to make changes this year, but being a chief is about getting things done, despite the obstacles."

Despite those obstacles, the Monterey Peninsula chiefs had a successful season. Among other evolutions, the chiefs and selects conducted an extensive cleanup of a portion of the Monterey Peninsula Coastal Recreation Trail. They also refurbished and relocated a memorial to those lost in the 1969 shootdown of a U.S. Navy EC-121 on the Presidio of Monterey, and conducted a Pearl Harbor Day commemoration.

It's not all fun and games, however. Those selected for chief are given significant tasking which they are rigorously held accountable for. The period of Chief Season means a lot of early mornings and late nights for both the selects and the chiefs running the show.

Senior Chief Cryptologic Technician (Interpretive) Thomas Bouwman, one of the leads for this year's season said, "There is a significant amount of stress placed on the selects. Being a chief is itself stressful and is a burden that no one person can bear alone. Coming to realize your own limitations and humbling yourself to leverage the power of the greater Chief's Mess is key to success during and after the season."

Master Chief Cryptologic Technician (Interpretive) Adam Shucard, IWTC Monterey's senior enlisted leader, sums up Chief Season saying, "Chief Petty Officer's Initiation is a time for leaders to come together, socially and professionally, and ensure that the standards from the past that made us great and vital to today's Navy are instilled in the next generation of Naval senior NCOs. Since our official birth in 1893 and well beyond that into the past, senior enlisted leaders on Naval vessels were the glue that held the crew together and the lynchpin between the officers' technical knowledge and the enlisted Sailors' deck plate know how. Being a chief in Monterey is a profound experience, not just because the Navy's Cryptologic Technician (Interpretive) "A" School is here and we have a longstanding presence in

Monterey, but because Naval leaders from centuries back have passed through these waters – from Junipero Serra and Sir Francis Drake to Commodore Sloat. The connection between Monterey and the U.S. Navy is longstanding and deep, and it reflects the connection between the chief petty officer and the Sailors we're charged with preparing to fight."

IWTC Monterey, as part of the Center for Information Warfare Training (CIWT), provides a continuum of foreign language and cryptologic technical training to Navy personnel, which prepares them to conduct information warfare across the full spectrum of military operations.

With four schoolhouse commands, a detachment, and training sites throughout the United States and Japan, CIWT trains over 22,000 students every year, delivering trained information warfare professionals to the Navy and joint services. CIWT also offers more than 200 courses for cryptologic technicians, intelligence specialists, information systems technicians, electronics technicians, and officers in the information warfare community.

DVIDS - News - Chiefs of the Monterey Peninsula Welcome New CPOs to the Mess (dvidshub.net)

Return to Index

Colorado State University alumna tapped to lead FEMA

(Coloradoan 3 Feb 21) … Molly Bohannon

President Joe Biden nominated Deanne Criswell, a Colorado State University alumna, to lead the Federal Emergency Management Administration.

Criswell went to CSU for her undergraduate education; she received a bachelor's degree in technology education. She later earned master's degrees in public administration and security studies from University of Colorado Denver and the **Naval Postgraduate School**, respectively.

Her Colorado connections don't stop there. Criswell worked as the head of Aurora's Office of Emergency Management and served in the Colorado Air National Guard for 21 years.

CSU President Joyce McConnell expressed excitement on Twitter following Criswell's nomination, writing, "We are so proud she is part of our CSU community!"

Criswell spent five years at FEMA during the Obama administration; she worked on the national incident management assistance team and on the federal coordinating officer cadre.

Most recently, Criswell has led New York City's emergency management as the department's commissioner. Following her nomination, Senate majority leader Chuck Schumer, D-N.Y., and New York City Mayor Bill De Blasio released statements of support.

In his January statement, Schumer called her an "outstanding choice" and her appointment will put the country "in a stronger place to mitigate and respond to increasingly severe natural disasters."

If her nomination is approved, Criswell will become the first woman to serve as the administrator of FEMA.

