HDIAC JOURNAL
The Journal of the Homeland Defense and Security Information Analysis Center

Volume 4 Issue 3 Fall 2017

Conformal, Wearable Batteries:

Powering Warfighter Equipment

HDIAC JOURNAL
The Journal of the Homeland Defense and Security Information Analysis Center

Volume 4 • Issue 3 • Fall 2017

Director: Stuart Stough • Deputy Director: Joseph Cole
sstough@hdiac.org jcole@hdiac.org

About this Publication

The Journal of the Homeland Defense and Security Information Analysis Center (HDIAC) is published quarterly by the HDIAC staff. HDIAC is a DoD sponsored Information Analysis Center (IAC) with policy oversight provided by the Assistant Secretary of Defense for Research and Engineering (ASD (R&E)), and administratively managed by the Defense Technical Information Center (DTIC). HDIAC is operated by Information International Associates (IIa) in Oak Ridge, Tenn. Reference herein to any specific commercial products, processes or services by trade name, trademark, manufacturer or otherwise, does not necessarily constitute or imply its endorsement, recommendation or favoring by the United States government or HDIAC. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States government or HDIAC and shall not be used for advertising or product endorsement purposes.

DoDIACs
Department of Defense Information Analysis Centers

Table of Contents

ON THE COVER

Pararescuemen Staff Sgt. Jeremy Diola (left) and Senior Airman Corey Farr (right) establish a security perimeter after exiting an HH-60G Pave Hawk during an operational training exercise in Iraq. The men are assigned to the 66th Expeditionary Rescue Squadron at Joint Base Balad. Image created by Jennifer Kruzic, HDIAC and adapted from U.S. Air Force photo by Staff Sgt. Aaron Allmon (available for viewing at http://www.af.mil/About-Us/The-Book/Duty-Badges/igphoto/2000675834/mediaid/55848/).

AE **Alternative Energy** | B **Biometrics** | CBRN **CBRN Defense** | CS **Cultural Studies** | CIP **Critical Infrastructure Protection** | HDS **Homeland Defense & Security** | M **Medical** | WMD **Weapons of Mass Destruction**

Contact

Jennifer Kruzic
Graphic Designer

Amanda Andrews
Editor

David McCarville
Social & Multi-Media Editor

HDIAC Headquarters
104 Union Valley Road
Oak Ridge, TN 37830
865-535-0088

Marisiah Palmer-Moore
Contracting Officer Representative/ Program Management Analyst
Office: 703-767-9109
Email: marisiah.v.palmer-moore.civ@mail.mil
DoD Information Analysis Centers
8745 John J. Kingman Road
Fort Belvoir, VA 22060

Michele Finley
DoDIAC Public Affairs Officer
Office: 703-767-8215
Email: michele.l.finley2.civ@mail.mil
Defense Technical Information Center (DTIC)
8725 John J. Kingman Road
Fort Belvoir, VA 22060

Message from the Director:

Stuart Stough
HDIAC Director

HDIAC provides technical innovation and excellence while balancing affordability and reducing bureaucracy. HDIAC collaborates with top governmental, academic, and industry-based research laboratories and institutions on scientific and technical (S&T) breakthroughs and research and development (R&D) opportunities.

These partnerships and relationships allow HDIAC to be at the forefront of the research spectrum, helping provide innovative solutions to the most difficult problems and requirements faced by the DoD. This approach reduces duplication and aids in the development of a clear, timely, and applicable solution. HDIAC provides cost-effective R&D by acquiring, analyzing, and disseminating relevant S&T information; collaborating with academic, industry, and government partners; and utilizing an extensive subject matter expert network.

During this last quarter, HDIAC worked closely with several strategic university partners, including Auburn University and Oregon State University, regarding R&D and S&T developments that may be used to enhance U.S. service member protection and treat various medical conditions. In collaboration with government research laboratories, HDIAC further refined these approaches into technical solutions geared toward meeting DoD requirements for advanced body armor, refining exposure assays, and improving future medical treatments for military members.

Through these valuable collaborations, government research laboratories and HDIAC personnel support firsthand the work being performed on behalf of the DoD by validating the usefulness of the data generated for next generation body armor. HDIAC analyzed and presented approaches regarding the application of novel technologies, such as sheer thickening fluid, shape-memory alloys, and woven spider silk matrices, to develop next generation body armor to protect U.S. service members. These capability developments reduce R&D and S&T redundancy and support numerous government organizations, including the Special Operations Forces community, component and warfighting laboratories, and law enforcement agencies.

Additionally, government laboratories, HDIAC subject matter experts, and academic researchers reviewed current and future applications regarding "organs on chips," which is a medical development involving an artificial/3-D printed organ that simulates the activities or responses performed by our natural organ systems. Specifically, these collaborations included approaches regarding biological agent identification and nanoparticle treatment for phosgene exposure using the organs on chips model. The approaches focused on the interconnectedness of various human organ systems, natural physiology, and validity of future treatments. Refining and developing these capabilities could provide the DoD medical research community the most realistic and applicable model for testing and treatment.

HDIAC's strategic collaboration reduces research duplication and incentivizes productivity across the government and DoD S&T and R&D landscape. Continuing to forge research partnerships and collaborate with DoD and government agencies across HDIAC's eight focus areas not only eliminates unproductive processes, controls costs, and achieves affordable programs – it also ensures the DoD safeguards battlefield superiority over the coming decades. ■

Strategic Advantages

1. **Achieve Affordable Programs**
2. **Control Costs Throughout the Product Lifecycle**
3. **Incentivize Productivity and Innovation in Industry and Government**
4. Eliminate Unproductive Processes and Bureaucracy
5. **Promote Effective Competition**
6. **Improve Tradecraft in Acquisition of Services**
7. **Improve the Professionalism of the Total Acquisition Workforce**

Wearable

Rajan Kumar,
Joseph Wang, Ph.D.
&
Shirley Y. Meng, Ph.D.

Introduction

When the U.S. first arrived in Afghanistan more than two decades ago, a typical unit required 2.07 kilowatt-hours (kWh) to power its devices [1]. Today, unit power consumption has increased to 31.35 kWh due to the proliferation of mission-critical electronics on which soldiers rely [1]. This power demand means the warfighter now carries an additional 16 pounds of batteries, equivalent to an unloaded Squad Automatic Weapon, on top of the 60-120 pounds of standard gear [2]. Portable power sources are a critical issue in military operations due to the logistical challenge of battery swaps. This additional weight may increase the risk of musculoskeletal injury and greatly diminishes mobility and combat radius [1,3]. An increase in this power requirement is likely as the military intends to implement more energy-hungry technologies such as lightweight, body-armored exoskeletons, vital sensor monitoring, flexible displays embedded in electronic textiles, improved heads-up display for communications, and electronic wearables [4]. Although these technologies are still in their infancy, existing technologies demand lighter, safer, conformal batteries that do not compromise power or efficiency. This concept is an important planning factor for future warfighter needs.

In the past, soldiers were given 3-pound, brick-shaped batteries that were specifically designed for battery boxes and nonportable devices. As soldiers began to pack more electronics, these bulky batteries multiplied with them [5]. The U.S. Army Communications-Electronics Research, Development and Engineering Center developed a solution called the Soldier Wearable Integrated Power Equipment System, known as SWIPES, that provides an integrated solution for mission-critical electronics that can flex and stretch with the body while reducing weight [5]. SWIPES integrates all electronics carried by the warfighter into one tactical vest. Each electronic device is housed in a specific pocket with an associated power cord, and all devices connect to one conformal battery [5]. The conformal battery is a thin (>1/2-inch thick) and flexible lithium-ion battery weighing just over 2 pounds [5]. Due to flammability associated with lithium-ion batteries, especially from ballistic damage, the battery is treated with a ballistic coating to protect the battery [5].

Benefits

The benefits of the conformal battery were studied with a squad power manager kit, as shown in Figure 1 [3]. A United States Military Academy study compared the confor-

Conformal, Batteries: Powering Warfighter Equipment

mal battery over battery swaps to power a PRC-154 Rifleman Radio and an end user device, an Android smartphone [3]. The study revealed use of the small unit power (SUP) kit provided a 10-30 percent reduction in weight load compared to battery swaps [3]. Also, the large power reservoir of the conformal battery provided constant connection over interrupted battery swaps, and prevented swapping out a partially-charged battery with a fully-charged battery [3]. The study concluded the use of conformal batteries reduces weight load and the physical and mental toll on warfighters on how, when, and where to swap a battery [3,5].

Battery Chemistries

Although the current conformal battery has shown potential benefits to replace swappable batteries, significant improvements to the battery chemistry, level of conformability, and fabrication cost are critical to the military's effort to power mission-critical electronics. The availability of numerous battery chemistries such as magnesium, aluminum, iron, zinc, and lithium-ion has been explored for rechargeable batteries, as shown in Figure 2 [6]. There has been significant interest in lithium-ion and many of its sub-chemistries due to their high theoretical specific energy (5,928 Wh/kg) and

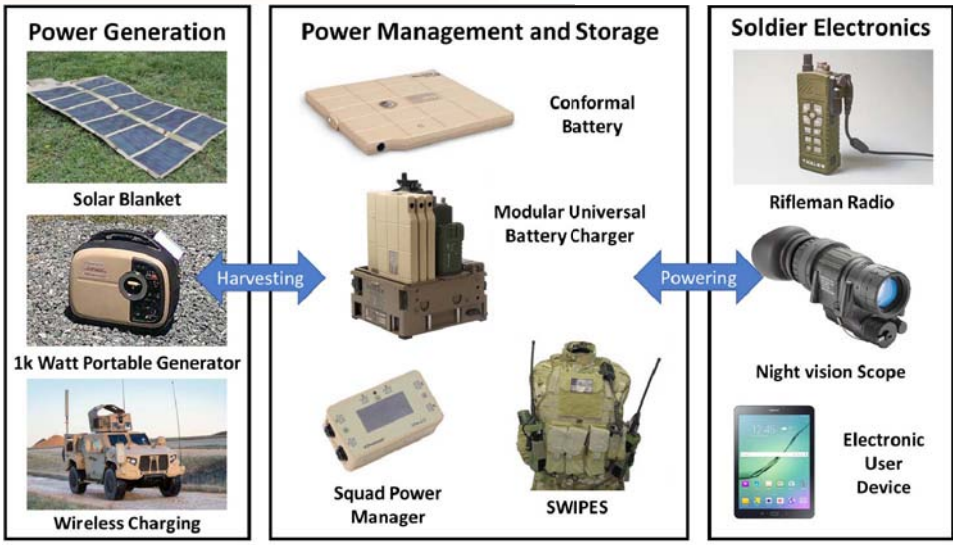


Figure 1: Operational view of power management for platoon [21-30].

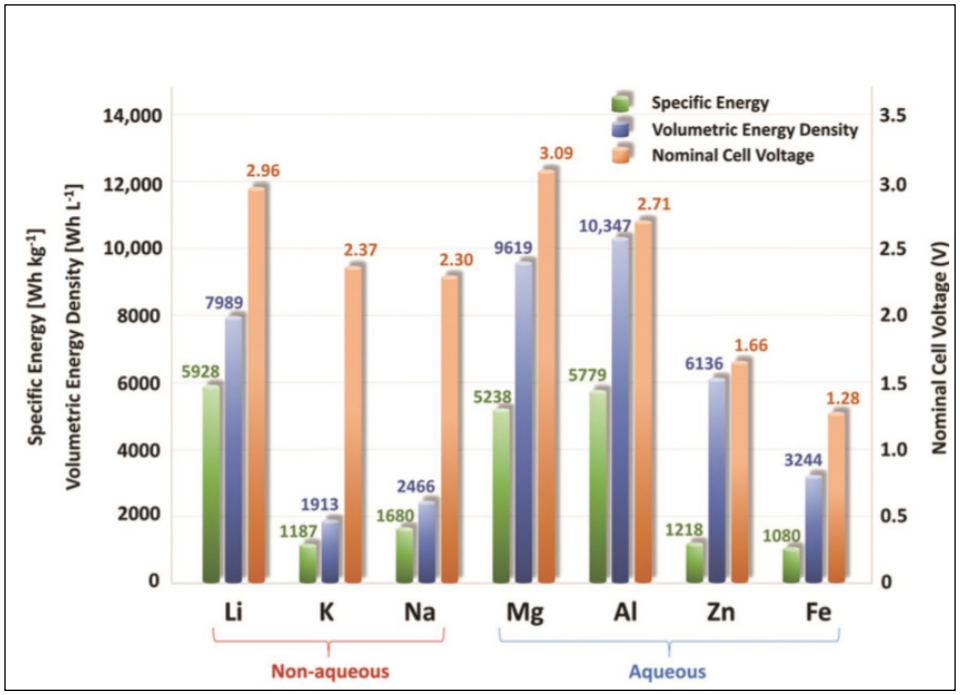


Figure 2: Theoretical specific energies, volumetric energy densities, and nominal cell voltages various metal anodes in aqueous and non-aqueous batteries [6]. (Released)

high cell voltage (2.96 V) [6]. For example, the military has recently funded research on lithium-sulfur batteries [7]. As for the next generation of lithium-ion batteries, many are looking to silicon anode because it has reported the highest known theoretical charge capacity (4,200 mAh/g) [8].

Silicon lithium-ion batteries remain in the prototype stage because of the large volume change (~400 percent) upon the insertion and extraction of lithium-ion, compared to the 10 percent volume change of graphite anodes [8]. The large volume change causes significant deformation and poor electronic contact thereby diminishing the capacity over time, with a cycle life no more than 10 cycles. Many groups have reported new approaches using silicon nanowires, incorporating self-healing polymers, and porous architecture resemblance of seeds packed in pomegranate [8-10]. Unfortunately, any type of lithium-ion chemistry will present safety issues due to its inherent instability and flammability, making it especially vulnerable to ballistic damage from ground combat [6]. The risks associated with the lithium-ion battery have grounded many technologies including the Boeing 787 Dreamliner, Samsung Note 7, and Fitbit Flex 2 [11-13]. Many wearable electronics companies are looking for safer battery chemistries, but the cost and performance of those batteries must be competitive before they can challenge lithium-ion.

Alternative chemistries such as magnesium and aluminum-air batteries are compatible with aqueous electrolytes and have demonstrated higher energy densities than lithium, but they experience rapid self-discharge and poor charging efficiency [6]. Zinc and iron have proven to be stable and safe chemistries, especially zinc-air and zinc-silver oxide. Zinc-based batteries are inherently safer, inexpensive, and more abundant, especially in the U.S., compared to lithium [6]. More importantly, zinc batteries have a relatively high specific energy (1,218 Wh/kg) and volumetric energy density (6,136 Wh/L) [6]. Recently, a U.S. Naval Research Laboratory team developed a novel, rechargeable, nickel-3D zinc battery as an energy-dense, safer alternative to lithium-ion [14]. When a zinc battery undergoes charging, dendrites will form and eventually grow to short the battery [14]. By implementing a porous zinc structure, the formation of dendrites is mitigated while maintaining a high capacity of 216 Wh/L along with tens of thousands recharge cycles [14].

This zinc chemistry presents a safer and cheaper battery chemistry alternative to lithium-ion with an estimated cost of $160 per kWh, when average lithium-ion battery prices are not expected to reach that value until 2025 [6,14]. Because zinc is inherently safer and all components can be exposed to air, simpler and inexpensive fabrication methods can be implemented. The complexity of lithium-ion battery fabrication amounts to nearly 40 percent of its overall cost, but screen printing can reduce the fabrication cost [6]. Screen printing is a low-cost, high-throughput fabrication where conductive inks can be applied to a patterned stencil, then a doctor blade will deposit the conductive inks onto the substrate through the holes of the pattern. Zinc batteries can be printed in four to five simple coating steps and in any desired shape. The use of conductive inks and printing technologies allows for battery conformability, enabling them to stretch, bend, flex, and twist.

Conformal Battery Development

Deterministic and random composite architecture are two approaches used to develop

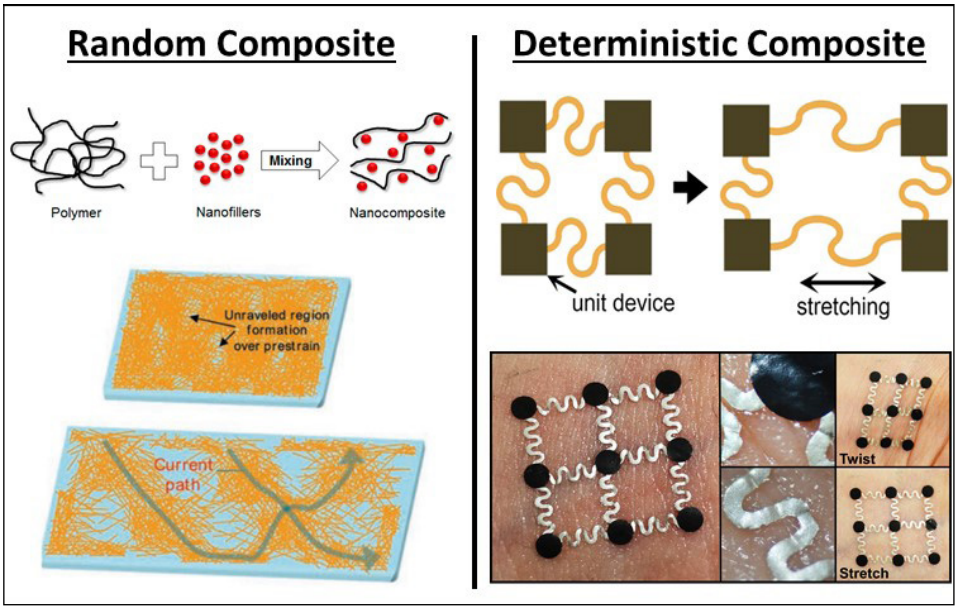


Figure 3: Approaches for engineering stretchable electronics [31] [32] (Licensed under Creative Commons) [33].

conformal batteries, as shown in Figure 3 [15]. In the deterministic approach, nonelastic, inorganic materials, such as metals are geometrically patterned into ultra-thin, serpentine bridges connected to rigid islands [15]. This method of strain engineering allows typically rigid materials to be more conformal by undergoing stretching and flexing. The random composite approach randomly embeds highly conductive fillers into an elastomeric matrix [15]. While random composite is highly strain-sensitive to any type of deformation, the ability to incorporate any combination of materials [15] is specifically attractive for developing conformal batteries that comprise various metallic and polymeric additives. The precise composition of conductive fillers, elastic binders, and solvents will result in formulations that can be readily applicable to inexpensive, printing technologies. This approach is compatible with air-stable, zinc-based chemistries that can be used to inexpensively print conformal batteries into a military vest.

