HDIAC Journal

The Journal of the Homeland Defense & Security Information Analysis Center

Volume 5 Issue 2 Summer 2018

DEFINING THE PROFILE OF POTENTIAL CYBERCRIMINALS

DISTRIBUTION A: APPROVED FOR PUBLIC RELEASE; DISTRIBUTION IS UNLIMITED

HDIAC JOURNAL

The Journal of the Homeland Defense & Security
Information Analysis Center

Volume 5 • Issue 2 • Summer 2018

Director: **Stuart Stough**
Deputy Director: **Joseph Cole**

The Journal of the Homeland Defense & 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 Under Secretary of Defense for Research and Engineering (USD (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.

ISSN 2578-0832 (print)
ISSN 2578-0840 (online)

Alternative Energy

Biometrics

CBRN Defense

Critical Infrastructure Protection

Cultural Studies

Homeland Defense & Security

Medical

Weapons of Mass Destruction

Table of Contents

Contact

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

Fatena Casey, Technical Office Manager
Tim Gould, Graphic Designer
Amanda Andrews, Editor
David McCarville, Social & Multi-Media Editor

Emese Horvath
Contracting Officer Representative

DoD Information Analysis Centers
8745 John J. Kingman Road
Fort Belvoir, VA 22060
571-448-9753
emese.i.horvath.civ@mail.mil

Michele Finley
Public Affairs Officer

Defense Technical Information Center
8725 John J. Kingman Road
Fort Belvoir, VA 22060
703-767-8215
michele.l.finley2.civ@mail.mil

Message from the Director

Stuart Stough
HDIAC Director

The Homeland Defense & Security Information Analysis Center (HDIAC) identifies relevant scientific and technical (S&T) information to develop and deliver timely, superior technical solutions to Combatant Commands, Program Executive Offices, operational units, leaders, project managers, researchers, and others in the Department of Defense (DoD) as well as other government agencies and the Homeland Defense and Security community. HDIAC collaborates with partner organizations and a robust network of Subject Matter Experts (SMEs) to identify cutting-edge technologies that may fill existing and future DoD gaps and requirements.

HDIAC continued to collaborate with its Communities of Interests and engaged with its SMEs from Defense Criminal Investigative Service, Sandia National Laboratories, Oak Ridge National Laboratory, Missouri University of Science and Technology, University of Sydney, and others. HDIAC's SMEs provided extensive support across all eight focus areas, with notable contributions in CBRN Defense, Critical Infrastructure Protection, Cultural Studies, Homeland Defense and Security, Medical, and WMD. Specifically, HDIAC provided original research products, such as *Defining the Profile of Potential Cyber Criminals*; *Synthetic Blood Products and the DoD*; *Predictive and Diagnostic Methodologies for Traumatic Brain Injuries*; and *Detecting Unexploded Ordnance Through Changes in Plant Health*.

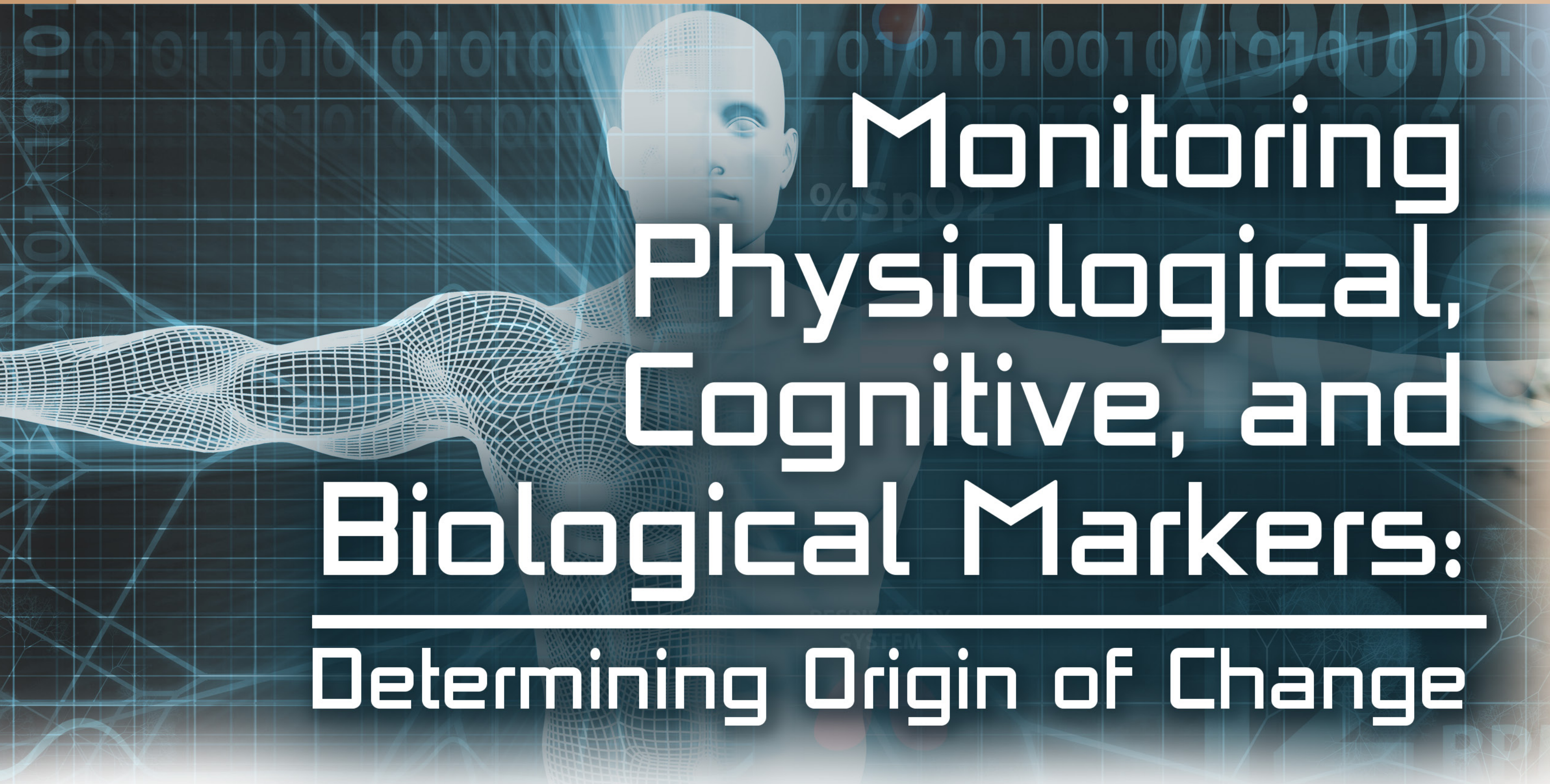
Last quarter, HDIAC SMEs completed a Core Analysis Task (CAT) for the U.S. Army Natick Soldier Research, Development and Engineering Center (NSRDEC) that focused on improving soldier performance, protection, and medical monitoring through advances in e-textiles and other soldier-wearable devices. HDIAC collaborated with NSRDEC, multiple DoD agencies, NASA, and component and national laboratories regarding R&D advances that will support NSRDEC's future efforts to improve tracking soldier performance, health status, and potential exposure to harmful substances.