Deanne Criswell, CSU alumna, is Biden's nomination to lead FEMA (coloradoan.com)

Return to Index

City Workers Graduate from Highly Competitive Naval Postgraduate School Emergence Program and Executive Leaders Program

(NOLA 4 Feb 21)

The Naval Post Graduate School Center for Homeland Defense and Security (CHDS) will be highlighting two NOHSEP employees for being two of very few who are accepted into this highly competitive program.

"These two professionals are highly regarded public servants and are critical to the City's efforts in ensuring the citizens of New Orleans are prepared and protected from any emergency situation," said Col.

Terry Ebbert USMC (Ret.), New Orleans Director of Public Safety. “Their leadership and skills are recognized by the nation's highest level of government.”

Laura Mellem, Public Engagement Manager for NOHSEP is the first and only person in Louisiana thus far who has graduated from the Naval Post Graduate School's CHDS Emergence Program.

The Emergence Program is a unique opportunity for homeland security/public safety professionals who are in the early stage of their career. The program provides an educational forum and innovation lab for participants to explore “emerging” trends in the world around us (e.g., technology, social, and terrorism). Participants discuss both the challenges associated with these complex trends as well as the opportunities to rethink how we protect our communities and the nation. In addition, program sessions assist participants in “emergence” strategies for implementing innovative ideas, being a leader, and for a successful homeland security career.

Michael Antoine, Deputy Director, NOHSEP is the first African American from the New Orleans area to be accepted into the Naval Post Graduate School's CHDS Executive Leaders Program.

The Executive Leaders Program provides a unique educational opportunity for senior-level homeland security/public safety leaders who are at the forefront of the Nation’s homeland security mission. This high-level educational program meets the immediate and long-term needs of leaders responsible for homeland security/public safety by bringing together a variety of disciplines and jurisdictions into one room. Each class consists of a diverse group of federal, state, local, territorial, tribal and private sector leaders who become enhanced decision makers and innovative collaborators.

Participants learn from each other by discussing relevant issues and complex problems while developing policies and strategies to enhance their organization or agency’s homeland security/public safety mission. The impact of the Executive Leaders Program is not only by learning from the experienced instructors and nationally recognized experts but also through the cross-jurisdiction and organization cultivation that occurs within the diverse group of senior-level leaders in the program. Graduates of the program emerge with a deeper understanding of homeland security issues and a broadened network of homeland security leaders from around the nation.

Mayor - News - February 2021 - City Workers Graduate from Highly Competitive Naval Post Graduate School Emergence Program and Execu - City of New Orleans (nola.gov)

Return to Index

Plurilock Adds Adm Jan Tighe to Advisory Board

(Yahoo Finance 4 Feb 21)

Retired Vice Admiral has held numerous executive roles in the U.S. Navy and National Security Agency and currently serves on the board of Goldman Sachs.

Victoria, British Columbia--(Newsfile Corp. - February 4, 2021) - Plurilock Security Inc. (TSXV: PLUR) (OTCQB: PLCKF) ("Plurilock" or the "Company"), an innovative cybersecurity company that provides frictionless and continuous authentication using machine learning and behavioral biometrics, is pleased to announce that retired U.S. Navy Vice Admiral, Jan E. Tighe has been appointed to the Company's Advisory Board.

Dr. Tighe was commissioned as a cryptologist who graduated from the Naval Postgraduate School, Monterey, California, with a Master of Science in Applied Mathematics and a Doctorate in Electrical Engineering.

Over a 20-year federal career, Dr. Tighe served as the Deputy Chief of Naval Operations for Information Warfare, Director of Naval Intelligence, Fleet Commander of the U.S. Fleet Cyber Command, and Deputy Director of Operations in the U.S. Cyber Command. As a managing director and technology leader on the corporate board of the U.S. Navy, Dr. Tighe was responsible for providing digital expertise and planning to support core infrastructure, many thousands of air and sea craft, and hundreds of thousands of federal employees.

As a senior leader and seasoned cyber operations expert, Dr. Tighe has followed her storied national service career by sitting as an independent director on the boards of Goldman Sachs, IronNet Cybersecurity, Progressive Insurance, and Huntsman Chemical.