Researchers at the University of California, San Diego Department of NanoEngineering have demonstrated the first fully-printed, stretchable, rechargeable battery using low-cost, screen printing of highly elastic, conductive inks [16]. Through the unique formulation of inks and screen printing, the batteries were printed in the form of "NANO" onto a polyurethane-coated spandex, as shown in Figure 4 [16]. The battery demonstrated a high, reversible areal capacity of ~2.5 mAh/cm^2 density even after multiple iterations of deformation including bending, twisting, indentations, and stretching twice its length [16]. Other approaches were attempted in order to produce stretchable batteries, but none of the systems were completely elastic [16] as traditional battery chemistries require encasement in a rigid protective shell. In addition, many of these approaches relied on lithographic, spray/dip coating, or "cut-and-paste" methods of fabrication that were extremely expensive and resulted in low-throughput [16].

While most applications do not require a significant amount of stretch (other than electronic textiles), flexibility is an essential form factor. For example, solar blankets in the SUP kit have ultra-thin solar cells that allow warfighters to either roll up or fold the blanket. Along with flexibility, the ability for batteries to recharge is another essential factor. Printable, zinc batteries are being developed but very few are rechargeable.

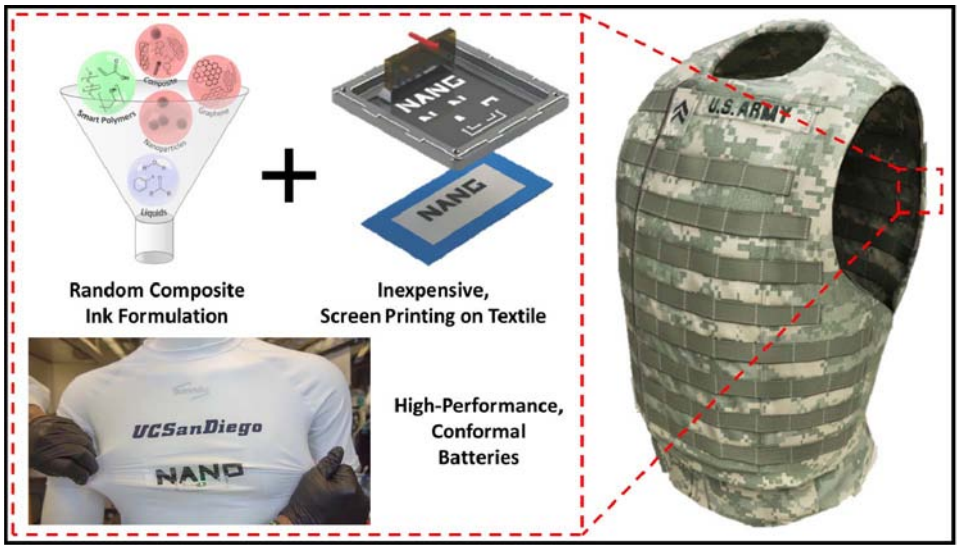


Figure 4: Random composite and screen-printing for high-performance, conformal batteries.

Blue Spark Technologies Inc. developed a printed battery with a capacity less than <1 mAh/cm^2, and they combined printed batteries and temperature sensors for a disposable temperature monitor for newborns [17]. Imprint Energy Inc. developed the only printed zinc battery that is rechargeable because of an innovative ionic-liquid electrolyte. However, this battery has a poor capacity of <1.5 mAh/cm^2 over the course of 100 recharge cycles [18].

Printable Batteries

Researchers at the University of California, San Diego initially used printed batteries for small patches to power wearable electronics. However, screen printing can be utilized to coat the entire inner area of a military vest. A typical military vest for an average male torso covers a surface area of 0.6 m^2 [19]. The areal capacity of printed batteries will be greater than 3.5 mAh/cm^2 to achieve a capacity nearly three times the capacity of the current conformal battery (7.3 Ah) used by SWIPES. Since technology implemented by the military must be more durable than conventional consumer electronics, a higher number of charge cycles is essential. If these screen printed batteries can meet this durability requirement, they would provide a low-cost, conformal, high-performance battery solution for the dismounted warfighter.

The ability to accomplish an area capacity beyond 3.5 mAh/cm^2 and a cycle life beyond 200 cycles is possible using zinc-silver oxide chemistry implemented in the printed, stretchable battery. The initial proof-of-concept was designed for more stretchable textiles, such as spandex or nylon. For military application, flexibility with some stretch is needed to enable the printed battery to be worn inside the shell of a military vest. The random composite can control the composition of elastomer and conductive fillers, where some stretch (<20 percent) can be reformulated for the printed battery. The design of the printed battery was in a lateral design, whereas a typical battery stacks the anode, cathode, and electrolyte. The stacked design will be a far more efficient use of the printed area. The current limitation for the stacked design is a printable electrolyte that is both flexible and stretchable. A printable electrolyte will require structural durability and high ionic conductivity for high-current charge/discharging. Further improvement of anode, cathode, and electrolyte materials as well as inexpensive screen printing techniques will enhance the production of high-performance, conformal batteries.

The printed, conformal battery integrated into a tactical vest addresses the military's vision to eliminate bulk cables using electronic textiles [5]. Ultra-thin, conductive wiring and a conformal battery can be printed into the textile to power various electronics in each designated pocket. The addition of printed, power transfer antenna in the back of the vest for wireless charging will simplify the top-down integration by enabling wireless charging by a vehicle. When a warfighter sits in a vehicle, wireless charging components embedded in the seat would seamlessly charge the printed power vest [5]. This presents a great tactical advantage in the

event a warfighter must quickly abandon the vehicle.

The conformal, wearable battery will require durability and performance testing under actual environmental conditions and power expectations of a 72-hour mission. Factors such as varied temperature and humidity could affect battery performance, especially in a 24-hour cycle. Therefore, these environmental factors must be evaluated. Additionally, determining if the battery is washable, especially when exposed to detergents or harsh temperatures and deformations from a typical tumble dry, must also be evaluated.

This concept can be further applied to other devices in the SUP kit. For example, batteries can be printed on the opposite side of a solar blanket, which would allow for additional energy storage and eliminate the setup time for the solar blanket with a modular universal battery charger and battery. The military has been considering implementing energy harvesting technologies into the warfighter uniform, such as wearable solar panels on the helmet or rucksack [5]. Other small kinetic devices that oscillate back and forth for harvesting energy from walking have also gained significant investment from the military [20]. Numerous energy harvesting technologies such as thermoelectric, piezoelectric, biofuel cells, and triboelectric have been studied to self-power wearable electronics, and all of these energy harvesting technologies could provide trickle charge to extend the life of the printed, conformal battery [5].

Conclusion

The Department of Defense has been at the forefront of developing and supporting new battery chemistries to maintain its technological advantage on the ground. As reliance on wearable electronics continues to grow, so does the burden of these conformal power technologies on warfighter mental and physical stamina. Debate will continue on which materials and battery chemistry will prevail based on cost and performance, but the fabrication and conformability of batteries is equally critical to the success of warfighter wearable systems. Inexpensive printing technologies offer a solution that enables the combination of deterministic and random architectures for implementation of conformal batteries into a tactical vest. Merging printing technologies and advanced materials will lessen warfighter weight load and seamlessly power warfighter electronics, allowing warfighters to focus on their mission and not on battery replacement. ■

References

1. Magnuson, S. (2017, June 1). Power-hungry devices challenge Army researchers. *National Defense*. Retrieved from http://www.nationaldefensemagazine.org/articles/2017/6/1/power-hungry-devices-challenge-army-researchers (accessed July 6, 2017)
2. Robinson, P. (June 10). What do soldiers carry and what does it weigh [Web log post]. Retrieved from https://protonex.com/blog/what-do-soldiers-carry-and-whats-its-weight/ (accessed July 6, 2017)
3. Aten, C., Michalowski, A., Williams, M., Stamm, C., & Evangelista, P. (2015). Soldier power operational benefit analysis. *Industrial and Systems Engineering Review*, *3*(2), 82-90. Retrieved from http://watsonojs.binghamton.edu/index.php/iser/article/view/41 (accessed July 6, 2017)
4. Machi, V. (2017, June 19). Sumo wrestlers inspire new exoskeleton tech. *National Defense*. Retrieved from http://www.nationaldefensemagazine.org/articles/2017/6/19/sumo-wrestlers-inspire-new-exoskeleton-tech (accessed July 6, 2017)
5. Armed with Science. (2014, February 18). SWIPES, the integrated power source [Web log post]. Retrieved from http://science.dodlive.mil/2014/02/18/swipes-the-integrated-power-source/ (accessed July 6, 2017)
6. Fu, J., Cano, Z. P., Park, M. G., Yu, A., Fowler, M., & Chen, Z. (2016). Electrically Rechargeable Zinc-Air Batteries: Progress, Challenges, and Perspectives. *Advanced Materials*, *29*(7), 1604685. doi:10.1002/adma.201604685
7. Casey, T. (2015, July 14). Yet another energy storage company takes on Tesla. Retrieved from https://cleantechnica.com/2015/07/14/yet-another-energy-storage-company-takes-tesla/ (accessed July 6, 2017)
8. Chan, C. K., Peng, H., Liu, G., Mcilwrath, K., Zhang, X. F., Huggins, R. A., & Cui, Y. (2007). High-performance lithium battery anodes using silicon nanowires. *Nature Nanotechnology*, *3*(1), 31-35. doi:10.1038/nnano.2007.411
9. Wang, C., Wu, H., Chen, Z., Mcdowell, M. T., Cui, Y., & Bao, Z. (2013). Self-healing chemistry enables the stable operation of silicon microparticle anodes for high-energy lithium-ion batteries. *Nature Chemistry*, *5*(12), 1042-1048. doi:10.1038/nchem.1802
10. Liu, N., Lu, Z., Zhao, J., Mcdowell, M. T., Lee, H., Zhao, W., & Cui, Y. (2014). A pomegranate-inspired nanoscale design for large-volume-change lithium battery anodes. *Nature Nanotechnology*, *9*(3), 187-192. doi:10.1038/nnano.2014.6
11. Irfan, U. (2014, December 18). How lithium ion batteries grounded the Dreamliner. *Scientific American*. Retrieved from https://www.scientificamerican.com/article/how-lithium-ion-batteries-grounded-the-dreamliner/ (accessed July 6, 2017)
12. Lee, S. (2017, June 27). Samsung revives once-exploding Galaxy Note 7 as 'Fan Edition' models [Web log post]. Retrieved from http://www.siliconbeat.com/2017/06/27/samsung-revives-exploding-galaxy-note-7-fan-edition-models/ (accessed July 6, 2017)
13. Golgowski, N. (2017, April 25). Fibit denies claim woman's device exploded. *HuffPost*. Retrieved from http://www.huffingtonpost.com/entry/woman-claims-fitbit-exploded_us_58ff54a7e4b0b6f6014ac404 (accessed July 6, 2017)
14. Parker, J. F., Chervin, C. N., Pala, I. R., Machler, M., Burz, M. F., Long, J. W., & Rolison, D. R. (2017). Rechargeable nickel–3D zinc batteries: An energy-dense, safer alternative to lithium-ion. *Science*, *356*(6336), 415-418. doi:10.1126/science.aak9991
15. Wang, Y., Zhu, C., Pfattner, R., Yan, H., Jin, L., Chen, S., . . . Bao, Z. (2017). A highly stretchable, transparent, and conductive polymer. *Science Advances*, *3*(3). doi:10.1126/sciadv.1602076
16. Kumar, R., Shin, J., Yin, L., You, J., Meng, Y. S., & Wang, J. (2016). All-printed, stretchable Zn-Ag2O rechargeable battery via hyperelastic binder for self-powering wearable electronics. *Advanced Energy Materials*, *7*(8), 1602096. doi:10.1002/aenm.201602096
17. Washington, J. (2017, June 28). Westlake's TempTraq monitors fevers through wearable patch synced with smartphone (video). Retrieved from http://www.cleveland.com/healthfit/index.ssf/2017/06/westlakes_temptraq_monitors_fe_1.html (accessed July 6, 2017)
18. Ho, C. (2017, June). Flexible Energy Storage. In Energy: Harvesting, Storage and Management for Flexible Systems in the IOT. Presentation conducted at the 2017 Flex Conference, Monterey, CA.
19. Barwood, M. J., Newton, P. S., & Tipton, M. J. (2009). Ventilated vest and tolerance for intermittent exercise in hot, dry conditions with military clothing. *Aviation, Space, and Environmental Medicine*, *80*(4), 353-359. Retrieved from https://www.ncbi.nlm.nih.gov/pubmed/19378904 (accessed July 6, 2017)
20. Stone, A. (2016, December 28). PowerWalk device converts soldiers' movments into energy. Retrieved from http://www.c4isrnet.com/articles/powerwalk-device-converts-soldiers-movement-into-energy (accessed July 6, 2017)
21. Tozer , J. L. (2013, May 7). Top tech: Solar blankets [Web log post]. Retrieved from http://science.dodlive.mil/2013/05/07/top-tech-solar-blankets/ (accessed July 6, 2017)
22. INI Power Systems. (n.d.). *INI Power Systems 1kW products*. Retrieved from https://www.inipowersystems.com/1kwproducts (accessed July 6, 2017)
23. Olsewski, S. (2016, April 7). *Video: Humvee replacement will be powered by banks*. Retrieved from http://www.dieselarmy.com/news/video-humvee-replacement-will-be-powered-by-banks/ (accessed July 6, 2017)
24. Inventus Power. (2016, May 27). *Helping solve the portable power needs of today's warfighter*. Retrieved from http://inventus-power.com/helping-solve-portable-power-needs-todays-warfighter/ (accessed July 6, 2017)
25. Thales. (n.d.). *Modular universal battery charger*. Retrieved from https://www.thalesgroup.com/en/worldwide/defence/what-we-do-radio-communications-land-communications-tactical-radios/modular (accessed July 6, 2017)
26. Protonex. (n.d.). *SPM-612*. Retrieved from https://protonex.com/products/spm-612/ (accessed July 6, 2017)
27. The Shephard News Team. (2013, February 25). Arotech receives US Army Swipes order [Web log post]. Retrieved from https://www.shephardmedia.com/news/mil-log/arotech-receives-us-army-swipes-order/ (accessed July 6, 2017)
28. SupplyNet. (n.d.). *AN/PRC-154 USB Dongle Cable*. Retrieved from http://www.tacticaleng.com/an-prc-154-usb-dongle-cable

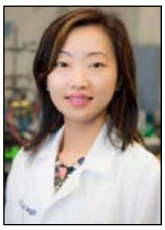
(accessed July 6, 2017)
29. [Digital image]. (n.d.). Retrieved from https://i5.walmartimages.com/asr/4928b9e7-3ec6-4b67-8be1-e507c51f0588_1.dd-83ba71cb4edccd2c5897bda3d37058.jpeg (accessed July 6, 2017)
30. [Digital image]. (n.d.). Retrieved from http://images.samsung.com/is/image/samsung/p5/au/tablets/galaxy-tab-s2.png?$ORIGIN_PNG$ (accessed July 6, 2017)
31. Pleşa, I., Noţingher, P., Schlögl, S., Sumereder, C., & Muhr, M. (2016). *Figure 21. Schematic representation of the mechanical mixing of nanoparticles with the polymer* [Figure]. *Polymers*, *8*(5), 173. doi:10.3390/polym8050173
32. Chortos, A., & Bao, Z. (2014). *Figure 1. Strategies for making electronics stretchable* [Figure]. *Materials Today*, *17*(7), 321-331. doi:10.1016/j.mattod.2014.05.006.
33. Lee, Y., Shin, M., Thiyagarajan, K., & Jeong, U. (2016). *Figure 1. Schematic representation of the different types of stretchabl devices* [Figure]. *Macromolecules*, *49*(2), 433-444. doi:10.1021/acs.macromol.5b02268

Rajan Kumar
Ph.D. Candidate, University of California, San Diego

Rajan Kumar is pursuing a Ph.D. in nanoengineering at the University of California, San Diego (B.S., SUNY Polytechnic Institute). His research is focused on implementing advanced materials and printing technology to develop wearable, energy harvesting technologies. He has a background in nanoscale fabrication for molecular imprinting polymers and lab-on-chip biosensors.