Our center engaged our user community regarding state-of-the-art developments and trends in medical monitoring for soldiers operating in deployed, austere, and rugged environments. In March, HDIAC SMEs Gregory Nichols (HDIAC) and Glory Emmanuel-Aviña (Sandia National Laboratories) hosted a well-attended online webinar on emerging wearables technology that may be used by DoD to monitor soldier performance. In May, HDIAC published a Tech Talk on the topic, *Physiological Monitoring and the DoD*.

In this issue of the *HDIAC Journal*, Emmanuel-Aviña discusses the particulars of her research, examining how suites of standard physiological monitoring devices can be combined to detect warfighter exposure to a CBRN agent—while also differentiating an exposure from performance decrement arising from fatigue. Emmanuel-Aviña concludes, "Identifying additional data streams that measure human performance in real-time and quantifying them through advanced wearable technology may allow us to both anticipate as well as make decisions about health in extreme environments."

HDIAC also investigated methods for mitigating the degradation of warfighter performance in hypoxic environments, an environmental risk for Special Operations Forces, military aircrew, and dismounted warfighters operating in high-altitude terrain. In particular, military aircraft have experienced multiple oxygen deficiency events in the past several years, which can significantly diminish pilot precision and control. HDIAC delivered a potential solution set to the Special Operations Community, Air Force, and Office of Naval Research, briefing them on methods for artificial acclimatization that include pharmaceutical-based and other tools for decreasing hypoxic risk.

Over the last quarter, HDIAC encountered a growing interest amongst our government and military clients and associates in several other critical areas. The Department of Homeland Security (DHS), Environmental Protection Agency (EPA), Drug Enforcement Agency, and state and local law enforcement agencies have seen a dramatic increase in the illegal use and sale of dangerous synthetic opioids. The class of opioid known as fentanyl has proven especially dangerous. HDIAC recently completed a Technical Inquiry for DHS on methods for detecting the presence of fentanyl. In May, the center completed an inquiry for EPA on leading options for indoor surface decontamination of fentanyl and similar derivatives. HDIAC is currently developing solution sets for this difficult and enduring problem facing our government stakeholders.



Monitoring Physiological, Cognitive, and Biological Markers:

Determining Origin of Change

Glory Emmanuel-Aviña, Ph.D.

Many communities have an interest in quantifying human performance, as the monitoring of physiological data helps to inform physical fitness performance, medical assessments, mental health, rehabilitation, and educational methods. The Department of Defense (DoD) may also benefit from real-time physiological monitoring. According to the Defense Science and Technology 2016 Human Systems Roadmap, the deployment of wearable sensor technology is a key mission area for protecting warfighters from threats in the environment. Both high-resolution, wearable kinematic sensors and real-time algorithm development are near and mid-term goals to aid warfighter performance [1].

Chemical and biological agent use has grown since 9/11 and remains a known threat to military forces [2], and the use of wearable technologies to analyze human behavior in real time could help to differentiate between fatigue and exposure to chemical and biological agents. Wearables, such as a wirelessly-connected ring, have been made to detect chemical and biological agents [3], but these devices detect threats present in a liquid or vapor phase. By equipping a group with wearable devices that monitor specific biomarkers, military analysts and decision-makers can track both an individual warfighter's health and monitor for group-level physiological responses that may indicate possible chem-bio exposure. Although wearable fitness devices can be used for real-time health monitoring, research is needed to understand what biomarkers would be indicative of individual health versus threat exposure.

