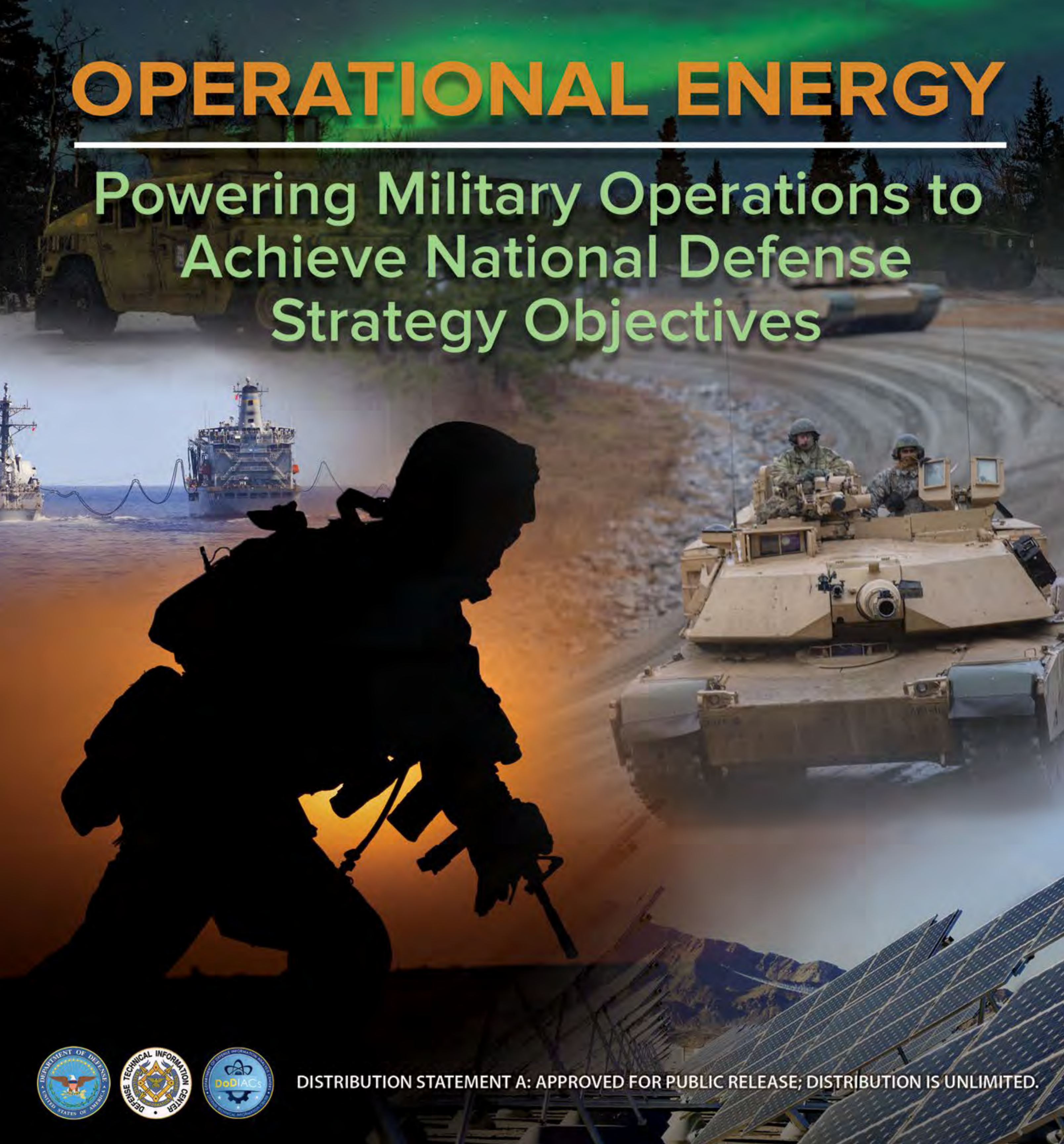
VOLUME 7 NUMBER 1
SPRING 2020

HDIAC JOURNAL

A Quarterly Publication of the Homeland Defense & Security Information Analysis Center

OPERATIONAL ENERGY

Powering Military Operations to Achieve National Defense Strategy Objectives



HOMELAND DEFENSE & SECURITY
CRITICAL INFRASTRUCTURE PROTECTION
WEAPONS OF MASS DESTRUCTION
CBRN DEFENSE
BIOMETRICS
MEDICAL
CULTURAL STUDIES
ALTERNATIVE ENERGY

HDIAC Homeland Defense & Security Information Analysis Center

ABOUT THE HDIAC

The Homeland Defense & Security Information Analysis Center is one of three Department of Defense Information Analysis Centers. HDIAC is responsible for acquiring, analyzing, and disseminating relevant scientific and technical information – in each of its eight technical focus areas – in support of the DoD and U.S. government Research & Development activities.

OUR MISSION

The mission of the HDIAC is to provide users with focused expert technical consulting and unbiased scientific and technical information through in-depth analysis and the creation of specialized information products in support of the HDIAC's eight vital technical focus areas:

- Homeland Defense and Security (HD)
- Critical Infrastructure Protection (CIP)
- Weapons of Mass Destruction (WMD)
- Chemical, Biological, Radiological, and Nuclear Defense (CBRN)
- Biometrics (BIO)
- Medical (MED)
- Cultural Studies (CS)
- Alternative Energy (AE)

Homeland Defense & Security
Information Analysis Center
www.hdiac.org

901 North Stuart Street, Ste 401
Arlington, VA 22203

266 Genesee Street
Utica, NY 13502

HOW WE CAN HELP

CORE ANALYSIS TASK (CAT) PROGRAM

PRE-COMPETED CONTRACT VEHICLE FOR SPECIALIZED TECHNICAL SUPPORT WITH EASY CONTRACT TERMS

- Work can begin in as little as six weeks
- Especially valuable for efforts that cross multiple technical focus areas
- Leverages an extensive SME network
- Draws from the most recent studies across the DoD

TECHNICAL INQUIRY SERVICE

FOUR FREE HOURS OF ANALYTICAL, SCIENTIFIC, AND PROFESSIONAL RESEARCH ACROSS OUR EIGHT TECHNICAL FOCUS AREAS

ADDITIONAL PRODUCTS

- Quarterly Technical Journal
- Weekly Homeland Defense Digest
- Monthly Online Webinars & Podcasts
- Analytical Tools & Techniques
- Bi-Annual State of the Art Report

GETTING STARTED

Contact HDIAC at
1-877-363-7422 or info@hdiac.org

HDIAC is sponsored by the Defense Technical Information Center, DoD IAC Program, Attn: DTIC-I, 8725 John J. Kingman Rd., Fort Belvoir, VA 22060-6218

HDIAC
Homeland Defense & Security
Information Analysis Center

JOURNAL EDITORIAL BOARD

ABOUT THE JOURNAL OF THE HOMELAND DEFENSE AND SECURITY INFORMATION ANALYSIS CENTER

ABOUT THIS PUBLICATION

The Journal of the Homeland Defense and Security Information Analysis Center is published quarterly by the Homeland Defense and Security Information Analysis Center (HDIAC). The HDIAC is a Department of Defense (DoD) Information Analysis Center (IAC) sponsored by the Defense Technical Information Center (DTIC) and operated by Quanterion Solutions Incorporated in Utica, NY.

Reference herein to any specific commercial products, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or the HDIAC. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or the HDIAC, and shall not be used for advertising or product endorsement purposes.

ARTICLE REPRODUCTION

Images and information presented in these articles may be reproduced as long as the following message is noted:

"This article was originally published in the HDIAC Journal of Homeland Defense and Security Volume 7, Number 1"

In addition to this print message, we ask that you notify HDIAC regarding any document that references any article appearing in the HDIAC Journal.

Requests for copies of the referenced journal may be submitted to the following address:

Homeland Defense and Security Information Analysis Center
901 N. Stuart St.
Suite 401
Arlington, VA 22203

Phone: 877-363-7422 / Fax: 315-732-3261 / E-mail: info@hdiac.org

COVER PHOTO

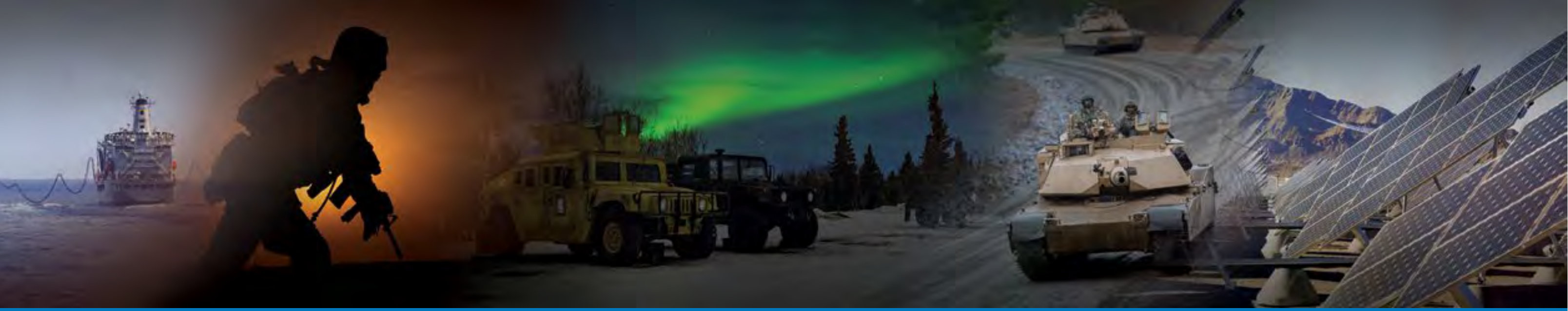
Cover Graphic Composite: Shelley Stottlar, Quanterion Solutions Inc., **Featuring U.S. Military Photos:** https://www.defense.gov/observe/photo-gallery/

An archive of past HDIAC Journals are available at:
https://www.hdiac.org/journal/.

*To unsubscribe from HDIAC Journal Mailings please email us at **info@hdiac.org** and request that your address be removed from our distribution mailing database.*

JOURNAL OF THE HOMELAND DEFENSE AND SECURITY INFORMATION ANALYSIS CENTER

Operational Energy: Powering Military Operations to Achieve National Defense Strategy Objectives



WELCOME TO THE SPRING 2020 ISSUE OF THE HDIAC JOURNAL! I AM CERTAIN THAT YOU WILL FIND ITS CONTENT INTERESTING AND RELEVANT TO THE HOMELAND DEFENSE AND SECURITY MISSION.

Our vision for the HDIAC is to create a DoD center of excellence and "first stop" for Homeland Defense and Security issues, positioning the Center as the hub for collection and analysis of HD-related scientific and technical data. We are dedicated to maintaining a committed outreach program, fostering awareness of the HDIAC mission and capability through our website, symposia attendance, and our social media presence.

If you have not already done so, I encourage you to sign up for product release notifications on our website, participate in our technical forums, and subscribe to our LinkedIn, Twitter, and Facebook pages. Also, be sure to visit the HDIAC website regularly, at https://www.hdiac.org to view our ever-changing content. At the beginning of the year, we began streaming two webinars a month as a result of increased outreach that generated additional topics of interest and new speakers. Additionally, we produce and post links to two podcasts on the website each month; the podcasts bring in subject matter experts from across the country to share their thoughts on current topics of interest. Finally, later this Spring, we will publish a State-of-the-Art Report titled, *Countermeasures Against the Degradation of Warfighter Capabilities due to Infectious Disease Threats*. You'll find this to be an informative HDIAC product that looks at the impact that infectious diseases have had on our warfighting capability.

Our goal is to leverage our community of practice to provide timely responses to the HD community as well as stay ahead of burgeoning technologies to keep our subscribers informed. We want to provide users with focused expert technical consulting and unbiased scientific and technical information through in-depth analysis and the creation of specialized information products in support of our eight vital technical focus areas: Homeland Defense and Security; CBRN Defense; Weapons of Mass Destruction; Critical Infrastructure Protection; Biometrics; Alternative Energy; and, Cultural Studies. If you want to assist in this effort, I'd like to invite readers of the Journal to join our subject matter expert (SME) network and contribute to the HDIAC's mission. Our SMEs are a key aspect of the HDIAC team as they provide a body of knowledge and depth of experience that is far greater than any single person or entity. Our volunteer SMEs participate at whatever level they desire, sharing their experiences and contributing to the HDIAC mission by writing journal articles, creating and giving live webinars, producing podcasts, and responding to questions and technical inquiries from the field. If interested, you can contact us at info@hdiac.org to request a SME questionnaire.

I hope you have a safe and productive Spring. Enjoy reading this issue of the HDIAC Journal; please reach out to me directly with any ideas, concerns, or suggestions - I look forward to hearing from you.

Best Regards and Semper Fidelis,

Steve Redifer
Director, Homeland Defense and Security Information Analysis Center

Photo Composite (top of page): Shelley Stottlar, Quanterion Solutions Inc.,
Featuring U.S. Military Photos: https://www.defense.gov/observe/photo-gallery/

Solar Photovoltaic Considerations for

Operational and Warfighter Support Capabilities

By: 2nd Lt **Dylan Martin-Abood**, Master's Degree Student, Electrical Engineering, Air Force Institute of Technology, Wright-Patterson Air Force Base, **Dr. Douglas Dudis,** Office Lead, Air Force Research Laboratory, Wright-Patterson Air Force Base, and **Lt Col Torrey Wagner,** Assistant Professor of Systems Engineering, Air Force Institute of Technology, Wright-Patterson Air Force Base

Solar photovoltaic (PV) technologies serve a wide range of applications beyond general terrestrial use, which afford opportunities to enhance the energy resilience and capabilities within 15 Department of Defense (DoD) mission areas.

THIS WORK HIGHLIGHTS the fundamental mechanisms and historical perspective for military PV technology applications and addresses the operational considerations for effectively deploying PV technology. PV materials, structures and architectures have matured into competitive and readily available energy technologies based on their levelized cost of energy (LCOE). However, enhancing warfighting capabilities requires attention to systems considerations beyond cost per watt or LCOE. While PV is impractical for fighters and bombers as it can meet less than 1% of their power requirements, there are numerous areas that could benefit from the application of PV technology. For example, installing PV arrays on all DoD land could meet the electrical energy requirement of the United States and two other industrialized nations.

Photo Credit (below): U.S. Air Force photo/150401-F-ZZ999-002

Introduction

The DoD develops, maintains and relies on energy systems to accomplish every mission in CONUS and abroad. All energy systems contain vulnerabilities which both state and non-state actors can attack. Any degradation to energy access across all DoD operational domains undermines to the ability of the United States to protect its allies and interests across the globe.

PV technologies have the potential to improve capabilities via enhanced resilience and longevity of DoD energy systems while reducing capital, operating, and maintenance costs. Effectively integrating PV technology into current DoD energy systems has the potential to improve energy independence, redundancy, and assurance. However, PV technology has its own unique limitations and is not a singular solution to DoD energy needs. However, in certain applications PVs outclass current energy technologies, and continued research, development, and testing will enhance warfighter capabilities [1].

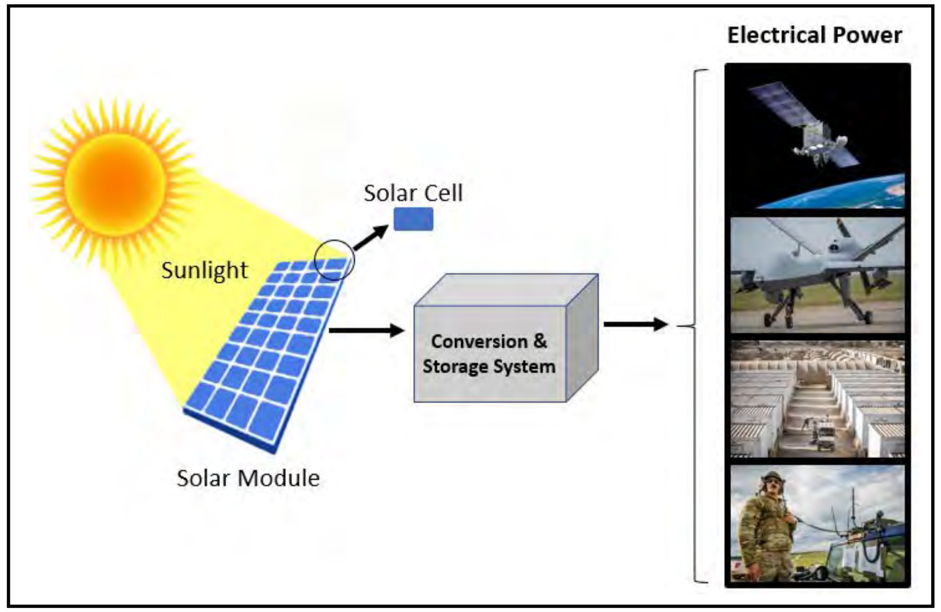


Figure 1: *Basic PV system and satellite, vehicle, ground base, and warfighter support applications. Images courtesy of the USAF.* - (Source: Author)

When the United States entered into war in Afghanistan (2001) and in Iraq (2003), with the exception of space operations, photovoltaic technologies had not yet matured. Improvements to set-up time, logistics, power to weight ratio, and dependability have furthered the capabilities and opportunities for military PV applications. PV systems are not suited for all power applications, but excel in several. Operations involving remote, low and intermittent power applications are where solar PV technologies are now able to outperform other energy technologies.

Basics Of Photovoltaic Technology

Solar PV systems generate power for end users by converting sunlight into electricity. A basic solar power system consists of PV modules connected with an energy conversion system to provide power to be utilized immediately or stored for use at a later time. Figure 1 depicts a basic PV system and some of the technologies they power.

PV cells encompass a broad category of materials which convert sunlight to electrical energy. These PV cells are grouped together into modules, also known as panels, to achieve the level of power output desired. Solar PV panels can be manufactured from a variety of technologies, as shown in Figure 2.

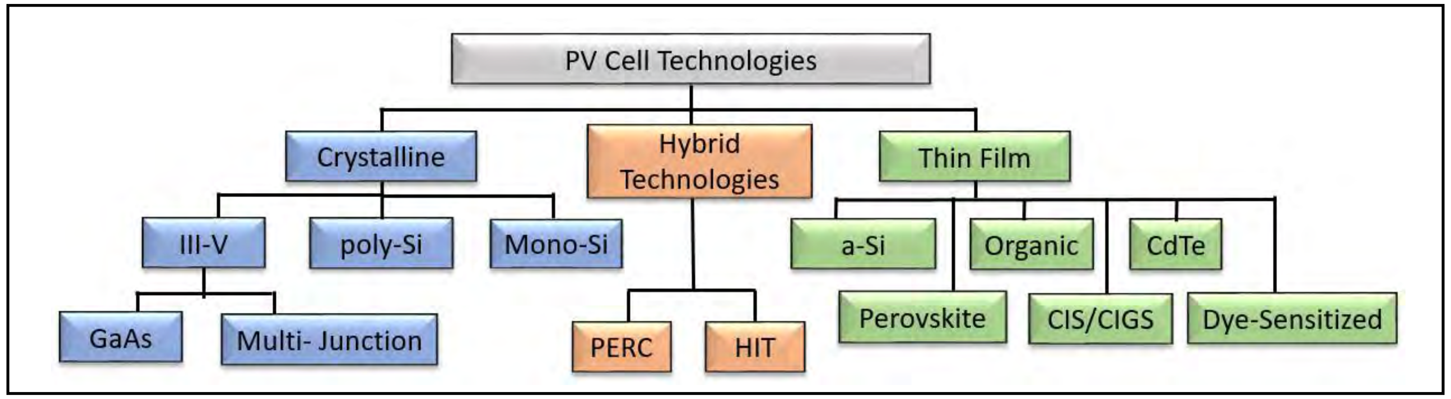


Figure 2: *PV cell technologies. In the figure the abbreviations are: GaAs Gallium Arsenide; III-V semiconductor family consisting of elements in the III and V groups of the periodic table; poly-Si polycrystalline Silicon; mono-Si monocrystalline Silicon; PERC passivated emitter rear contact; HIT heterojunction with intrinsic thin layer; a-Si amorphus Silicon; CIS Copper Indium Selenide; CIGS Copper Indium Gallium Selenide; CdTe Cadmium Telluride.*

Current viable and developing commercial solar PV cells can be loosely grouped into crystalline, thin film, and hybrid technologies. Each group contains unique variations of materials and structures which affect overall cell performance, stability, and cost.