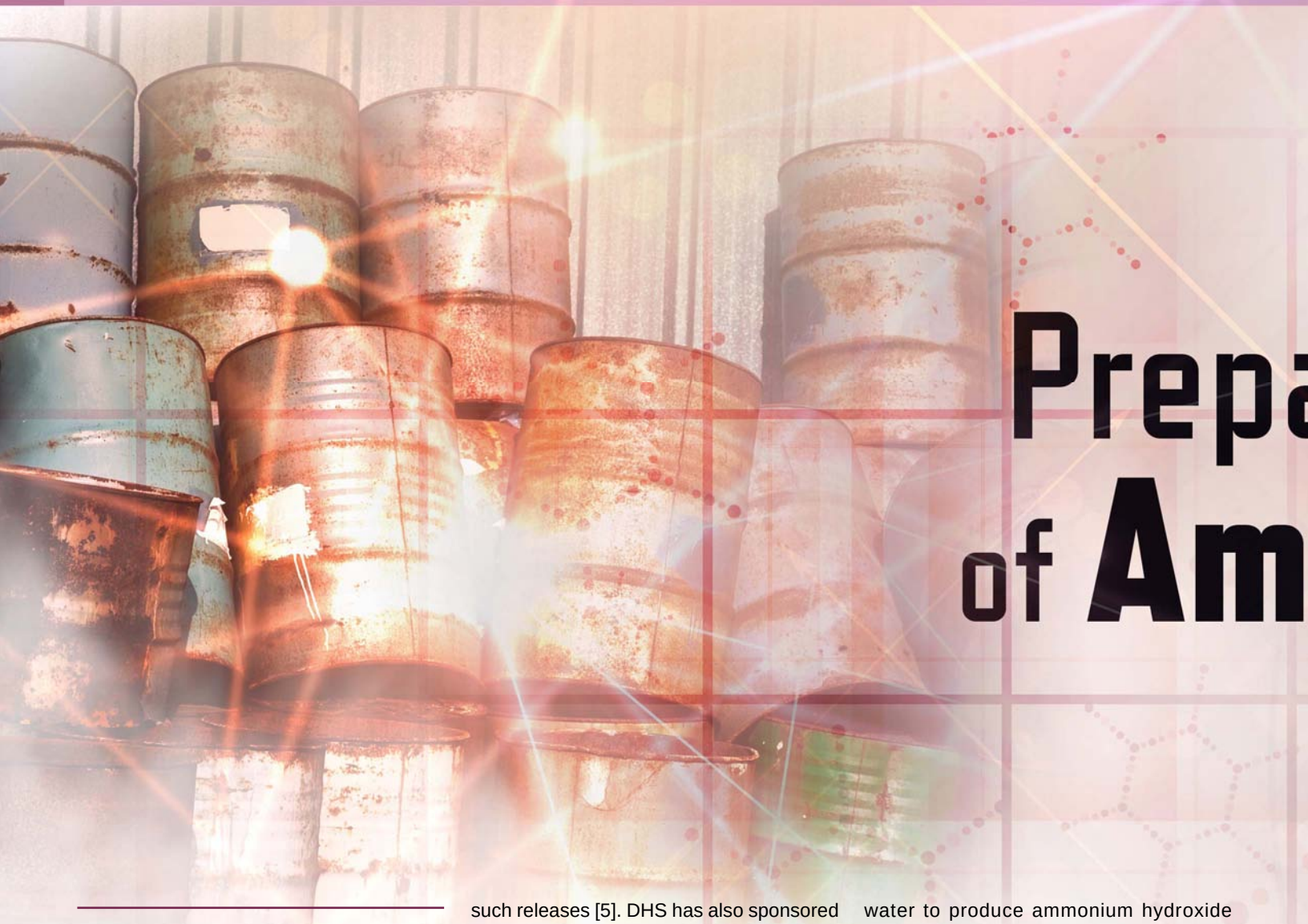
Joseph Wang, Ph.D.
Distinguished Professor, SAIC Endowed Chair, and Chair of NanoEngineering, University of California, San Diego

Joseph Wang is a distinguished professor, SAIC endowed chair, and chair of nanoengineering at the University of California, San Diego. He joined the University of California San Diego NanoEngineering Department in 2008. His research interests include the development of nanomotors and nanorobots, wearable devices, printed electronics, and bioelectronics and biosensors.



Shirley Y. Meng, Ph.D.
Associate Professor, University of California, San Diego

Shirley Y. Meng is an associate professor of nanoengineering at the University of California, San Diego. She heads an interdisciplinary laboratory focused on energy storage (batteries and supercapacitors) and conversion (solar and magnetic). Meng's research group, Laboratory for Energy Storage and Conversion, is focusing its efforts on the basic science and applied research for the design and development of energy storage and conversion materials.



Prepa of Am

Jamie Glover, MPH

Introduction

Ammonia and chlorine are essential to modern life. Processes relying on ammonia and chlorine provide safe public water supplies, abundant agriculture products, and numerous other goods that enhance quality of life for U.S. warfighters and civilians [1,2]. However, ammonia and chlorine are classified as toxic industrial chemicals (TICs) because they also pose significant health threats [3,4]. Not only are they used as chemical weapons, but they can also cause substantial harm through accidental mass releases [4]. Given their ubiquity in modern life, it is essential to prepare for chlorine and ammonia releases, whether occurring as industrial accidents or when used as chemical weapons against the warfighter. Several federal agencies, including the Department of Homeland Security (DHS), work to prevent and prepare for such releases [5]. DHS has also sponsored research conducted by Edgewood Chemical Biological Center scientists at the U.S. Army Dugway Proving Ground that is making a substantial contribution to ammonia and chlorine event preparedness [6].

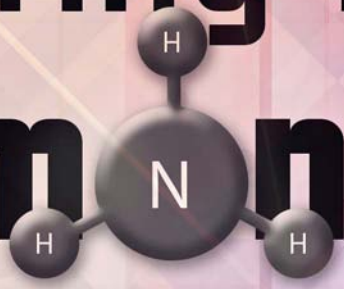
Ammonia & Chlorine

The U.S. produces more than 9 million tons of ammonia [7] and 15 million tons of chlorine each year [2]. Eighty percent of ammonia produced in the U.S. is used as fertilizer, making it essential to American agriculture. Ammonia is also common in refrigeration systems, including those that the Defense Commissary Agency is installing in military base commissaries [8]. Chlorine is used in paper, plastic, and chemical product manufacturing, as well as municipal sewage and drinking water treatment [2].

Despite their pervasiveness, ammonia and chlorine pose substantial health hazards. When ammonia (NH_3) comes into contact with human cells it reacts with cellular water to produce ammonium hydroxide (NH_4OH), a highly corrosive compound [9]. Exposure through inhalation can result in nasopharyngeal burns, tracheal burns, bronchiolar and alveolar edema, and airway destruction that can ultimately cause respiratory distress or failure [1]. Skin and eye contact with ammonia can be harmful at concentrations as low as 100 ppm, with higher concentrations resulting in skin burns, permanent eye damage, and even blindness (see Figure 1).

Chlorine's toxicity is also tied to its reaction with water. Elemental chlorine (Cl_2) reacts with water to produce hypochlorous and hydrochloric acids, and these acids then react to produce oxygen free radicals. This leads to both acute and chronic health effects by damaging cell walls, amino acids, and enzyme systems. Exposure can cause inflammation of upper airways, eye and skin injuries, and alveolar and endothelial cell death that can result in Acute Respiratory Distress Syndrome and pulmonary edema [2].

aring for the Threat
monia & Chlorine



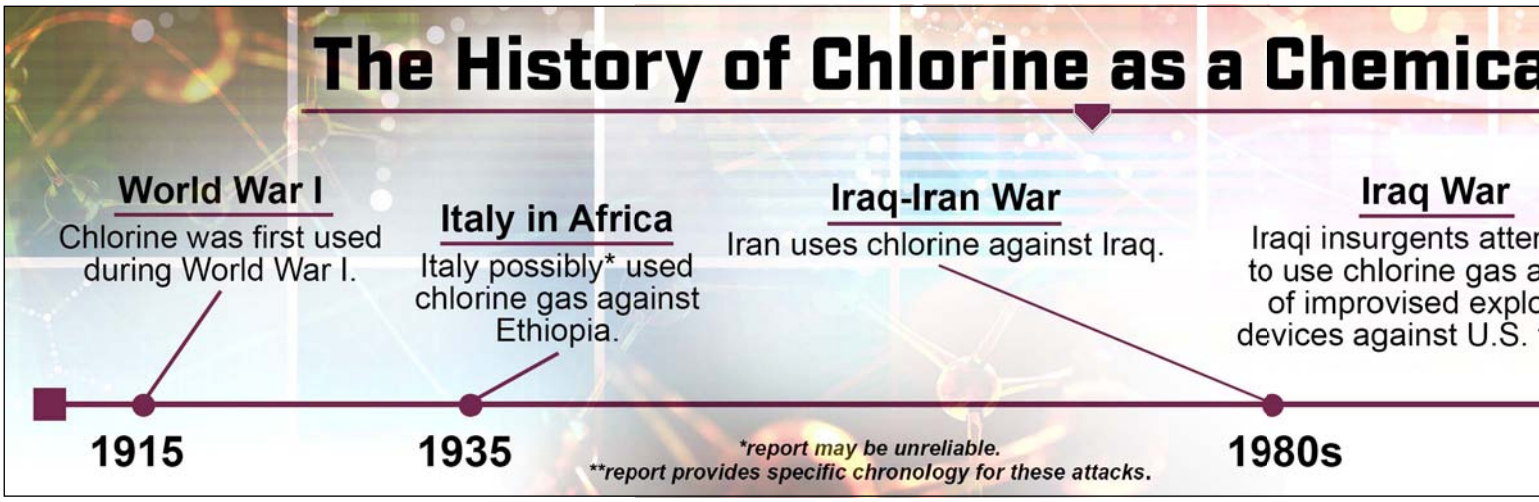
The Threat of Ammonia & Chlorine

Ammonia and chlorine present threats through accidental mass releases and as chemical weapons that can be used against U.S. warfighters and civilians. Chlorine has been used as a chemical weapon since World War I [3]. Salafi jihadist groups, including the Islamic State [10] and al-Qaida [11], have used chlorine gas in roadside bombs in Iraq for over a decade, including during Operation Iraqi Freedom [2]. Since 2014, the Syrian government has used chlorine as a chemical weapon in the Syrian Civil War against civilians, rebel forces, and terrorist groups [3]. Some U.S. government and military officials view ammonia as a more probable terrorist threat than chlorine due to its extensive use in industrial refrigeration [12]. In late 2016, the United Nations reported ISIS had stockpiled ammonia in Mosul and raised concerns of possible intent to use it in chemical weapons [13,14].

Like all chemical weapons, ammonia and chlorine are attractive to terrorists because of their negative health consequences, high casualty counts, and their ability to incite mass public panic [15]. Chemicals are also easier to access than other high-impact weapons. This is especially true for TICs because their production and use is not prohibited like other chemical weapons. The Chemical Weapons Convention (CWC), agreed to by the U.S. and 191 other countries, prohibits the development, production, acquisition, transfer, storage, and use of chemical weapons [16]. However, the CWC does not apply to legitimate industrial applications of TICs, such as ammonia and chlorine [17]. This makes it easy for TICs to be weaponized by releasing them directly from industrial facilities or during transit. In 2015, DHS reported that the risk of insider threat was increasing for the chemical sector, meaning an intentional release by an industrial employee may be more likely [5].

Additional security challenges arise for ammonia and chlorine because their production is geographically concentrated and large quantities are transported and stored around densely populated urban areas and military bases [2]. Under the right meteorological conditions, an intentional or unintentional release could envelope a large city or military base in a cloud of toxic gas [15].

Accidental mass releases are a common occurrence. In 2005, a train carrying 60 tons of liquid chlorine crashed into a parked locomotive in Graniteville, South Carolina, due to human error [4]. The crash resulted in the release of 60 tons of chlorine at a textile mill with 183 employees inside. At least 529 people sought medical treatment – leaving 72 hospitalized and nine dead. A similar incident occurred in Texas in 2004, where human error resulted in the release of 90,000 pounds of chlorine gas. The exposures left two dead and 41 injured, including six injured first responders [18]. In 2002, nearly 17,000 pounds of chlorine gas were released from a railroad car in Missouri when an automatic shut-off valve and emergency shut-off system failed. The incident injured 67 people, but no deaths were reported [18].



Response Considerations

In the occurrence of a domestic mass release, local, state, and federal governments may be involved in response efforts. Federal response to domestic releases is typically led by DHS with support from the Department of Defense (DoD), in accordance with the National Response Framework and National Incident Management System guidelines. Initial response requires first responders to enter a "hot zone" with the highest potential for hazardous exposure [19].

When responders enter an area with an undetermined chemical threat that could be chlorine or ammonia, Level A personal protective equipment (PPE) is necessary. This level of protection includes an Encapsulating Chemical Protective suit with a full-face-piece CBRN self-contained breathing apparatus with a positive pressure ventilation system. Level A protection also requires responders to wear coveralls, long underwear, and a hard hat under their protective suit, with chemical resistant gloves and boots [20,21].

This cumbersome PPE shields responders from the hazards of chlorine and ammonia exposures. However, Level A protection, and even lesser levels of protection, restrict movement, vision, and communication, and can induce both psychological and heat stress. This limits safe use of Level A PPE to only 30 minutes [22].

It also requires responders to have a great deal of skill, training, and experience to operate effectively while wearing proper PPE. Responders can safely use less cumbersome protective equipment with more information about potential exposures [20,21]. An initial assessment of the nature of the release, damage and injury reports, weather conditions, geography, terrain and public reaction can better inform response efforts. A thorough assessment can also help prepare for the possibility of a secondary incident/device used after an intentional mass release that could result in further damage and harm first responders [19].

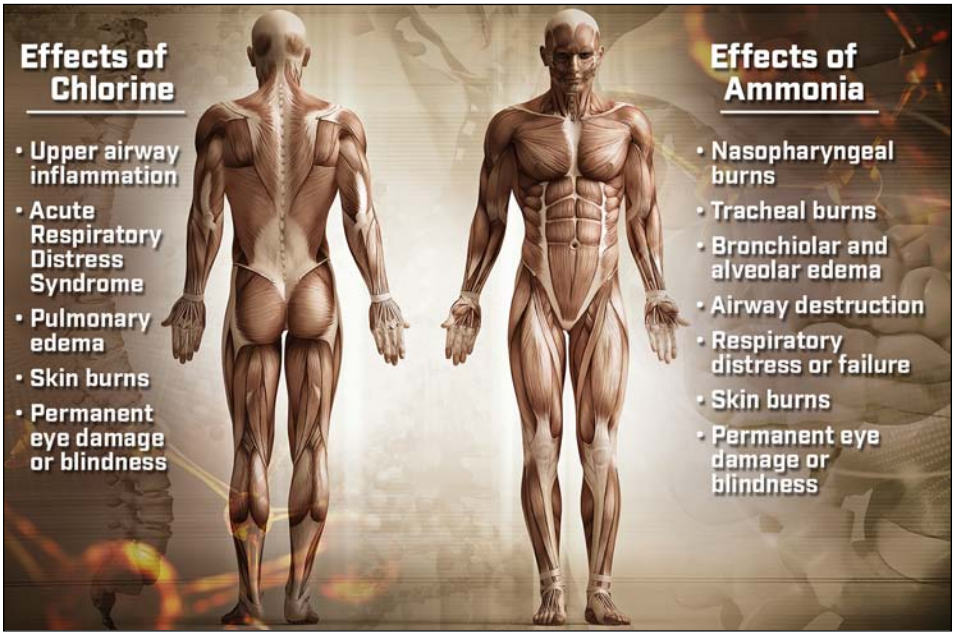


Figure 1: The effects of chlorine and ammonia on the human body.

Mitigation Efforts

Federal agencies, including the Centers for Disease Control and Prevention [23], Department of Transportation [24], and DHS [5], work to prevent intentional releases and mitigate effects of accidental releases of hazardous materials, including ammonia and chlorine. Specifically, DHS oversees the chemical sector as one of 16 total critical infrastructure sectors and collaborates with the private sector to ensure security of chemical products to prevent use by nefarious actors [5]. Through the Federal Emergency Management Agency's Emergency Management Institute, DHS trains emergency management professionals, "to prepare for, protect against, respond to, recover from, and mitigate the potential effects of all types of disasters and emergencies on the American people" [25]. DHS has also prioritized research that will improve understanding of toxicological and dispersion data of dense gases to better comprehend certain chemicals' hazards [5].

Project Jack Rabbit

In response to Congressional concerns regarding TICs, the DHS Transportation Security Administration collaborated with the Chemical Security Analysis Center to conduct Project Jack Rabbit (PJR) by Edgewood Chemical Biological Center scientists at the U.S. Army Dugway Proving Ground in 2010 [6]. The goal of PJR was to further the understanding of chlorine and anhydrous ammonia behavior during rapid, large-scale

Timeline References

1. Ahuja, M. (2013, August 26). Timeline of chemical weapon use. *The Washington Post*. Retrieved from https://www.washingtonpost.com/apps/g/page/world/timeline-of-chemical-weapon-use/417/ (accessed July 6, 2017)
2. Grip, L., & Hart, J. (2009). The use of chemical weapons in the 1935–36 Italo-Ethiopian War. *SIPRI Arms Control and Non-proliferation Programme*. Retrieved from https://chilot.files.wordpress.com/2011/01/the-use-of-chemical-weapons-in-the-1935-36-italo-ethiopian-war.pdf (accessed July 6, 2017)
3. Ali, J. (2001). Chemical weapons and the Iran-Iraq War: A case study in non-compliance. *Nonproliferation Review*, *8*(1), 43-58. Retrieved from https://www.nonproliferation.org/wp-content/uploads/npr/81ali.pdf (accessed July 6, 2017)
4. Shea, D. A. (2013, September 13). *Chemical weapons: A summary report of characteristics and effects* (CRS Report R42862). Retrieved from https://fas.org/sgp/crs/nuke/R42862.pdf (accessed July 6, 2017)
5. Arms Control Association. (2017, April 7). Timeline of Syrian chemical weapons activity, 2012-2017. Retrieved from https://www.armscontrol.org/factsheets/Timeline-of-Syrian-Chemical-Weapons-Activity (accessed July 6, 2017)

release events from railcars [26]. Before PJR, the only understanding of gas behavior during a large release was developed from tests using gases other than chlorine and ammonia.