Currently, physiological data is the primary source for quantifying human performance. Through human-subject studies, individuals can be instrumented with wearable fitness devices capable of measuring physiological markers such as heart rate, cadence, breathing rate, etc. Statistical models then analyze this data to connect physiological markers to performance.

Monitoring neurocognition and blood chemistry provides other datasets that could serve as early indicators of health, performance, fatigue, and exposure. However, the technology for quantifying cognitive ability and blood markers are not as advanced as physiological, wearable devices. Neurocognitive data, which quantifies brain activity engaged during physical movement, is indirectly measured through cognitive tasks before and after, or periodically during, an activity. Therefore, it is difficult to develop a device that can measure neurocognitive activity in non-laboratory environments.

As far as we know, there is no adequate device to quantify neurocognition in real time or while performing a physically engaging activity. While blood composition is a measure of human performance, it is collected through invasive procedures (e.g., blood draws) and must also be analyzed post-activity. However, biomarkers have been non-invasively and passively measured through wearable, microneedle patches, which lightly penetrate the surface of the skin.

Dermal interstitial fluid (ISF), for example, can be drawn by microneedles and have been found to measure biomarkers that are usually measured through blood draws. Identifying additional data streams that measure human performance in real time and quantifying them through advanced wearable technology may allow us to both anticipate as well as make decisions about health in extreme environments.

By quantifying attributes of physical fatigue, we can differentiate physiological responses from chemical and biological threats. This is important because military personnel are often subject to high-consequence, extreme environments where physical abilities are challenged. Additionally, they may be vulnerable to biological threats in austere environments.

Although real-time monitoring of data collected from wearable technologies may help to monitor personnel behavior during a mission, analysts must be able to differentiate

Image Credit | *Photo illustration created by HDIAC and adapted from Adobe Stock and a photo by GySgt Robert B. Brown Jr. (Available for viewing at http://www.centcom.mil/MEDIA/IMAGERY/igphoto/2001703082/)*

between individual health events (e.g., heat stroke, hyponatremia, dehydration, altitude sickness) and exposure to chem-bio agents (e.g., anthrax, sarin, hydrogen cyanide).

Research studies funded by government agencies that serve the DoD are examining chem-bio threats from various perspectives. Some projects study the threat agents themselves to determine how they work. Other studies examine how animals react to such agents, how to protect and defend against these agents, or the impact of attacks on large populations.

A critical body of research uses human-subjects research to study how chem-bio agents may be detected in humans. A subset of that research focuses on wearable technologies. Specifically, the Defense Threat Reduction Agency (DTRA) is funding research projects that investigate how wearable technologies may be used to detect exposure, one of which is led by the author, the Wearables at the Canyon for Health (WATCH) project.

Researchers are investigating multiple ways that wearables may be used to detect chem-bio exposure. One approach is to quantify physiological, cognitive, and biological markers to evaluate human performance and physical fatigue in extreme environments. Another method is to collect physiological data on individuals who are sick with common health ailments (e.g., influenza, common cold) and determine how wearable technology data differentiates between healthy and sick individuals. Researchers are also testing how ISF, which is extracted from a simple wearable microneedle patch on the surface of the skin, can replace invasive and static blood draws so that biomarker data can be continuously collected and analyzed.

This article presents WATCH project methodologies and findings of human-subjects research that can be applied to high-consequence scenarios where chem-bio threats are prevalent. First, recent research in wearable technologies related to sensor development, smart clothing, and data management is presented. Then human-subjects research regarding how wearable technologies can be applied to chem-bio threat detection is examined. Finally, the need to expand human-subjects research in wearable technologies and how such R&D will continue to serve the DoD is discussed.

Wearable Technology Research for the DoD

Physiological Monitoring

Wearable sensors through fitness devices are the most common way to obtain physiological data. However, challenges arise when attempting to use these commercially available wearables for consistent medical monitoring. Proper fit of the device to avoid chafing and/or inhibition of movement, a robust signal, battery life, valid data, longevity of the device, and robustness in harsh environmental conditions are just a few of these challenges. Attempts have been made to improve form, fit, and function of devices by reducing size and improving design and materials used [4]. For example, pulse rate is a physiological marker that sheds light on work load. Photoplethysmography (PPG) pulses, which access oxygen saturation, can be assessed through pulse oximeters.

Pulse oximeters are small, wearable, pulse rate sensors, which use infrared light-emitting diodes (LEDs) and photodetectors to create a simple, reliable, low-cost way to noninvasively monitor pulse rate [5]. Skin-worn, temporary tattoos may also soon provide real-time non-invasive analysis of key electrolytes and metabolites. In addition, they may also be used to measure physiological markers, such as heart rate, electroencephalogram (EEG), and electrocardiogram (ECG), that are usually captured through bulky or uncomfortable devices [6, 7].

Furthermore, different approaches may be used to improve battery life, such as minimizing power consumption by using electrocardiographic waveforms to turn devices on and off to save battery power [8] and harvesting human and ambient energy sources using electromagnetic generators [9].

Figure 1. Hikers are asked to complete a short cognitive battery before, during, and after the hike and wear a suite of fitness, wearable devices. (Source: Sandia National Laboratories)

Smart Clothing

Smart clothing is an attractive alternative to wearables because they are easily worn, making them more integrated with human activity. Electronic textiles (e-textiles) are fabrics with electronics and interconnections either woven into them or embedded in the fibers themselves. E-textile fabrics can detect the activity and physiological status of the user. Different types of e-textiles present trade-offs between flexibility, ergonomics, low power consumption, integration, and autonomy [10]. Although smart clothing is a step forward for ease of use and integration with individual users, there are challenges with fit and flexibility. For example, with silicone-based, LED clothing, there is an intrinsic stiffness of inorganic semiconductors, which makes them uncomfortable to wear. Innovative methodologies are being researched to address this, including the fabrication of thin and flexible emitting fabric that utilizes organic light-emitting diodes [11].