"Plurilock's use of AI for identity assurance is quite compelling as they seek to deliver innovative authentication solutions that can protect against both insider and cyber threats," said ADM Tighe. "Given that Plurilock's authentication technology is designed to solve many of today's cyber-related problems, I am excited to assist this groundbreaking company in bringing their technology to a wider audience."

"We are delighted to have Dr. Jan Tighe onboard at Plurilock where her guidance in mission critical cybersecurity work will be vital in expanding our outreach to security conscious enterprises across North America," said Ian L. Paterson, CEO of Plurilock. "With our company currently in growth phase, having a retired Vice Admiral on our advisory board will enable us to establish a stronger presence in the North American and Federal Government verticals."

Plurilock granted Dr. Tighe an option to acquire 50,000 shares at an exercise price of $0.50 per share and vesting over three years from the date of grant.

About Plurilock

Plurilock is an innovative, identity-centric cybersecurity company that reduces or eliminates the need for passwords, extra authentication steps, and cumbersome authentication devices. Plurilock's software leverages state-of-the-art behavioral-biometric, environmental, and contextual technologies to provide invisible, adaptive, and risk-based authentication solutions with the lowest possible cost and complexity. Plurilock enables organizations to compute safely-and with peace of mind.

Plurilock Adds ADM Jan Tighe to Advisory Board (yahoo.com)

Return to Index

Wrap Technologies Inc. [WRAP] is 48.24% higher this YTD. Is it still time to buy?

(DBT News 5 Feb 21) … Annabelle Farmer

Wrap Technologies Inc. [NASDAQ: WRAP] price surged by 16.99 percent to reach at $1.04. The company report on January 11, 2021 that Former Police Chiefs Kathleen O'Toole and Sylvia Moir Join WRAP as Senior Advisors.

Wrap Technologies, Inc. (the "Company" or "WRAP") (Nasdaq: WRAP), an innovator of modern policing solutions, announced the appointment of Kathleen O'Toole, retired Commissioner of Boston and Seattle Police Departments, and Sylvia Moir, retired Chief of Tempe Police Department, to join the Company's public safety technology development and agency relations efforts.

Gold bugs are shouting from the rooftops in excitement, but that doesn't mean you rush out and just buy any gold stock…That's why we laid out The 2021 Ultimate Gold Portfolio – to dissect the treasure from the trash.

Ret. Chief O'Toole and Ret. Chief Moir will be working with the WRAP Reality team on the development of a virtual reality-based training simulator focusing on topics of de-escalation, use of force, crisis intervention and officer wellness. Both will advise on R&D and training development, as well as conduct outreach and liaison with law enforcement executives and community stakeholders."As WRAP continues to drive innovations in public safety, we are proud to welcome two highly accomplished leaders," said Tom Smith, President and Interim CEO at WRAP. "Ret. Chief O'Toole and Ret. Chief Moir each hold decades of career experience in law enforcement as well as historic positions as inaugural female chiefs of their respective departments. As trailblazers of reform, we look forward to their contributions to police training and education in partnership with WRAP."Kathleen O'Toole has held several executive positions in the public and private sectors and is widely recognized for her principled leadership and successful reform efforts in North America and Europe.As a law school student, O'Toole accepted a position as patrol officer with the Boston Police Department and worked a number of field, investigative and supervisory assignments as she rose through the ranks. She served as Chief of the Metropolitan District Commission Police in Boston, Lieutenant Colonel overseeing Special Operations in