The tests examined releases of 60 to 90 tons of compressed liquefied chlorine and ammonia gases [6]. In each of 10 experiments, researchers released 1 to 2 tons of pressurized, liquefied chlorine or ammonia for 30 seconds from a downward-facing pipe two meters above ground. Tanks were custom designed and constructed for the experiment releases. Two 1,000-gallon propane tanks were used for ammonia releases, and two 500-gallon propane tanks were used for chlorine. Manual knife gate valves and remotely controlled ball valves were used for these releases.

The release site was a 2-meter-deep depression with a 25-meter radius. Measurements were taken within 500 meters from the release site. Data were collected using several types of instrumentation, including chemical, meteorological, and photonic means of measurement, shown in Table 1.

A major project finding was the effects of wind conditions on gas dispersal and indicated extremely hazardous zones for victims and emergency responders within 250 meters of the release point [6]. Chlorine vapor remains close to the ground for 250 meters from the point of release, after which it mixes with air and reduces concentration levels. The vapor will be mixed enough to be carried away by wind after 500 meters. The findings of PJR led to a second iteration of the project.

Project Jack Rabbit II (PJR II), which began in 2013 [6], tested larger scaled chlorine releases, between five and 10 tons, from a six-inch tank opening in 50 seconds or less to produce a "worst-case release scenario." PJR II tests were conducted in simulated urban environments, including building simulations; detection devices in and outside of vehicles downwind from releases; and additional upwind monitoring. Results revealed that chlorine vapor clouds remain within the urban environment for up to 20 minutes; liquid from releases can pool over concrete pads; vapor moves over one-story structures, but not higher structures; release concentrations take as long as 20 minutes to dissipate; and sheltering in vehicles does not reduce exposure within 200 meters of the release point. More in-depth details are not available for public release [23].

Tests in phase two of PJR II increased chlorine amounts from 10 to 20 tons. Tests were conducted among vehicle and simulated structures to further improve urban environment modeling, understand reactivity of chlorine within the urban environment, and improve emergency response preparedness and hazard mitigation capabilities [6]. Data gathered from the project is being evaluated in 2017 [24].

Table 1:
Data From Project Jack Rabbit Release Event

Instrument	Type	Detection
UV Canary	Chemical	Chlorine
UV Sentry	Chemical	
JAZ Detectors	Chemical	Ammonia & Chlorine
miniRAE	Chemical	
FTIR Spectrometer	Chemical	Ammonia
Bubblers	Chemical	Chlorine
Thermocouple	Meteorological	Temperature
Tripod PWIDS	Meteorological	Wind direction, Wind speed, Temperature, Relative humidity, Pressure
32m Tower PWIDS	Meteorological	
Tripod Sonics	Meteorological	Wind direction, Wind speed, Turbulence
32m Tower Sonics	Meteorological	
SD Berm Camera	Photonic	Ammonia & Chlorine
SD Tower Camera	Photonic	
Standoff HD Camera	Photonic	
Standoff IR Camera	Photonic	Ammonia IR Spectrum

Table 1: Data collected from Project Jackrabbit that was initiated from the collaboration of the DHS Transporation Security Administration and the Chemical Security Analysis Center. Adapted from [26].

Results from these projects have provided valuable data that has been used to enhance preparedness and response to ammonia and chlorine release, including better protection of emergency responders and warfighters. Emergency response and preparedness professionals have applied PJR findings to their strategies [6]. Data from PJR has also been used to enhance the Naval Surface Warfare Center, Dahlgren Division's RAILCAR4 Toxic Industrial Chemical Source Characterization Program [25]. Results from phase two of PJR II are expected to further enhance its contribution to protecting U.S. warfighters, emergency professionals, and civilians.

Conclusion

Each year, the U.S. produces a combined 24 million tons of ammonia and chlorine [2,7]. The threat of accidental mass release, along with insider threat and terrorist actions, drives ongoing efforts by several federal agencies and the DoD. These endeavors, along with further research, are paramount to protecting U.S. warfighters and civilians from the threats posed by ammonia and chlorine. ■

References

1. Agency for Toxic Substances & Disease Registry. (n.d.). Toxic substances portal - ammonia. Retrieved from https://www.atsdr.cdc.gov/mmg/mmg.asp?id=7&tid=2 (accessed July 3, 2017)
2. Jones, R., Wills, B., & Kang, C. (2010). Chlorine gas: An evolving hazardous material threat and unconventional weapon. *Western Journal of Emergency Medicine*, 11(2), 151–156.
3. Geiger, D. (2017, March 23). How chlorine gas became a weapon in Syria's civil war. Al Jazeera. Retrieved from http://www.aljazeera.com/indepth/features/2017/03/chlorine-gas-weapon-syria-civil-war-170314110043637.html (accessed July 3, 2017)
4. Wenck, M. A., Van Sickle, D., Drociuk, D., Belflower, A., Youngblood, C., Whisnant, M. D., ... Gibson, J. J. (2007). Rapid assessment of exposure to chlorine released from a train derailment and resulting health impact. *Public Health Reports*, *122*(6), 784–792.
5. Department of Homeland Security. (2015). *Chemical sector-specific plan: An annex to the NIPP 2013*. Retrieved from https://www.dhs.gov/sites/default/files/publications/nipp-ssp-chemical-2015-508.pdf (accessed July 3, 2017)
6. Noll, G. G., & Byrnes, A. (2016, November 11). The Jack Rabbit tests: Catastrophic releases of compressed liquefied gases. Fire Engineering. Retrieved from http://www.fireengineering.com/articles/print/volume-169/issue-11/features/the-jack-rabbit-tests-catastrophic-releases-of-compressed-liquefied-gases.html (accessed July 3, 2017)
7. U.S. Geological Survey. (2017, January). Nitrogen (fixed) – ammonia. In *Mineral Commodity Summaries*, (pp. 118-119). Retrieved from https://minerals.usgs.gov/minerals/pubs/commodity/nitrogen/mcs-2017-nitro.pdf (accessed July 3, 2017)
8. Environmental Protection Agency. (2015). Low-GWP alternatives in commercial refrigeration (Rep. No. EPA 430F14023). Retrieved from https://www.epa.gov/sites/production/files/2015-10/documents/deca_commercial_refrigeration_case_study.pdf (accessed July 3, 2017)
9. New York State Department of Health. (n.d.). The facts about ammonia. Retrieved from https://www.health.ny.gov/environmental/emergency/chemical_terrorism/ammonia_general.htm (accessed July 3, 2017)
10. BBC News. (2015, March 12). Islamic State 'using chlorine gas' in Iraq roadside bombs. BBC News. Retrieved from http://www.bbc.com/news/world-middle-east-31847427 (accessed July 3, 2017)
11. Roggio, B. (2007, March 17). Al Qaeda's chlorine attacks: The dirty war in Anbar. FDD's Long War Journal. Retrieved from http://www.longwarjournal.org/archives/2007/03/al_qaedas_chlorine_a.php (accessed July 3, 2017)
12. Norton, R. A. (2016, June 7). Industrial chemical systems threat mitigation—an important element in food defense [Food Safety Magazine blog post]. Retrieved from http://www.foodsafetymagazine.com/blog/industrial-chemical-systems-threat-mitigationan-important-element-in-food-defense/ (accessed July 3, 2017)
13. Cumming-Bruce, N. (2016, November 11). ISIS is massacring Mosul civilians as troops advance, U.N. says. *The New York Times*. Retrieved from https://www.nytimes.com/2016/11/12/world/middleeast/isis-mosul-iraq.html (accessed July 3, 2017)
14. The Associated Press. (2016, November 11). U.N. reveals fresh evidence of ISIS using chemical weapons in Iraq. CBS News. Retrieved from http://www.cbsnews.com/news/un-evidence-isis-using-chemical-weapons-iraq/ (accessed July 3, 2017)
15. National Research Council, Division on Engineering and Physical Sciences, Committee on Science and Technology for Countering Terrorism. (2002). Toxic chemicals and explosive materials. In *Making the nation safer: The role of science and technology in countering terrorism* (pp. 107-112). Washington, D.C.: The National Academies Press.
16. Organisation for the Prohibition of Chemical Weapons. (n.d.). Genesis and historical development. Retrieved from https://www.opcw.org/chemical-weapons-convention/genesis-and-historical-development/ (accessed July 3, 2017)
17. National Academies, & Department of Homeland Security. (2004). *Communicating in a crisis: Chemical attack* (Fact sheet). Retrieved from https://www.dhs.gov/xlibrary/assets/prep_chemical_fact_sheet.pdf (accessed July 3, 2017)
18. Centers for Disease Control and Prevention. (2005, January 28). Public health consequences from hazardous substances acutely released during rail transit --- South Carolina, 2005; Selected States, 1999--2004. In *The Morbidity and Mortality Weekly Report* (Rep.) (pp. 64-67). Retrieved from https://www.cdc.gov/mmwr/preview/mmwrhtml/mm5403a2.htm (accessed July 3, 2017)
19. Joint Chiefs of Staff. (2016). Chemical, Biological, Radiological, and Nuclear Response (JP 3-41). Washington, DC. Retrieved from http://www.dtic.mil/doctrine/new_pubs/jp3_41.pdf (accessed July 25, 2017)
20. National Institute for Occupational Safety and Health. (n.d.). Ammonia solution (UN 3318); ammonia, anhydrous (UN 1005): Lung damaging agent. Retrieved from https://www.cdc.gov/niosh/ershdb/emergencyresponsecard_29750013.html (accessed July 25, 2017)
21. National Institute for Occupational Safety and Healt. (n.d.). Chlorine: Lung damaging agent. Retrieved from https://www.cdc.gov/niosh/ershdb/emergencyresponsecard_29750024.html (accessed July 25, 2017)
22. Chemical Hazards Emergency Medical Management. (n.d.). Personal Protective Equipment (PPE). Retrieved from https://chemm.nlm.nih.gov/ppe.htm (accessed July 25, 2017)
23. National Institute for Occupational Safety and Health. (n.d.). Chlorine: Lung damaging agent. Retrieved from https://www.cdc.gov/niosh/ershdb/emergencyresponsecard_29750024.html (accessed July 3, 2017)
24. Department of Transportation. (2016). 2016 Emergency response guidebook. Retrieved from https://www.phmsa.dot.gov/staticfiles/PHMSA/DownloadableFiles/Files/Hazmat/ERG2016.pdf (accessed July 3, 2017)
25. Federal Emergency Management Agency Emergency Management Institute. (n.d.). Federal Emergency Management Institute. Retrieved from https://training.fema.gov/emi.aspx (accessed July 3, 2017)
26. Storwold, D. P., Jr., Argenta, E., Jr., White, J. W., Pace, J. C., & Fox, S. B. (2011, January). *American Meteorological Society (AMS) extended abstract for the Jack Rabbit test program trial summary* (ATEC Project No. 2010-DT-DPG-SNIMT-E5835) [Extended abstract]. In *Special Symposium on Applications of Air Pollution Meteorology*. Symposium conducted at the American Meteorological Society 91st Annual Meeting, Seattle, WA
27. Hedrick, A., Nicholson, D., & Serguievski, P. (2015). *Methodology investigation plan for the Jack Rabbit (JR) II dissemination method testing* (WDTC Document No. WDTC-IP-15-055). Dugway, UT: West Desert Test Center, U.S. Army Dugway Proving Ground.

Jamie Glover
Research Associate, Homeland Defense and Security Information Analysis Center

Jamie Glover is a research associate with the Homeland Defense and Security Information Analysis Center (HDIAC), contributing to research, analysis, and thought leadership across the center's eight focus areas (MPH and M.S., University of Tennessee). Prior to joining HDIAC, Jamie spent more than eight years in public health practice and research in academic, government, non-profit, and private sectors.

Trust Management for Cyber-Physical Systems

Janice Cañedo,
Austin Hancock,
&
Anthony Skjellum, Ph.D.

Introduction

The internet of things (IoT) is a growing network of billions of connected devices. In 2015, approximately 15.4 billion devices were part of the IoT, and current research indicates 30.7 billion devices partaking in the network by 2020 [1]. The IoT is now part of the every day, integrated into homes by way of cameras and door locks and into infrastructure through Cyber-Physical Systems (CPS), such as the smart grid and the Internet of Battlefield Things (IoBT). The IoT provides the framework for internet-connected CPS, which are closely integrated, context-aware, mission-critical systems that perform actions and interact with the physical world (see Figure 1) [2-4]. CPS are evolving and expanding with many applications still in research and development stages.

Smart systems (platforms such as CPS that incorporate IoT) have become an important component of infrastructure, particularly those aspects regulated, maintained, and utilized by federal agencies. The adoption of the IoT within the federal government has been largely driven by the Department of Defense (DoD), the Department of Homeland Security, and the National Aeronautics and Space Administration [5]. The expansion of smart systems has affected operations within DoD so much that the Defense Information Systems Agency, which is essentially DoD's information technology combat support agency, has acknowledged the urgent need to keep demands related to this shift at the forefront of defense architecture [6]. In general, the impact of the IoT has garnered the attention of DoD leadership prompting the release of policy recommendations for the IoT in 2016 [7]. As smart systems, particularly CPS, become more widespread, it is necessary to adopt a standard framework for their integration into existing aspects of infrastructure [8]. When considering the implementation of IoT/CPS into infrastructure, security is a primary concern.

All IoT/CPS systems require the devices in the system be able to securely communicate (even though that communication will often conform to a sparse interconnection topology). In IoT/CPS systems, there are two primary categories of devices: edge devices and gateways. Edge devices are limited resource devices containing sensors and actuators. The edge devices collect and transmit data to the gateway(s) or perform actions requested by the gateway(s). The gateway device is responsible for collecting and aggregating data from edge devices, providing directives for the edge devices, connecting the edge devices to the internet (or intranet), and transmitting data to a cloud or private data store.

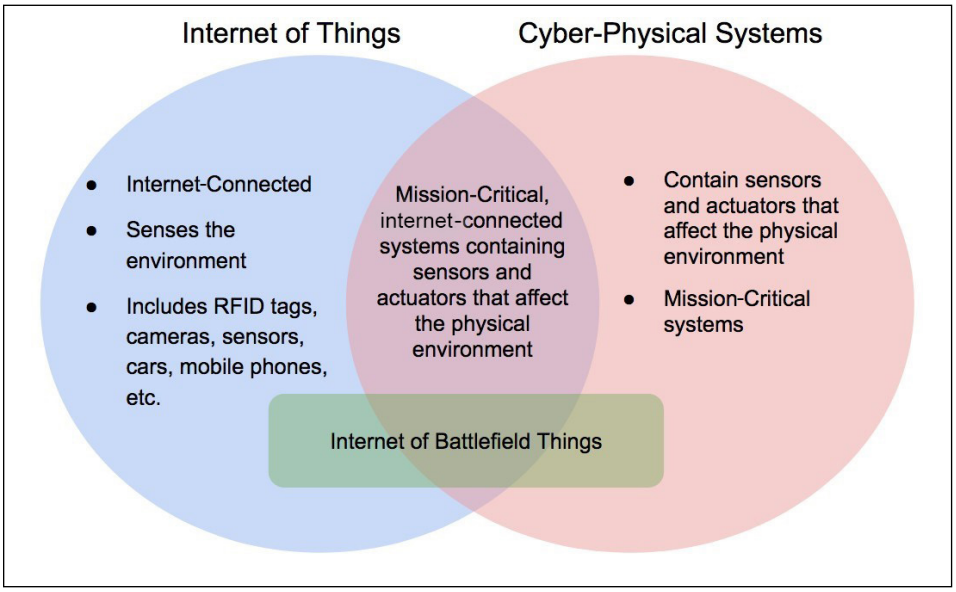


Figure 1: IoT and CPS intersection with IoBT.

Cyber Security Challenges

Many cyber security challenges exist for the IoT, CPS, and IoBT. Networking of these devices is accomplished via multiple protocols, such as radio-frequency identification, Wi-Fi, and Bluetooth – among others. Furthermore, the devices composing the IoT/CPS incorporate a variety of hardware specifications and chipsets. Proper implementation of standard security measures is made more difficult by the inherent abundance of factors that must be considered within a network composed primarily of IoT/CPS devices.

Additionally, the mobility of IoT/CPS devices raises a unique set of security concerns. Devices not bound to fixed locations (whose distance between other devices and access points is not constant) will have variable connectivity. Additional security concerns that must be accounted for include lost data packets and unattended devices that may become compromised. In systems composed of distributed devices, communication between the devices is pivotal for facilitating the proper function of the system. A lack of resiliency is an inability to identify and adapt to the presence of nodes within the system that exhibit weak or outright negative performance, which can cripple the utility provided by the system.

Finally, the resource constraints that IoT/CPS devices face must be taken into consideration. Redundancy and encryption would at least mitigate, and could solve, some of the aforementioned problems, but the devices within these systems must be strategic in the functions on which they choose to expend energy. Thus, it is critically important for less resource-heavy security methods to be strategically evaluated and implemented.