Neurocognitive Data

Neurocognitive data, which is cognitive function while performing and completing a task, is of increasing interest. Neurocognitive monitoring examines an individual's ability to make decisions, remember information, maintain alertness, and respond to threatening stimuli. This is important for military settings since sleep, focused attention, decision-making, and other cognitive activities are tasked in high-consequence mission contexts [12]. Impaired cognitive function could be an earlier indicator of health decline, both for physical fatigue and chem-bio exposure. If we could measure neurocognitive data well, it would help to better quantify human performance. If we could measure neurocognitive data in real time, it could serve as an early predictor of performance decline. Currently, neurocognitive processes are best quantified in highly controlled laboratory settings. Wearable neurocognitive monitors are not suited for activities that require heavy movement and are usually limited to stationary tasks [13]. Neurocognition can also be measured before and after an activity by, for example, having an individual complete a cognitive task that measures focused attention pre- and post-hike, but this does not quantify brain activity during physical exhaustion or chem-bio exposure.

There are various ways to measure neurocognitive activity. Portable, wearable eye trackers have the potential to measure this activity via gaze location, blink rate, and/or pupil dilation. Similarly, portable, reduced-electrode EEG devices may provide insight into brain function. Eye trackers are often used to gain insight into underlying mental processes, such as attention, situational awareness, cognitive load, and behavior-directed intentions [14-16]. Much like the wearable technologies field, eye tracking research is on the rise, with lightweight, increasingly portable machines becoming more accessible and numerous than ever before (e.g., eye tracking "glasses"). Portable EEG machines that are quick to set up and have a reduced number of electrodes are now readily available. In relatively uncontrolled settings, these machines are best used for determining general alertness or activity (e.g., the ratio of alpha- to beta-band activity), which has been linked to fatigue during intense activity in laboratory environments [17]. However, EEG studies are limited to controlled environments because of the delicateness of the equipment, the consequence of sweat on device fit, and overall discomfort of device when moving around.

Advances are being made to enable EEG for more active behaviors [18], but this technology is not yet mature for intense activity, such as hiking or running. Transcranial direct-current stimulation (tDCS) is another neurocognitive application that has been linked to improvements in working memory capacity [19]. Application of tDCS as part of a wearable device in extreme settings could have positive effects, but the research in this area is both sparse and difficult to conduct without proper technology development.

Human-subjects Research for Wearable Technologies

By studying hikers in an environment with significant changes in temperature and altitude, the WATCH study is creating a dataset that measures cognitive and physiological markers that could help predict performance decrement from physical stress. WATCH collects data from hikers hiking from the Grand Canyon's South Rim to its North Rim. These hikers each wear multiple wearable, commercial-off-the-shelf (COT), fitness devices provided by the research team to monitor their physical activity [20, 21]. Cognitive data is also collected by requiring hikers to complete a 5-10 minute cognitive battery every 5 miles during the hike. Data is collected from two different cohorts: civilian volunteers and military personnel. The purpose of this study is to identify physiological and cognitive markers most relevant to health and task performance and to assess which COT wearable devices are best for such measurement in extreme environments.

It also focuses on developing statistical models to identify markers that are the most predictive of benign versus traumatic health events. This study is funded by DTRA's Chemical and Biological Technologies department. Below are figures that show data collection at the Grand Canyon trailhead with human subjects as well as data from fitness devices illustrating how heart rate can be displayed for individuals wearing multiple fitness devices.