The most common metric for evaluating PV performance is efficiency, which correlates to the amount of power (Watts) a panel can produce from a fixed amount of incident sunlight. Efficiencies are measured under industry standard test conditions (STC) using an AM1.5 spectrum at 1000 W/m^2 at a cell temperature of 25 degrees Celsius, which allows for PV cell and module performance to be easily compared. The theoretical maximum efficiency of a single-junction PV cell is approximately 30% [2]. Multi-junction solar PV cells, which stack multiple layers of PV materials on top of each other to absorb a greater range of wavelengths, possess a theoretical maximum efficiency greater than 60% [3].

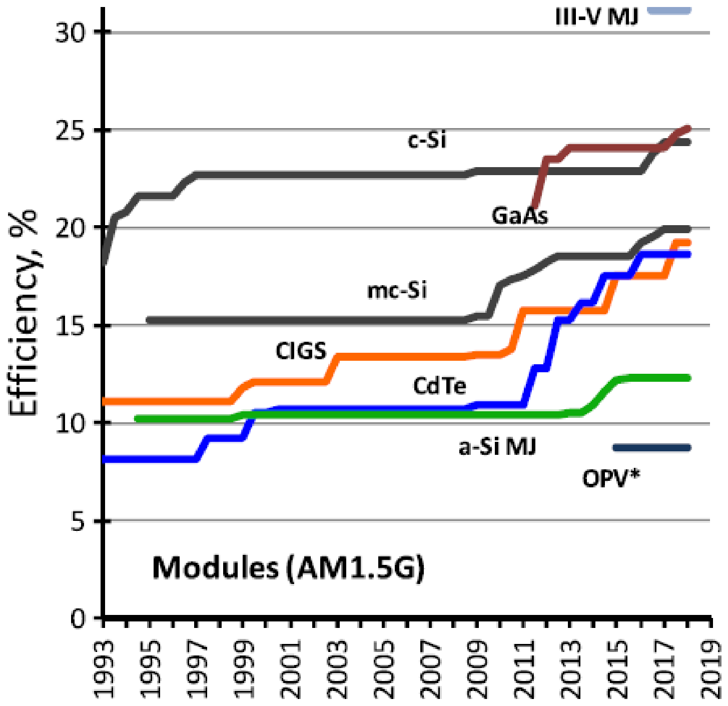


Figure 3: *Improvements in module efficiencies over a twenty-five year period for modules ≥ 800 cm^2 [6]. In the figure, abbreviations are: c-Si crystalline Silicon which is equivalent to monocrystalline Silicon; mc-Si multicrystalline Silicon which is equivalent to polycrystalline Silicon; MJ multi-junction; OPV organic photovoltaic.*

Laboratory performance under STC does not always reflect performance in real world conditions, and common analyses of solar PV modules are often based solely on efficiency and cost/watt under STC. Additional considerations must be accounted for in real-world operation as environmental factors including weather, humidity, average solar irradiation, soiling, salinity, and temperature. Each consideration impacts a PV module's performance and longevity differently.

Modern Photovoltaic History and Development

The first silicon photovoltaic cell was reported by Bell Labs in 1941 with an efficiency of less than 1% [4]. Subsequently, the commercial semiconductor industry, supported by NASA and the U.S. Air Force, developed PVs as a means of powering satellites. The first U.S.-developed single-junction silicon solar PV array in space had an efficiency of 10% and was launched aboard the Vanguard I on March 17, 1958 [5]. In 1977 the U.S. Department of Energy (DOE) was established, bringing together dozens of organizational entities, and since then, the DOE is credited with 30% of patents in the solar energy field. DOE's Solar Technologies Office (SETO) has directly funded more than half of all solar efficiency records [1]. Today, under laboratory conditions, state of the art single-junction silicon PV cells now

Figure 4: *Nellis II, a 19 MW solar PV array at Nellis Air Force Base, Nevada [8].* - (Source: U.S. Air Force photo/150401-F-ZZ999-002)

exceed 27% efficiency and top performing multi-junction solar PV cells have reached efficiencies of nearly 39% [6].

The performance and cost per watt of terrestrial solar technologies have improved significantly and broadened the range of applications for PVs. These improvements are depicted in Figure 3, which shows solar PV module efficiencies between 1993 and 2019, measured under STC.

The efficiency, reliability, and ease of application of PV systems as a whole, not just PV cells, have dramatically improved in recent years. PV systems have evolved from engineering problems with significant deployment challenges into simple and dependable plug-and-play solutions. The enhancement of PV reliability, stability, and longevity have allowed PV to compete with, and even surpass, established energy technologies in many applications. According to Lazard's levelized cost of energy analysis, in some cases it is more cost effective to build and operate new PV projects than operate existing conventional power generation plants [7].

PV Operational Applications

PV technology can support DoD operations in land, sea, air, space, and cyberspace domains, powering ground bases, vehicles, individual warfighter equipment, and satellites. Applications of solar PV for military applications are shown in Table 1, and each application possesses unique selection criteria and operational considerations. Also included in Table 1 are references to technologies and systems demonstrated within each application.

Solar PV technologies are not suitable for certain applications, such as fighters/bombers, airlift, and ground combat vehicles that require high power, including rapid acceleration. For example, even if the wings of an F-22A or Boeing 747 were *completely* covered with the highest efficiency solar PV cells to date (38.8% [17]), and these cells were producing at full power, they would meet less than 1% of the aircraft's power requirements. These calculations were performed using the thrust required to maintain an airspeed of 265 m/s at 20,000 ft altitude. In such applications, PV cells will never be a viable energy alternative. However, in many other applications solar PV technologies offer opportunities to reduce costs and improve operational effectiveness.

Ground Bases

Ground bases can be classified as fixed installations or contingency bases. Fixed DoD installations are permanent and most rely primarily on the U.S. electrical grid, one of the largest and most complex man-made energy systems in existence, which remains highly vulnerable to threats from natural disasters, physical attacks and cyber-attacks [18] [19]. PV systems can enhance the energy resilience of fixed installations while reducing long-term energy costs. The Nellis I and Nellis II arrays shown in Figure 4 are industrial sized arrays operating at Nellis AFB, Nevada. When combined they form the largest solar PV array in the DoD.

The Nellis arrays were built on excess DoD land. The DoD owns, leases, or otherwise possesses 26.1 million acres of land [20]. If all of the land the DoD possesses were to be utilized for solar PV arrays, this would equate to 6.4 million GWh/yr of generation; 99.7% of the yearly electrical power consumption of

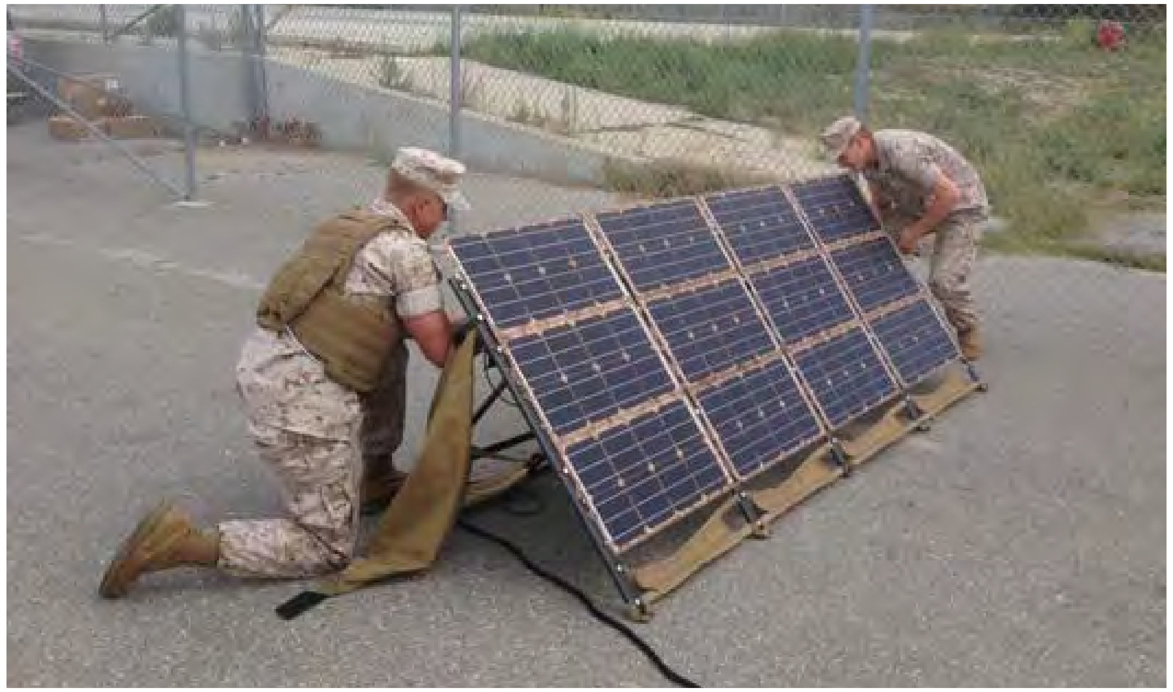


Figure 5: *AISPCA Lightweight Solar Array [9].* - (Source: Author)

Table 1: *Military Applications for Photovoltaics*

Application	Main Selection Criteria	Operational Considerations	Applicable Technology	Demonstrated Examples
Ground Bases				
Fixed Installation	Cost, Lifetime, Maintenance, Area	Permanent, no time constraints for set up and tear down	Mono- or poly-crystalline, Thin-Film, Hybrid	Nellis AFB arrays [8]
Large Contingency Base	Cost, Lifetime, Area, Reliability, Durability	Ease of installation, maintenance, and tear-down	Mono- or poly-crystalline, Thin-Film, Hybrid	N/A
Medium Contingency Base	Mobility, Power to Weight Ratio (PWR), Reliability, Durability	Ease of installation, maintenance, and tear-down	Mono- or poly-crystalline, Thin-Film, Hybrid	N/A
Small Contingency Base	Mobility, PWR, Reliability, Durability	Rapid installation and tear-down	Thin-Film	NAVSEA GREENS & AISPCA [9]
Vehicles				
UAV, Large	PWR, Reliability, Durability	Low speed, long range, long-term missions, high altitude	Thin-Film	Zephyr [10]
UAV, Small	PWR, Reliability, Durability	Low speed, short range, short-term missions, low altitude	Thin-Film	C-Astral LRS [11] AeroVironment Puma AE [12]
Fighter, Bomber	Power, Range	High speed, rapid acceleration, large power requirements	N/A	N/A
Airlift	Power, Range	High speed, large power requirements	N/A	N/A
Ground Combat Vehicle	Power, Range	High speed, rapid acceleration, long range	N/A	N/A
Warfighter Support				
Remote Sensors	Weight, Cost	Low power, ease of installation, mobility	Thin-Film	OK Solar Wireless Military Video Surveillance [13]
Airfield Lighting	Reliability, Durability	Low power, mobility	Thin-Film	Battlefield Military Solar Lights Tower [14]
Aircraft Maintenance	Reliability, Robustness, Durability	High power, battery storage, mobility	Thin-Film	Hybrid Flightline Generator Pathfinder [27]
Wearable electronics	Weight, Cost, Flexibility	Rapid to field, ease of use, disposable	Thin-Film	Rucksack Enhanced Portable Power System (REPPS) [15]
Communications Equipment	Mobility, Reliability, Durability	Rapid to field, ease of use	Thin-Film	NAVSEA SPACES [9]
Satellites				
Satellites	PWR, Critical, Durability, Lifetime, Reliability	State-of-the-art, custom, high efficiency, radiation hardened	Multi-junction Mono-crystalline, Thin-Film, or Tandem	ROSA [16]

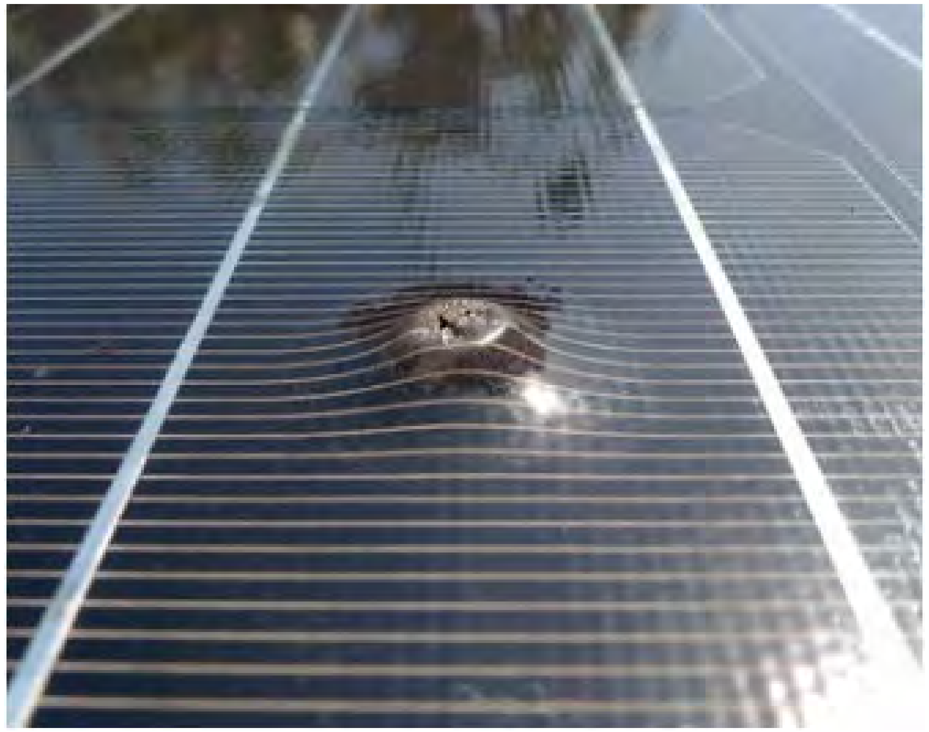


Figure 6: *Ultra-light PV module after a .308 caliber ballistics test at 75 yards [22].* - (Source: Author)

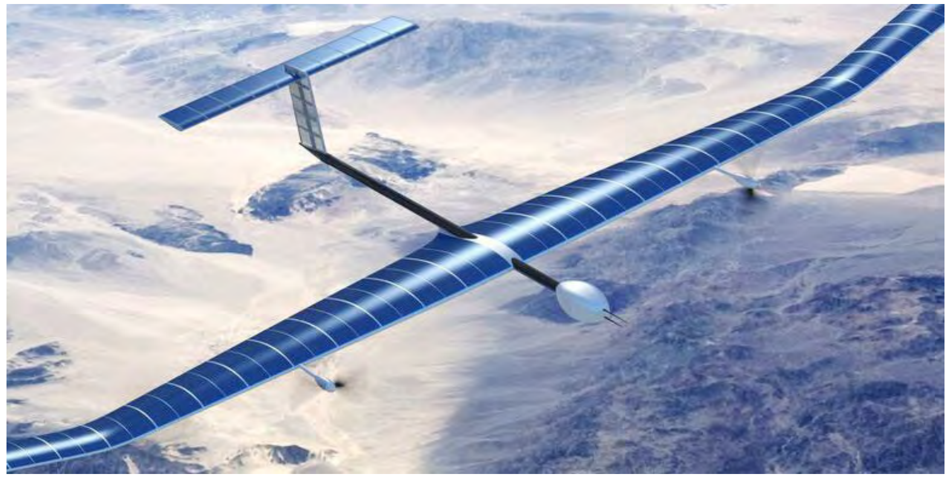


Figure 7: *Zephyr High Altitude Pseudo-Satellite (HAPS) which completed a maiden flight lasting approximately 26 days without landing [10].* - (Source: Author)

the United States, India, and Russia combined. The calculation was performed using an average value of 4.1 acres/GWh/yr for industrial-scale PV arrays [26].

PV arrays are not the only method to utilize excess land – another example is that in 2018, the U.S. Army and Hawaiian Electric Company (HECO) completed the 50 MW biofuel Schofield Generating Station without cost to U.S. taxpayers [21]. The Army provided a 30-year lease of unused land on Schofield Barracks allowing HECO to build and operate the power plant. In the event of a grid outage or natural disaster, HECO will give priority to military energy needs. The result is a secure and cost-effective method of procuring power for DoD fixed installations and the surrounding community. It also allows for grid stabilization and improved integration of renewable resources.

Military contingency bases are often located in austere and/or hostile locations. Remote installations and equipment rely on fuel supply chains which can be cut or degraded and cause significant risk to mission capability. Single-factor dependency on energy requirements pose major risks for all DoD ground bases, and PV technologies have historically demonstrated the ability to improve base load resiliency, redundancy, and offset energy costs. One example of a contingency base PV system is the AISPCA Lightweight Solar Array, which has been demonstrated and is shown in Figure 5.

Improvements to the weight and durability of PV modules will improve the range of applications and functionality for military applications. Figure 6 shows a commercial PV module whose performance is only slightly degraded after being perforated by small arms fire. These modules are also optimized for logistics, and utilize a honeycomb design to decrease their weight by 70 to 80% when compared to a conventional glass-covered panel.

Vehicles

In certain applications, PV systems provide additional capabilities over competing energy technologies. The Zephyr High Altitude Pseudo-Satellite (HAPS) is shown in Figure 7. It is a viable candidate for PV due to its relatively low power requirement and large wing area. The Zephyr can carry intelligence gathering and communications payloads; operating over 100 days without have to land or refuel [10].

Zephyr HAPS meets the capabilities of many satellite systems at a fraction of the cost to build and deploy. The Zephyr operates above 60,000 ft, above most weather disturbances and air traffic. Replacing one conventional UAV with a Zephyr would save 2,000 tons of fuel each year [10].

Individual Warfighter Equipment

Individual warfighter equipment is a broad category with examples including communications equipment optics, lighting and sensors. One PV example in this category is the Solar Portable Alternative Communications Energy System (SPACES), a PV-powered 124W communications suite shown in Figure 8.

Additionally, PV systems can be used for perimeter and airfield lighting, with an example shown in Figure 9. These systems require no refueling reducing operational risk and personnel workload.