Trust Management Systems for Internet of Things/ Cyber-Physical Systems

Trust management systems (TMS) are used to establish trust between two entities and are used in many areas of computing including peer-to-peer networks [9,10], wireless sensor networks [11,12], and, more recently, IoT systems [13-15]. The TMS must be adaptable for a wide range of scenarios and applications. Trust propagation is the method in which peers propagate evidence to one another in a centralized or distributed fashion. In the proposed approach, trust propagation will occur in a hybrid fashion wherein devices propagate information to each other as well as a central trust data store when they are able. The centralized data store enables devices to move throughout the system while maintaining a certain level of trust. This can keep a malicious device from corrupting one part of the system, being blacklisted from that section, and moving to a new section to cause corruptions. The central data store would provide the information allowing that section of the system to know the device is blacklisted. Distributed trust management is ideal for the IoT and allows the system to compute scores for only small subsets of known neighbors, which are devices within direct communication based on being within one hop of communication.

The calculation of the trust scores is accomplished through trust aggregation (the method by which the data will be aggregated for trust score calculations) by fuzzy sets, game theory, and Bayesian analysis [16,17]. Fuzzy logic uses *if-then* rule sets to solve the trust problem and provide a multi-logic value [17]. Bayesian trust models use Bayes' theorem as a foundation for aggregation and have been widely used and implemented over the last decade. They are studied in wireless sensor networks, peer-to-peer networks applications, and IoT systems [17-20]. Game theory models compute a trust score using minimal resources, which is an advantage in limited-resource devices, such as IoT edge devices [21]. Unlike Bayesian trust models and fuzzy logic trust models, game theory models don't predict what will occur. Instead, they mathematically estimate the behavior of the participants [17].

Trust composition will include direct and indirect observations, such as the success of packet transmissions and performing an action. Direct observations will have the most impact in calculating the trust of another device. However, the indirect observations are important to provide a balance and better understanding of the true nature of a device. The observations are taken on a range of [0,1], where 0 indicates the device did not perform some particular action and 1 indicating the device perfectly performed that action. This allows for fractional outcomes. A device could receive a 0.75 rating for an action, meaning it was successful in performing the action but not 100 percent. An average of all direct observations *OD* is taken, and the incremental average of indirect observations *OI* for device *n* for the *ith* observation is sent (*ODi*) using the incremental average such that

$$OD.new = OD + \frac{OD_i - OD}{i}.$$

The same can be done for indirect observation *OI* as they are propagated. This is used when calculating the probability of success for a device's reputation through data aggregation.

To aggregate the data to calculate a trust score, a dual approach with Bayesian and game theory is advantageous. Game theory provides a lightweight method for edge devices to determine trust through a trust matrix, whereas Bayesian analysis

provides a more in-depth trust score calculation that can occur in a gateway and be propagated to the edge device when necessary. Bayesian analysis attempts to predict the probability of a device performing a desired action given the device's previous actions. The previous actions are both the direct and indirect observations that are propagated through firsthand experience and by the neighbors. The probability that a device D will successfully complete tasks is calculated using Bayes Theory such that

$$Pr(S|D) = \frac{Pr(D|S) \times Pr(S)}{Pr(D)}.$$

In this particular case, *Pr(S)* = 1 since success is expected. For *Pr*(*D*|*S*), this probability is identified based on direct and indirect observations. Indirect observations can be weighted by a factor of ω, such that

$$Pr(D|S) = OD + \frac{OI}{\omega}.$$

Given this, the probability of D is all observations of the data such that

$$Pr(D) = \left(OD + \frac{OI}{\omega}\right) + (1 - OD + \frac{1-OI}{\omega}).$$

To generalize, the trust score *TS* for device *n* is

$$TS_n = \frac{OD_n + OI_n}{(OD_n + OI_n) + ((1 - OD) + \frac{1-OI}{\omega})}.$$

Figure 2 illustrates the lifecycle events of TMS for a device. It shows a device D_1 entering into a new system and connecting to a gateway. D_1 can be either an edge device or gateway device entering the system. The following steps occur for D_1 as the device learns about neighboring devices and maintains status within the system.

1. Device D_1 enters the system and is given a neutral trust score with the gateway G_1 and with device neighbors N_1 and N_2.
2. D_1 performs actions as requested by G_1, N_1 , and N_2.
3. With each request, G_1, N_1, and N_2 update their trust of D_1.
4. Periodically, G_1, N_1, and N_2 share their trust score of D_1 with each other, and G_1 will share the scores with the central data store.
5. The process maintains as long as D_1 is in the system.
6. If D_1 moves throughout the system and belongs to a new gateway, G_2, the central data store can be reached, if available, to set an initial score for D_1 that is a more accurate level of trust than the initial neutral trust score.
7. If the device trust score ever drops below a desired threshold, the device can be quarantined until further intervention occurs (such as a higher-level algorithm, system administrator/operator review, or an offline forensic test).

This system provides a mechanism for monitoring devices while they are in use. Through this implementation, misbehaving devices may be detected, both malicious and faulty, and alert the system administrator of the problem.

Use Cases

As IoT/CPS systems become more prevalent, they are also beginning to have an impact on the battlefield – referred to as the IoBT [22]. Figure 1 shows the attributes and intersection of IoT and CPS and how the IoBT incorporates qualities from both. The IoBT is the collection of devices that can be attached to vehicles or worn by soldiers in the battlefield, such as drones, sensors, and cameras. These devices must maintain secure communication in order to effectively work. If the devices are continuously moving throughout the system, it's imperative they maintain authentication into the system and continuous correct functionality.

Implementation of a TMS would enable these devices to maintain a trust score as they are used in the system. To accommodate mobility (and in some cases the transient nature) of these devices, a central data store can provide the means for a device to maintain its trust as it moves around. This provides a framework to keep malfunctioning and malicious devices from corrupting the entire system. If a device is blacklisted in one section of the system, it can't move to a new section to cause corruptions because the trust score propagates. The TMS provides a reliable means of monitoring devices as well as activity associated with these IoBT-enabled devices used by warfighters moving throughout the system. Earlier this year, the U.S. Army Research Laboratory established a Collaborative Research Alliance to address challenges in IoBT including heterogeneity, connectivity, scalability, and interdependence of networked elements [23].

Another major area of research in CPS is the smart grid. The smart grid is the use of cutting-edge technologies, equipment, and operations to make the delivery of electricity more reliable and efficient [24] than legacy systems. The Department of Energy defines seven key requirements for a smart grid: self-healing, motivates and includes the consumer, resists attacks, provides power quality, accommodates generation and storage options, enables markets, and optimizes assets for efficient operation [25,26]. The goal of the smart grid is to provide an infrastructure capable of handling distributed generation, renewable energy sources, electric vehicles, and demand-side management electricity [25]. As these technologies work together to control the delivery of electricity, it's imperative they maintain acceptable performance. A TMS can be used to evaluate whether each device in the system is reliable for performing its designated task. Furthermore, a TMS can revoke privileges to any device that becomes unreliable or faulty. The aforementioned TMS incorporates both dimensions of faultiness and potential cyber threat.

Conclusions and Further Explorations

IoT and CPS are quickly becoming integrated into civil infrastructure and the battlefield. ATMS provides a key mechanism for establishing, maintaining, and revoking trust of devices within IoT/CPS systems. This provides a foundation to establish a more secure and resilient system by blacklisting devices not performing desired actions. It is imperative that such functionality exist in the context of highly mobile devices that would otherwise be capable of compromising multiple parts of a system. On-going research is needed to continue development of TMS for IoT/CPS with the aim of strengthening the speed at which misbehaving devices are detected and improving the ability to identify malicious versus faulty devices. ■

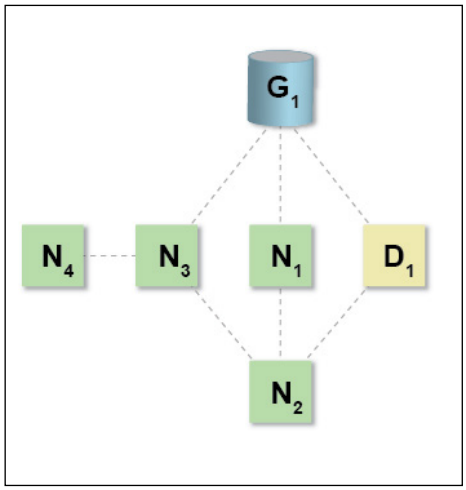


Figure 2: Device Entry into TMS.

References

1. Columbus, L. (2016, November). Roundup of internet of things forecasts and market estimates. *Forbes*. Retrieved from https://www.forbes.com/sites/louiscolumbus/2016/11/27/roundup-of-internet-of-things-forecasts-and-market-estimates-2016/#4d5e1228292d (accessed July 19, 2017)
2. Banerjee, A., Venkatasubramanian, K. K., Mukherjee, T., & Gupta, S. K. (2012). Ensuring safety, security, and sustainability of mission-critical cyber-physical systems. *Proceedings of the IEEE*, *100*(1), 283-299. doi:10.1109/jproc.2011.2165689
3. Shi, J., Wan, J., Yan, H., & Suo, H. (2011). A survey of cyber-physical systems. In *2011 International Conference on Wireless Communications and Signal Processing (WCSP)* (pp. 1-6). IEEE. doi:10.1109/WCSP.2011.6096958
4. Baheti, R., & Gill, H. (2011). Cyber-physical systems. In *The Impact of Control Technology* (pp. 161-166). IEEE Control Systems Society. Retrieved from http://ieeecss.org/general/impact-control-technology (accessed July 19, 2017)
5. Goldstein, P. (2016, June 10). DOD, DHS and NASA are driving adoption of internet of things sensors. *FedTech Magazine*. Retrieved from https://fedtechmagazine.com/article/2016/06/dod-dhs-and-nasa-are-driving-adoption-internet-things-sensors (accessed July 19, 2017)
6. Defense Information Systems Agency. (2015). *DISA Strategic Plan 2015-2020*. Retrieved from http://www.disa.mil/~/media/files/disa/about/strategic-plan.pdf (accessed July 19, 2017)
7. Department of Defense. (2016). *DoD Policy Recommendations for the Internet of Things (IoT)*. Department of Defense, Office of the Chief Information Officer. Retrieved from https://www.hsdl.org/?abstract&did=799676 (accessed July 19, 2017)
8. National Institute of Standards and Technology. (2013). *Foundations for Innovation in Cyber-Physical Systems* (Workshop Report). Retrieved from https://www.nist.gov/sites/default/files/documents/el/CPS-WorkshopReport-1-30-13-Final.pdf (accessed July 19, 2017)
9. Kamvar, S. D., Schlosser, M. T., & Garcia-Molina, H. (2003). The Eigentrust algorithm for reputation management in P2P networks. In *Proceedings of the 12th International Conference on World Wide Web, WWW 2003* (pp. 640-651). New York, NY: ACM. doi:10.1145/775152.775242
10. Xiong, L., & Liu, L. (2004). PeerTrust: Supporting reputation-based trust for peer-to-peer electronic communities. *IEEE Transactions on Knowledge and Data Engineering*, *16*(7), 843-857. doi:10.1109/tkde.2004.1318566
11. Jadidoleslamy, H., Aref, M. R., & Bahramgiri, H. (2016). A fuzzy fully distributed trust management system in wireless sensor networks. *International Journal of Electronics and Communications*, *70*(1), 40-49. doi:10.1016/j.aeue.2015.09.017
12. Ganeriwal, S., & Srivastava, M. B. (2004). Reputation-based framework for high integrity sensor networks. In *Proceedings of the 2nd ACM workshop on Security of ad hoc and sensor networks* (pp. 66-77). New York, NY: ACM. doi:10.1145/1029102.1029115
13. Chen, I., Guo, J., & Bao, F. (2016). Trust management for SOA-based IoT and its application to service composition. *IEEE Transactions on Services Computing*, *9*(3), 482-495. doi:10.1109/tsc.2014.2365797
14. Mendoza, C. V., & Kleinschmidt, J. H. (2016). Defense for selective attacks in the IoT with a distributed trust management scheme. *2016 IEEE International Symposium on Consumer Electronics (ISCE)*, 53-54. doi:10.1109/isce.2016.7797367
15. Dorodchi, M., Abedi, M., & Cukic, B. (2016). Trust-based development framework for distributed systems and IoT. 2016 IEEE 40th Annual Computer Software *and Applications Conference (COMPSAC)*, 437-442. doi:10.1109/compsac.2016.21318.
16. Jøsang, A., Ismail, R., & Boyd, C. (2007). A survey of trust and reputation systems for online service provision. *Decision Support Systems*, *43*(2), 618-644. doi:10.1016/j.dss.2005.05.019
17. Yu, Y., Li, K., Zhou, W., & Li, P. (2012). Trust mechanisms in wireless sensor networks: Attack analysis and countermeasures. *Journal of Network and Computer Applications*, *35*(3), 867-880. doi:10.1016/j.jnca.2011.03.005
18. Han, G., Jiang, J., Shu, L., Niu, J., & Chao, H. (2014). Management and applications of trust in Wireless Sensor Networks: A survey. *Journal of Computer and System Sciences*, *80*(3), 602-617. doi:10.1016/j.jcss.2013.06.014
19. Guo, J., Chen, I., & Tsai, J. J. (2017). A survey of trust computation models for service management in internet of things systems. *Computer Communications*, *97*, 1-14. doi:10.1016/j.comcom.2016.10.012
20. Thirunarayan, K., Anantharam, P., Henson, C., & Sheth, A. (2014). Comparative trust management with applications: Bayesian approaches emphasis. *Future Generation Computer Systems*, *31*, 182-199. doi:10.1016/j.future.2013.05.006
21. Mehdi, M. M., Raza, I., & Hussain, S. A. (2017). A game theory based trust model for Vehicular Ad hoc Networks (VANETs). *Computer Networks*, *121*, 152-172. doi:10.1016/j.comnet.2017.04.024
22. U.S. Army Research Laboratory. (n.d.) Internet of battlefield things (IOBT). Retrieved from https://www.arl.army.mil/www/default.cfm?page=3050 (accessed July 19, 2017)
23. Blinde, L. (2017, March 6). ARL launches Internet of Battlefield Things CRA. Retrieved from http://intelligencecommunitynews.com/arl-launches-internet-of-battlefield-things-cra/ (accessed July 19, 2017)
24. U.S. Department of Energy. (n.d.). Grid modernization and the smart grid. Retrieved from https://energy.gov/oe/services/technology-development/smart-grid (accessed June 29, 2017)
25. Sridhar, S., Hahn, A., & Govindarasu, M. (2012). Cyber–physical system security for the electric power grid. *Proceedings of the IEEE*, *100*(1), 210-224. doi:10.1109/jproc.2011.2165269
26. National Energy Technology Laboratory. (2007). *A systems view of the modern grid* (Rep. for the U.S. Department of Energy Office of Electricity Delivery and Energy Reliability).

Janice Cañedo
Ph.D. Candidate, Auburn University

Janice Cañedo is pursuing a Ph.D. in computer science and software engineering at Auburn University (M.S., Columbus State University). Her research centers on the IoT, and her work includes innovative security design of malware, network structure, operating system resiliency, and data analytics for IoT systems.

Austin Hancock
Ph.D. Candidate, Auburn University

Austin Hancock is pursuing a Ph.D. in computer science and software engineering at Auburn University (B.S., Auburn University). His research involves evaluation of cloud forensics strategies as well as digital forensics for IoT and mobile devices. He presented research pertaining to malware detection on mobile devices at the 2016 American Academy of Forensic Sciences Annual Meeting.

Anthony (Tony) Skjellum, Ph.D.
Professor, Chair of Excellence, and SimCenter Director, University of Tennessee, Chattanooga

Anthony Skjellum is a professor of computer science, chair of excellence, and SimCenter director at the University of Tennessee, Chattanooga (Ph.D., California Institute of Technology). He is the former director of the Auburn Cyber Research Center. From 2003 to 2013, Skjellum was professor and chair of the University of Alabama at Birmingham Department of Computer and Information Sciences. He is a senior member of the Association for Computing Machinery and the Institute of Electrical and Electronics Engineers and is an associate member of the American Academy of Forensic Science, Digital & Multimedia Sciences Division.

HDIAC
Homeland Defense & Security
Information Analysis Center

Technical Inquiry Services

Four **Free Hours** of Research within our eight focus areas
Available to **academia, industry,** and other **government agencies**

Focus Areas

Alternative Energy
Biometrics
CBRN Defense
Critical Infrastructure
Cultural Studies
Homeland Defense
Medical
WMD

Log On
to **hdiac.org** to submit a technical inquiry form

or Contact
inquiries@hdiac.org


RED TEAMI
& DISRUPTIVE INNOVA

NG TION: ANTICIPATING THE UNEXPECTED

Tate Nurkin

Introduction

In October 2016, Iran's Tasnim News Agency revealed efforts by the naval wing of the Islamic Revolutionary Guard Corps (ISR) to develop the world's first unmanned ground effect vehicle (UGEV) [1]. The report and accompanying photos posted on its website offered a window into Iranian efforts to create a new intelligence, surveillance, and reconnaissance system that could take off and land on any stretch of calm sea.

Tasnim took the photos down hours after they were posted, inciting speculation that the ISR mission may not be the only, or even primary, mission for the UGEV. *IHS Jane's Defence Weekly* assessed that, "while far slower than a conventional missile, a UGEV-derived munition would move far faster than any boat, potentially making it harder to engage with anti-surface weapons" [1]. Jeremy Binnie, *IHS Jane's Defence Weekly* Middle East/North Africa Desk editor, later noted that in a strike role the UGEV "may well be a sitting duck" but only if existing systems were prepared to meet a threat they had not previously seen - if "someone has thought to set up defenses to counter it" [2].

Binnie's insight is a useful reminder of an often-overlooked component of U.S. efforts to anticipate, dissuade, and defeat threats from a growing range of possible state and non-state actors in an environment of dynamic and rapid technological innovation.