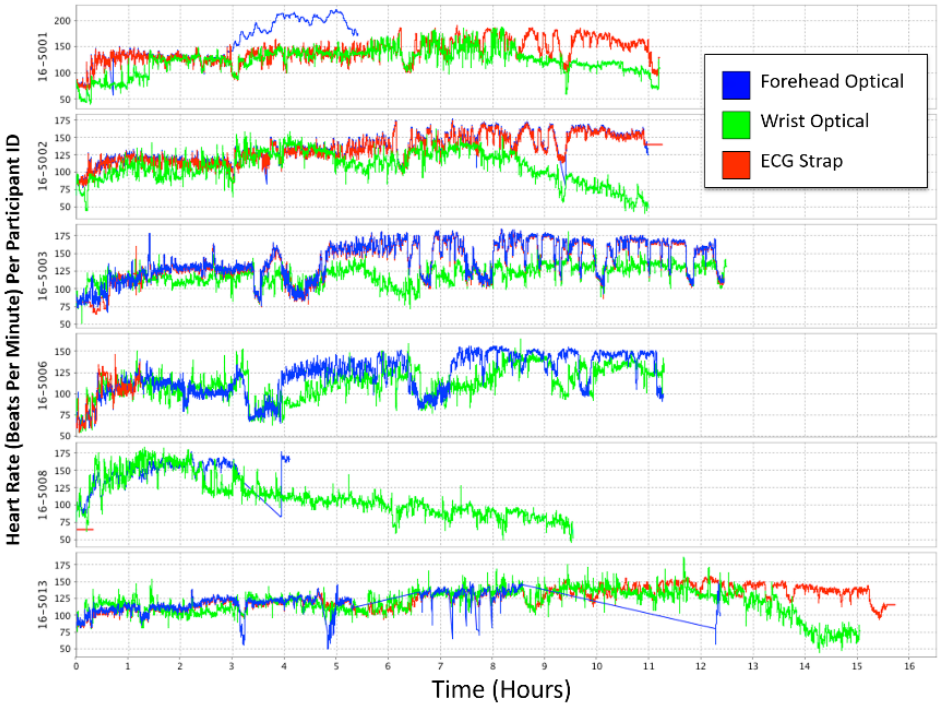


Figure 2. Parallel recordings of heart rate using 3 types of sensors on each of 6 participants. Their completion times for the hike range from 9.5 to 15.5 hours. (Source: Sandia National Laboratories)

Another study conducted by the Naval Warfare Center [22] examines how sleep patterns, heart rates, respiration rate, and body temperature are disrupted by bodily infection or other altered health statuses. These disruptions are also present for military personnel in a mission context. This project aims to collect wearable device data from individuals to establish baseline physiological parameters for healthy individuals when they are normally functioning and when they are exposed to common infections (cold, flu, etc.). The goal is to develop an early warning system that monitors physiological endpoints using state-of-the-art COT biomonitoring devices that correlate the data with actual health status and medical readiness. Devices test for personal identifiable information (PII) security, performance, robustness, data security controls, and reliability in monitoring and recording physiological parameters of interest. In addition, statistical algorithms have been developed using programming languages to analyze subject time-series data. The algorithms monitor sleep, heart rate (from inter-beat-intervals), and diurnal patterns in order to establish baselines in the dataset.

Wearable technologies are also being used to collect biological fluids in real time, such as sweat [23] and ISF [24]. For example, microneedles are used to sample ISF for clinical monitoring and diagnosis. Although ISF can be extracted through microneedles, little is known about ISF's composition and the information it provides on human chemistry and behavior. Another study funded by DTRA develops a novel microneedle array as a wearable device to collect dermal ISF from three healthy human donors. This data is then compared with matching serum and plasma samples [25]. This study, using a shotgun quantitative proteomic approach, confirmed that ISF is highly similar to both plasma and serum. ISF was found to be highly homogeneous and nearly indistinguishable for protein diversity from serum and plasma. Additional research has found that dermal ISF possesses transcriptomic and proteomic content highly similar to serum and plasma, and, therefore, it could be a proxy for blood in health monitoring [26]. Consequently, ISF could serve as a minimally invasive alternative for blood-derived fluids with potential for real-time monitoring applications.

Recommendations for Further Research

Predictive and Real-time Analytics

In addition to R&D advances, innovative statistical models must also be developed to appropriately analyze continuous, physiological data. An algorithm named Presymptomatic Agent Exposure Detection (PRESAGED) has been designed by researchers from MIT Lincoln Laboratory, the U.S. Army Medical Research Institute of Infectious Diseases, and the National Institutes of Health Integrated Research Facility. PRESAGED uses real-time physiological data to predict the probability that a person was exposed to a pathogen, such as a virus or bacteria [27].

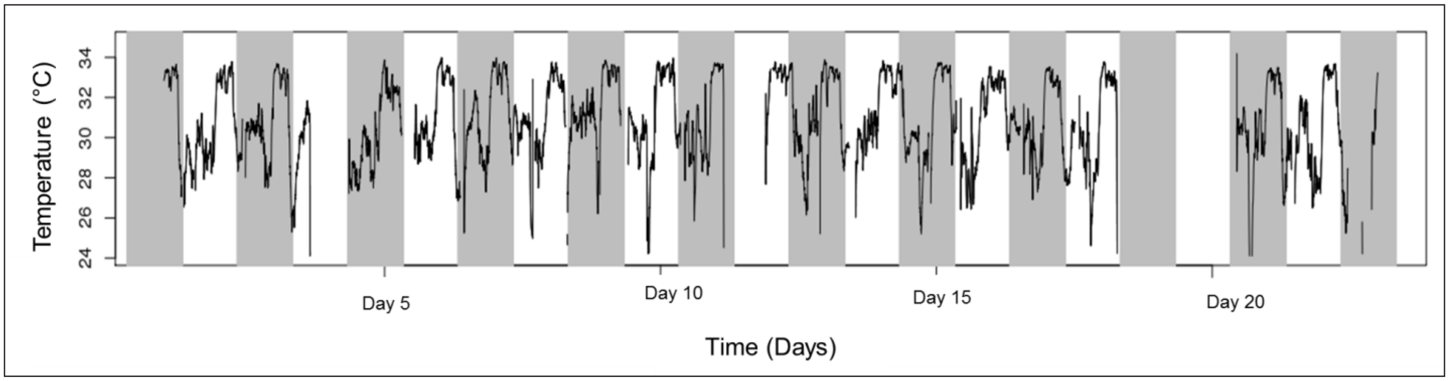


Figure 3. The Naval Warfare Center developed a statistical algorithm to identify diurnal patterns within subjects utilizing a wrist-worn COTS biomonitor. (Source: Naval Surface Warfare Center Dahlgren Division)