> ***"Significant improvements in PV cost and performance increases the number of DoD applications where PV technology is suitable, including ground bases, vehicles, individual warfighter equipment, and satellites."***

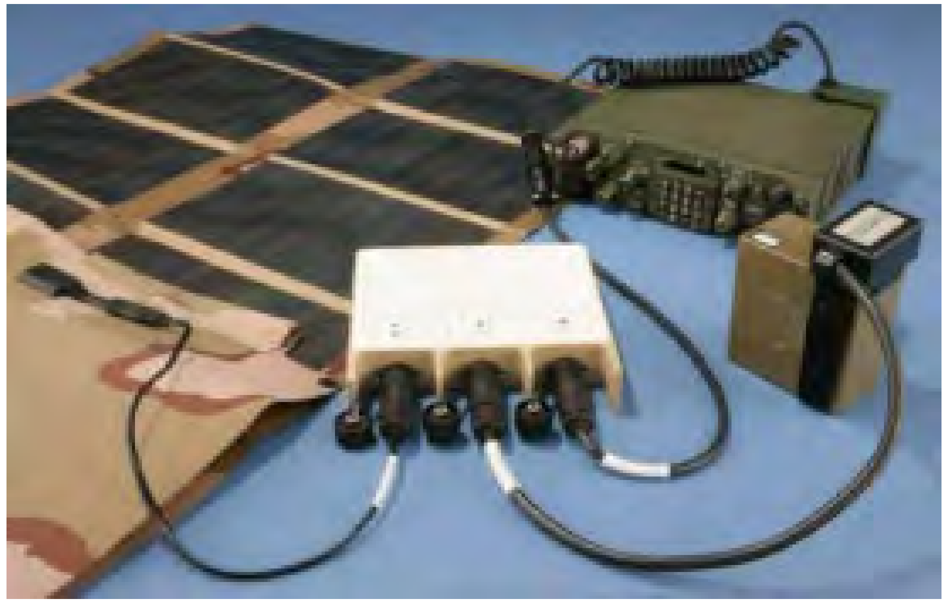


Figure 8: *Solar Portable Alternative Communications Energy System (SPACES) [9].* - (Source: Author)

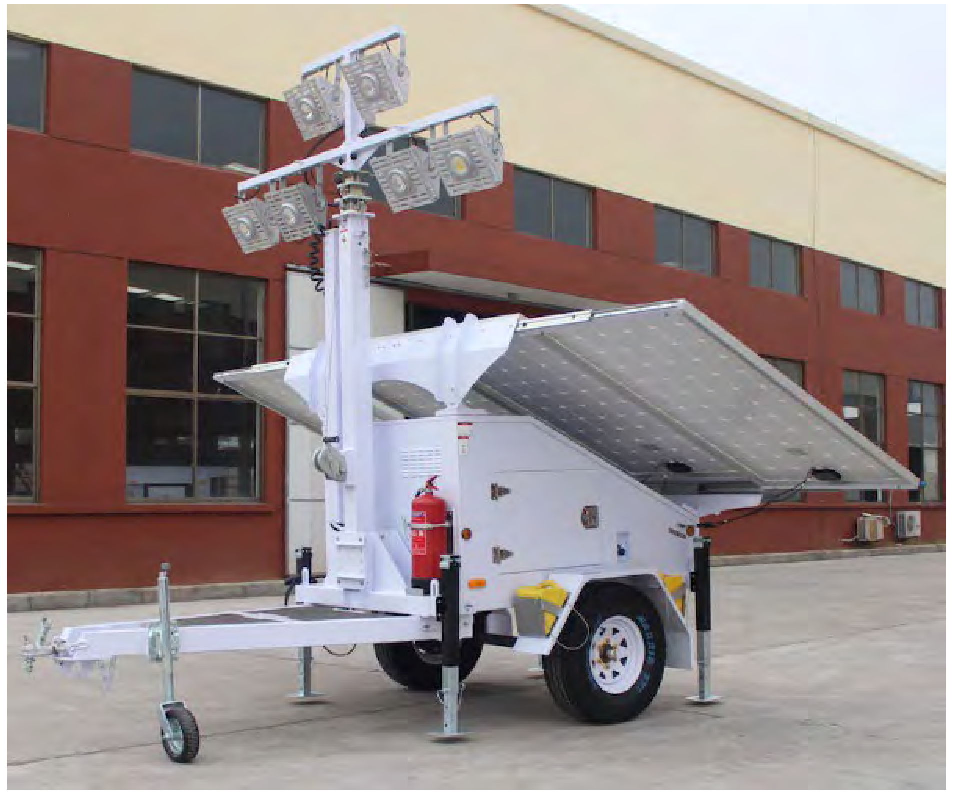


Figure 9: *Battlefield Military Solar Lights Tower [14].* - (Source: Author)

One emerging PV technology involves cheap, flexible, thin-film materials which can be used to power individual warfighter equipment. The potential applications of these devices include but are not limited to heart rate monitors, optical devices, communications equipment, and more. Flexible and wearable PV technologies would be suitable for cheap, mass produced, disposable PV power systems.

Satellites

Space is a tremendously hostile environment – extreme temperature fluctuations, volatile electromagnetic radiation, vacuum pressure and zero gravity. Such an environment requires robust, dependable, PV systems with long lifetimes. The DoD's satellite network contains numerous PV-powered satellites that provide GPS, weather, communications, and intelligence capabilities. A PV example in this category is shown in Figure 10; the Roll Out Solar Array (ROSA) is the largest solar array currently being commercialized for the next generation of GEO spacecraft [16] [23].

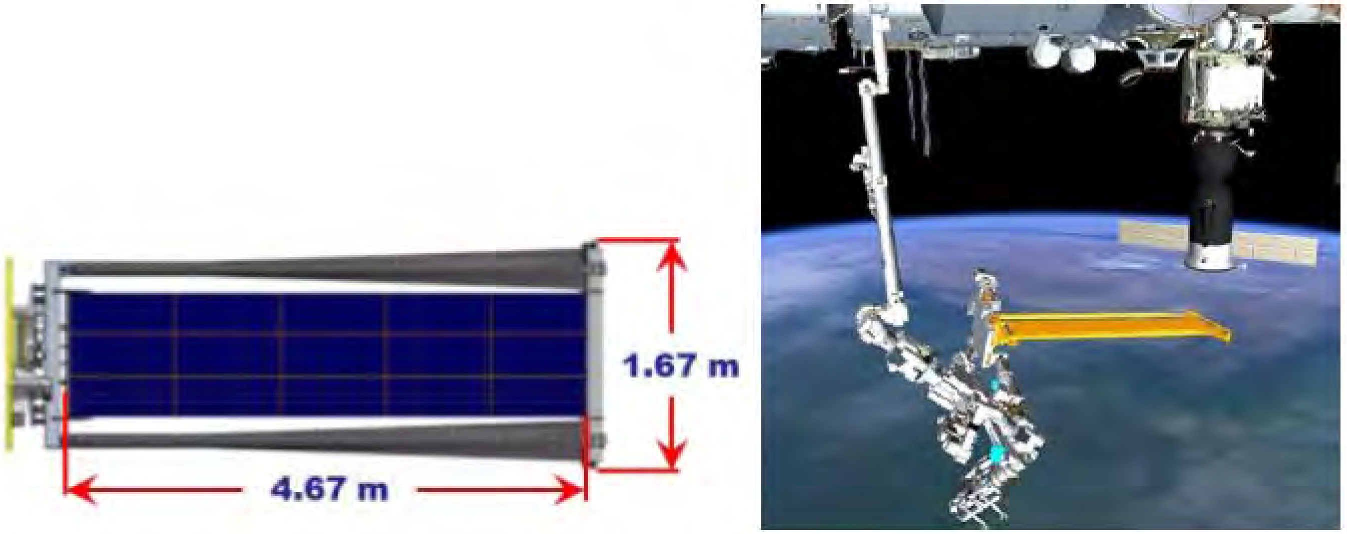


Figure 10: *The Roll Out Solar Array (ROSA) undergoing validation testing on the International Space Station in June 2017 [16] [23].* - (Source: Author)

PVs have already demonstrated their capabilities for space operations and will continue to play a vital role in satellite systems. Ongoing research is also exploring opportunities for large PV arrays in orbit to provide terrestrial energy or power UAVs via wireless transmission [24] [25].

Conclusion

Significant improvements in PV cost and performance increases the number of DoD applications where PV technology is suitable, including ground bases, vehicles, individual warfighter equipment, and satellites. This work provides a survey of fielded technologies, and highlights the operational considerations for effectively deploying PV modules in a variety of DoD applications, and gives examples of currently fielded PV-powered systems. PV technology has the potential to increase DoD capability, improve resilience and cut costs, and the DoD can play a key role in the research, development, demonstration and utilization of PV in a variety of mission areas. ■

References

[1] Office of the Assistant Secretary of Defense for Energy Installations and Environment, "Department of Defense 2016 Operational Energy Strategy," 2016.

[2] W. Shockley and H. J. Queisser, "Detailed balance limit of efficiency of p-n junction solar cells," ***Journal of Applied Physics,*** vol. 32, no. 3, pp. 510-519, 1961.

[3] S. Kurtz, D. Myers, W.E. McMahon and M. Steiner, "A comparison of theoretical efficiencies of multi-junction concentrator solar cells," ***Progress in Photovoltaics: research and applications,*** vol. 16, no. 6, pp. 537-546, 2008.

[4] M. A. Green, "The path to 25% silicon solar cell efficiency: history of silicon cell evolution.," ***Progress in Photovoltaics: Research and Applications,*** vol. 17, no. 3, pp. 183-189, 2009.

[5] P. A. Jones and B. R. Spence, "Spacecraft Solar Array Technology Trends," in ***1998 IEEE Aerospace Conference Proceedings***, 1998.

[6] D. H. Levi, M. A. Green, Y. Hishikawa, E. D. Dunlop, H.-E. Jochen and A. W. Y. Ho-Baillie, "Solar Efficiency Tables (Version 51)," ***Progress in Photvv***. Levi, M. A. Green, Y. Hishikawa, E. D. Dunlop, H.-E. Jochen and A. W. Y. Ho-Baillie, "Solar Efficiency Tables (Version 51)," ***Progress in Photovoltaics,*** vol. 26, no. 7, 2018.

[7] Lazard, "Lazard's Levelized Cost of Energy Analysis - Version 12.0," 2018.

[8] Elliot, Kevin, Air Force Civil Engineer Center, 04 April 2015. [Online]. Available: https://www.af.mil/News/Article-Display/Article/583512/nellis-breaks-ground-on-dods-largest-solar-array/. [Accessed 2019 July 28].

[9] M. Huffman, ***DoD Expeditionary Renewable Energy Current and Future Needs,*** NSWC Advanced Power & Energy Branch (APEB), 2019.

[10] Airbus, "Airbus Defence," [Online]. Available: https://www.airbus.com/defence/uav/zephyr.html. [Accessed 2019 July 28].

[11] C-Astral Aerospace Ltd, "Unmanned Systems," [Online]. Available: https://www.c-astral.com/en/unmanned-systems. [Accessed 30 July 2019].

[12] AeroVironment Inc, "Tactical Unmanned Aircraft Systems," [Online]. Available: https://www.avinc.com/uas/view/puma. [Accessed 2019 July 30].

[13] OK Solar, "Renewable Energy Systems," [Online]. Available: https://www.oksolar.com/lion/Item/80007/solar-powered-wireless-military-video-surveillance. [Accessed 11 September 2019].

[14] General Renewable Energy Solutions, [Online]. Available: https://www.generalcommunications.com/store/solar-energy/item-detail/military-battlefield-solar-light-tower/military/8024/battlefield-military-solar-lights-tower. [Accessed 30 July 2019].

[15] Bren-Tronics, [Online]. Available: https://www.bren-tronics.com/systems.html. [Accessed 9 September 2019].

[16] Merril et al., "Advanced Photovoltaic Power System Development at the U.S. Air Force Research Laboratory," Air Force Research Laboratory, 2017.

[17] M. A. Green, Y. Hishikawa, E. D. Dunlop, D. H. Levi, J. Hohl-Ebinger, M. Yoshita and A. W. Ho-Baillie, "Solar cell efficiency tables (Version 53)," ***Progress in Photovoltaics: Research and Applications,*** vol. 27, no. 1, pp. 3-12, 2018.

[18] G. Chen, Z. D. Dong, D. J. Hill, G. H. Zhang and K. Q. Hua, "Attack structural vulnerability of power grids: A hybrid approach based on complex networks," ***Physica A: Statistical Mechanics and its Applications,*** vol. 389, no. 3, pp. 595-603, 2010.

[19] E. W. Prehoda, C. Schelly and J. M. Pearce, "US strategic solar photovoltaic-powered mircrogrid deployment for enhanced national security," ***Renewable and Sustainable Energy Reviews,*** vol. 78, pp. 167-175, 2018.

[20] C. H. Vincent, L. A. Hanson and J. P. Bjelopera, "Federal land ownership: Overview and data," Congressional Research Service, Washington, DC, 2017.

[21] Hawaiian Electric Company, "Hawaiian Electric, U.S. Army announce completion of Schofield Generating Station," 31 May 2018. [Online]. Available: https://www.hawaiianelectric.com/hawaiian-electric-us-army-announce-completion-of-schofield-generating-station. [Accessed 9 September 2019].

[22] Armageddon Energy, "Solarclover - Military," [Online]. Available: https://www.armageddonenergy.com/military. [Accessed 2019 July 30].

[23] Montgomery, Kyle, et al., "Advanced Space Power Technology Development at the Air Force Research Laboratory," in ***AIAA Scitech 2019 Forum***, 2019.

[24] A. Fayaz and M. R. Husain, "Energy replenishment using renewable and traditional energy resources for sustainable wireless sensor networks: A review," ***Renewable and Sustainable Energy Reviews,*** vol. 45, pp. 769-784, 2015.

[25] M. Simik, C. Bil and V. Vojisavljevic, "Investigation in wireless power transmission for UAV charging," ***Procedia Computer Science,*** vol. 60, pp. 1846-1855, 2015.

ABOUT THE AUTHORS

LT MARTIN-ABOOD received a BS in Electrical Engineering from the United States Air Force Academy in 2018. While pursuing his undergraduate degree he participated in a five week internship at MIT Lincoln Laboratory, building and testing a portable solar power system intended for disaster relief operations. He is currently pursuing a MS in Electrical Engineering at the Air Force Institute of Technology (AFIT), Wright-Patterson Air Force Base (WPAFB), Ohio, studying microelectronics and micro-electromechanical systems. His research is focused on non-planar photolithography and reactive ion etching for additive manufacturing on integrated circuits.

LT COL WAGNER received the BS in Electrical Engineering from the University of Minnesota, Minneapolis, Minnesota, the MS degree in Aerospace Systems Engineering from Loughborough University, UK, and the Ph.D. degree in Electrical Engineering from AFIT, WPAFB, Ohio. He is currently with AFIT in the Department of Systems Engineering & Management, and research interests include agile software systems engineering, and DoD-focused energy systems engineering for fixed installations, contingency bases & individual warfighter equipment.

DR. DUDIS received the BS in Chemistry from the University of Dayton, Dayton, Ohio and the Ph.D. degree in Inorganic Chemistry from Case Western Reserve University, Cleveland, Ohio. He is currently the Air Force Research Laboratory Energy Office Lead, WPAFB, Ohio, and provides guidance to professional societies and strategic energy forums at the USAF, DoD, interagency, and international levels. He has experience leading research in an active laboratory and has supervised and mentored numerous masters and doctorial students, faculty, and postdoctoral researchers.

[26] S. Ong, C. Campbell, P. Denholm, R. Margolis and G. Heath, "Land-use requirements for solar power plants in the United States," NREL, Golden, 2013.

[27] K. Thuloweit, "Hybrid generator could make aircraft maintenance more efficient, effective, user friendly," 412th Test Wing Public Affairs, USAF, 17 April 2018. [Online]. Available: https://www.edwards.af.mil/News/Article/1494886/hybrid-generator-could-make-aircraft-maintenance-more-efficient-effective-user. [Accessed 9 September 2019].

Are you ready

to shape the future of the world's greatest military?

Our service members

are counting on you to field cutting-edge technologies
to maintain their edge on the battlefield.

Let Defense Technical Information Center (DTIC) help you get started.

For almost 75 years, DTIC has served the information needs of the defense communities through the collection and preservation of the DoD's multi-billion dollar annual investment in science and technology. We have over 4.5 million S&T documents in our collection—technical research, budget reports, conference proceedings, grant awards, and international agreements—to enable eligible users from the DoD labs, academia, federally-funded research and development centers, and industry partners to better align their resources, test novel concepts, and develop new capabilities. Our tools and resources provide insights on research outcomes, technology development, and maturity; enable tracking of DoD investments and capability gaps; and help identify partnership opportunities.

Give us a try.

We're ready for you.

Visit: https://go.usa.gov/xd62Y today.

Defense Technical Information Center (DTIC) | Fort Belvoir, Virginia 22060
https://discover.dtic.mil (Public) | https://www.dtic.mil (NIPR) | https://www.dtic.smil.mil (SIPR)

The New START Treaty's Role in Arms Control and its Future

By: **Dirk Plante**, Deputy Director, HDIAC

This is a pivotal year in the life of the New START Treaty, as 2020 marks the tenth and final year of the treaty, in which the United States and Russia may agree to extend the treaty for a period of no more than five years. If allowed to expire it will remove all limits on the number of deployed as well as non-deployed strategic weapons and delivery systems that both sides can have.

ENTERED INTO FORCE ON February 5, 2011, during the Obama Administration, the New Strategic Arms Reduction Treaty (START) (formally known as the Treaty between the United States of America and the Russian Federation for the Further Reduction and Limitation of Strategic Offensive Arms) succeeded the previously negotiated Moscow Treaty (formally known as the Treaty between the United States of America and the Russian Federation on Strategic Offensive Reductions) [1]. The Moscow Treaty was finalized during the George W. Bush Administration and signed in 2002.

At the time of this publication, Russia has said that it is prepared to sign on to the five-year extension without preconditions [2]. The United States has not made a similar statement regarding a decision on whether to seek an extension [3]. In recent remarks, President Trump stated that he was considering replacing the bilateral discussions to renew or replace the New START Treaty with a trilateral discussion that would engage China, Russia and the United States in nuclear arms reduction talks [3, 4]. With less than a year until the New START Treaty is set to expire, unless extended or superseded by a new agreement, now is a good time to better understand the New START Treaty.

This article takes a look at what the New START Treaty is, the limits it places on strategic weapons and delivery vehicles, and discusses potential consequences if the treaty is not extended.

> *"Russia has said that it is prepared to sign on to the five-year extension without preconditions [2]. The United States has not made a similar statement regarding a decision on whether to seek an extension [3]."*

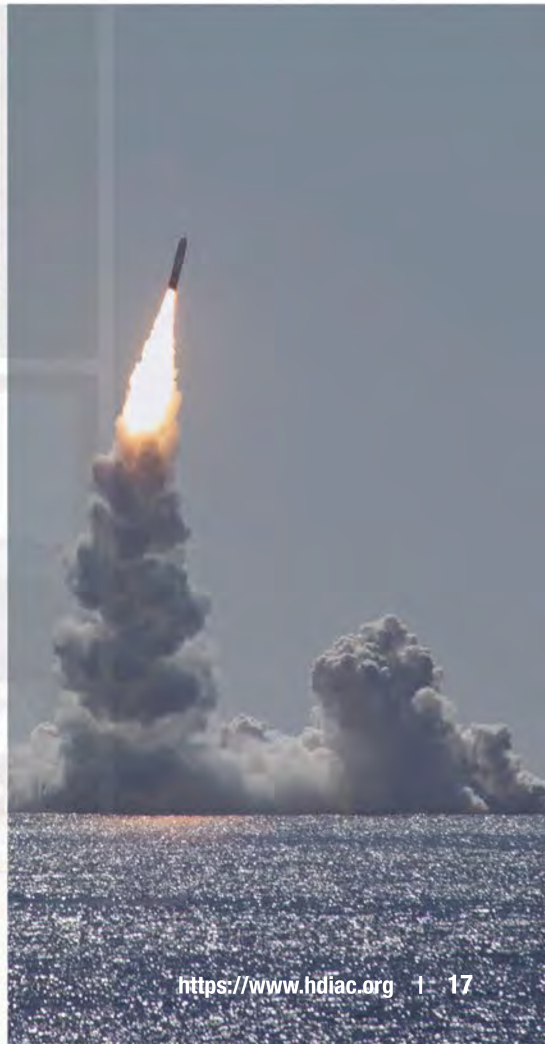


Photo Credits: Air Force Airman 1st Class Christina Carter\200308-F-PJ022-1001Y, 726731-C-FFH15-078, Navy Petty Officer 2nd Class Thomas Gooley\200212-N-EA818-0055, Lt. Cmdr. Michael Smith\180311-N-TC277-0076C, Air Force Senior Airman Clayton Wear\200105-F-XJ735-1005M

What is the Old START Treaty?

Discussing the New START Treaty must begin by answering, "What is the Old START Treaty?" From the late 1960s and continuing to the present day, the United States has negotiated a number of bi-lateral agreements and treaties with Russia, and the Soviet Union previously, to limit the number of strategic nuclear weapons and reduce the risk of their inadvertent use. Each succeeding treaty reduced the number of deployed nuclear weapons. For the United States, the number is down more than 85 percent from its Cold War high [5]. Table 1 lists the treaties that the United States and the Soviet Union/Russia have negotiated and signed over the past 50 years to reduce the number of strategic nuclear weapons [6].

It's important to note the distinction between a treaty being signed and a treaty being ratified. A treaty is signed, following its negotiation, by the leaders of the countries, typically in a public signing ceremony. And a treaty is ratified, following its signing, by the legislatures of the countries. Only after ratification does the treaty enter into force, which then requires the countries to meet their treaty obligations.

> *"If New START is not extended it will not be the first time that the United States and Russia have gone without a ratified treaty to obligate limits on their strategic nuclear weapons."*

Negotiations for the "old" START Treaty began in the early 1980s, during the Reagan Administration, and concluded in 1991, during the George H.W. Bush Administration, with the signing of the Treaty at Moscow on July 31, 1991. Later that year the Soviet Union collapsed, formally ceasing to exist on December 26, 1991, and the republics that made up the Soviet Union declared their independence. Russia was now one of four countries from the former Soviet Union possessing strategic nuclear weapons. The other three were Ukraine, Kazakhstan, and Belarus. In the Spring of 1992, those four nations and the United States negotiated a protocol to the START Treaty that "recognized Russia as the successor state to the Soviet Union's nuclear rights and obligations [7]," which resulted in the return of all of the former Soviet Union's weapons and delivery systems to Russia.