Attention is paid to the *what* of technological innovation, the specific technologies that specific adversaries are prioritizing and the technologies in which the U.S. should invest to better pursue its interests, protect the homeland and drive competitions in salutary directions. However, the pace and scale of the diffusion of these technologies to a growing range of actors also places a premium on understanding the *how* of technology and capability use – that is, the operational concepts of current and emerging adversaries and the proclivities, mindsets, objectives, and priorities that shape these concepts.

Staying ahead of the multidimensional challenge of adversary disruptive innovation will require renewed and enhanced emphasis on red teaming and other alternative methods that allow the Department of Defense (DoD) to challenge existing assumptions, explore unconventional thinking about adversaries, anticipate new threats and challenges and, ultimately, identify capabilities and concepts to meet an expanding range of fast-moving and opaque threats.

Approaches to Evaluating Impact of Disruption

Growing assertions that the global defense and security environment has, over the course of the 21st century, become more complex, uncertain, and fast moving have become axiomatic but also relevant for DoD analysts and decision-makers. Erosion of constraints against crisis and conflict and diffusion of the power to disrupt to a broader range of state and non-state actors together have significant implications for not just what DoD analysts examine but also how they do it.

Traditional analytical methods and filters may no longer be sufficient, in and of themselves, to determine the origin, nature, pace, and trajectory of existing and emerging threats to the U.S. and its national interests. The incorporation of a number of alternative analysis methods is becoming increasingly critical in efforts to effectively identify, assess, and plan for fast-moving and unanticipated situations. These methods can be divided into two broad categories: competitive and blue sky [3].

Competitive techniques include methods such as multiple advocacy (also known as Team A/Team B) and analysis of competing hypothesis (ACH), both of which leverage defined and structured processes to compare the validity of range of usually already established and understood alternative outcomes, interpretations, and possible decisions against each other.

Multiple advocacy is an approach introduced by Stanford University professor Alexander L. George in 1972 [4]. It asks individual or small groups of analysts to essentially role-play as advocates of particularly strongly held views and make arguments to a broader team of analysts about why this view is correct. The competitive process of multiple advocacy typically either reveals particularly strong arguments or creates new and more robust hypotheses.

ACH is a system first proposed in the 1970s by former CIA analyst Richards J. Heuer, Jr. through a series of internal CIA articles and fully captured in his book *The Psychology of Intelligence Analysis* [5]. It involves an eight-step process for systematically identifying, assessing, and evaluating various hypotheses about a threat, event, or out-

come. For example, ACH could be used to assess varying perspectives on the scale and nature of a shifting Islamic State threat to the U.S. homeland.

ACH requires an analyst to explicitly identify all reasonable interpretations and theories and then assess and score the reliability and validity of evidence for each alternative hypothesis. The method has gained traction in many forecasting and analytical communities and several software programs are available that facilitate construction of ACH matrices, including one from the Palo Alto Research Center [6].

Blue sky methods differentiate from competitive ones not by the absence of structure, but rather by an emphasis on developing more flexible and permissive structures that feature collaborative forums and encourage expansion of the alternative hypotheses and outcomes being considered rather than rigorous evaluation of those already known.

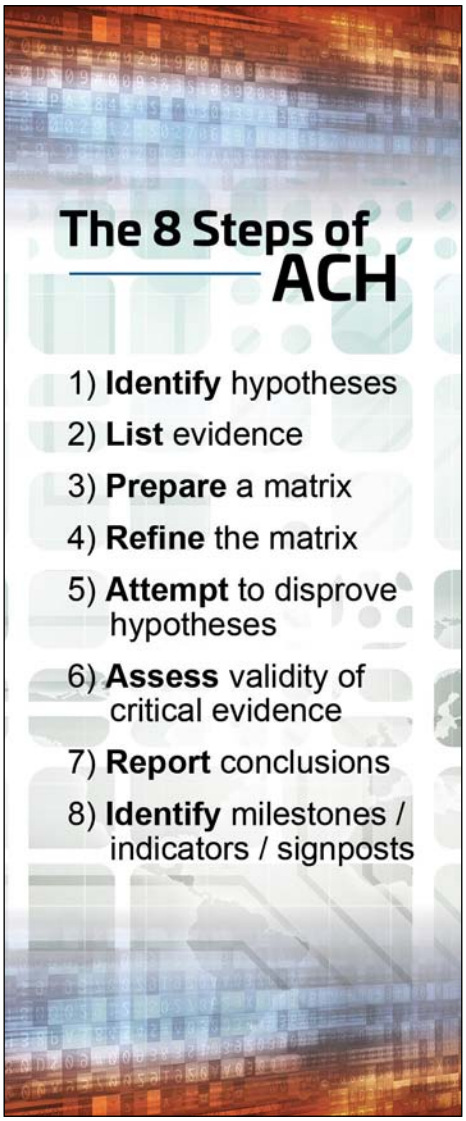


Figure 1: Steps of ACH.

Scenario planning stands out as a powerful blue sky technique through which analysts and decision-makers identify and evaluate a range of scenarios or alternative visions of the future with a particular focus on the possible and plausible over the likely. Small groups of analysts and experts discuss a range of scenario pathways and outcomes (typically in workshop or exercise settings) that seek to engender the expression of provocative, but informed, and exploratory views of the future that may run counter to current accepted organizational perspectives. By identifying a set of representative possible and plausible futures, assessing how DoD can best operate in and across these environments and identifying signposts that individual scenarios are more or less likely to come to pass, scenario planning can help DoD bound and anticipate novel threats and identify effective measures and capabilities to deter, dissuade or defeat these threats.

Red Teaming to Anticipate Novel Threats

Red teaming is a method that combines the structural focus of competitive approaches with the innovative and collaborative focus of blue sky techniques. It stands as a highly relevant means of generating the creative and, in some cases, counterintuitive thinking that the current and emerging threat environments demand. The terms “red teams” and “red teaming” are widely-used and connote different things to different individuals and communities – “for every red team that exists, a slightly different definition for red teaming also exists” [7].

Most frequently, “red teaming” is used to describe the process of injecting intentionally critical, frequently heretical, thinking into established analytical, evaluation, and decision-making processes.

The 2016 *Joint Doctrine Note 1-16: Command Red Team* gives a broad, but useful, definition: “Command red teams help commanders and staffs think critically and creatively; challenge assumptions; mitigate groupthink; reduce risks by serving as a check against complacency and surprise; and increase opportunities by helping the staff see situations, problems, and potential solutions from alternative perspectives” [8].

Red teams also regularly have a particular focus on understanding how an adversary thinks, decides, and behaves in order to avoid mirror imaging – the psychological and analytical trap that assumes all actors are influenced by the same cultural, historical, ethical, moral, educational, strategic, and operational proclivities as the DoD.

Of course, adversary analysis can be difficult without participation by individuals experienced in the decision-making processes of adversaries. However, effectively tasked groups of multidisciplinary experts capable of thinking in creative and provocative ways can provide valuable insight and perspective. Setting up structures to solicit and incorporate this insight and perspective is critical in the current environment in which more actors are in pursuit and command of more and better capabilities and are using these capabilities in more unpredictable, previously unseen ways.

Applications of Red Teaming

Jane’s Strategic Assessment and Futures Studies Center has sought to bind this expansive issue of disruptive innovation by identifying and assessing four linked revolutions: perception, processing and cognition; human and materials performance; manufacturing and logistics; and communication, navigation, targeting, and strike [9].

Within this framework, three dynamics in particular underscore the amplified demand for red teaming to better understand adversaries and how specific technologies may evolve.

First, the pathway from development of innovative technology to deployment of a disruptive capability necessitates a series of complementary innovations in operational concepts, organizational structures, training, procurement processes, industry alignment, infrastructure and ethical, legal, and regulatory issues [9]. Aligning all components of innovation typically takes time and can involve the trackable milestones that allow the DoD to assess the maturity and pace of disruptive innovation by other states.

However, some U.S. adversaries and competitors have proven increasingly effective in navigating these adjacent innovations and have simultaneously demonstrated a lack of concern about the ethical, legal, and regulatory implications of using these capabilities, espe-

cially in light of what Jane's Strategic Assessment and Futures Studies Center believes is the ongoing and rapid deterioration of rules-based geopolitical norms that have pervaded for much of the last several decades [10].

For example, China's government is providing technical and material support of its large commercial fishing fleet, which includes, among other things, provision of "inter-operable electronics"; position, navigation, and timing technologies; and even military training. The result is the establishment of a novel and difficult to detect maritime militia [11].

Non-state armed groups, transnational networks, and ideologically imbued individuals are even less encumbered by traditional constraints, allowing them more options to optimize the effects of the technologies they possess. Consider the improvised explosive device (IED), which is possibly the most strategically disruptive capability of the first two decades of the 21st century. According to the Department of Homeland Security, "IEDs consist of a variety of components that include an initiator, switch, main charge, power source, and a container" [12] – all roles that can be filled by mundane commercial items [13]. IEDs also use a variety of "commonly available materials, such as fertilizer, gunpowder, and hydrogen peroxide" as the explosive materials, which must be accompanied by fuel and an oxidizer [12]. Estimated costs of IEDs vary, but in 2015 Defense One assessed that particularly advanced Iranian-developed IEDs known as explosively formed penetrators cost $30 or less [14].

This low-tech weapon was deployed by Islamist extremist and insurgent groups in Iraq and Afghanistan in unexpected ways contrary to the conventions of modern warfare, driving tactical, operational, and strategic disruption for the U.S. and coalition war efforts in these theaters. A short list of cost-imposing effects of the IED includes the establishment of the Joint IED Defeat Organization; increased expenditure on new capabilities (the Government Accountability Office estimates $75 billion was spent on Mine-Resistant Ambush Protected trucks, ground-penetrating radar, jamming, a range of surveillance techniques, and body armor and other capabilities) [15]; investment in the development, testing, and deployment of new tactical and operational concepts; and, most critically, more than 3,000 U.S. forces killed and 33,000 wounded in Iraq and Afghanistan from 2005 to 2011 [15,16].

Second, not all actors seeking to develop capabilities in individual revolutions, or across multiple ones, will have the engineering or budgetary capacity, strategic/mission need, or overall interest to pursue the highest-end technologies or applications of these technologies.

For example, increased demand for unmanned aerial systems is a notable feature of the modern defense and security market. The military market for unmanned systems has essentially doubled from around $3 billion in 2009 to $6 billion in 2015 [17]. However, the types of unmanned systems that are diffusing most widely are not the highest-end technologies requiring the most advanced engineering, materials, testing and scale of effects, such as High-Altitude Long Endurance platforms that can fly at or above 50,000 feet or aerostats that are essentially pseudo-satellite capabilities.

Only 5 percent of the 63,000 unmanned systems forecast to be sold to military and security communities between 2016 and 2025 will be the Class III systems, which weigh more than 600 kg and are capable of carrying the most sophisticated payloads at the highest altitudes for long periods of time [17].

Approximately one-quarter (23 percent) of this future demand is expected to be met by systems weighing between 2 kg and 20 kg that are more disposable systems designed for more tactical or close-in surveillance missions (which do sometimes include novel technologies) [17]. Add in the increasing availability of small commercial drones and quadcopters, and the picture of the use of unmanned systems for defense and security purposes becomes even more layered, with considerable activity taking place in lower-cost, shorter-range, less advanced intelligence, surveillance, and reconnaissance payload systems, some of which are commercially available. However, this does not mean that compelling and disruptive innovation in low-end applications is not taking place.

Applications of directed energy weapons offer a useful example. At the highest-end application, directed energy is being considered as a low-cost of shot solution for the growing threat of the saturation of existing missile defenses by low-cost, but increasingly accurate, cruise and ballistic missiles [18]. Directed energy is also being tested as a close-in defense weapon to deal with small boat and unmanned threats by the U.S. Navy aboard the USS Ponce and by China as a riot control weapon and aboard paramilitary ships [19].

In addition, because low-end versions of this technology are commercially available, some less sophisticated forms of directed energy requiring considerably less investment, research and development, and systems engineering (generating a significantly smaller scale of effects such as laser pointers) have been used by non-state actors and individuals to disrupt commercial airline pilots [20] and harm Coast Guard personnel and equipment [21]. In 2013, 3,960 laser strikes against aircraft were reported, leading the FBI to trial a rewards program in 2014 for information leading to the arrest of individuals carrying out these low-cost, potentially high-impact attacks [20].

Third, high-end and low-end versions of technologies of interest to the four revolutions (and ideas on how to use them) are diffusing through more pathways, ensuring a broader range of actors not only have interest in, but also access to, advanced military, dual-use, or even commercial technologies that can enable disruptive threats.

Commercial diffusion of advanced technologies is particularly salient to the discussion of red teaming. Companies across several industries (high-tech, automotive, commercial aerospace, energy, and maritime) all share an interest in developing and commercializing at scale many of the same types of capabilities relevant to each of the four revolutions, notably: autonomy and unmanned systems, smart key technologies, machine learning, cyber and electromagnetic spectrum capabilities, composites and smart materials and energy capture and storage. Many of these technologies are sold commercially, and others are transferred as part of joint ventures, partnerships, and export sales.

As Paul Scharre, director of the 20YY Warfare Initiative at the Center for a New American Security, noted, "many of the underlying technologies behind increased autonomy are driven by commercial sector innovation, and as a result will be available to a wide range of state and non-state actors" [22].

Indeed, there is an established history of Islamist extremist groups and insurgents in Iraq, Syria, and across the Middle East leveraging commercially available technologies (software, encryption technologies,

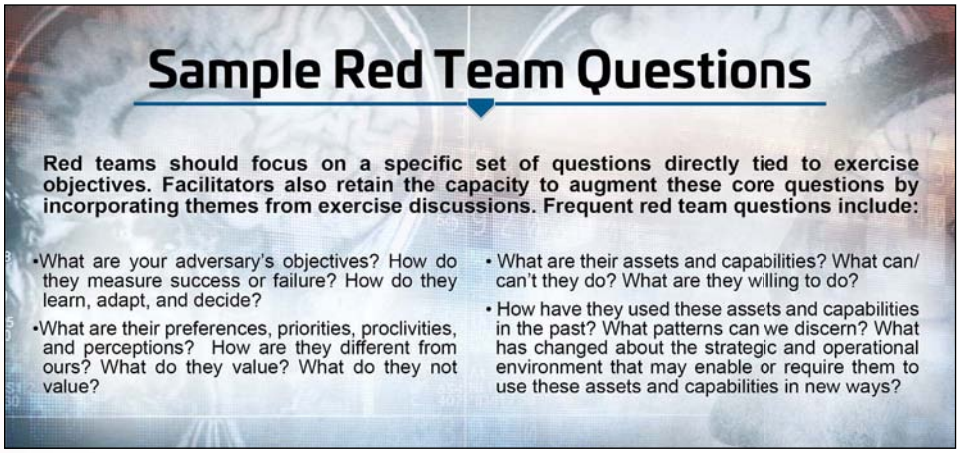


Figure 2: Samples of Red Team questions.

electromagnetic jammers, and drones) to either present novel threats to U.S. interests and personnel or to counteract advanced U.S. capabilities. For example, in either late 2014 or early 2015, an Islamic State supporter posted a document, "How to Kill UAVs," to the Justpaste.it website [23].

Another indicative example of the intersection of non-state armed group tactical innovation and enhanced technical capacity occurred in December 2009 when Iraqi Shiite militants used commercially available SkyGrabber software to tap into Predator drone live video feeds. Although the Iraqi fighters were unable to manipulate the feed or control the $4.5 million drone, the $26 software did allow them to view drone surveillance, enabling them to avoid detection and maintain operational security [24].

The bottom line of the collision of these three dynamics is that many actors that seek to harm the U.S. and disrupt worldwide interests are both increasingly less constrained by technical capacity and nearly unconstrained in devising means of leveraging this capacity. This reality places building pressure on the U.S. homeland security and defense enterprise as well as U.S. allies and partners to quickly develop new and enhanced methods and mindsets (ways of thinking about emerging threats) to meet an expanding, dynamic threat. As a recent United Kingdom's Ministry of Defence white paper noted, "we must continue to adapt to stay ahead, finding ways to be more innovative in the ways we think, the ways we develop capabilities, and the ways we operate ourselves" [25].

Implementation

Implementation of red teaming is rarely a simple process and requires a delicate mix of structure, creativity, and intuition across four phases of execution.

First is the conceptualization and design phase during which stakeholders determine exercise objectives, parameters, structure, questions of interest, resources, and timelines.

The design phase also involves the selection of red team participants. Most successful red teams incorporate a mixture of creative thinkers, devil's advocates, and deep subject matter experts, including, when relevant, individuals who share similar cultural or national backgrounds or operational experiences as the adversaries of interest. However, successful team composition goes well beyond finding the most experienced or well-established experts on a given topic. Indeed, it requires an expansive view of relevant perspectives and the courage to include non-traditional viewpoints or experiences that will help stakeholders achieve their overall objective.

For example, in the aftermath of the 2012 Taliban attack against Camp Bastion in Afghanistan, U.S. Marine Corps Task Force Belleau Wood formed a red team to mitigate against future failures of imagination in defense of the base. The red team did not engage senior officers with decades of operational experience. Instead, it was comprised largely of enlisted personnel who were unconstrained by the habits and expectations of experience and were more willing to consider bizarre attack modes that are "video game caliber" [26].

Supporting research is the second phase of effective red team execution. Exercise read-ahead and game materials offer participants an opportunity to fill gaps in their understanding of key issues and identify patterns in decision-making, tactics, techniques, attack modes, and adaptation efforts. A 2012 article entitled "Force Protection and Suicide Bombers: The Necessity of Two Types of Red Teams" published in the *Canadian Military Journal* highlights the utility of in-depth research efforts in support of red team exercises [27].