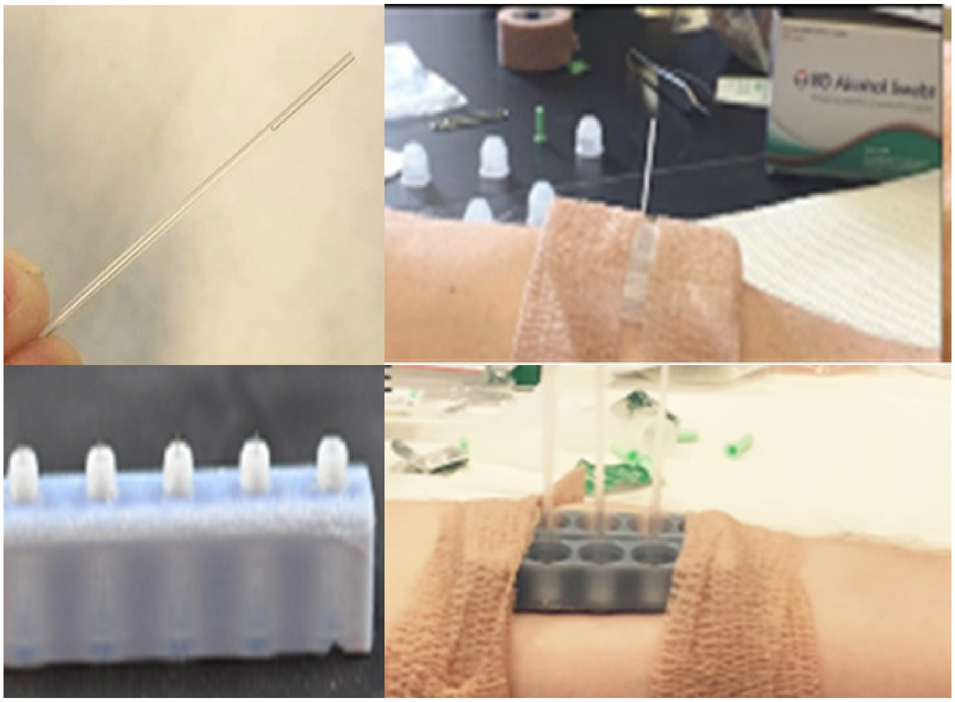


Figure 4. Development of microneedles as a wearable technology. (Source: Sandia National Laboratories)

To date, this algorithm has been tested on datasets acquired from non-human primates. To test algorithms such as PRESAGED, datasets that quantify human performance under physical health events must be compared to datasets that quantify human performance under chemical/biological events.

However, we must first be able to clearly differentiate between markers of health decline in extreme environments and markers stemming from chem-bio exposure. Confirmatory and exploratory statistical analyses will help differentiate between health decline and exposure. The objective of confirmatory analyses is to validate how physiological, cognitive, and biological markers quantify health and fatigue in extreme environments using datasets created from human-subjects. Confirmatory statistical methodology will emphasize robustness and interpretability. We propose using a derived variable analysis [28] to build summary measures from the longitudinal data collected through human-subjects studies.

Machine learning strategies can be used to build models with complex interactions between variables. Features can also be used that can be reliably constructed outside the environment of the original study for predictive purposes. In current datasets, we propose to first use derived variable analysis to generate features from the device data and then traditional machine learning methods, such as support vector machine or neural nets, to build the predictive model and validate the model using cross-validation. We will then move toward real-time data processing. Further statistical analyses need to be developed from predictive models to rapidly and accurately fuse and assess incoming data streams.

Security Considerations

The goal is for wearable technologies to equip military personnel and DoD decision-makers with information about personal health as well as the possibility of chemical, biological, and radiological exposures [29]. However, in order to operationalize real-time data, security protocols to keep data secure must be implemented. This is evidenced by the January 2018 event in which it was discovered that location information obtained from wearable fitness watches and GPS tracking applications was being released through GPS tracking app Strava [30].

As there is a movement to integrate patient wearable data with electronic medical records, personal health records, patient portals, and clinical data repositories [31], this data must be securely transmitted. Innovative methods are being developed to prevent the exploitation of sensitive user data. One recent study determined and presented techniques that allow an adversary to extract data from smartwatches, including text messages, contact information, and biomedical data [32]. Overall, the type of data being collected by wearable devices, the way the data is being extracted and released, the information that can be deduced from the data, and who should and should have access to this information are all critical questions that should inform data management. Although an infrastructure must be created to protect data extraction and communication, this is a complex challenge. Specifically, it is difficult to create solutions for extracting device data in extreme environments, especially where there are limited network sources. It is even more difficult to protect data so that it is only accessible by a subgroup of users once it has been extracted. There is currently very limited open source literature regarding potential solutions. Most solutions are based on devices that use privacy-preserving data aggregation in cloud-assisted wireless wearable communication, but tactics include: secure multiparty computation, fully homomorphic encryption, and the one-way (trapdoor) function [33].

Conclusion

The use of wearable technologies presents an opportunity to enhance human performance. These devices are being further developed to enhance performance functions ranging from those used by individuals personally monitoring their health to military personnel monitoring their environment. However, challenges remain regarding the use of wearables for physiological monitoring in military contexts. Devices must obtain valid, useful data and remain powered for long periods of time. They must be robust enough to withstand extreme environments, multiple types of terrains, temperature swings, and variable climates. They must also enhance human performance without added distraction, weight, or discomfort, and acquired data must be securely monitored and stored.