the Massachusetts State Police, Massachusetts Secretary of Public Safety, Boston Police Commissioner and Seattle Chief of Police. She also served as Chief Inspector of the Garda Síochána, the Irish national police service. She was a member of the Independent Commission on Policing during the Northern Ireland Peace Process and recently chaired the Commission on the Future of Policing in the Republic of Ireland. O'Toole has served on several other review and reform panels. She provides services as a subject-matter expert to the US Department of Justice Civil Rights Division. She was appointed as Monitor to oversee a federally supervised consent decree in East Haven, CT. She was an advisor to the Illinois AG's Office during the development of a settlement agreement between the City of Chicago and the State, and now serves as a member of the monitoring team overseeing the project. She also serves as a member of the monitoring team in Baltimore.O'Toole has substantial private sector experience as well. As a practicing attorney, she has represented clients on civil matters and acted "of counsel" to a Boston law firm. She once served as a corporate security manager at Digital Equipment Corporation and had global responsibility for executive protection, crisis management and threats of violence in the workplace. She has provided a diverse range of consulting services to several multi-national corporations based in North America and Europe. O'Toole regularly provides lectures at academic institutions throughout the US and Europe and presents frequently at professional conferences. She has served as an adjunct faculty member at Northeastern University, University of Ulster and Seattle University. O'Toole received a Bachelor of Arts Degree from Boston College, a Juris Doctor from New England School of Law and was admitted to the bar as a practicing attorney. She also earned a PhD at the Business School of Trinity College Dublin. Sylvia Moir is principal for The Macrae Group, a consulting firm formed in late 2020 specializing in organizational assessment, analysis, evaluation, and advising on modern law enforcement training and education.Moir's extensive background in law enforcement and public safety includes both agency leadership and thought leadership across multiple areas of police training, strategy, policy and reform. A California native, Chief Moir has over 30 years of experience in local police practice. Sylvia joined the Tempe Arizona Police Department as the Chief in March 2016 and led the department through October 2020."Reimagining policing must include innovations which confront where policing has fallen short. As police executives and communities search for solutions to enhance how police officers provide effective and equitable service, we demand innovations like WRAP's Virtual Reality Simulator to fill existing gaps," said Moir. "The WRAP Reality platform shows great promise in enhancing police officer decision making and may simultaneously boost officer wellness and resilience; this promise is why I am eager to contribute to this progressive tool." Previously, Moir was the Chief of the El Cerrito Police Department from 2010 until her appointment as the Police Chief in Tempe, Arizona. Chief Moir spent most of her early career with the Sacramento Police Department where she served in every division of the department. She was the Incident Commander on hundreds of planned and spontaneous events, a trainer in several policing subjects, and a member of the Sacramento Police Honor Guard. She completed rigorous training with the US Army Old Guard at Fort Myer, VA and Arlington National Cemetery.California Governor Jerry Brown appointed Chief Moir to the Commission on California Peace Officer Standards and Training for two terms. Moir served on the Executive Committee for the California Police Chiefs Association and as the President of the Police Executive Research Forum. She is currently an Executive Fellow for the National Police Foundation, Chair of the Community Policing Committee of the International Association of Chiefs of Police, an advisor for the American Law Institute, and a member of the Law Enforcement Immigration Task Force Chief Moir holds a Bachelor of Science in Criminal Justice from California State University, Sacramento, a Master of Arts in Organizational Management, and a Master of Science degree from the **Naval Postgraduate School** – Center for Homeland Defense and Security. In 2019, Moir presented a TEDx Talk on mindfulness in policing.About WRAPWRAP Technologies, Inc. is an innovator of modern policing solutions.

The Company's BolaWrap 100 product is a patented, hand-held remote restraint device that discharges an eight-foot bola style Kevlar® tether to restrain an individual at a distance from 10 to 25 feet. Developed by award winning inventor Elwood Norris, the Company's Chief Technology Officer, the small but powerful BolaWrap 100 assists law enforcement in safely and effectively deescalating encounters, especially those involving an individual in crisis. BolaWrap 100 has already been used to

safely apprehend suspects without injury in a number of cities including Los Angeles, Sacramento, Fresno, Bell, Albuquerque, Minneapolis, West Palm Beach, Fort Worth, and Oak Ridge.