Table 1: *Negotiated Treaties between the United States and the Soviet Union/Russia*

Nuclear Weapons Treaty	Year Signed
Strategic Arms Limitation Talks (SALT I)	1969
SALT I Interim Agreement	1972
Strategic Arms Limitation Talks II (SALT II)	1979
Intermediate-Range Nuclear Forces (INF) Treaty	1988
Strategic Arms Reduction Treaty (START)	1991
Strategic Arms Reduction Treaty II (START II)	1993
The Moscow Treaty	2002
New Strategic Arms Reduction Treaty (New START)	2010

Article II of the START Treaty limited both sides to no more than 6,000 total warheads within seven years of entry into force. This figure of 6,000 total warheads was counted as individual warheads loaded on various delivery platforms: deployed intercontinental ballistic missiles (ICBMs), submarine-launched ballistic missiles (SLBMs), deployed ICBMs on mobile launchers (note: the Soviet Union had mobile launchers, the United States did not), and deployed heavy bombers [8].

The START Treaty was set to expire in 2009, but before then the two countries negotiated, signed and ratified a new treaty. Known informally as the Treaty of Moscow, and officially as the Treaty Between the United States of America and the Russian Federation on Strategic Offensive Reductions (SORT)), it entered into force on June 1, 2003. It limited both sides to no more than 2,200 operationally deployed warheads. Although set to expire in 2012, it would be replaced New START in 2011.

How Many Weapons Can Each Nation Have under the New START Treaty?

Surprisingly, the answer to how many weapons does each side have under the treaty is, "It depends!" Although the New START Treaty limits both sides to 1,550 strategic nuclear weapons, to be achieved within seven years of entry into force, determining what counts as a strategic nuclear weapon may lead to a number greater than 1,550, yet not violate the treaty.

Under the New START Treaty, total warheads are counted differently than they were in previous treaties, specifically regarding heavy bombers. Rather than continuing to count unique individual strategic nuclear weapons that can be delivered via heavy bombers, the New START treaty actually counts the number of heavy bombers in its total warhead count, regardless of how many warheads the heavy bombers can deliver. For example, if the United States has 20 heavy bombers capable of carrying 40 nuclear weapons, the total number of weapons counted against the Treaty limit is 20, and not 40. Article III of the Treaty states, "[F]or the purposes of counting toward the aggregate limit provided for… in this Treaty: … One nuclear warhead shall be counted for each deployed heavy bomber [9]." However, the same unique counting does not happen with ICBMs and SLBMs. For example, if an ICBM or SLBM has eight warheads, the aggregate count towards the treaty limit is eight, not one. Thus, with the unique counting of weapons carried by heavy bombers, it is possible for either side to possess more than 1,550 strategic nuclear weapons, yet not be in violation of the treaty.

The New START Treaty allows for 1,550 warheads spread among no more than 700 deployed ICBMs, deployed SLBMs and deployed heavy bombers, and among no more than 800 total **deployed and non-deployed** ICBM launchers, SLBM launchers, and heavy bombers. [8] As of 1 September 2019, the United States counted 668 ICBMs, SLBMs, and heavy bombers as deployed, with 1,376 total warheads [10].

What Happens if Both Sides do Nothing?

If the United States and Russia allow the New START Treaty to expire it will remove the current limits on the number of deployed and non-deployed strategic weapons and delivery systems. However, it is unlikely this would lead to a new arms race that sees both sides increase their arsenals to Cold War highs of tens of thousands of weapons. It is unlikely that the United States arsenal would increase. The Department of Defense's 2018 Nuclear Posture Review (NPR) assessed that even in an evolving and uncertain international security environment, the United States reaffirmed a commitment to "the ultimate global elimination of nuclear, biological, and chemical, weapons [4]." And more specifically, the NPR points out that the United States met its New START Treaty obligations ahead of the 2018 deadline, and it doesn't call out for increasing the number of nuclear weapons or delivery systems during the modernization efforts of the nuclear enterprise.

Currently, both sides are able to conduct up to 18 on-site verification inspections annually, something that would be halted if the treaty is not extended. Although there are benefits to on-site inspections if the treaty is extended, both countries certainly have national technical means to aid in gathering intelligence and determining nuclear activities to varying degrees of thoroughness. However, what would be lost without on-site inspections is the face-to-face interactions between Russian and American officials, which contribute to building of successful, positive long-term relations between the two countries.

If New START is not extended it will not be the first time that the United States and Russia have gone without a ratified treaty to obligate limits on their strategic nuclear weapons. For example, in 1979 the countries signed the second Strategic Arms Limitation Talks (SALT II) Treaty, but the treaty was not ratified, and thus it did not enter into force. However, both countries followed the terms of SALT II well into the next decade. It was during the 1980's when the countries held negotiations for the first START Treaty, which was signed in 1991.

Conclusion

Clearly, it is better to have arms control treaties between the two countries with the largest nuclear warhead stockpile than it is to not have such agreements. Beginning with the SALT I Treaty, negotiated in 1969 during the Nixon Administration, the two countries have always sought negotiations to put limits on their nuclear arsenals. The trend has always been further reductions in deployed weapons on both sides with each succeeding treaty. With or without an extension, if the result is that New START is replaced by a treaty that further reduces nuclear weapon stockpiles of the United States and Russia, that will be the outcome welcomed by the international community. ■

References

[1] The official New START website for the United States can be found at the following United States Department of State website: https://www.state.gov/new-start/

[2] Brennan, David. "America is risking a nuclear 'free-for-all' by delaying New START extension with Russia: Former National Security Official." Newsweek, accessed at https://www.newsweek.com/america-risking-nuclear-free-all-delaying-new-start-extension-russia-national-security-official-1482542, on January 22, 2020.

[3] Pifer, Steven. "Trumps Bid to Go Big on Nuclear Arms Looks Like a Fizzle." Defense One, accessed at https://www.defenseone.com/ideas/2020/02/trumps-bid-go-big-nuclear-arms-looks-fizzle/162914/, on February 5, 2020.

[4] Oronez, Franco. "Trump's Push for Lofty Nuclear Treaty Sparks Worry over Current Deal." NPR, accessed at https://www.npr.org/2020/01/01/792725906/trumps-push-for-lofty-nuclear-treaty-sparks-worry-over-current-deal, on January 17, 2020.

[5] *2018 Nuclear Posture Review*. (February 2018). Washington, DC: Department of Defense.

[6] Treaties of the United States can be found on the Department of State's Bureau of Arms Control, Verification, and Compliance website at: https://www.state.gov/key-topics-bureau-of-arms-control-verification-and-compliance/

[7] Reed, Thomas C. and Stillman, Danny B. (2009). The Nuclear Express: A Political History of the Bomb and its Proliferation. Minneapolis, MN: Zenith Press.

[8] Treaty Between the United States of America and the Union of Soviet Socialist Republics on the Reduction and Limitation of Strategic Offensive Arms, U.S. Government Printing Office: 1991.

[9] The full text of the New START Treaty can be found at the Department of State website at: https://2009-2017.state.gov/documents/organization/140035.pdf

[10] Fact Sheet, New START Treaty Aggregate Numbers of Strategic Offensive Arms, January 1, 2020; Bureau of Arms Control, Verification, and Compliance, United States Department of State, accessed at https://www.state.gov/wp-content/uploads/2019/12/AVC-New-START-Jan-2020.pdf, on January 2, 2020.

ABOUT THE AUTHOR

DIRK PLANTE is the Deputy Director of the Homeland Defense and Security Information Analysis Center. He retired from the United States Army in 2019 following a 30-year career as a basic branch Engineer officer and a functional area 52 (Nuclear and Counterproliferation) officer. From 2011 to 2014 he served on the Army Staff working treaty compliance matters for the Army, including New START Treaty compliance visits by the Russians. His final assignment in the Army was as Chief, Survivability & Effects Analysis Division at the U.S. Army Nuclear and Countering WMD Agency, Fort Belvoir, VA, overseeing the Army CBRN Survivability Program, and the Army Reactor Office. He holds a M.S. in Nuclear Engineering from the Air Force Institute of Technology, Wright-Patterson Air Force Base, OH and a M.S. in Strategic Studies from the Army War College, Carlisle Barracks, PA. His email address is dplante@hdiac.org.

Capitalizing on the Super-Recognition Advantage:

A Powerful, but Underutilized, Tool for Policing and National Security Agencies

By: **Josh P. Davis, Ph.D.**, University of Greenwich, and **David J. Robertson, Ph.D.**, University of Strathclyde

Accurate identity judgements are critical in ensuring that suspects can be apprehended by law enforcement and national security agencies, and that identity fraud attacks do not go undetected at border control points. Research has shown that typical human observers are poor at facial recognition in these contexts. However, there is now a decade's worth of psychological science which shows that some individuals - known as super-recognizers - excel at such tasks. This article reviews the latest super-recognition science for agencies to consider implementing to enable a powerful and cost-effective identity verification advantage.

Photo Credit: Deposit Photos/peshkov

Introduction

Police have long been aware of the fallibility of eyewitness memory and subsequent testimony. In over 70 percent of 365 DNA-exoneration cases, innocent defendants were identified by mistaken witnesses [1]. More routinely, 25 percent of witnesses identify known-innocent foils from United States (U.S.) and United Kingdom (U.K.) line-ups, despite instructions that the perpetrator may not be present [2]. Closed circuit television (CCTV) implementation was marketed as a solution, allowing permanent crime scene image retention to facilitate suspect identification without necessarily having to draw on human memory. Even with low-quality images, highly familiar face recognition is normally reliable [3], although suspect familiarity will vary (i.e. since last encounter). However, most police officers are unfamiliar with most suspects, and unfamiliar face recognition is highly prone to error, even when high-quality images are available [4]. Recent research, however, has demonstrated large individual differences in unfamiliar face recognition ability [5], with those at the top end labelled as 'super-recognizers' (SRs) [6]. Over the past 10 years, a small number of international police forces, identity verification organizations (i.e. border control), and businesses have deployed SRs to take advantage of their superior facial identity verification skills [7, 8].

Establishing The Super-recognizer Advantage

While the first scientific study on super-recognition was published in 2009 [6], it was not until April 2011 that real-world cases of super-recognition within a policing context were first detected. The lead author, working in collaboration with London's Metropolitan Police Service ('the MET'), found that a particular set of officers were making frequent and highly accurate suspect identifications ('idents') from CCTV images captured across London. Subsequent research on these SRs by Davis et al. [7] and Robertson et al. [8] found that they outperformed typical face recognisers on a number of facial recognition tests. These tests used both familiar, learned, and unfamiliar faces, and which tapped memory for faces (i.e. recognizing a suspect from CCTV) and simultaneous face matching (i.e. deciding whether the face of the individual in the interview room matched the face of the suspect held on file). Since 2016, a number of additional peer-reviewed scientific studies have shown that the SR advantage is sustained even if the ethnicity of the target identity is not that of the SR observer [9] (see Fig. 1), if the targets are very young children [10], or are placed within complex visual scenes such as crowd videos [11]. Superior performance in SRs appears to be a face-specific and due to heritable individual differences unrelated to experience or training (i.e. we cannot train typical recognisers to be SRs [12, 13]).

Super-recognizers' Successes in Policing

Following the research described above [7], 20 of the MET SRs recruited to the study made more than 600 idents of often-disguised London rioters after lawlessness erupted across the city in August 2011. One SR correctly identified 180 suspects [14]. These MET SRs had rarely met rioters in person, or if familiar, had sometimes not encountered them for many years. In these cases, rioters had been tracked through different CCTV feeds to extract the best quality image for matching against mugshot databases. Most SR-identified rioters were convicted (> 70 percent), after inculpating evidence was secured, such as stolen property, confessions, or clothing matching that seen in the CCTV images. This success, which was generated simply by identifying existing officers within the force who excelled at facial recognition, was followed up by expanded testing and the identification of more MET SRs. A full-time New Scotland Yard Super-Recognition Unit became operational in May 2015. A German SR unit has now also been set up in Munich by the Bavarian State Police after similar testing of 5000 police officers (see [15] for a review).

The MET statistics reported in the media [16] show that this new Super-Recognition Unit led to substantially increased identification rates, as well as prosecutions and convictions for volume (theft, robbery) and highly serious crimes (murder, attempted murder, rape). MET SR Unit officers accomplished this by matching new images with those stored in a central repository of London's unsolved crimes. Other MET SRs worked in front line roles. Prioritized viewing of images of crime-types for which they were an expert or those from their vicinity resulted in multiple familiar suspect identifications. MET SRs sometimes committed to memory large numbers of facial photos of suspects prior to large public events, aiming to recognize them in the crowds. Others reported spontaneously spotting wanted fugitives, for instance, on public transport while off-duty. While the SRs do have an exceptional talent for facial identification, they, like automatic facial algorithms [17] are not infallible. It is not possible to estimate how many suspects they missed in similar circumstances. Nevertheless, using SRs, identified through short scientific tests which can be completed online to ensure that frontline police time is not affected, can significantly improve suspect identification rates in a variety of contexts.

Super-recognizer's in Border Control/Facial Image Matching Contexts?

As outlined above, the scientific basis allied with case study support from the MET suggests that introducing SR units would be advantageous to all police forces. SRs are also likely to enhance the detection of identity fraud attacks at border control points (or indeed any identity task in which one has to match a face to a face photo in an identity document). At border control, passport checking officials are required to match the face of an unfamiliar traveller standing in front of them, to the face photo in their passport. Typical recognizers perform poorly at this task with typical error rates in ideal viewing conditions of around 10 percent, which is a non-trivial level of error [18]. Identity fraudsters seeking to enter a country illegally will often present a stolen passport showing an individual to whom they bear a likeness. Checking officials must detect when the faces mismatch, and research has shown that SRs are also likely to excel at this task [7]. SRs are more likely to spot a fraud attack in which a fraudster's face and the passport photo they present actually show two different, but similar looking, individuals.

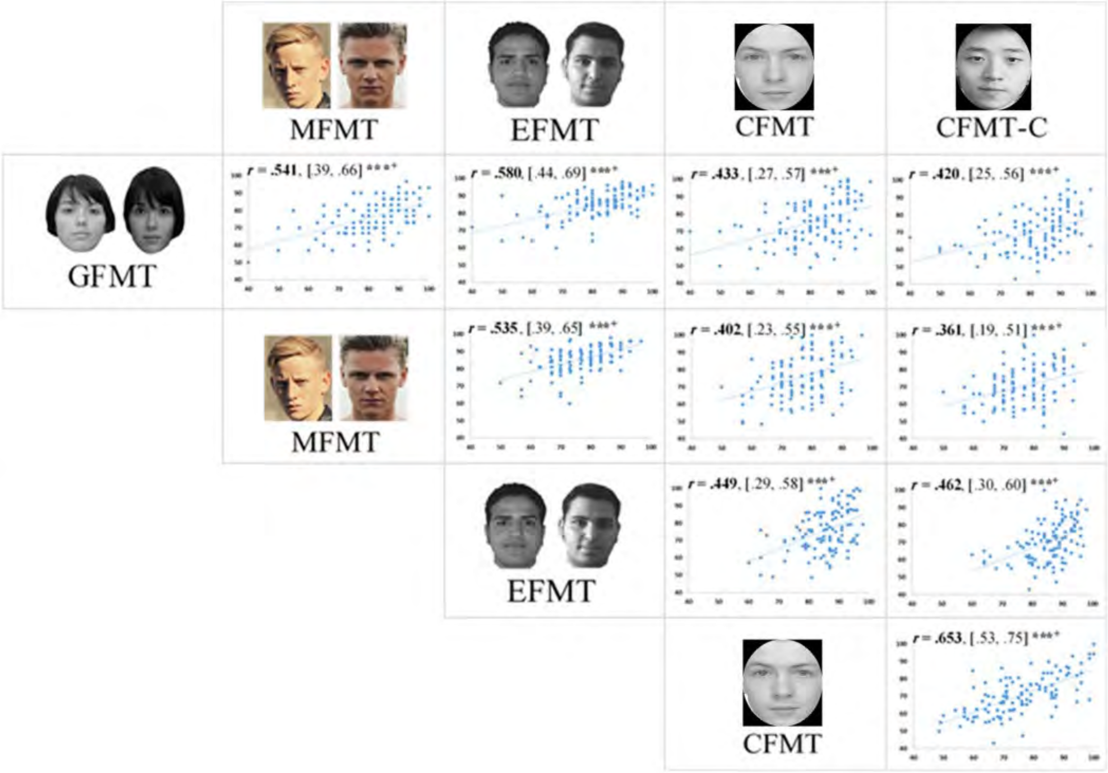


Figure 1: *Data from [9] showing that individuals at the top end of the facial recognition ability spectrum excel across a variety of face-based tasks. This ability remains even when the target face is from a different ethnic group than that of the observer (Glasgow Face Matching Test (GFMT), Models Face Matching Test (MFMT), Egyptian Face Matching Test (EFMT) - unfamiliar face matching; Cambridge Face Memory Test (CFMT), Cambridge Face Memory Test-Chinese version (CFMT-C) - learned face memory).*

Are There Limitations to Super-recognizer's Skills?

There are important limitations to SR's abilities, however. First, the SR advantage appears to be specific to faces [13]. SRs perform no better at identifying non-face objects (e.g. cars) than typical recognizers. Such individuals would be likely of little use in supporting the recovery of stolen vehicles or other goods. Second, only two percent of the population possess the SR ability as it is currently defined. However, dependent on task, workplace operations may also be enhanced by recruiting those at the 'top end of typical', while redeploying poor recognizers to non-identity based tasks. Third, recent research suggests that identity recognition performance is not connected to the ability to detect hyper-realistic face masks [9, 19]. Also, only small correlations have been reported between identity verification accuracy and the ability to detect fraudulent passport morphs (e.g., [20]).

What About Facial Recognition Algorithms?

In terms of morph and hyper-realistic mask fraud attacks, computerized face recognition algorithms may be more accurate (e.g. for morph detection, see [21]). Indeed, in many operations, such as passport checking at border control, in which thousands of daily identity verification decisions are required, algorithms facilitate fast accurate checking of the passports of most lawful travellers. However, current facial recognition algorithms, like SRs, will not always provide perfect levels of identity verification performance [22, 23]. More generally, concerns have been raised by privacy advocates, politicians and the public about their indiscriminate use in other types of public space [24]. National Institute of Science and Technology appraisals have shown that some systems are more likely to misidentify members of specific ethnic groups [25]. Furthermore, highly publicized police tests in the street and at sports stadiums in the United Kingdom resulted in police questioning innocent people, wrongly identified as being fugitives from justice [26]. Most errors were quickly rectified following human review - and this is the conundrum. In legal settings, it is human system operators -- police officers, or jury members -- who determine identity, and not the algorithms. This has led to a call to pair our current best performing algorithms with SRs to achieve current best possible performance.

How Can We Best Achieve Best Possible Identity Verification Right Now?

Algorithm performance can be predicted by certain factors. These include image quality, changes in physical appearance of targets (i.e. age, skin tone, facial hair) and most importantly the size of the Photo-ID database against which a target image is being compared, and the associated risk of doppelgänger identification [26]. Only one study has directly compared algorithms and SRs at one-to-one matching of twenty pairs of high-quality facial images previously identified as being extremely hard to match [17]. The performance of the top-performing commercial algorithm matched the mean scores of the SRs, with both significantly outperforming controls. Intriguingly, the fusion of algorithm and SR decision-making resulted in the highest levels of accuracy. This effect is similar to the wisdom of the crowd paradigm.

Amalgamating independent simultaneous face matching decisions from individuals in order to form a 'crowd,' is more accurate than individual decisions alone (e.g. [27]). Davis et al. [28] showed that face matching accuracy may be further enhanced when the crowd is made up of SRs. After forensic facial examiners declined to assist an investigation because the key image was not of sufficient quality, the authors assisted police in verifying identification of a 1970's facial photograph of a drowned man. They created a line-up containing a photo of a man who was reported missing to police at about the same time (the target) and seven foils depicted in contemporary photos. These foils were of the same 'age, appearance and position in life'. Compared to individual police controls and SRs, and to a crowd of police controls, a crowd of police SRs was more likely to confidently match the deceased and target photo. A coroner ruled that this case study, and other documents provided sufficient evidence to allow a death certificate to be issued on the assumption that both photos depicted the same person.

From Science to Society: How Can Police Forces/ Security Agencies Select and Implement Super-recognizer Teams?