Current research projects funded by DoD agencies are generating datasets that quantify the effects of physical and cognitive fatigue as well as biological responses when exposed to common infections. Researchers are exploring how to make wearable technologies that can continuously collect biological data related to human performance. This research will assist in the development of enhanced wearables technologies that may be used by DoD to determine the origin of change in physiological, cognitive, or biological markers.

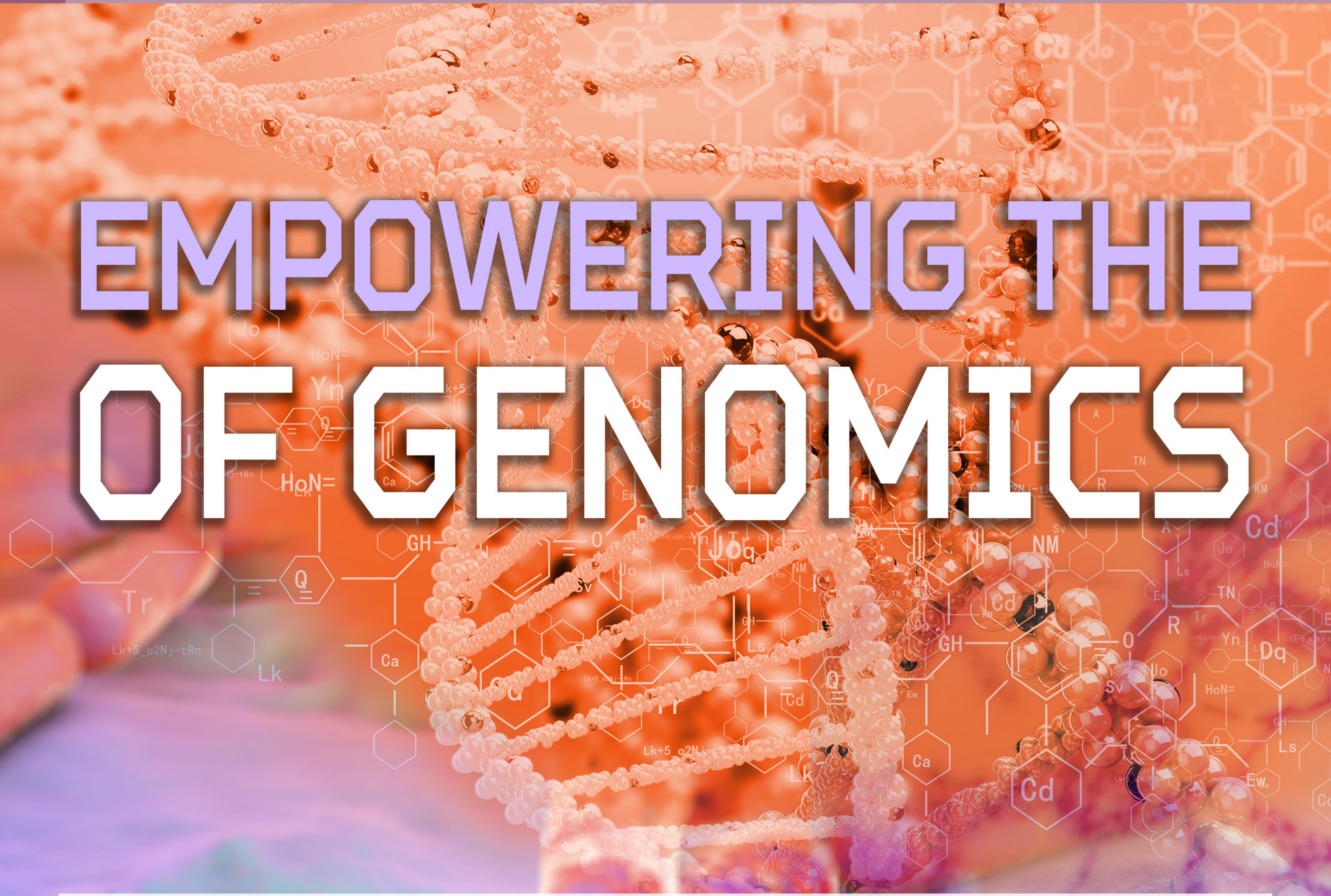
References

1. Tangney, J. (2016). Human systems roadmap review. Defense Science & Technology. Retrieved from http://www.defenseinnovationmarketplace.mil/resources/NDIA_Human_Systems_Conference_2016_HSCOI_DistroA_FINAL.pdf
2. Johnston, R. (2017). Summary of historical attacks using chemical or biological weapons. Retrieved from http://www.johnstonsarchive.net/terrorism/chembioattacks.html
3. Sempionatto, J. R., Mishra, R. K., Martin, A., Tang, G., Nakagawa, T., Lu, X., Campbell, A. S., Lyu, K. M., & Wang, J. (2017). Wearable ring-based sensing platform for detecting chemical threats. *ACS Sensors*, *2*(10), 1531-1538. doi:10.1021/acssensors.7b00603
4. Tharion, W. J., Buller, M. J., Karis, A. J., & Hoyt, R. W. (2010). Development of a remote medical monitoring system to meet soldier needs. *Army Research Institute of Environmental Medicine, Biophysics and Biomedical Modeling Division*. Retrieved from http://www.dtic.mil/dtic/tr/fulltext/u2/a525122.pdf
5. Tamura, T., Maeda, Y., Sekine, M., & Yoshida, M. (2014). Wearable photoplethysmographic sensors—Past and present. *Electronics*, *3*(2), 282-302. doi:10.3390/electronics3020282
6. Bandodkar, A. J., Jia, W., & Wang, J. (2015). Tattoo-based wearable electrochemical devices: A review. *Electroanalysis*, *27*(3), 562-572. doi:10.1002/elan.201400537
7. Windmiller, J. R., & Wang, J. (2012). Wearable electrochemical sensors and biosensors: A review. *Electroanalysis*, *25*(1), 29-46. doi:10.1002/elan.201200349
8. Rohm Semiconductor. (2015). Innovative wearable key device. Retrieved from http://www.rohm.com/web/global/news-detail?news-title=2014-06-25-wearable-key-device&defaultGroupId=false
9. Padasdao, B., & Boric-Lubecke, O. (2011). Respiratory rate detection using a wearable electromagnetic generator. *2011 Annual International Conference of the IEEE Engineering in Medicine and Biology Society*. doi:10.1109/IEMBS.2011.6090875
10. Stoppa, M., & Chiolerio, A. (2014). Wearable electronics and smart textiles: A critical review. *Sensors*, *14*(7), 11957-11992. doi:10.3390/s140711957
11. Choi, S., Kwon, S., Kim, H., Kim, W., Kwon, J. H., Lim, M. S., . . . & Choi, K. C. (2017). Highly flexible and efficient fabric-based organic light-emitting devices for clothing-shaped wearable displays. *Scientific Reports*, *7*(1), 6424. doi:10.1038/s41598-017-06733-8
12. North Atlantic Treaty Organization (2010). *Real-time physiological and psychophysiological status monitoring* (Rep. No. TR-HFM-132). RTO/NATO. ISBN 978-92-837-0093-7