Research into suicide attack modes and target types over time of eight terrorist groups "readily provide data points concerning the range of casualties (minimums and maximums) of successful operations and other important information including the time of day, type of attack, number of perpetrators, and so on" [27]. Assessment of these patterns provides insight into how specific groups behave and can serve as a useful jumping off point for red team discussions of how these patterns may evolve under new strategic, operational, or tactical exigencies and realities.

The third phase of red team implementation is execution and facilitation. Experienced facilitators are crucial in balancing the need for rigorous structure and unconstrained thinking in a way that does not "unconsciously stifle dissent and subtly discourage alternative thinking" [7]. Intuition is particularly important in this phase in shaping and guiding the conversation and understanding when and why to stray from the structure and questions developed in phase one in order to explore potentially fruitful analytical pathways.

Ultimately, facilitators are responsible for serving as a sherpa (guiding team members through a dynamic and occasionally taut process), a traffic cop (ensuring collaborative discussions and driving team members to reach decisions within exercise timelines either through consensus or team votes), and a devil's advocate (periodically asking why and why not to force participants to articulate their core assumptions and consider additional alternatives).

The final phase of effective red team implementation is the use and incorporation of exercise outputs. Rapporteur notes on red team themes, insights, decisions, uncertainties, and tensions serve as the basis for red team outputs, typically after-action reports and hotwash briefings designed to challenge widely-held or

long-standing assumptions and help decision-makers expand the range of challenges and solutions they consider.

Red team outputs are rarely deterministic. Most frequently, these outputs are incorporated as one particularly stimulating and independent component of a broader process to diagnose, assess, or respond to a threat, challenge, or competition. Because red teams are designed to offer a check against and challenge to organizational bias and commonly-held assumptions, red teams must balance a need for independence and the need to have top-down organizational and stakeholder buy-in that the results – whatever they may be – are to be considered on their merits.

In addition, while ad hoc red teams can be useful to analysts and decision-makers, red teaming is most effective when it is built into broader processes of both DoD capability development and threat evaluation programs from the start. According to *Red Team Journal* Editor Mark Mateski, "to validate concepts and capabilities up front and throughout the engineering lifecycle is canonical to systems engineers" [28], but program managers and procurement officers may see regular attempts to find vulnerabilities in their programs as adding expense, time, uncertainty, and, potentially, political or procurement risk.

Conclusion

Red teaming is an increasingly important component of meeting the complex, uncertain, and contested environments and disruptive threats driven by the future of technological innovation and diffusion. If designed and implemented well, red teaming can help decision-makers uncover possible threats and vulnerabilities that may not be visible through traditional methods and filters – a valuable tool for furthering the defense of U.S. interests and assets, domestic or abroad. ■

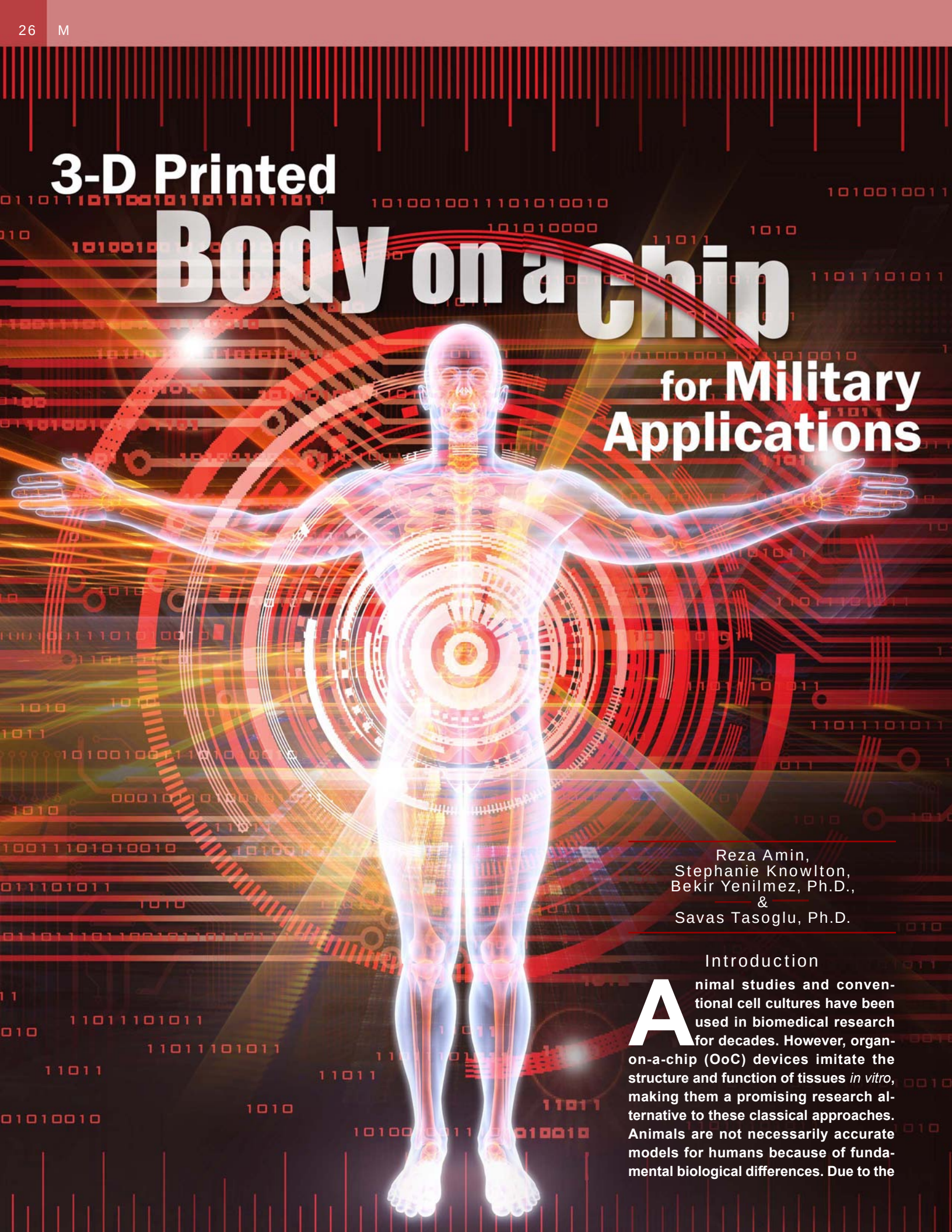
References

1. Binnie, J. (2016, October 27). Iran unveils unmanned ground effect vehicle. *IHS Jane's Defence Weekly*. Retrieved from http://www.janes.com/article/64968/iran-unveils-unmanned-ground-effect-vehicle (accessed July 19, 2017)
2. Binnie, J. (2017, January 27). Telephone interview.
3. Jane's Strategic Assessments and Futures Studies Center uses this construct in its alternative analysis training curriculum. It is derived from both Jane's experts' experience in designing and applying a wide range of alternative analysis methods and training defense and intelligence communities on these methods as well as extensive research on the topic.
4. George, A. L. (1972). The case for multiple advocacy in making foreign policy. *American Political Science Review*, *66*(3), 751-785. doi:10.2307/1957476
5. Heuer, R. J. (1999) Chapter 8: Analysis of competing hypotheses. In *The psychology of intelligence analysis*. Center for the Study of Intelligence.
6. Palo Alto Research Center. (n.d.). Analysis of Competing Hypotheses (ACH). Retrieved from http://www2.parc.com/istl/projects/ach/ach.html (accessed July 19, 2017)
7. Mateski, M. (2009, June). Red teaming: A short introduction (1.0). *Red Team Journal*. (p.21) Retrieved from http://redteamjournal.com/papers/A%20Short%20Introduction%20to%20Red%20Teaming%20(1dot0).pdf (accessed July 19, 2017)
8. The Joint Chiefs of Staff. (2016, May 16). *Joint Doctrine Note 1-16: Command Red Team* (p. V, Rep. No. JDN 1-16). Retrieved from https://fas.org/irp/doddir/dod/jdn1_16.pdf (accessed July 19, 2017)
9. Nurkin, T. (2016, June). *Promise and peril: Dimensions, dynamics and challenges of disruptive innovation in defense and security*. Paper presented at Eurosatory Conference, Paris.
10. IHS Jane's Strategic Assessment and Futures Studies Centre. (2016, November). *Rising tensions: Air and missile defence in Europe*. IHS Global Limited. Retrieved from https://ihs.uberflip.com/i/754983-1680503jdw/0?m4= (accessed July 19, 2017)
11. Clad, J., & Manning, R. (2016, December 15). Catching controversy: China's maritime militia. *IHS Jane's Defence Weekly Online*.
12. Barclay, J. (2017, January 24). Telephone interview.
13. The National Academies, & The Department of Homeland Security. (n.d.). *IED attack: Improvised explosive devices*. Retrieved from https://www.dhs.gov/xlibrary/assets/prep_ied_fact_sheet.pdf (accessed July 19, 2017)
14. Weisgerber, M. (2015, September 8). *How many US troops were killed by Iranian IEDs in Iraq? Defense One*. Retrieved from http://www.defenseone.com/news/2015/09/how-many-us-troops-were-killed-iranian-ieds-iraq/120524/ (accessed July 19, 2017)
15. Zoroya, G. (2013, December 18). How the IED changed the U.S. military. *USA Today*. Retrieved from https://www.usatoday.com/story/news/nation/2013/12/18/ied-10-years-blast-wounds-amputations/3803017/ (accessed July 19, 2017)
16. Watson Institute of International and Public Affairs, Brown University. (n.d.). *Costs of war*. Retrieved from http://watson.brown.edu/costsofwar/ (accessed July 19, 2017)
17. Maple, D. (2016, November 10). Unmanned systems: The reign of the persistent warriors. *IHS Jane's Intelligence Briefing Series*.
18. O'Rourke, R. (2015, June 12). *Navy shipboard lasers for surface, air, and missile defense: Background and issues for Congress* (CRS Rep. No. R41526). Congressional Research Service. Retrieved from https://fas.org/sgp/crs/weapons/R41526.pdf (accessed July 19, 2017)
19. Fisher, R., & Hardy, J. (2014, November 27). China's Poly Group unveils WB-1 directed-energy crowd-control weapon. *IHS Jane's Defence Weekly Online*.
20. FBI. (2014, February 10). *Protecting aircraft from lasers: New program offers rewards for information*. Retrieved from https://www.fbi.gov/news/stories/protecting-aircraft-from-lasers (accessed July 19, 2017)
21. The Maritime Executive. (2016, September 27). USCG helicopter grounded following laser incident. *The Maritime Executive*. Retrieved from http://www.maritime-executive.com/article/uscg-heli-briefly-grounded-following-laser-incident (accessed July 19, 2017)
22. Scharre, P. (2014, October 20). The coming swarm: Robotics on the battlefield. RealClear Defense. Retrieved from http://www.realcleardefense.com/articles/2014/10/20/the_coming_swarm_robotics_on_the_battlefield_107499.html (accessed July 19, 2017)
23. Barclay, J. (n.d.). How to kill UAVs. *IHS Jane's 360*.
24. Farrell, M. B. (2009, December 17). SkyGrabber: Hack of US drones shows how quickly insurgents adapt. The Christian Science Monitor. Retrieved from http://www.csmonitor.com/USA/2009/1217/SkyGrabber-hack-of-US-drones-shows-how-quickly-insurgents-adapt (accessed July 19, 2017)
25. The Ministry of Defence. (2016, September 16). *Advantage through innovation: The Defence Innovation Initiative prospectus*. London: Ministry of Defence. Retrieved from https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/553429/MOD_SB_Innovation_Initiative_Brochure_v21_web.pdf (accessed July 19, 2017)
26. Kovach, G. C. (2014, May 10). Protecting troops at war's end. *The San Diego Union-Tribune*. Retrieved from http://www.sandiegouniontribune.com/military/sdut-camp-leatherneck-security-task-force-belleau-wood-2014may10-story.html (accessed July 19, 2017)
27. Bunker, R. J. (2012). Force protection and suicide bombers: The necessity for two types of Canadian military red teams. *Canadian Military Journal*, (12)4, 35-43.
28. Mateski, M. (2017, January 25). Telephone interview.

Tate Nurkin
Executive Director, Strategic Assessments and Futures Studies Center, Jane's by IHS Markit

Tate Nurkin specializes in applying scenario planning, wargaming, red teaming, and net assessment methodologies to emerging defense and security competitions, and in the development of competitive and hedging strategies (M.S., Georgia Institute of Technology). He is the research lead for Jane's Promise and Peril: Dimensions, Opportunities, and Challenges of Disruptive Innovation in Defense and Security research initiative.

3-D Printed Body on a Chip for Military Applications



Reza Amin,
Stephanie Knowlton,
Bekir Yenilmez, Ph.D.,
&
Savas Tasoglu, Ph.D.

Introduction

Animal studies and conventional cell cultures have been used in biomedical research for decades. However, organ-on-a-chip (OoC) devices imitate the structure and function of tissues *in vitro*, making them a promising research alternative to these classical approaches. Animals are not necessarily accurate models for humans because of fundamental biological differences. Due to the

species-specific differences in drug uptake and toxicities, results of a drug trial in an animal do not necessarily translate well to the results of human studies. Further, in light of emerging alternatives that may be even more accurate, it may no longer be efficient to conduct drug trials in animals. 2-D cultures of human cells are sometimes used for similar applications, but the activity of a cell closely depends on its microenvironment – a petri dish does not sufficiently mimic the 3-D environment and physiological conditions of a human body [1]. OoC devices closely mimic human physiological systems, and therefore can be used as a platform to understand and predict the effects of chemical and biological agents on human tissues and organs, perform forensic analyses, and develop and test medical treatments.

Defense agencies actively seek such biological screening technologies in the interest of national defense. In 2013, the Defense Threat Reduction Agency (DTRA) and Edgewood Chemical Biological Center (ECBC) partnered on a five-year project to investigate the effects of chemical warfare agents (CWA) on humans [2,3]. In another DTRA-funded project, researchers developed a Pulmonary Lung Model, or PuLMo, an organ-on-a-chip device that can be used to study the flow of particles within a lung [4]. However, challenges with high-throughput fabrication of these devices remain a barrier to innovation in the field and to widespread implementation.

Researchers at the University of Connecticut are now using 3-D printing for rapid prototyping to simplify the traditionally complex fabrication process of these devices with the aim of facilitating rapid advances in the OoC concept and moving closer to realizing a practical body-on-a-chip (BoC) technology.

3-D Printing

3-D printing is a fabrication method that enables rapid and precise transformation of 3-D computer designs into physical models. It relies on the use of additive patterning of a material in a layer-by-layer manner using a print head, nozzle, or other mechanism. Common 3-D printing approaches include stereolithography (SLA) (see Figure 1a), fused deposition modeling (FDM) (see Figure 1b), photopolymer inkjet printing, selective laser sintering, and binder jetting [5-8]. FDM involves melting a thermoplastic polymer using a heated nozzle and depositing layers that solidify and form a 3-D structure. SLA employs a beam of light to polymerize layers of a liquid photo-curable resin. Hybrid 3-D printers, such as multijet modeling printers, combine FDM and SLA techniques by depositing a photo-curable resin and polymerizing it using light. Over the last decade, these methods have been vastly improved in terms of their accuracy, precision, and compatibility with a broad range of materials.

The Department of Defense already uses 3-D printing for medical applications. The 3-D Medical Applications Center at the Walter Reed National Military Medical Center conducts research on medical applications of 3-D printing, including orthopedic and craniofacial reconstruction as well as dental implants [9]. Additionally, the technology can be used to manufacture devices for on-site diagnosis and health tracking of troops [10,11]. 3-D printing could also be utilized by the military to print spare parts and tools on-site for maintenance and repairs at isolated operation bases [12].

3-D Printed Living Cells Within Microfluidic Devices

Microfluidic devices can be fabricated to serve as a physical environment where living cells can be spatially patterned and survive and grow over days and weeks – referred to as OoC. Human cells are a necessary condition of OoC. Cells can be obtained from a human cell line and will proliferate indefinitely from stem cells that have the ability to turn into any cell type (or even skin cells that are dedifferentiated into stem cells). This allows for studies on any tissue in the body, including tissues from people of different genders and genetic mutations (for example, those with immune disorders) by harvesting a small sample of cells from a range of subjects.

Microfluidic systems serve as the foundation for OoC systems, and offer the precise control of the flow of fluid through microscale channels, and the ability to closely tune the physical environment to conditions that mimic those of the human body. Of the many 3-D printing techniques, FDM, SLA, and photopolymer inkjet printing show the most promise for use in microfluidic chip fabrication [5]. Microfluidic devices have been shown to enable the construction of numerous OoCs including cardiac and skeletal muscle and cancer tissues [1]. The devices can also be 3-D printed. For example, University of Connecticut researchers demonstrated patterning of tissue constructs into 3-D printed chips [13]. Results show that UV-crosslinked hydrogels in transparent chips that were printed via low-cost desktop printers can provide a suitable environment for cells to proliferate. This approach demonstrates strong promise for co-patterning of different cell lines to create an even more biomimetic environment.

Bioprinting is a modification of 3-D printing where the printing material is replaced with a "bioink," comprised of living cells, a cell-compatible scaffold, and growth factors important to promote cell survival after printing. Bioprinting has shown potential in constructing complex 3-D cellular structures, which mimic the 3-D complexity of human tissues. The intersection of bioprinting with microfluidics gives rise to highly useful 3-D cell culture systems. For example, liver tissue can be printed directly into microfluidic channels, which are then covered with another polydimethylsiloxane (PDMS) layer to form a functional microfluidic device as a bioreactor to maintain long-term viability of cells [14]. Following fabrication, the device was perfused with cell media at an appropriate flow rate to provide adequate nutrients and oxygen to the microtissues without interfering with the biomarkers secreted by the cells. Using both direct bioprinting into the microfluidic device followed by bioreactor-like microfluidic perfusion made this approach unique. This microfluidic platform mimics the 3-D culture environment of the human body and could be used to study drug-induced toxicity.