The logical approach, and the prevailing view within the literature, is that SRs must be selected on the basis of consistently high scores across a battery of facial recognition tests. Such tests must reflect the types of identity checks, interfaces, ages, ethnicities, time pressure, and work pattern factors that the officer or official is likely to encounter on the job (e.g. [29]). Applied cognitive science has a battery of tests that could assist police forces or government agencies in identifying potential SRs. Then, new job-specific tasks would be created which match, as closely as possible, the real-world role/interface. Only prospective SRs who perform well on the existing tests, and who have their SR status confirmed by performance on specific tasks should be recruited for that role. For organizations seeking to increase the pool of top-level identity checkers, the 'top end of typical' could also be recruited in the same way. It is important not to sacrifice significant improvements, through the selection of SRs and better-than average performers coupled with the redeployment of poor recognizers, in the search for perfection (i.e. SR-only units).

Conclusion

This article has provided a short review of the latest in SR science and provided some examples of real-world SR successes. There are limitations to the abilities of SRs, but there is now strong evidence which supports more widespread consideration of SRs among police forces and security agencies. Pairing SRs with our best algorithms is the most likely approach to provide superior levels of performance. Working with psychological science, police forces and security organizations will find support for the implementation of SRs, and at lower cost compared to automated systems. ■

References

[1] Innocence Project (2019). Exoneration statistics and databases. Retrieved 15 March 2020 from, https://www.innocenceproject.org/exoneration-statistics-and-databases/

[2] Horry, R., Memon, A., Wright, D., & Milne, R. (2012). Predictors of eyewitness identification decisions from video lineups in England: A field study. Law and Human Behavior, 36(4), 257-265.

[3] Burton, A. M., Wilson, S., Cowan, M., & Bruce, V. (1999). Face recognition in poor quality video: Evidence from security surveillance. Psychological Science, 10, 243–248.

[4] Burton, M., White, D., & McNeill A. (2010). The Glasgow face matching test. Behavior Research Methods, 42, 286-291.

[5] Tardiff, J., Morin Duchesne, X., Cohan, S., Royer, J., Blais, C., Fiset, D., Duchaine, B., & Gosselin, F. (2019). Use of face information varies systematically from developmental prosopagnosics to super-recognizers. Psychological Science, 30(2), 300-308.

[6] Russell, R., Duchaine, B., & Nakayama, K. (2009). Super-recognizers: People with extraordinary face recognition ability. Psychonomic Bulletin & Review, 16, 252-257.

[7] Davis, J. P., Lander, K., Evans, R., & Jansari, A. (2016). Investigating predictors of superior face recognition ability in police super-recognisers. Applied Cognitive Psychology, 30(6), 827-840.

[8] Robertson, D. J., Noyes, E., Dowsett, A. J., Jenkins, R., & Burton, A.M. (2016). Face recognition by Metropolitan Police super-recognisers. PLOS, One, 11(2): e0150036.

[9] Robertson, D. J., Black, J., Chamberlain, B., Megreya, A. M., & Davis, J. P. (2020). Super-recognisers show an advantage for other race face identification. Applied Cognitive Psychology, 34(1), 205-216.

[10] Belanova, E., Davis, J. P., & Thompson, T. (2018). Cognitive and neural markers of super-recognisers' face processing superiority and enhanced cross-age effect. Cortex, 108, 92-111.

[11] Davis, J. P., Forrest, C., Treml, F., & Jansari, A. (2018). Identification from CCTV: Assessing police super-recogniser ability to spot faces in a crowd and susceptibility to change blindness. Applied Cognitive Psychology, 32(3), 337-353.

[12] Towler, A., Kemp, R. I., Burton, A. M., Dunn, J. D., Wayne, T., Moreton, R., & White, D. (2019). Do professional facial image comparison training courses work? PLOS One, 14(2), e0211037.

[13] Wilmer, J. B., Germine, L., Chabris, C. F., Chatterjee, G., Williams, M., Loken, E., ... & Duchaine, B. (2010). Human face recognition ability is specific and highly heritable. Proceedings of the National Academy of Sciences, 107(11), 5238-5241.

[14] Manzoor, S. (5 November 2016). You look familiar: On patrol with the Met's super-recognisers. The Guardian. https://www.theguardian.com/uk-news/2016/nov/05/metropolitan-police-super-recognisers

[15] Davis, J. P. (2019). The worldwide impact of identifying super-recognisers in police and business. The Cognitive Psychology Bulletin; Journal of the British Psychological Society: Cognitive Section, 4, 17-22.

[16] O'Keefe, P. (22 August 2016). The detectives who never forget a face. New Yorker. http://www.newyorker.com/magazine/2016/08/22/londons-super-recognizer-police-force

[17] Phillips, P. J., Yates, A. N., Hu, Y., Hahn, C. A., Noyes, E., Jackson, K., ... & Chen, J. C. (2018). Face recognition accuracy of forensic examiners, superrecognizers, and face recognition algorithms. Proceedings of the National Academy of Sciences, 115(24), 6171-6176.

[18] [18] White, D., Kemp, R. I., Jenkins, R., Matheson, M., & Burton, A. M. (2014). Passport officers' errors in face matching. PLOS One, 9(8), e103510.

[19] [19] Schofield, H. (2019). The fake French minister in a silicone mask who stole millions. Retrieved 23rd March 2020 from https://www.bbc.co.uk/news/world-europe-48510027.

[20] Robertson, D. J., Mungall, A., Watson, D. G., Wade, K. A., Nightingale, S. J., & Butler, S. (2018). Detecting morphed passport photos: a training and individual differences approach. Cognitive research: principles and implications, 3(1), 1-11.

[21] Kramer, R. S., Mireku, M. O., Flack, T. R., & Ritchie, K. L. (2019). Face morphing attacks: Investigating detection with humans and computers. Cognitive Research: Principles and Implications, 4(1), 28.

[22] del Rio, J. S., Moctezuma, D., Conde, C., de Diego, I. M., & Cabello, E. (2016). Automated border control e-gates and facial recognition systems. Computers & Security, 62, 49-72.

[23] Vine, J. (2011). Inspection of border control operations at Terminal 3, Heathrow Airport. Retrieved 23rd March 2020 from, http://icinspector.independent.gov.uk/inspections/inspection-reports/2012-inspection-reports/

[24] Big Brother Watch (10 February 2020). Big Brother Watch response to Met's first operational facial recognition deployment. https://bigbrotherwatch.org.uk/2020/02/big-brother-watch-response-to-mets-first-operational-facial-recognition-deployment/

[25] Grother, P., Ngan, M., & Hanaoka, K. (2019). Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects. National Institute of Science and Technology (NIST) NISTIR, 8280.

[26] Fussey, P., & Murray, D. (2019). Independent report on the London Metropolitan Police Service's trial of live facial recognition technology. University of Essex, https://48ba3m4eh2bf2sk-sp43rq8kk-wpengine.netdna-ssl.com/wp-content/uploads/2019/07/London-Met-Police-Trial-of-Facial-Recognition-Tech-Report.pdf

[27] White, D., Burton, A. M., Kemp, R. I., Jenkins, R. (2013). Crowd effects in unfamiliar face matching. Applied Cognitive Psychology, 27(6), 769–777.

[28] Davis, J. P., Maigut, A., & Forrest, C. L. D. (2019). The wisdom of the crowd: A case of post- to ante-mortem face matching by police super-recognisers. Forensic Science International, 109910.

[29] Ramon, M., Bobak, A., & White, D. (2019). Super-recognizers: From the lab to the world and back again. British Journal of Psychology, 110(3), 461-479.

ABOUT THE AUTHORS

JOSH P. DAVIS, PH.D., is a Reader in Applied Psychology at the University of Greenwich. His PhD was on the "Forensic Identification of Unfamiliar Faces in CCTV Images" (2007) and he has since published research on human face recognition and eyewitness identification, the reliability of facial composite systems (e.g., E-FIT, EFIT-V), and methods used by expert witnesses to provide evidence of identification in court ('facial comparison evidence'). He is a member of the Experimental Psychology Society and the British Psychological Society. He regularly features in the international media (e.g., BBC, ITV, Sky TV (UK), CBS (USA), TV 2 (Denmark), Galileo (Germany), Fantastico (Brazil), South China Morning Post (Hong Kong), NHK (Japan), NBC, New York Times, Washington Post (USA) and his first co-edited book "Forensic Facial Identification: Theory and Practice of Identification from Eyewitnesses, Composites and CCTV" (Wiley Blackwell) was published in 2015 (Valentine & Davis, 2015).

DAVID J. ROBERTSON, PH.D., is a Lecturer in Psychology at the University of Strathclyde (Glasgow) School of Psychological Sciences and Health. David completed his PhD at the UCL Institute of Cognitive Neuroscience before going on to work as a post-doctoral researcher in Professor Mike Burton's FaceVar lab. He joined the University of Strathclyde in 2017 where he established the Strathclyde Applied Cognitive Psychology Lab (www.strathacpl.com), which focuses on applied face recognition research. He has published several scientific papers on individual differences in facial recognition ability, and the detection of emerging face-based identity fraud techniques. He has presented this research at national and international conferences to both academic and practitioner audiences including the UK Home Office and Europol. David is also a keen science communicator, his research on face averages received global media attention, and he is a regular contributor to The Conversation.

Photo Graphic Composite: Shelley Stottlar, Quanterion Solutions Inc.,
Featuring Photos: Deposit Photos/zhuzhu, Deposit Photos/ekkasit919,
and Deposit Photos/phonlamai.

A Foundation of Automation for Future Artificial Intelligence Strategy

By: **Maj Aaron Celaya**, U.S. Space Force, and **Sriraj Aiyer**, Research Assistant, University of Oxford, UK

In the 18th century, Europe and the United States (U.S.) saw the beginnings of the first industrial revolution. Textiles, steam power, and machine tools mechanized the production of items that had previously been created by the hands of human workers. The first industrial revolution extended beyond improvements in the manufacturing process to include societal impacts such as population growth and average household income.

THE SECOND INDUSTRIAL REVOLUTION occurred from about the late 19th century to the early 20th century and was also known as the Technological Revolution. Innovations during this period included the telephone, typewriter, lightbulb, motor cars, and powered flight. The third industrial revolution, the Digital Revolution, began around 1950 and ranged through the 1970s. This Digital Revolution advanced computing and telecommunications by transitioning from analog to digital products and services. The fourth industrial revolution, as described by Klaus Schwab [1], builds on

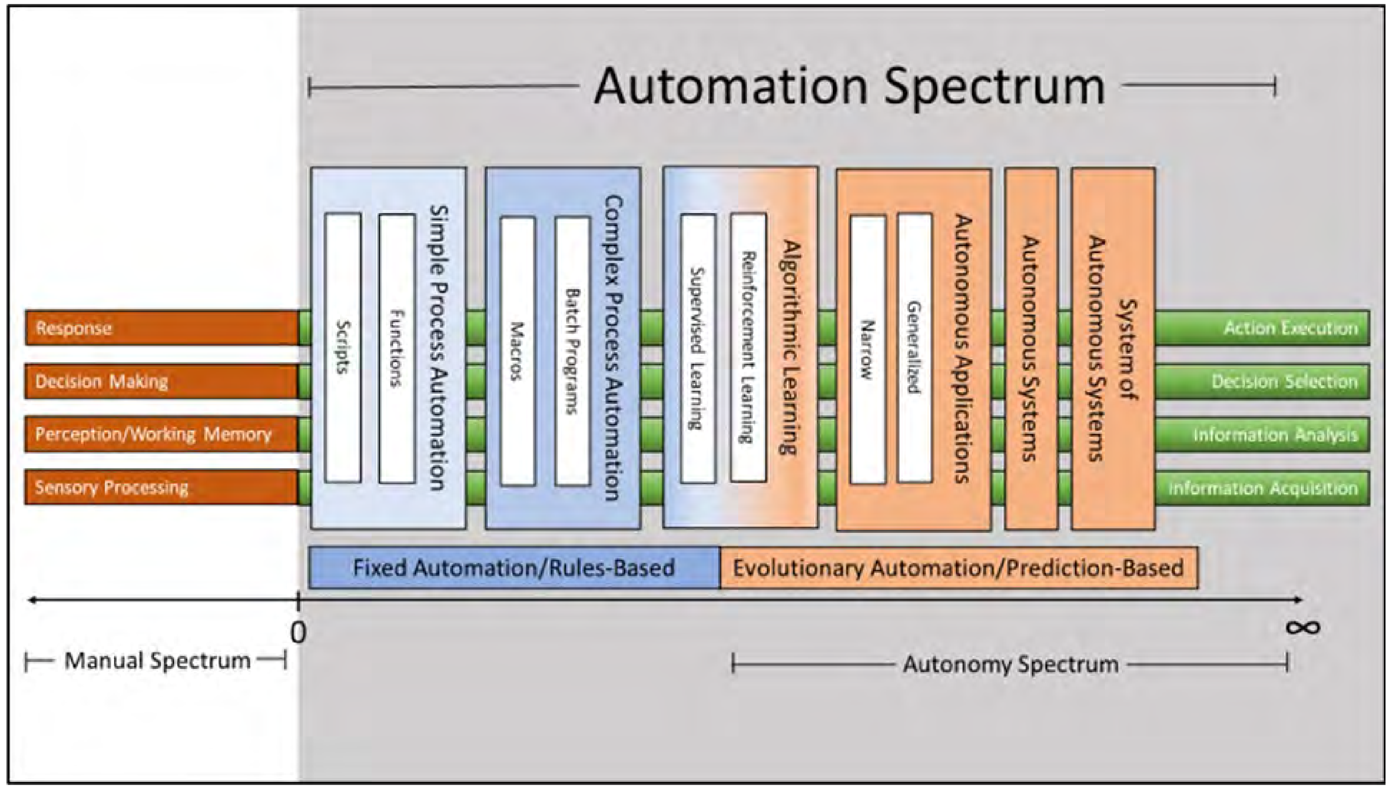


Figure 1: *Automation Spectrum* - (Source: Author)

the third industrial revolution and is characterized by the fusion of the physical, digital, and biological spheres. The fourth industrial revolution is distinguished from the third by the velocity, scope, and systems impacts of the emerging technologies. These technologies include Artificial Intelligence (AI), robotics, and quantum computing, among others [1].

As the fourth industrial revolution takes shape, many countries, businesses, and non-governmental organizations place acquiring these technologies at the forefront of their objectives. In 2018 the United States released its AI Strategy which directed the U.S. Department of Defense (DoD) to use AI to "transform all functions of the Department" [2]. The DoD was expected to scale AI's impact across the department through a common foundation. This foundation would be comprised of shared data, reusable tools, frameworks, and standards. In parallel with this common foundation, the DoD was to digitize existing processes and to automate wherever possible [2]. Schwab [1] asserted that technologies in the fourth industrial revolution should build on the principles and technologies from the third industrial revolution. In the case of AI, enterprise-wide digitization and automation for human-centric processes must occur to enable data creation, tagging, and storage for future AI applications. Algorithmic training will be incomplete without the digitization and automation of these processes. Dr. Launchbury from the Defense Advanced Research Projects Agency (DARPA) summed up the impacts of incomplete and inaccurate data when he stated that "skewed training data creates maladaptation" [3] of resultant AI.

Despite the national guidance for digitization and automation, there is no specific implementation guidance for automation in many organizations. The DoD has begun the process of developing specific automation guidance. Many DoD efforts in this domain are currently top-down directed with a narrow focus on AI in specific projects. A bottom-up strategy will enable Program Managers (PMs), responsible for different systems, to generate procurement requirements to incrementally advance technology across the automation spectrum. An automation foundation will provide the broad network of data capabilities for successful development and deployment of future AI-enabled applications and technologies.

A bottom-up implementation strategy requires a common understanding and lexicon for developing requirements. Using definitions from academia or professional literature could prove problematic. Such definitions must be broad enough to cover all procurement aspects while still being standardized. For example, there are many published AI descriptions which are so different that they defy standardization. Published definitions range from conceptual to operational and published categorizations range from 3, 4, 5, or 7 types of AI categories depending on your source document [4, 5, 6, 7].

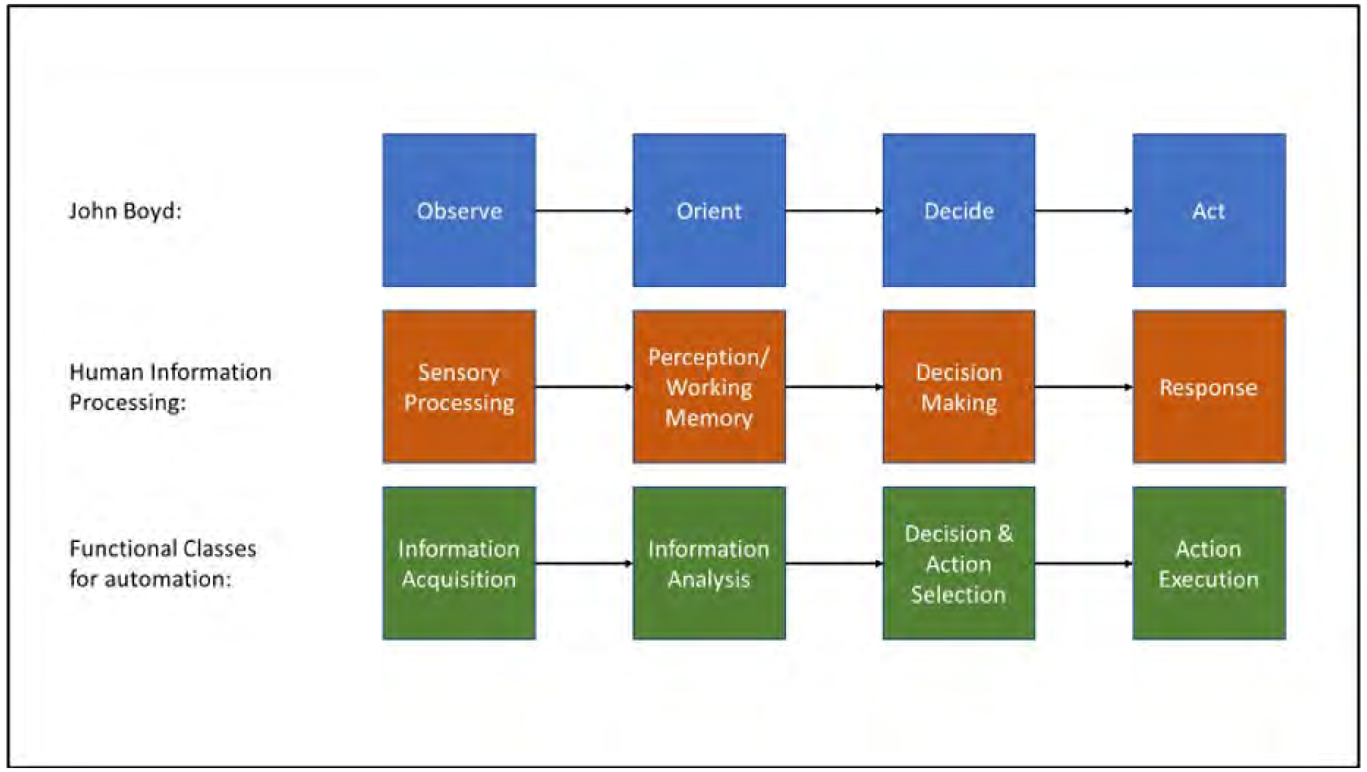


Figure 2: *Mapping of Parasuraman et al.'s functional classes onto human information processing and John Boyd's OODA Loop.* - (Source: Author)

For the purposes of generating, codifying, and communicating system requirements a different approach is required. That approach must be broad enough to apply to a multitude of capabilities but be adequately standardized. Therefore, we propose utilizing the automation spectrum [8].

The Automation Spectrum

The Automation Spectrum includes all automation possibilities ranging from fixed automation, which is rules-based, to evolutionary automation, which is based on statistical methods for learning how to produce desirable outcomes (see Fig. 1). As the capability moves towards fully automated self-control, the complexity also increases. The range of automation capabilities could include simple automation such as a windmill or an alarm clock to more complex automation such as macros or batch programs to autonomous capabilities.

Within the automation spectrum is the autonomy spectrum or the spectrum for those capabilities that are self-governing. AI falls within the autonomy spectrum and includes the many different types of AI, AI training methodologies, and applications of AI. Using the automation spectrum, AI is a part of the broader automation construct. Thus, all AI is automation but not all automation is AI. This axiom differs from some of the published categorization schemes for AI. However, the delineation in Fig. 1 will prove vital in acquisition processes and especially in cross-domain research and analyses. Therefore, the principle of automation and autonomy spectrums must be the foundation for establishing procurement and requirements guidance.