Wrap Technologies Inc. [WRAP] is 48.24% higher this YTD. Is it still time to buy? | The DBT News

Return to Index

Black History Month Feature: Blacks Walking in Space Victor Glover walks in space this week

(Pride Publishing Group 5 Feb 21) … Cass Teague

In November 2020, NASA astronaut Victor Glover launched on his first spaceflight, becoming the first Black astronaut to live on the International Space Station as part of a long-duration mission. Glover is the first African American ISS Expedition crewmember to live on the ISS, not just visit the ISS for a short stay like on the Space Shuttle as an ISS assembly astronaut, as have most of the 14 other Black Americans NASA has sent to space out of a total of more than 300 NASA astronauts.

SpaceX Crew Dragon capsule Resilience launched on November 15, 2020, carrying Glover as the pilot together with two other NASA astronauts (Michael S. Hopkins and Shannon Walker) as well as Soichi Noguchi of Japan. They arrived at the space station on November 17.

Glover and Hopkins concluded their first spacewalk at 12:24 p.m. CST, on Wednesday, January 27, after completing a number of tasks designed to upgrade International Space Station systems. This was the first spacewalk for Glover with a total of 6 hours and 56 minutes. Glover and Hopkins concluded their second spacewalk at 12:16 p.m. CST, on Monday, February 1, after 5 hours and 20 minutes, completing work to replace batteries that provide power for the station's solar arrays and upgrade several of the station's external cameras. Glover now has spent a total of 12 hours and 16 minutes spacewalking.

Space station crew members have conducted 234 spacewalks in support of assembly and maintenance of the orbiting laboratory. Spacewalkers have now spent a total of 61 days, 7 hours, and 7 minutes working outside the station. Two additional spacewalks are planned for the near future. During the next spacewalk, Glover and NASA astronaut Kate Rubins will work outside the station to prepare its power system for the installation of new solar arrays to increase the station's existing power supply. For a following spacewalk, Rubins and Japan Aerospace Exploration Agency (JAXA) astronaut Soichi Noguchi will continue upgrading station components. The dates have not yet been set for these two events.

Glover joins a very select fraternity of now five African Americans who have walked in space, among the 15 total who have traveled there. Bernard A. Harris Jr. was the first African American to walk in space, in 1995; followed by Winston E. Scott, veteran of three spacewalks; Robert Curbeam, veteran of seven spacewalks; Robert Satcher, whose two EVAs were on November 19 and November 23, 2009; and Alvin Drew, veteran of two spacewalks, February 28 and March 2, 2011.

Here are photos of all fifteen Black astronauts who have traveled in space, including Guion Bluford (the first African-American astronaut in space), Ronald McNair (who died in the Space Shuttle Challenger disaster), Frederick D. Gregory (the first African American to pilot and command a Space Shuttle mission and acting Administrator of NASA in 2005), Charles Bolden (Administrator of NASA, 2009 – 2017), Mae Jemison (first African-American woman in space), Michael P. Anderson (who died in the Space Shuttle Columbia disaster), Stephanie Wilson (veteran of three shuttle missions), Joan Higginbotham, and Leland D. Melvin (Associate Administrator for Education at NASA).

Special Black History Month Note: Robert Henry Lawrence Jr., born October 2, 1935, died December 8, 1967, was the actual first African-American astronaut. He was selected for astronaut training in 1967 for the MOL program, but died tragically in an aircraft accident.

Meet Victor Glover

Victor Jerome Glover (born April 30, 1976) is a NASA astronaut of the class of 2013, and Pilot on the first operational flight of the SpaceX Crew Dragon to the International Space Station. Glover is a commander in the U.S. Navy where he pilots an F/A-18, and is a graduate of the U.S. Air Force Test Pilot School. He is a crew member of Expedition 64, serving as a station systems flight engineer.

Glover, who grew up in Pomona, California, graduated from Ontario High School (California) in 1994, where he was a quarterback and running back for the Jaguars. He was awarded Athlete of the Year 1994. He attended California Polytechnic State University in San Luis Obispo, California on a wrestling scholarship and received his Bachelor of Science degree in General Engineering in 1999. Glover is a member (1996) of Phi Beta Sigma fraternity.