Toward Single-Step Biofabrication of Organs-on-a-Chip via 3-D Printing

Single-step biofabrication of the entire OoC using multimaterial 3-D printing represents a promising future direction in this field [15]. Currently, most microsystems are fabricated using a soft lithography technique with PDMS, a synthetic elastomer that can be poured around a mold and cured. This process requires multiple steps and

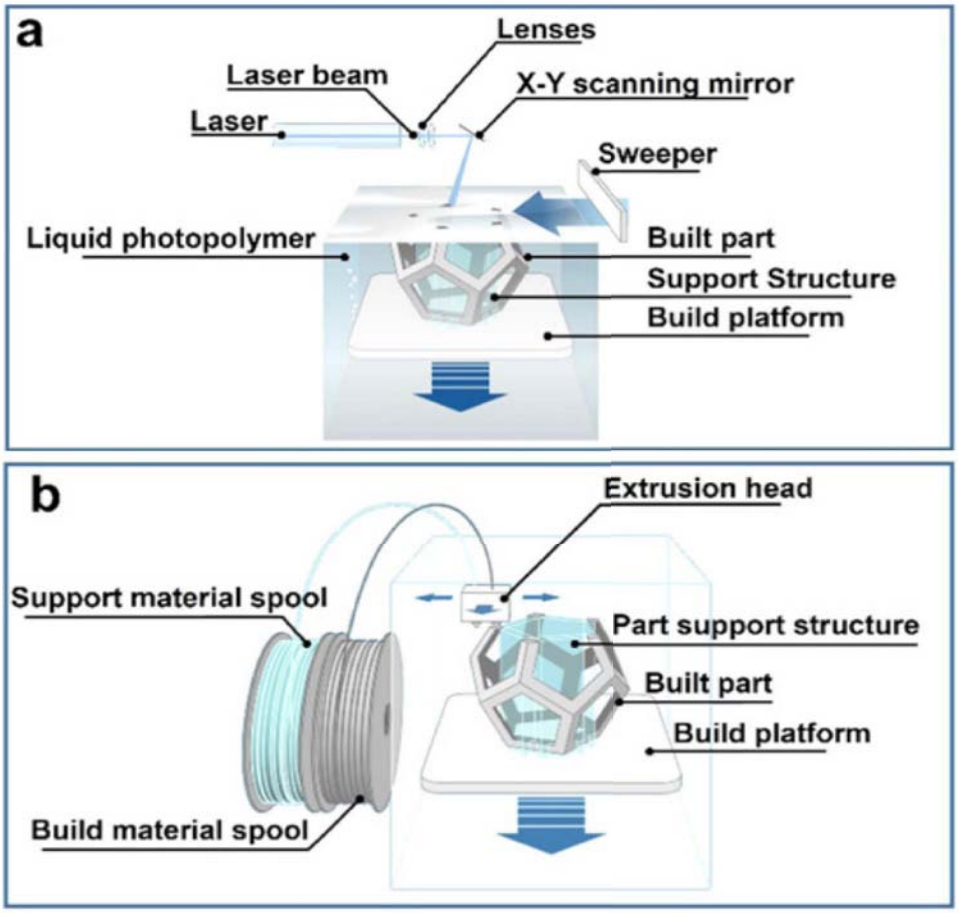


Figure 1: 3-D printing technologies used in fabrication of microfluidics: (a) SLA and (b) FDM [17]. (Released)

costly, dedicated tools, and limits rapid prototyping and customization during the design process. Using multimaterial 3-D printing of viscoelastic inks, a wide range of structural, functional, and biological materials can be patterned in a single-step automatized fabrication process. 3-D printing allows these devices to be rapidly created and customized at a low cost. This approach may be more impactful than traditional OoC construction due to the ability to perform rapid design iterations and high-throughput fabrication. Multimaterial 3-D printing of OoC has been demonstrated by the Lewis Lab at Harvard University [16]. With this technique, a fully 3-D printed microphysiological device is fabricated to provide a continuous electronic readout of the contractile stress of multiple laminar cardiac microtissues.

Body-on-a-Chip

While the idea of culturing human tissue on a chip is not new, combining several organs in the same device using 3-D printing is at an early development stage. BoC devices are an extension of OoC devices, and include multiple organs in fluidic communication with one another. Because signaling between organs is an important component of the body's functions, BoC devices can more accurately predict a systemic reaction to diseases or toxins. A BoC could model the human response to drugs, chemical toxins and biologic agents.

The BoC concept could be fabricated on the scale of a few centimeters and be connected to fluid channels and sensors to facilitate long-term viability and continuous monitoring of individual organs and interactions of different organs. The *in vitro* BoC platform will offer more human-relevant studies to evaluate efficiency and toxicity of drugs for different organs. For instance, a drug that is useful in treating heart disease can be metabolized by the liver, causing toxic effects that would only be realized in a body-wide study. In uniquely human diseases, such as asthma, no animal testing can imitate the human response. A BoC, engineered with human cells, can truly mimic physical environments of human tissue including fluidic shear stresses and microparticle transport across different fluid-tissue boundaries. The concept has been proven to be a more realistic model for drug discovery, which could surge drug development and enable researchers to perform experiments considered risky for human subjects at high-throughput.

Each 3-D printed BoC device can be fabricated at a low cost in a reasonably short amount of time, which helps with their application for high-throughput drug discovery. This development could be used to study how a warfighter's body and major organs react to CWAs, as recently demonstrated by a research team led by DTRA [9].

Military Applications for Organs-on-a-Chip

As aforementioned, 3-D printing can be used by government organizations, such as the Department of Homeland Security and U.S. Special Forces, to rapidly fabricate OoCs in a single step with higher reliability (compared to existing methodologies). Becasue these screening devices can be printed on demand, it is not necessary to know what exposures may be encountered. Once an agent of concern is suspected, the device can be printed and utilized to assess the effects of the agent on specific body tissues and recommendations for protection can be made. This creates an agnostic screening tool that eliminates the need for transporting specific screening tools. Because of this, minimal resources are used, saving space and time.

The OoC technology could provide more insight into surviving harmful environmental exposures, such as contaminated toxic water and air, which could result in irremediable health issues. In order to more accurately reflect total system response to contaminants, multiple OoCs must be used. A small-size, low-cost microphysiological BoC system could be used to examine and estimate the body's reaction to toxic environmental assaults or CWAs. OoCs could be a useful tool for high-throughput and rapid study of the effects of new biological or chemical weapons. Governmental agencies, including DTRA and ECBC, could continue research to develop more accurate toxicological models that will aid in developing medical countermeasures for identifying threats.

Applications of this emerging technology also include studying biological process-

es in health and disease over time, and developing and testing clinical therapies. Closely studying the human cells in the OoC over the course of a viral infection can ultimately lead to more effective antiviral treatments. Another application includes the PuLMo, which allows real-time assessment of how a human's lungs react to certain drugs [4]. OoC devices enable military agencies such as the U.S. Army Medical Research and Materiel Command and Naval Health Research Center to rapidly develop treatments for warfighters based on current demands. ■

References

1. Bhatia, S. N. & Ingber, D. E. (2014). Microfluidic organs-on-chips. *Nature Biotechnology*, 32, 760-772. doi:10.1038/nbt.2989
2. Army, academia develop human-on-a-chip technology. U.S. Army. Retrieved from https://www.army.mil/article/112149 (accessed July 19, 2017).
3. ECBC Public Affairs (2015, August 24). ECBC at the forefront of advanced toxicological research. U.S. Army Research Development and Engineering Command, Edgewood Chemical Biological Center. Retrieved from https://www.ecbc.army.mil/news/2015/ecbc-forefront-advanced-toxicological-research-human-on-chip.html (accessed July 19, 2017).
4. Arrington, Y. (2017, January 30). DoD's 'organ-on-a-chip' innovation wins big. Armed With Science. Retrieved from http://science.dodlive.mil/2017/01/30/dods-organ-on-a-chip-innovation-wins-big/ (accessed July 19, 2017).
5. Amin, R., Knowlton, S., Hart, A., Yenilmez, B., Ghaderinezhad, F., Katebifar, S., … Tasoglu, S. (2016). 3D-printed microfluidic devices. *Biofabrication*, *8*(2). doi:10.1088/1758-5090/8/2/022001
6. Au, A. K., Huynh, W., Horowitz, L. F., & Folch, A. (2016). 3D-Printed microfluidics. *Angewandte Chemie International Edition*, *55*(12). doi: 10.1002/anie.201504382.
7. Waheed, S., Cabot, J. M., Macdonald, N. P., Lewis, T., Guijt, R. M., Paull, B., & Breadmore, M. C. (2016). 3D printed microfluidic devices: Enablers and barriers. *Lab on a Chip*, 16, 1993-2013. doi:10.1039/C6LC00284F
8. Ho, C. M., Ng, S. H., Li, K. H., & Yoon, Y. J. (2015). 3D printed microfluidics for biological applications. *Lab on a Chip*, *15*(18), 3627-3637. doi:10.1039/c5lc00685f
9. 3-D medical applications center (3DMAC) (n.d.) Walter Reed National Military Medical Center. Retrieved from http://www.wrnmmc.capmed.mil/ResearchEducation/3DMAC/SitePages/Home.aspx (accessed July 19, 2017).
10. Yenilmez, B., Knowlton, S., Yu, C. H., Heeney, M. M., & Tasoglu, S. (2016). Label-free sickle cell disease diagnosis using a low-cost, handheld platform. *Advanced Materials Technologies*, *1*(5). doi:10.1002/admt.201600100
11. Yenilmez, B., Knowlton, S., & Tasoglu, S. (2016). Self-contained handheld magnetic platform for point of care cytometry in biological samples. *Advanced Materials Technologies*, *1*(9). doi:10.1002/admt.201600144
12. Rider, T. (2014). 3-D printing benefits for logistics. *Army Technology Magazine*, *2*(4), 8. Retrieved from https://www.dodmantech.com/mantechprograms/Files/Army/Army_Technology_Mag_3D_Printing.pdf (accessed July 19, 2017).
13. Knowlton, S., Yu, C. H., Ersoy, F., Emadi, S., Khademhosseini, A., & Tasoglu, S. (2016). 3D-printed microfluidic chips with patterned, cell-laden hydrogel constructs. *Biofabrication*, *8*(2). doi:10.1088/1758-5090/8/2/025019
14. Bhise, N. S., Manoharan, V., Massa, S., Tamayol, A., Ghaderi, M., Miscuqlio, M., … Khademhosseini, A. (2016). A liver-on-a-chip platform with bioprinted hepatic spheroids. *Biofabrication*, *8*(1). doi:10.1088/1758-5090/8/1/014101
15. Knowlton, S., Yenilmez, B., & Tasoglu, S. (2016). Towards single-step biofabrication of organs on a chip via 3D printing. *Trends in Biotechnology*, *34*(9), 685-688. doi:10.1016/j.tibtech.2016.06.005
16. Lind, J. U., Busbee, T. A., Valentine, A. D., Pasqualini, F. S., Yuan, H., Yadid, M., … Parker, K. K. (2016). Instrumented cardiac microphysiological devices via multimaterial three-dimensional printing. *Nature Materials*, 16, 303-308. doi:10.1038/nmat4782
17. Additively Ltd. (n.d.). Retrieved from https://www.additively.com/en/ (accessed July 19, 2017).

Reza Amin
Ph.D. Candidate, University of Connecticut

Reza Amin is pursuing a Ph.D. in mechanical engineering (M.S., Sharif University of Technology, Iran). His field of research is at the intersection of mechanical, electrical, and biomedical engineering. Amin's research interests are lab-on-a-chip, biofabrication, 3-D printed microfabrication, point of care diagnostics, bio-inspired engineering systems, and systems biology.

Stephanie Knowlton
Ph.D. Candidate, University of Connecticut

Stephanie Knowlton is pursuing a Ph.D. in biomedical engineering (B.S., University of Connecticut). Her research interests include tissue engineering and regenerative medicine, neural engineering, and microfluidics for tissue engineering applications. Knowlton is a member of the Biomedical Engineering Society, the Society of Women Engineers, and Phi Sigma Rho, a sorority for women in engineering.

Bekir Yenilmez, Ph.D.
Postdoctoral Researcher, Tasoglu Lab

Bekir Yenilmez is a postdoctoral researcher at the Tasoglu Lab (Ph.D., Koc University, Turkey). His current research interests include systems engineering for bioprinting, while his prior research focused on modelling and simulation of liquid composite molding processes of glass-fiber reinforced composites. Yenilmez also has experience in designing experimental setups, PC–embedded system interfacing, automation, and data processing. His work has been published in notable journals such as *Composites Part A*, *Composites Science and Technology*, and *Advanced Materials Technologies.*

Savas Tasoglu, Ph.D.
Assistant Professor, University of Connecticut

Savas Tasoglu is an assistant professor in the Department of Mechanical Engineering at the University of Connecticut (Ph.D., University of California, Berkeley). Tasoglu held a postdoctoral appointment at Harvard Medical School and Harvard-MIT Division of Health Sciences and Technology until 2014. His research interests are point-of-care diagnostic devices, bioprinting, magnetic focusing and levitation, microfluidics, and regenerative medicine.

HDIAC SERVICES

Core Analysis Task (CAT)

PRE-AWARDED PRE-COMPETED CONTRACT VEHICLE

RAPID START TIME
Work can begin in as little as six weeks, once the statement of work is approved.

EXPANSIVE TECHNICAL FOCUS AREAS
HDIAC's broad scope is especially valuable for the efforts that cross multiple focus areas.

EXTENSIVE SME NETWORK
HDIAC is able to leverage support from its expansive SME network.

ACCESS TO THE LATEST SCIENTIFIC & TECHNICAL DOD FINDINGS
HDIAC draws from the most recent studies performed across the DoD, and the results from all of HDIAC's CATs are collected, stored and used to support HDIAC's future efforts.

Technical Inquiry Services

HDIAC provides four free hours of analytical, scientific and professional research within our eight focus areas. These services are available to academia, industry and other government agencies. To utilize HDIAC's free technical inquiry service, log in and submit a technical inquiry form at **hdiac.org** or contact **inquiries@hdiac.org**.

HDIAC Basic Center of Operations & Mission

The Homeland Defense & Security Information Analysis Center (HDIAC) 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 focus areas, in support of the DoD and U.S. government R&D activities.

HDIAC's mission is to provide authoritative, responsive solutions by generating, acquiring, processing, analyzing and disseminating relevant information and analysis to our customers.

Through our Basic Center of Operations, subject matter expert network and extensive database collection, HDIAC is positioned to help support the nation's toughest scientific and technical challenges. HDIAC provides a wide range of additional services, including:

- Access to the HDIAC Journal, a quarterly publication featuring scientific and technical innovations within our focus areas.
- A network of subject matter experts in each of the focus areas.
- Participation in key technical conferences and forums to engage and network with the science and technology (S&T) community.

HDIAC
Homeland Defense & Security
Information Analysis Center

www.hdiac.org
104 Union Valley Rd. • Oak Ridge, TN • 37830
865 • 535 • 0088
info@hdiac.org

HDIAC FOCUS AREAS

Alternative Energy | Biometrics | CBRN Defense | Critical Infrastructure Protection | Cultural Studies | Homeland Defense & Security | Medical | WMD








Calendar of Events

September 2017

09/18/17 - 09/20/17 • **San Diego, CA**
CIP Power Grid Resilience

09/19/17 - 09/21/17 • **Washington, DC**
CBRN NCT CBRNe USA Conference

October 2017

10/02/17 - 10/03/17 • **Charlotte, NC**
HDS Nuclear Decommissioning and Used Fuel Strategy Summit

10/03/17 - 10/05/17 • **Tampa, FL**
AE, CIP HDS, M Department of Defense Innovation Summit

10/11/17 - 10/13/17 • **San Diego, CA**
AE 10th EESAT Conference

10/23/17 - 10/25/17 • **Wilmington, DE**
HDS MILCOM 2017

10/26/17 • **El Paso, TX**
HDS Fort Bliss Tactical & Tech Day

10/31/17 - 11/02/17 • **Honolulu, HI**
CIP TechNet Asia-Pacific 2017

November 2017

11/04/17 - 11/08/17 • **Atlanta, GA**
M American Public Health Association Annual Meeting & Expo

11/07/17 - 11/08/17 • **Orlando, FL**
HDS 12th Annual Homeland Security Professionals Conference

11/14/17 • **Chantilly, VA**
HDS DHS Intelligence Enterprise Industry Day

Call for Papers

HDIAC **is now accepting abstracts and articles for consideration for future publications. For more information, contact the Publications Team at** publications@hdiac.org.

The HDIAC Journal is a quarterly publication, focusing on novel developments and technology in the Alternative Energy, Biometrics, CBRN, Critical Infrastructure Protection, Cultural Studies, Homeland Defense and Security, Medical, and Weapons of Mass Destruction focus areas.

- Articles must be relevant to one of the eight focus areas and relate to Department of Defense applications.
- Articles should be submitted electronically as a Microsoft Word document.
- We require a maximum of 2,500 words.
- All submissions must include graphics or images (300 DPI or higher in JPG or PNG format) to accompany the article. Photo or image credit should be included in the caption.

Publications

Volume 4; Issue 4
(Publish Dec. 2017)
Abstract deadline: 7/15/17
Article deadline: 8/15/17

Volume 5; Issue 1
(Publish March 2018)
Abstract deadline: 10/13/17
Article deadline: 11/13/17

Volume 5; Issue 2
(Publish June 2018)
Abstract deadline: 1/5/18
Article deadline: 2/2/18