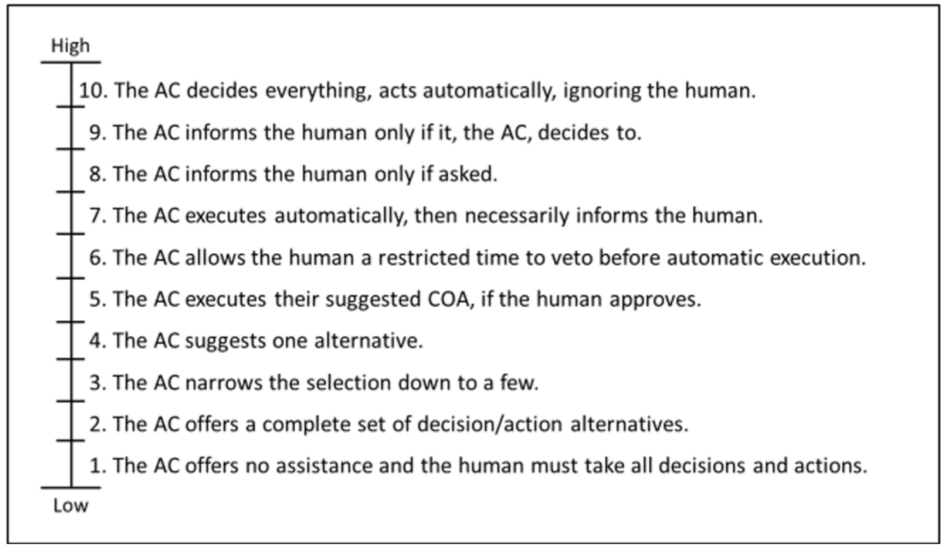
The world of automation possibilities seems endless and may prove too cumbersome to sift through to establish acquisition requirements. It may be useful to examine the approach of Parasuraman, Sheridan, & Wickens [9]. They created four functional categories of automation: Information Acquisition, Information Analysis, Decision and Action Selection, and Action Execution. It was observed that the resulting functional classes were closely linked to human information processing [9] as well as being closely linked to John Boyd's OODA (Observe Orient Decide Act) loop [10] (See Fig. 2).

The Levels and Costs of Automation

Within a given functional class of automation, technology can take many forms with varying complexity. Technological application variance can be described and organized by defining levels of automation (LOAs). In the work previously mentioned by [9], the authors defined LOAs using a scale from 1 to 10 (see Fig. 3). Level 1 represented unassisted human operation and level 10 represented complete superseding of the human by the automated system. Like many models, abstractions in the

LOA scale are unlikely to correspond exactly with one of the defined levels.

It is important to note that levels 2 through 10 of the LOA scale can be applied to any section of the automation spectrum. For example, at its basic definition, level 2 of the LOA scale is the “Automated Counterpart (AC) offers a complete set of decision/action alternatives.” In simple automation, the decision/action alternatives could be produced from rules-based programming such as pre-determined ‘if-then’ statements in scripts or functions. Or, using an autonomous AC, the decision/action alternatives could be produced from machine learning and AI applications.



10. The AC decides everything, acts automatically, ignoring the human.
9. The AC informs the human only if it, the AC, decides to.
8. The AC informs the human only if asked.
7. The AC executes automatically, then necessarily informs the human.
6. The AC allows the human a restricted time to veto before automatic execution.
5. The AC executes their suggested COA, if the human approves.
4. The AC suggests one alternative.
3. The AC narrows the selection down to a few.
2. The AC offers a complete set of decision/action alternatives.
1. The AC offers no assistance and the human must take all decisions and actions.

Figure 3: *Levels of Automation adapted from Parasuraman et al. [9].*

When assessing current and desired future automation states for specific technology capabilities, the LOA scale should first be applied to each of the four functional classes of automation individually. Then each functional class, with its LOAs, should be applied to each subsection of the automation spectrum individually. From this point, PMs can assess current LOA and functional class within the automation spectrum for the selected technology. Once the automation assessment is complete, the next step is to discern the requirements for moving the technology to the next LOA. This method of analysis provides the necessary common framework for assessing the extent to which a process is automated on an incremental basis. Methodologically, this analytical model is superior to previous simple binary classifications of whether a process is automated or not.

Oftentimes during the assessment process and creation of desired future states, there are unnecessary cultural pushes to develop more sophisticated autonomous capabilities when a simpler LOA might be better suited for the task. Factors to consider when creating desired future states consist of monetary investments for technology maturity or human skill degradation, among others. Taken together, these factors comprise the overall cost of incrementally increasing the LOA for a given technology.

In order to project overall cost, it is important to realize that the distance between adjacent LOAs is not constant and the overall cost is exponential as opposed to linear, see Fig. 4. For example, the difference between levels 2 and 3 requires an algorithm to search through the problem space of possible alternatives and use a utility function to choose options that reach a particular threshold. Hence, while moving from level 2 to level 3 is not trivial, it is not a difficult task. However, if we consider moving between levels 8 and 9, more work needs to be done. Namely, an appropriate model needs to be developed for algorithmic decision making, and there needs to an appropriate verification and validation of the system at level 8 to minimize risk from removing the human’s ability to be informed of the system’s operation at level 9. The system must have demonstrated a level of accuracy and safety. But that might take years of development, assessment, and regular field usage. There are also ethical considerations associated with determining responsibility and accountability should automation errors result in loss of life, or damage to property, etc. Consequently, the prerequisites for moving from level 8 to 9 are much higher than for levels 2 to 3.

Trust and Proper Reliance

A common misconception when discussing increasing algorithmic capabilities in the workplace is the role of trust in human-machine teams (HMT). It is often asserted that if the machine counterpart performs well, then the human user will trust it more. The fallacy here is linking machine performance directly to trust when machine performance is actually defined as the “ability” of the machine. Ability is a component of HMT trust. According to Mayer et al., characteristics of a trustee are a combination of the trustee’s ability, benevolence, and integrity [11]. Further, Hancock et al. [12] conducted a metanalysis looking at the factors that comprise HMT trust to determine which factors are the most influential in an HMT. While ability of the algorithmic counterpart was ranked highest among all the factors, there were many other factors which also affected HMT trust. Additional factors that were included in Hancock et al.’s metanalysis spanned three categories: human-related factors, automation-related factors, and environmental factors. Human-related factors covered items such as operator workload, expertise, demographics, propensity to trust, self-confidence, and task competency. Automation-related factors looked at the automation’s predictability, transparency, failure rate, false alarms, adaptability, and anthropomorphism. Finally, the environmental factors considered in the metanalysis consisted of team or tasking considerations and included items such as in-group membership, culture, communication, shared mental models, task type, task complexity, multi-tasking requirements, and the physical environment [12].

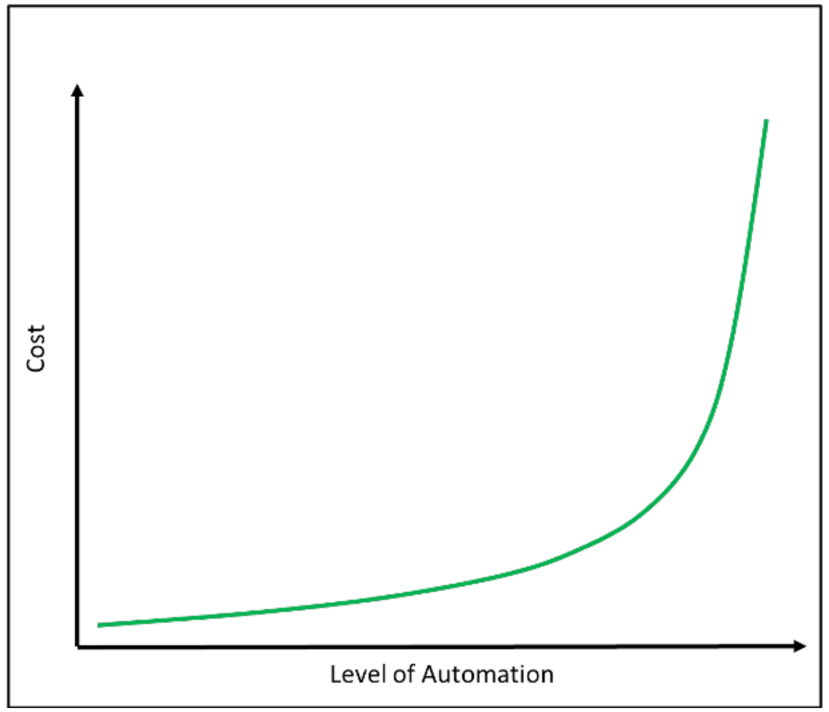


Figure 4: *Representation of the relationship between increasing LOA and overall cost. The relationship is exponential as opposed to linear.* - (Source: Author)

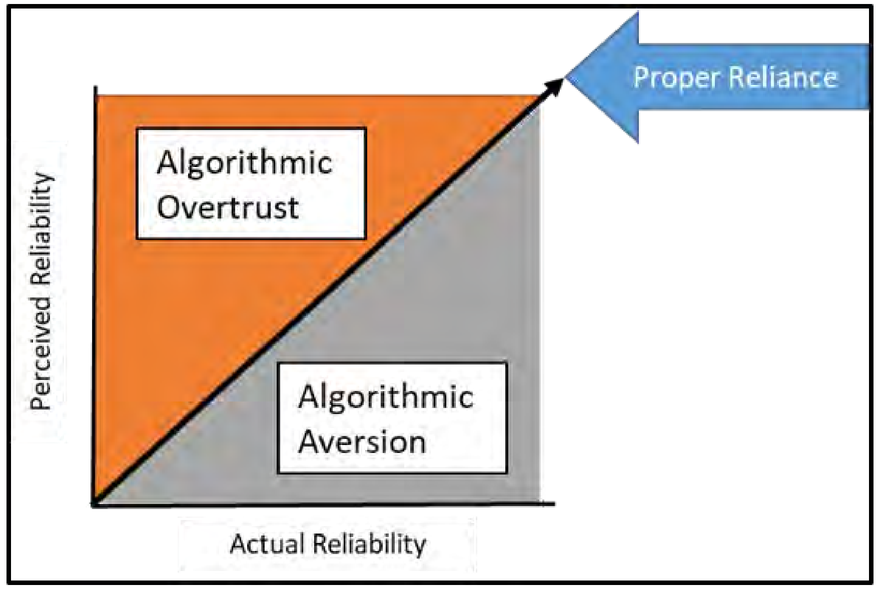


Figure 5: *Graphical representation of proper reliance, adapted from Gempler [15].*

Hoff & Bashir applied the model from Mayer et al. [11] to the findings from Hancock et al.’s metanalysis [12] and devised an integrated model of trust with associated factors in HMTs [13]. Hoff & Bashir separated pre-interaction factors into three categories: dispositional trust, situational trust, and initial learned trust. These categories exist prior to any system interaction and could bias the user well before any interaction takes place. The post-interaction category is termed dynamic learned trust and is comprised of system performance and system design features. Taken together, these pre- and post-interaction categories of factors combine to form a system reliance strategy which is dynamic and changes as various components of the model change or are altered [13]. The ultimate aim of utilizing these models is to encourage appropriate user reliance on automated counterparts [14]. All of the associated factors are considerations that creators of such technologies should consider when designing for appropriate human reliance on automated technologies.

The chart in Fig. 5 depicts a simple linear reliance strategy by a human user on their algorithmic counterpart. In an effective relationship with a proper reliance strategy, actual reliability and perceived reliability increase at an equal rate. Algorithmic overtrust [16] occurs when human perception of AC reliability exceeds truth. In these cases, humans overly rely on and comply with their algorithmic counterparts. Singh et al. termed this ‘automation-induced complacency’ [17], where there is a tacit and misguided assumption that users will rely on automation more than is desired, since the system is assumed to behave optimally in most situations. In some overtrust scenarios, human users comply with ACs even when they are clearly wrong in a given task [16]. Conversely, algorithm aversion occurs when the human user believes that the AC’s actual reliability is less than reality. Algorithm aversion is especially prevalent after human users observe machine counterparts err [18]. Human users experiencing algorithm aversion may partially or entirely dismiss their machine counterpart's contributions, advice, or inputs even if they are correct. Algorithmic overtrust and algorithm aversion can have negative consequences on factors such as performance or situational awareness. These situations can be especially hazardous within safety-critical contexts, such as medical, military or other defense scenarios.

The trust of human operators is an important consideration for developing automation. As the Australian Defense, Science and Technology Group put it: "future work on the human side of human–autonomous system interactions should include the development of a psychometrically reliable and valid instrument for measuring attitudes and beliefs about the general propensity to trust automated and autonomous systems." [19] The general public and those working in policy are concerned. As the European Commission noted in their White Paper on Artificial Intelligence, trust is a prerequisite for the uptake of technology [20].

The impacts of trust and reliance are apparent in the following example. Most human decisions and actions follow a basic outline. The fundamental building blocks of this process were laid out in Fig. 2 and labelled as human information processing. In Fig. 6, the human information processing steps are visualized on a notional timeline. A false assumption regarding automation implementation is that the automation will replace the corresponding human information processing step.

For example, if an automated agent were developed for information acquisition, some might assume that human sensory processing would no longer be needed. This is an incorrect assumption. Even if information acquisition is automated, the human user must 'sense and process' the outputs of the automated agent. However, as depicted in Fig. 7, the inclusion of automation will indeed shorten the human information processing timeline, without directly replacing any human processes.

If the human user has an appropriate reliance strategy, then compressed and effective time savings in Fig. 7 should remain constant. Additionally, other benefits may arise as a result of appropriate automation inclusion such as increased decision quality and refined confidence of the human user.

However, human trust and reliance are susceptible to fluctuations in AC ability and other factors such as usability features of the system, system appearance, ease-of-use, communication style, transparency, or the operator's level of control [21]. As previously discussed, human users are already potentially biased by their perceptions of the system, which are informed by pre-existing dispositional factors and contextual situational factors as defined by Hoff & Bashir [13]. The combination of these factors could result in deviations from an appropriate reliance strategy resulting in the human user drifting towards algorithmic overtrust or algorithm aversion.

Fig. 8 depicts the impacts of algorithm aversion on the notional timeline. Unless the effects of ability fluctuations and operator bias are minimized, inclusion of automation could result in worse performance than if the AC were never included.

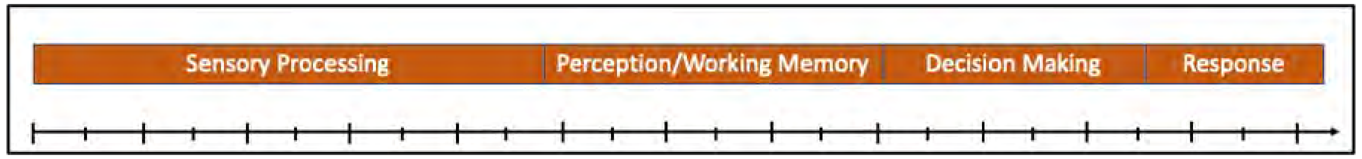


Figure 6: *Timeline of Human Information Processing* - (Source: Author)

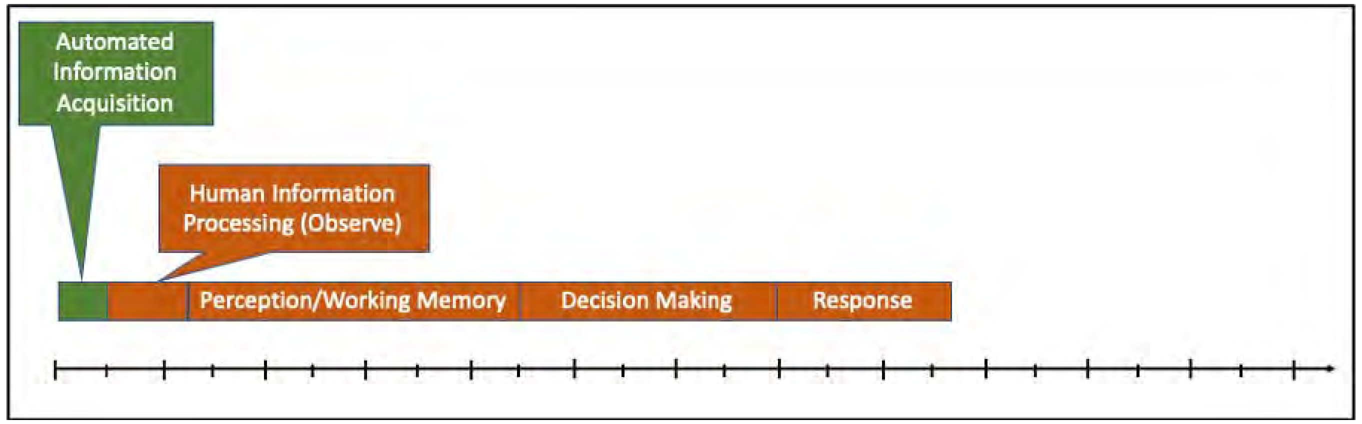

Automated Information Acquisition
Human Information Processing (Observe)
Perception/Working Memory
Decision Making
Response

Figure 7: *Human Information Processing Timeline with Automated Information Acquisition* - (Source: Author)

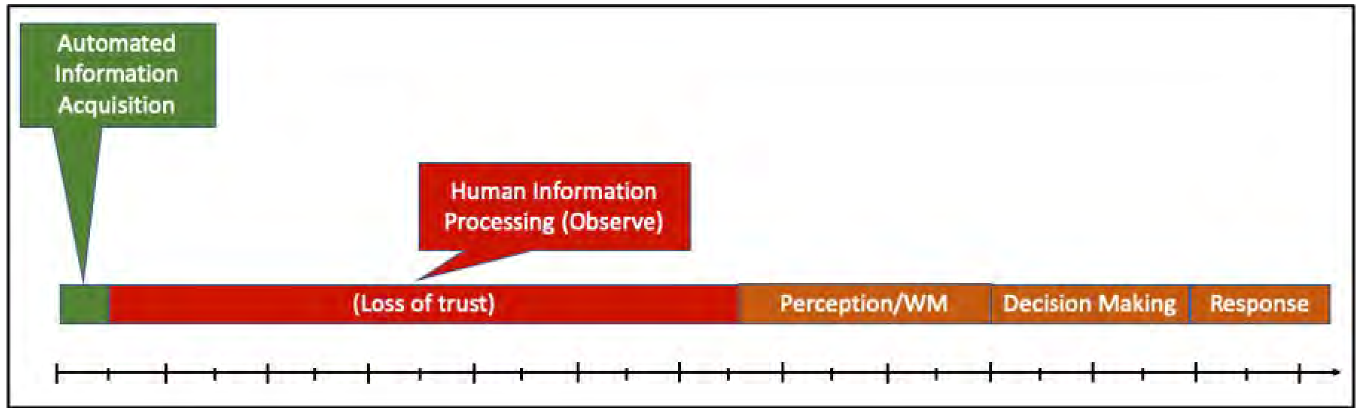

Automated Information Acquisition
Human Information Processing (Observe)
(Loss of trust)
Perception/WM
Decision Making
Response

Figure 8: *Timeline of Human Information Processing with algorithm aversion. (Source: Author)*

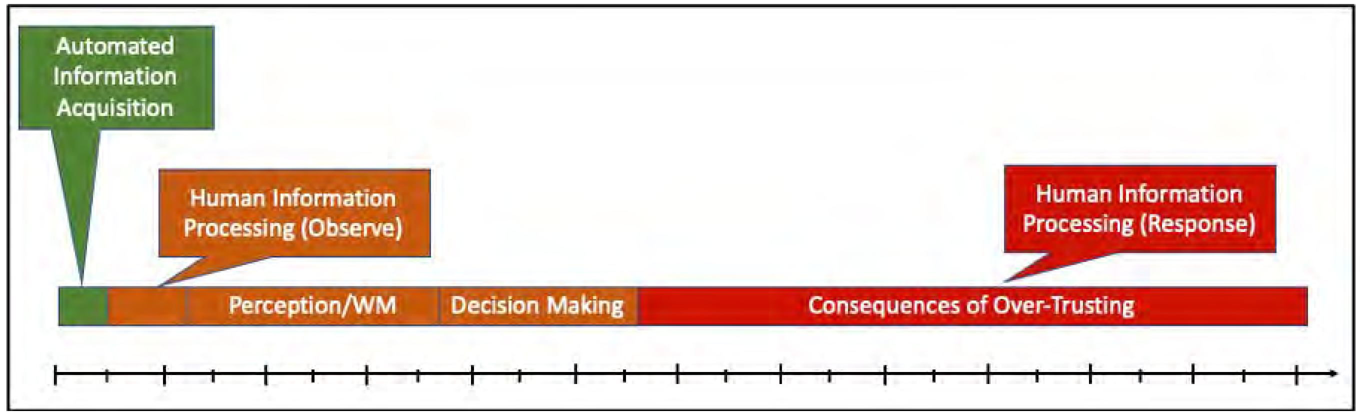

Automated Information Acquisition
Human Information Processing (Observe)
Human Information Processing (Response)
Perception/WM
Decision Making
Consequences of Over-Trusting

Figure 9: *Timeline of Human Information Processing with algorithm overtrust.* - (Source: Author)

Conversely, if algorithmic overtrust occurs as depicted in Fig. 9, the human user may neglect monitoring the AC due to overestimating the AC's ability. As a result, the system may perform unchecked erroneous actions, cause incidents, or fail without immediate notice. This chain of events leads to greater resources and time required to diagnose and understand problems which are only noticed by the human user after the fact.