Glover has three Master of Science degrees: Master of Science in Flight test engineering, Air University (United States Air Force) (USAF TPS), Edwards Air Force Base, California, 2007; Master of Science in Systems Engineering (PD-21), **Naval Postgraduate School**, 2009; and Master of Military Operational Art and Science, Air University (United States Air Force), Montgomery, Alabama, 2010. Glover also completed a Space Systems Certificate from the **Naval Postgraduate School** whilst on deployment, and a Certificate in Legislative Studies at Georgetown University whilst serving as a Legislative Fellow.

Glover joined the US Navy, completing advanced flight training in 2001, later training for the F/A-18C with the Marine Fleet Replacement Squadron. In 2003 he was assigned to Strike Fighter Squadron 34 stationed in Virginia, and embarked on the final deployment of USS John F. Kennedy in support of Operation Iraqi Freedom. After attending the Air Force Test Pilot School, in 2007 he was designated a test pilot, serving with the VX-31 in California. In 2011, he served as a department head in Strike-Fighter Squadron 195 (VFA-195) stationed at Naval Air Facility Atsugi, Japan and embarked on the USS George Washington.

Glover's call-sign is "Ike", a name given to him by one of his first commanding officers, standing for "I Know Everything". He has accumulated 3,000 flight hours in more than 40 aircraft, over 400 carrier arrested landings and 24 combat missions for the United States Navy. In 2012 he served as a legislative fellow working on the personal staff of John McCain. It was during this time that he was selected for the 2013 NASA Astronaut group.

In August 2018 Glover was introduced as one of the Commercial Crew astronauts, assigned to fly on the first operational flight, and the second crewed flight overall, of SpaceX's Crew Dragon, and piloted the craft on ISS Expeditions 64 and 65. He is married to Dionna Odom Glover and they have four daughters.

Black History Month Feature: Blacks Walking in SpaceVictor Glover walks in space this week - Nashville PRIDE, Inc. (pridepublishinggroup.com)

Return to Index

TRAINING:

Monterey naval installation conducting security drills

(Monterey Herald 5 Feb 21) … Dennis L. Taylor

If anyone in Monterey or Del Rey Oaks has recently seen or heard police sirens entering a naval annex: don't worry, this is just a drill.

Naval Support Activity Monterey this week and next is conducting an annual active shooter training drill at one of its annex locations in Del Rey Oaks. The drill is taking place from its Monterey installation where the **Naval Postgraduate School** is located out to the U.S. Navy's Fleet Numerical Meteorology and Oceanography Center in Del Rey Oaks.

The installation is home to 15 naval operations, called tenant commands, including the Naval Postgraduate School. Naval Support Activity Monterey provides base services in support of its Central Coast tenant commands that include such things as facilities support, quality of life services, dining, religious services and a gym.

"The activity includes sirens on police cars as naval security personnel transited from our main location to the annex, which might lead the local community to think there's a real-life emergency occurring," said Tina Stillions, Naval Support Activity Monterey's public affairs officer.

The active-shooter scenario is simulated in a building at the Oceanography Center where people were working, providing for a real-life scenario for those security teams involved and personnel working in nearby offices, Stillions said. The drill involves a lone shooter, a person who had been shot and someone running from the building, which provides for spot decision-making for the Navy's security personnel.

Updated information on the drill is available on Naval Support Activity Monterey's Facebook page: https://www.facebook.com/NSAMonterey.

The drills are called Citadel Shield and Solid Curtain, which are joint exercises between the U.S. Fleet Forces Command and Navy Installations Command, the latter being what Naval Support Activity Monterey falls under. It is held annually on all Navy installations in the continental United States, typically during February.

The Citadel Shield component is a field training exercise led by the Installations Command that focuses on local tactics and procedures. Solid Curtain is an exercise led by Fleet Forces Command that focuses on driving an integrated response between commands and security forces across the nation.

"Both exercises provide opportunities for security forces to hone their security skills through realistic scenarios designed to ensure security forces are at peak readiness to deter and respond to potential security threats," Stillions said.

Monterey naval installation conducting security drills – Monterey Herald

Return to Index