Conclusion

This simple example highlights the complex nature of trust in HMTs. The impact of automation inclusion in human decision processes can be a powerful and positive one but must be implemented thoughtfully. Incremental progression up the LOA scale, within functional classes and across the automation spectrum, will be essential to creating the foundation called for in U.S. national guidance as it pertains to AI and, more broadly, automation.

First, organizations implementing an automation or seeking to increase automation capabilities should establish a lexicon and common understanding for all parties associated with the generation of technology requirements, program management, acquisition, science and technology, and leadership. Second, organizations should apply the principles in this article to self-assess and make incremental technology goals. Third, as automation technology is acquired and used operationally, organizations should capture lessons learned and create quantitative methods for calculating risk, ability, feedback mechanisms, and statements of confidence from automated counterparts. These refinements are necessary to develop HMT trust across the automation spectrum. ■

References

[1] Schwab, Klaus. The fourth industrial revolution. Currency, 2017.

[2] U.S. Department of Defense. (2018). Summary of the 2018 Department of Defense Artificial Intelligence Strategy: Harnessing AI to Advance our Security and Prosperity. Washington D.C.

[3] Launchbury, John. "DARPA Perspective on AI." DARPA. https://www.darpa.mil/about-us/darpa-perspective-on-ai (accessed May 11, 2020).

[4] Uj, Anjali. "Understanding Three Types of Artificial Intelligence." Analytics Insight. https://www.analyticsinsight.net/understanding-three-types-of-artificial-intelligence/ (accessed May 11, 2020).

[5] Hintze, Arend. “Understanding the Four Types of Artificial Intelligence.” Government Technology. https://www.govtech.com/computing/Understanding-the-Four-Types-of-Artificial-Intelligence.html (accessed May 11, 2020)

[6] Bekker, Alex. “5 Types of AI to Propel Your Business.” Science Soft. https://www.scnsoft.com/blog/artificial-intelligence-types (accessed May 11, 2020).

[7] Joshi, Naveen. “7 Types of Artificial Intelligence.” Forbes. https://www.forbes.com/sites/cognitiveworld/2019/06/19/7-types-of-artificial-intelligence/#436af704233e (accessed May 11, 2020).

[8] Flemisch, Frank, Anna Schieben, Johann Kelsch, and Christian Löper. “Automation spectrum, inner/outer compatibility and other potentially useful human factors concepts for assistance and automation.” Human Factors for assistance and automation (2008).

[9] Parasuraman, Raja, Thomas B. Sheridan, and Christopher D. Wickens. “A model for types and levels of human interaction with automation.” IEEE Transactions on systems, man, and cybernetics-Part A: Systems and Humans 30, no. 3 (2000): 286-297.

[10] Marra, William C., and Sonia K. McNeil. “Understanding the Loop: Regulating the Next Generation of War Machines.” Harv. JL & Pub. Pol’y 36 (2013): 1139.

[11] Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). An integrative model of organizational trust. Academy of management review, 20(3), 709-734.

[12] Hancock, P. A., Billings, D. R., Schaefer, K. E., Chen, J. Y., De Visser, E. J., & Parasuraman, R. (2011). A meta-analysis of factors affecting trust in human-robot interaction. Human factors, 53(5), 517-527.

[13] Hoff, K. A., & Bashir, M. (2015). Trust in automation: Integrating empirical evidence on factors that influence trust. Human factors, 57(3), 407-434.

[14] Celaya, A. & Yeung, N. (2019). Human Psychology and Intelligent Machines. NDC Research Papers No. 6: The Brain and the Processor, Rome, Italy. [Online]. Available : http://www.ndc.nato.int/research/research.php?icode=0. (accessed May 11, 2020).

[15] Gempler, Keith Stewart. Display of predictor reliability on a cockpit display of traffic information. ILLINOIS UNIV AT URBANA, 1999.

[16] Robinette, P., Li, W., Allen, R., Howard, A. M., & Wagner, A. R. (2016, March). Overtrust of robots in emergency evacuation scenarios. In The Eleventh ACM/IEEE International Conference on Human Robot Interaction (pp. 101-108). IEEE Press

[17] Singh, I. L., Molloy, R., & Parasuraman, R. (1993). Automation-induced” complacency”: Development of the complacency-potential rating scale. The International Journal of Aviation Psychology, 3(2), 111-122.

[18] Dietvorst, B. J., Simmons, J. P., & Massey, C. (2015). Algorithm aversion: People erroneously avoid algorithms after seeing them err. Journal of Experimental Psychology: General, 144(1), 114.

[19] Davis, S. E. (2019). Individual Differences in Operators’ Trust in Autonomous Systems: A Review of the Literature, Joint and Operations Analysis Division, Defence Science and Technology Group, Australian Government.

[20] European Commission (2020). White Paper on Artificial Intelligence: A European Approach to Excellence and trust, [Online]. Available: https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf (accessed: May 11, 2020).

[21] Celaya, A. & Yeung, N. (2019). Confidence and Trust in Human-Machine Teaming. HDIAC Journal, 6(3), 20-25. [Online]. Available: https://www.hdiac.org/journal-article/confidence-and-trust-in-human-machine-teaming/ (accessed: May 11, 2020).

ABOUT THE AUTHORS

MAJOR AARON W. CELAYA is the Artificial Intelligence Liaison and Deputy Branch Chief for Doctrine and Concepts at Headquarters, U.S. Space Force. He is concurrently an Air Force Institute of Technology Doctoral Student, New College, Department of Experimental Psychology, University of Oxford, United Kingdom. His research includes metacognition, trust, and decision confidence in human-machine teams with an emphasis on algorithmic advisement sources. His research is conducted within the Attention and Cognitive Control Laboratory, Department of Experimental Psychology, University of Oxford, United Kingdom.

SRIRAJ AIYER is a Research Assistant working at the Attention and Cognitive Control Lab in the University of Oxford’s Department of Experimental Psychology. He comes from a BSc and MSc background in Computer Science and Human-Computer Interaction respectively. His current research activities are in human-machine trust & teaming and the neural mechanisms of attention and confidence.

MOSAICS

More Situational Awareness for Industrial Control Systems (MOSAICS):

Engineering and Development of a Critical Infrastructure Cyber Defense Capability for Highly Context-Sensitive Dynamic Classes

Part 1 – Engineering

By: **Aleksandra Scalco**, Naval Information Warfare Center – Atlantic, Data Science & Analytics Competency, and **Dr. Steven Simske,** Colorado State University, Department of Systems Engineering

There is a Department of Defense (DOD) operational need for cyber defense capabilities to defend critical infrastructure from cyber attack. Critical infrastructure systems, such as power, water and wastewater, and safety controls, affect the physical environment.

THESE SYSTEMS TRADITIONALLY RELIED ON PHYSICAL SECURITY such as physical access control. The introduction of the Industrial Internet of Things (IIOT) to traditional Operational Technology (OT) systems evolved critical infrastructure systems into cyber-physical systems, making these systems susceptible to cyber attacks such as ransomware. Extended technology refresh cycles of 20 years or more undermine the ability to address vulnerabilities with engineering upgrades. Further, OT and Information Technology (IT) experts have varying contextual approaches to their respective domains. Systems engineering principles, when deployed in the engineering and post-development phases, is a mechanism for integration of contextual information from cyber-physical systems into a model for cyber defense capabilities for highly context-sensitive critical infrastructure dynamic classes. More Situational Awareness for Industrial Control Systems (MOSAICS) is piloting an initial capability to address cyber defense of critical infrastructure. The MOSAICS capability concept was to automate the existing manual procedures to detect, mitigate and recover from a cyberattack using effective system baselining and segmentation of the ICS network to help prevent malware breach and proliferation, combined with the best of breed technologies related to analytics, visualization, decision support, and information sharing. This paper examines engineering and post deployment of a demonstration for the transition and integration into fielded systems.

In early 2016, two Combatant Commands identified an operational need to defend DoD mission-critical infrastructure. Sandia National Laboratories (SNL) and the Naval Facilities Engineering Command (NAVFAC) responded with a concept to address the operational need by bringing the best of breed tools to the DoD and named the initiative "MOSAICS," or More Situational Awareness for Industrial Control Systems. The MOSAICS capability concept was to automate selected procedures to detect, mitigate and recover from a cyberattack, combined with the best of breed technologies related to analytics, visualization, decision support, and information sharing [1].

System studies identified three initial MOSAICS capabilities: 1) an operational capability to enable defense of control systems; 2) an Industrial Control Systems (ICS) baselining tool for Programmable Logic Controller (PLC) sensors; and 3) tailored visualizations, analytics, and automated cybersecurity orchestration for improved remediation strategies. Systems engineering principles were applied during the concept development phase to convert operational needs into an engineering-oriented view in several modes.

The MOSAICS development proposed a proof-of-concept prototype for an OT threat surface, which includes ICS and Supervisory Control and Data Acquisition (SCADA) systems to the subsystem component level of PLCs or Discrete Process Control Systems (DPCs). ICS is an operational segment within OT used to monitor and control industrial processes (e.g., power consumption on electrical grids). ICS is often managed by a SCADA system that provides Graphical User Interfaces (GUI) for operators (e.g., out-of-band operation alarm indicators). ICSs are typically either a continuous process control system managed by PLCs, or DPCs used as batch control devices.

The Department of Homeland Security (DHS) identifies 16 critical infrastructure sectors: Chemical; commercial facilities; communications; critical manufacturing; dams; defense industrial base; emergency services; energy; financial services; food and agriculture; government facilities; healthcare and public health; information technology; nuclear reactors, materials, and waste; transportation; and water and wastewater systems [2]. The initial MOSAICS Joint Capability Technology Demonstration (JCTD) prototype development is for an energy system. MOSAICS will later be applied to water, and other sectors. ML (Machine Learning) and AI (Artificial Intelligence) capabilities will be incorporated to minimize human actions where possible.

Systems engineering principles provide a mechanism to integrate cyber defense capabilities into context-sensitive critical infrastructure dynamic classes. Context-sensitive critical infrastructure dynamic classes are systems interpreted by 1) the view of the OT or IT operator, 2) the critical infrastructure sector, and 3) dynamically classified at the time of operation rather than as a static set of classes.

The OT operator manages physical processes and machinery while the IT operator manages information flows of digital data. There is a substantial distinction between static and dynamic classes of critical infrastructure systems. Each critical infrastructure sector is dynamic, and within each sector, every cyber-physical system is dynamic. The potential risk introduced by the context-sensitive critical infrastructure dynamic classes must be addressed as early as possible and revisited throughout the systems engineering lifecycle. "As a system's diversity, connectivity, interactivity, or adaptivity increases, the risk associated with using simpler methods and simplifying assumptions also increases, and more advanced techniques may be needed. Tools and techniques apply differently to systems on a spectrum of increasing complexity" (INCOSE, 2015) [3]. Unlike many applications in machine learning, where acute consideration of training data can lead to overfitting, in cybersecurity all training data generally must be taken seriously. This may be an important branching point for the future of ML/AI in cybersecurity compared to normal machine intelligence. An automated test harness is being explored to test the consistency of the MOSAICS system.

"The convergence of OT and IT makes cyber-physical systems equally susceptible to cyber-attacks, yet OT is contextually and dynamically distinct from IT."

The software has a significant influence on the design of a system as a driver. MOSAICS uses the expanding role of orchestration to implement the requirements, functionality, and behaviors of the system. Software trade-offs determine if the right quality attributes are promoted in the design. Software constraints are also limiting factors to options for making design decisions. An operating system is an example of such a constraint. Building software systems for a solution that works on Windows or Linux is a software constraint that influences the design of the system. Other examples would be the selection of an algorithm or a specific interface protocol. MOSAICS uses open Application Protocol Interfaces (APIs) to address this constraint, and to avoid vendor lock. APIs are sets of protocols used for building software applications that specify how components interact.

Tests can demonstrate necessary corrections in software code after each spiral development. The goal is to fail fast and fail early to avoid an expensive cycle of debugging codes later. Tests that should be performed such as functionality testing to ensure that the software does not crash; code review to uncover any problems; static code analysis; unit testing to make sure the unit is working as expected by testing in a range of both valid and invalid inputs; and user performance testing in a real world environment [4].

The reasons complex system developments incur risks include incomplete specifications until late in the development lifecycle, unclear requirements definitions, unaddressed risks, and a lack of required expertise or inadequate expertise in the new technology. At the time of this publication, MOSAICS is scheduled for a test during Trident Warrior 2020, an annual large-scale Navy field experiment. The Trident Warrior experiment series selects and evaluates initiatives to address capacity gaps in an operational environment. During the advanced development phase, uncertainties are resolved. Small sets of requirements are developed using spiral development, allowing for incremental releases and refinement through each iteration. The principal purpose of this approach is to reduce risk. This phase is especially critical as MOSAICS concepts significantly depart from traditional OT system security approaches. Requirements analysis reexamines the validity of the functional specifications and identifies components that require further development.

Many new complex system developments incur significant risks because they choose immature technology. In these cases there are often insufficient laboratory tests to measure the performance parameters in order to make analytical performance predictions. MOSAICS buys down risk in a laboratory by using more mature Commercial-Off-the Shelf (COTS) technology. Selection and use of COTS technology helps drive innovation and competition in the commercial sector, as it offers opportunity for not only initial implementation but also for follow-on work as the government is not in the business of lifecycle product support. This COTS approach further serves to lower risk as all of the asset inertia from field deployment has fed back design flaws for version-based incremental improvement over time. COTS is essential to speed innovation as well as incremental improvements to the warfighter. Technology Readiness Level (TRL) is a standard for evaluating the maturity of a technology to determine if it is a useable choice for complex system development. TRL 1 is the lowest level of maturity, and TRL 9 is the highest. Utilizing COTS, MOSAICS is TRL 7 and higher.

Extended technology refresh cycles of 20 to 30 years or more in critical infrastructure systems undermines the ability to address vulnerabilities. Because of the extended refresh cycle, MOSAICS enhancements will have to perform requirements well beyond those expected from similar IT systems, as there is no predecessor system for OT. The extended refresh cycle of critical infrastructure systems frequently results in the use of older technologies designed for functionality requirements rather than cybersecurity requirements. The convergence of OT and IT makes cyber-physical systems equally susceptible to cyber attacks, yet OT is contextually and dynamically distinct from IT. Components that use new technology can be attractive options for consideration of new system development to meet performance requirements for many years beyond the original design. Component expertise has varying contextual technological approaches to respective domains and varying behavioral approaches and responses, particularly to Human-Introduced Cyber Vulnerabilities (HICV) [5].

"Extended technology refresh cycles of 20 to 30 years or more in critical infrastructure systems undermines the ability to address vulnerabilities."

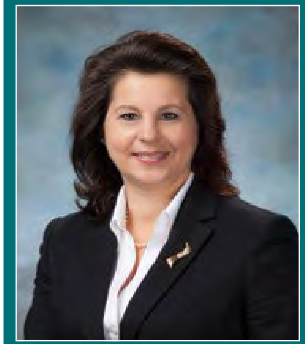
The resilience of these systems becomes a potentially valuable metric for this diverse group of systems that may be used to complement risk frameworks such as the DoD risk-based "Cybersecurity Framework," designed for IT systems. Quantitative assessment of the resilience of networked cyber-physical systems might be measured by critical functionality based on a time-specific performance control time function (Tc (time over which system performance is evaluated)) derived by the operational input [6]. Complex adaptive systems are a challenge to discuss without a model. While a particular model may represent conditions within one system, variables to user states may carry different meanings from one system of systems to another. Several candidate approaches are used to address complexity, such as seeking to understand the big picture, observing how elements within the system change, identifying the system structure relationship to system behavior, and understanding test assumptions. The recommended solution architecture is designed to "provide robustness and timely recovery to a minimally functional state." (INCOSE, 2015).

An example of the "design for resilience" principle may be found in the Integrated Adaptive Cyber Defense (IACD) component of MOSAICS [7]. IACD is an extensible, adaptive framework to improve the effectiveness of the system defenses. While the framework was created to address IT environments, it is being applied to an OT environment using systems engineering principles. The assumption is that if the approach were applicable for IT complexity, then the same approach would also apply to OT complexity. This application of systems engineering reuse is a benefit in installing, maintaining, and upgrading the system throughout the lifecycle of the system.

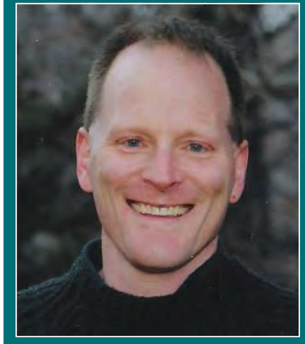
Unknown unknowns can be expected to appear during engineering design. One way to estimate the number and scope of unknown unknowns is to thoroughly examine a given percentage p of the code base for them, and then scale the number based on 1/p. Potential deficiencies are addressed in MOSAICS by employing experienced designers and testers employed "in combination with disciplined software design procedures" (Kossiakoff, 2011) [8]. This approach is relevant to hardware, as well. Potential "unknown unknowns lurk in untrusted components, can come from insider threats, and may result from externally introduced malware that can penetrate OT previously considered to be "air-gapped" in an increasingly networked computer world. Detection may be difficult, hence the need for experienced Red-Team testing, which has proven to be a critical part of security testing and evaluation. Viruses, worms, and spyware may be embedded in a system before the implementation of a defensive solution. A challenge is understanding what "normal" or "known good" looks like in the absence of a virus (if a virus is already present). Solutions today are only able to detect what is known, or, in other words, known malware. The cost of modeling and simulation technologies is prohibitively expensive for one-off (or "snowflake" systems). Without the demonstration of a "smoking gun" (i.e., existing malware in the system), few system owners will accept the high cost of new development. Since there are few rules or signatures in cyberattacks on critical infrastructure systems, assigned personnel must have both cybersecurity and OT knowledge. The culmination of engineering design is the realization of a final MOSAICS design (e.g., requirements analysis, functional analysis and design, component design, and design validation). At this point, all the modular components have to fit together to meet the operational requirements.

Part 1 of this article has described the engineering of the MOSAICS JCTD prototype pilot. In Part 2 the authors will describe the MOSAICS development of this initial cyber defensive capability for industrial control systems. ■

ABOUT THE AUTHORS



ALEKSANDRA SCALCO is an engineer with the Naval Information Warfare Center (NIWC) Atlantic. She is working towards a Systems Engineering Ph.D. at Colorado State University (CSU). Her research field is cyber resilience for Operational Technology (OT). She earned a Master's Degree in Engineering from Iowa State University in 2012, and a Master's Degree in Business Administration (MBA) in 2009. She is a member of the Defense Acquisition Corps in engineering. Ms. Scalco is Defense Acquisition Workforce Improvement Act (DAWIA) career certified Level 3 Engineering, Level 1 Science & Technology, and Level 1 Program Management. She holds ITIL Intermediate Certifications. Before joining NIWC Atlantic Ms. Scalco was a member of the National Security Agency (NSA) workforce as an Information System Security Designer (ISSD). As an ISSD, she provided technical expertise to clients on cyber assurance to advance the state of cybersecurity solutions to harden the National Security Enterprise against adversarial threats.



DR. STEVEN SIMSKE joined Colorado State University in 2018 as a Professor in Systems, Mechanical, and Biomedical Engineering. Before then, he was an HP Fellow and a Research Director in HP Labs. He led HP in research and development in algorithms, multi-media, labels, brand protection, security and secure printing, imaging, 3D printing, analytics and life sciences. He is a long-time member of the World Economic Forum Global Agenda Councils (2010-2016), leads the Steering Committee for the ACM DocEng Symposium, and is former President of the Imaging Science and Technology professional organization. Dr. Simske has nearly 200 granted US patents and more than 400 professional publications, including the recent books, Meta-Algorithmics and Meta-Analytics. He is an Honorary Professor in Computer Science at the University of Nottingham, UK. Dr. Simske was a payload specialist on a dozen Space Shuttle missions, and has designed devices ranging from exercise-responsive pacemakers to impedance tomography systems.

References

[1] Aleksandra Scalco, M. J., Steve Simske (2019). "More Situational Awareness for In-dustrial Control Systems (MOSAICS) Joint Capability Technology Demonstration (JCTD): A Concept Development for the Defense of Mission Critical Infrastructure." Homeland Defense & Security Information Analysis Center.

[2] (CISA), D. o. H. S. D. C. I. S. A. (2019). "Critical Infrastructure Sectors." Retrieved December 6, 2019, from https://www.dhs.gov/cisa/critical-infrastructure-sectors.

[3] INCOSE, 17.

[4] Steve Simske. (2019). ENGR 501 Guest Lecture. Colorado State University (CSU).

[5] Terry Merz, C. F., Aleksandra Scalco (2019). "A Context-Centered Research Approach to Phishing and Operational Technolo-gy in Industrial Control Systems." The Journal of Information Warfare (JIW).

[6] Zachary A. Collier, M. P., Alexander A. Ganin, Alex Kott, Igor Linkov (2016). Securi-ty Metrics in Industrial Control Systems.

[7] JHU APL, (2019). "Integrated Adaptive Cyber Defense (IACD)." Integrated Adaptive Cyber Defense (IACD). Retrieved December 9, 2019.

[8] Alexander Kossiakoff, W. N. S., Samuel J. Seymour, and Steven M. Biemer (2011). Systems Engineering Principles and Practice, John Wiley & Sons, Inc. Publication.

MOSAICS

More Situational Awareness for Industrial Control Systems (MOSAICS):

Engineering and Development of a Critical Infrastructure Cyber Defense Capability for Highly Context-Sensitive Dynamic Classes

Part 2 – Development

By: **Aleksandra Scalco**, Naval Information Warfare Center – Atlantic, Data Science & Analytics Competency, and **Dr. Steven Simske,** Colorado State University, Department of Systems Engineering

There is a Department of Defense (DOD) operational need for cyber defense capabilities to defend critical infrastructure from cyber attack. Critical infrastructure systems, such as power, water and wastewater, and safety controls, affect the physical environment.

"MOSAICS," or More Situational Awareness for Industrial Control Systems, is a Department of Defense (DOD) response to an operational need to defend mission-critical infrastructure. The MOSAICS capability concept was to automate selected procedures to detect, mitigate and recover from a cyberattack. It is combined with the best of breed technologies related to analytics, visualization, decision support, and information sharing [1].

Systems engineering principles were applied during the concept development phase to convert operational needs into an engineering-oriented view in several modes leading into the engineering phase. Implementing Model-based Systems Engineering (MBSE) is valuable during this phase. The Navy is moving from document-based systems engineering to a standard, enterprise-wide architecture model. The objective is to support the Fleet with warfighting capabilities more effectively. A significant benefit is managing requirements and system baselines that remain for many years before replacement systems are deployed. Using an MBSE approach enables the engineers to integrate upgrades and better integrate the system into systems of systems. "A new system that is to be developed to replace a current obsolescent system will inevitably have performance requirements well beyond those of its predecessor" (Kossiakoff, 2011) [2].

Among the challenges of transitioning to the MBSE is an ingrained culture that resists change, and the cost of MBSE software. A more practical challenge is that MBSE must be injected at the start of a program. MBSE can, however, help to reduce risk through requirements validation. Modeling the requirements statements into the model itself allows stakeholders to validate the subject system's functional requirements in an understandable language. Risk Analysis also can be integrated into the MBSE process. Disadvantages of MBSE are an initial investment, the need for employee training, and increasing complexity. In contrast, the advantages include cost reduction, cost-effectiveness, and risk reduction during production. This last area is where the most significant impact of failure can occur in a program's lifecycle.

External system interface requirements are particularly important in the development because of the large integrated extension of smart sensors, instruments, and other devices networked together with computer applications. Most of the OT systems were engineered before today's interconnected, highly computer-networked environments. They faced static causal relationships of accidents and human factors. HICVs change that dynamic. Regardless of the amount and level of training, cybersecurity training does not defend against cyber exploitation attack vectors such as phishing and spear phishing. The most poignant observations made during data collection efforts of a DOD Joint Test known as Joint Base Architecture for Secure Industrial Control Systems (J-BASICS), were from users operating at the traditional IT enterprise levels of ICS who did not behave any differently than those ICS operators who had not been exposed to the same cybersecurity training when confronted with phishing attacks [3]. J-BASICS showed that even cyber security trained experts may not practice good cyber hygiene even knowing the potential negative consequences. This is why automated course of action is needed. The human is best suited for final decision making rather than near-real time response actions.

"Transition of MOSAICS to commercial industry will help to ensure continued viability for the various classes of OT systems and components across sectors."

Accidents in OT are typically attributed to the complexity of systems and scenarios. Automation addresses this complexity, which is introduced by smart sensors, instruments, and other devices networked together. Without automation, the possibility for correction in more complex environments is likely to remain unchecked. If this premise is correct, then the design of systems warrants the engineering of more significant computer-aided correction of Course Of Action (COA) or automated systems. Interestingly, the most significant resistance to the integration of automated systems is the perception that automated course of action creates a greater significant potential for accidents or failures of the desired effect. Whereas, if the J-BASICS findings are correct, then human-in-the-loop may not be the ideal system design. The ideal system design would be human out-of-the-loop with the fallback redundancy allowing for a human to manually intervene when they observe an error.

Functional analysis emphasizes a modular configuration, software design in a modular architecture, and effective human interactions of user interfaces. "Among the most critical elements in complex systems are those concerned with the control of the system by the user — analogous to the steering wheel, accelerator, shift lever, and brakes in an automobile" (Kossiakoff, 2011) [4].

Systems engineering principles support the integration of cyber defense capabilities into these context-sensitive critical infrastructure dynamic classes. OT systems are vulnerable to cyber attacks such as ransomware directed at OT hardware and software that monitors and controls physical devices, processes, and events in critical infrastructure. Cyber attacks bring an element of physical risk that OT operators traditionally did not consider for OT systems. These are powerfully protected, in many cases, by anomaly detection algorithms and process violation reporting. "While both IT and OT [operators] may be equally susceptible to phishing attacks, more nuanced evaluation of the user's respective context domains would reveal that IT and OT operators are exposed to different context variables. These could create very different outcomes relative to a user's response to phishing attacks" [5]. "[T]he objective of [risk management] is to minimize the total cost of managing each significant risk area" (Kossiakoff, 2011) [6]. The functional design must provide test points for fault isolation, maintenance, environmental provisions, and opportunity for future growth [7]. Prototyping of actual hardware and software are integrated into the system for laboratory functional technical validation and verification. A second field demonstration includes operators to validate and verify the MOSAICS system design.

Transition of MOSAICS to commercial industry will help to ensure continued viability for the various classes of OT systems and components across sectors. Component design becomes a commoditized industry. Modern electronic component production dramatically reduced production costs by standardizing components. Customization of components increases the cost. This standardization contributes to transforming the design, development, production, and delivery of electronic components. It also impacts cost, reliability, and Design for Manufacture (Dfx). Typical activities of design validation include "conducting test and evaluation of engineered components concerning function, interfaces, reliability, and producibility, correcting deficiencies and documenting product design" (Kossiakoff, 2011) [8].

Configuration Management (CM) contributes to the integrity of the system design. It maintains vital system development baselines, which include the functional baseline, the allocated baseline, and the product baseline, all essential elements throughout the system lifecycle. "Formal change control of system-level changes is usually exercised by a designated group composed of senior engineers with recognized technical and management expertise capable of making judgments among performance, cost, and schedule," (Kossiakoff, 2011) [9]. The goal of integration is to engineer the new system into a compelling operating whole.

During test planning and preparation, the MOSAICS prototype becomes real, and interface issues are resolved. Deviations from expected test results can be due to deficiencies in the equipment, procedures, execution, analysis, the system under test, or excessive stringent requirements. Dealing with a test failure must be traced for understanding so that corrective action can be made. Steps taken prior, during, and after a test, contribute to the diagnosis of a test failure. Before Trident Warrior 2020, a final prototype baseline will be locked down, and no further late injection of technologies introduced. "A typical test configuration consists of the system element (component or subsystem) under test, a physical or computer model of the component or subsystem, an input generator that provides test stimuli, and output analyzer that measures element test responses, and control and performance analysis units," (Kossiakoff, 2011) [10]. The system test configuration subjects the system to operational and environmental conditions in which it will perform. Some critical systems, however, require continuous operations and cannot be stopped or paused for test [11].

A model is a useful tool in systems engineering. It helps developers think about and understand complications that are difficult to observe independent of context. Human factors from behavioral science can add to the complexity of a system observed. A complex system has multiple stable, transient, continuous evolution, or no lasting states. "A complex system may have multiple stable states (meaning each state is metastable), transient states, or even no lasting stable states, exhibiting continuous evolution. Perturbations in the system may result in recovery to the former state but may also lead to transitions to another state and consequent radical changes of properties. Besides, details seen at the fine scales can influence large-scale behavior" (INCOSE, 2015) [12]. Advanced Persistent Threats (APT's) leverage of phishing against OT to attack critical infrastructure assets demonstrates this point. "Today phishing, a human-focused exploit, constitutes 91% of successful attack vectors against Federal assets. This means HICV's are the weakest cyber link. The success of these attacks also suggests HICV's are not well understood nor mitigated" (Merz, 2019) [13].

Test planning can ensure that MOSAICS is substantially better positioned for testing. Preparing the test environment and constraints, and using small scale tests to collect information all contribute to test planning. Verification is the evaluation of a system or component to determine if it is built correctly to satisfy the conditions imposed at the start. Validation is the evaluation of a system or component to determine if the right product was built to meet user operational requirements. Verification is performed during Developmental Test (DT). DTs are one-on-one tests performed in controlled environments testing to specifications for precise performance objectives. The operational test is the evaluation of a real production item by an independent agency in as realistic an environment as practical with normalized operators performing activities for validation. Personnel training and knowledge transfer to the user responsible for operations is vital for adequate preparation of the transition to a new system. Human error is often less a factor in the failure of a system than an error triggered by poor design, or violation of use and maintenance [14]. "Among the most critical elements in complex systems are those concerned with the control of the system by the user" (Kossiakoff, 2011) [15]. Human factors have to be taken into consideration as a potential reliability issue whereby components may present operating hazards if not used as designed and intended. Scenario brainstorming is so important to determine the best way to deter malicious effort to gain privileged access from privileged access holders. Psychology is a key in these tests of deterrence.

Development Stage

Of the production operations, the establishment of an active Information System (IS) is one critical to support successful production operations. In production operation systems, the engineering organization coordinates with users, developed component engineering, production, assembly, integration and acceptance test, and subcontractor engineering [16]. The manufacture of a new complex system without an effective IS can hinder production operations. IS supports organizations integrating hardware, software, data, people, and processes.

"Of the production operations, the establishment of an active Information System (IS) is one critical to support successful production operations."

Several factors contribute to the complexity of a system production phase, including: 1) advancing technology; 2) requirement to ensure compatibility of new processes with workforce organization and training; 3) design of communications among distributed production facilities; 4) acceptance test equipment; 5) manufacturing information management; and 6) provisions for change. Acquiring services under contracts to support operations is comparable to the complexity of the design of the actual system itself. Similar to the concept development phase, planning, design, and implementation occurs in production.

Concurrent engineering involves engineering analysis, design, simulation, and testing to examine components for producibility and transition. Installing, maintaining, and upgrading the MOSAICS system requires systems engineering principles and expertise throughout the operational lifecycle. Integrated Product Teams (IPTs) assemble expertise from various organizational units and external interfaces. Members of the IPT perform specialist activities such as mission assurance, or science and technology research. Concurrent engineering may run risks, as well. "The problem of making concurrent engineering effective is that design specialists, as the name implies, have a deep understanding of their disciplines but typically have only a limited knowledge of other disciplines, and hence a lack of common vocabulary (and frequently interest) for communicating with specialists in other disciplines," (Kossiakoff, 2011) [17]. Concurrent engineering brings together the appropriate functional disciplines throughout the systems engineering "Vee" [18]. Systems engineers lead the process of orchestrating specialty engineers. Systems engineering is to "serve as coordinators, interpreters, and, where necessary, as mentors" (Kossiakoff, 2011) [19]. Experienced operators and users bring system knowledge. Critical systems engineering principles are: 1) concurrent engineering takes place throughout system development; 2) the transition process of a new system from development to production can be particularly tricky; and 3) commercial development and production may be a dedicated separate phase in the system life cycle. This includes a preproduction prototype and selection of manufacturing procedures and equipment [20].

Conclusion

MOSAICS is the first prototype to address the operational need for cyber defense capabilities to defend mission-critical infrastructure from cyber attacks. Eventually, this prototype will be shared with commercial industry through DOD Industry Days for further research and development. This approach can lead to an innovative, game-changing capability. These planned Industry Days are good opportunities for industry to better understand the MOSAICS JCTD Transition Management (XM) plans and needs. It is also allows for industry to ask questions and provide feedback to the MOSAICS JCTD Integrated Management Team (IMT), and provide a valuable feedback mechanism to the JCTD Technical Management (TM) team early in the engineering and development life cycle.

Few professionals possess the skills to traverse both IT and OT systems. Finding the right personnel and quantifying cybersecurity risk is also a challenge. A more significant challenge is calculating the reliability of components for cyber resiliency, and developing methods to test for resiliency when thresholds are almost impossible to define in today's lexicon. Estimating how much more testing, red team/blue team, and scenarios are needed to estimate the size of the remaining problem set is key to risk mitigation strategies. It is important to understand red team offensive techniques to engineer effective defensive threat-based countermeasures prioritized by potential impact severity. Systems engineering principles can provide a mechanism to integrate contextual information from cyber-physical systems into context-sensitive critical infrastructure dynamic classes. This will improve cyber resilience in OT, and successfully transition MOSAICS to operations [21]. ■

References

[1] Aleksandra Scalco, M. J., Steve Simske (2019). "More Situational Awareness for Industrial Control Systems (MOSAICS) Joint Capability Technology Demonstration (JCTD): A Concept Development for the Defense of Mission Critical Infrastructure.» Homeland Defense & Security Information Analysis Center.

[2] Ibid.

[3] Merz, T. (2019).

[4] Kossiakoff, 2011.

[5] Ibid.

[6] Ibid.

[7] Ibid.

[8] Ibid.

[9] Ibid.

[10] Ibid.

[11] Ibid.

[12] INCOSE, 17.

[13] Merz, 2019.

[14] Miller, E. (2019). Human Factors in the Design of Complex Systems. E. 501. November 6, 2019, Colorado State University (CSU).

[15] Kossiakoff, 2011.

[16] Ibid.

[17] Ibid.

[18] INCOSE. 2012. Systems Engineering Handbook: A Guide for System Life Cycle Processes and Activities, version 3.2.2. San Diego, CA, USA: International Council on Systems Engineering (INCOSE), INCOSE-TP-2003-002-03.2.2.

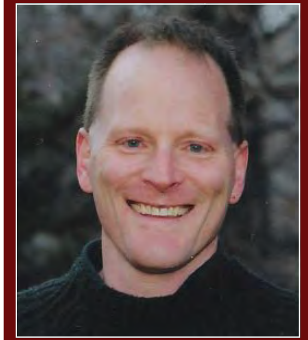
[19] Kossiakoff, 2011.

[20] Ibid.

[21] Scalco, 2019.

ABOUT THE AUTHORS

ALEKSANDRA SCALCO is an engineer with the Naval Information Warfare Center (NIWC) Atlantic. She is working towards a Systems Engineering Ph.D. at Colorado State University (CSU). Her research field is cyber resilience for Operational Technology (OT). She earned a Master's Degree in Engineering from Iowa State University in 2012, and a Master's Degree in Business Administration (MBA) in 2009. She is a member of the Defense Acquisition Corps in engineering. Ms. Scalco is Defense Acquisition Workforce Improvement Act (DAWIA) career certified Level 3 Engineering, Level 1 Science & Technology, and Level 1 Program Management. She holds ITIL Intermediate Certifications. Before joining NIWC Atlantic Ms. Scalco was a member of the National Security Agency (NSA) workforce as an Information System Security Designer (ISSD). As an ISSD, she provided technical expertise to clients on cyber assurance to advance the state of cybersecurity solutions to harden the National Security Enterprise against adversarial threats.



DR. STEVEN SIMSKE joined Colorado State University in 2018 as a Professor in Systems, Mechanical, and Biomedical Engineering. Before then, he was an HP Fellow and a Research Director in HP Labs. He led HP in research and development in algorithms, multi-media, labels, brand protection, security and secure printing, imaging, 3D printing, analytics and life sciences. He is a long-time member of the World Economic Forum Global Agenda Councils (2010-2016), leads the Steering Committee for the ACM DocEng Symposium, and is former President of the Imaging Science and Technology professional organization. Dr. Simske has nearly 200 granted US patents and more than 400 professional publications, including the recent books, Meta-Algorithmics and Meta-Analytics. He is an Honorary Professor in Computer Science at the University of Nottingham, UK. Dr. Simske was a payload specialist on a dozen Space Shuttle missions, and has designed devices ranging from exercise-responsive pacemakers to impedance tomography systems.

FUTURE EVENTS

HDIAC Homeland Defense & Security Information Analysis Center

JUNE

S	M	T	W	T	F	S
	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30				

JULY

S	M	T	W	T	F	S
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30	31	

AUGUST

S	M	T	W	T	F	S
						1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30	30					

JUNE 2020

June 16-18
5th Annual Defense One Tech Summit
Washington, DC

June 17-18
National Homeland Security Conference
Virtual Event

JULY 2020

July 14-16
International Hazardous Materials Response Teams Conference
Virtual Event

July 21-22
Utility Cyber Security Forum
Virtual Event

July 28-30
MegaRust 2020
San Diego, CA

July 29-30
Border Security and Intelligence Summit
Alexandria, VA

AUGUST 2020

August 17-21
TechNet Augusta 2020
Augusta, GA

August 23-26
Preparedness Summit
Dallas, TX

August 24-28
International Wireless Communications Exp 2020
Virtual Event

Please note that events are being impacted by the COVID-19 pandemic. For the most current calendar of events, visit https://www.hdiac.org/event/

HDIAC's latest

STATE OF THE ART REPORT (SOAR)

IS NOW AVAILABLE ONLINE:

HDIAC

Countermeasures Against the Degradation of Warfighter Capabilities due to Infectious Disease Threats

Be sure to view HDIAC's other SOAR publications:

- *Methods for Investigating Chemical-Biological Weapons Use*
- *Artificial Intelligence and Machine Learning for Defense Applications*
- *Critical Infrastructure Resilience*
- *PTSD: Applications & Future Directions in Behavioral Medicine & Clinical Neuroscience*
- *Use of Nanotechnology on Surfaces for Military Applications*

AVAILABLE AT
https://www.hdiac.org/hdiac-report/

Homeland Defense & Security Information Analysis Center
www.hdiac.org

901 North Stuart Street, Ste 401 Arlington, VA 22203
266 Genesee Street Utica, NY 13502

Homeland Defense and Security Systems
Information Analysis Center
901 N. Stuart St
Suite 401
Alrington, VA 22203

THE CENTER OF EXCELLENCE IN HOMELAND DEFENSE AND SECURITY INFORMATION SYSTEMS

Leveraging the best practices and expertise from government, industry, and academa in order to solve your scientific and technical needs.

https://www.hdiac.org/journal

To subscribe to the HDIAC Journal please email us at ***info@hdiac.org****, and to learn more about the HDIAC please visit us at* ***https://www.hdiac.org*** *and register to become a member of the HDIAC community of practice.*

HDIAC Mission Statement

The mission of the HDIAC is to provide users with focused expert technical consulting and unbiased scientific and technical information through in-depth analysis and the creation of specialized information products in support of the HDIAC's eight vital technical focus areas.