13. Xu, J., Mitra, S., Van Hoof, C., Yazicioglu, R. F., & Makinwa, K. A. (2017). Active electrodes for wearable EEG acquisition: Review and electronics design methodology. *IEEE Reviews in Biomedical Engineering*, 10, 187-198. doi:10.1109/rbme.2017.2656388
14. Holmqvist, K., Nyström, M., Andersson, R., Dewhurst, R., Jarodzka, H., & Van de Weijer, J. (2011). *Eye tracking: A comprehensive guide to methods and measures*. Oxford: Oxford University Press.
15. Kovesdi, C. R., Rice, B. C., Bower, G. R., Spielman, Z. A., Hill, R. A., & LeBlanc, K. L. (2015). *Measuring human performance in simulated nuclear power plant control rooms using eye tracking* (Rep. No. INL/EXT-15-37311). Idaho Falls, ID: Idaho National Lab. doi:10.2172/1261061
16. Park, H., Lee, S., Lee, M., Chang, M. S., & Kwak, H. W. (2016). Using eye movement data to infer human behavioral intentions. *Computers in Human Behavior*, 63, 796-804. doi:10.1016/j.chb.2016.06.016
17. Ftaiti, F., Kacem, A., Jaidane, N., Tabka, Z, & Dogui, M. (2010). Changes in EEG activity before and after exhaustive exercise in sedentary women in neutral and hot environments. *Applied Ergonomics*, *41*(6), 806-811. doi:10.1016/j.apergo.2010.01.008
18. Mullen, T. R., Kothe, C. A., Chi, Y. M., Ojeda, A., Kerth, T., Makeig, S., ... & Cauwenberghs, G. (2015). Real-time neuroimaging and cognitive monitoring using wearable dry EEG. *IEEE Transactions on Biomedical Engineering*, *62*(11), 2553-2567. doi:10.1109/tbme.2015.2481482
19. Ruf, S. P., Fallgatter, A. J., & Plewnia, C. (2017). Augmentation of working memory training by transcranial direct current stimulation (tDCS). *Scientific Reports*, *7*(1), 876. doi:10.1038/s41598-017-01055-1
20. Emmanuel-Aviña, G., Abbott, R., Anderson-Bergman, C., Branda, C., Divis, K. M., Jelinkova, L., . . . Femling, J. (2017). Rim-to-Rim Wearables at the Canyon for Health (R2R WATCH): Experimental Design and Methodology. In A*ugmented Cognition, Neurocognition and Machine Learning* (pp. 263-274). Springer International Publishing. doi:10.1007/978-3-319-58628-1_21
21. Divis, K., Anderson-Bergman, C., Abbott, R., Newton, V., & Emmanuel-Aviña, G. (2018). Physiological and cognitive factors related to human performance during the Grand Canyon Rim-to-Rim Hike. *Journal of Human Performance in Extreme Environments*, *14*(1), 5. doi:10.7771/2327-2937.1095
22. Maple, L. (2017, November). Correlating sleep and temperature patter*ns in Navy warfighters with current and future health status. Evaluation of wearable technologies for earlier warning of health changes* [Abstract]. Poster session presented at the meeting of the CBD S&T Conference, Long Beach, CA. Retrieved from https://www.cbdstconference.com/agenda-download-abstract?AbstractId=98
23. Gualandi, I., Marzocchi, M., Achilli, A., Cavedale, D., Bonfiglio, A., & Fraboni, B. (2016). Textile organic electrochemical transistors as a platform for wearable biosensors. *Scientific Reports*, *6*(1). doi:10.1038/srep33637
24. Polsky, R., Miller, P. R., & Baca, J. T. (2016). *U.S. Patent Application No. 15/078,870*. Washington, DC: U.S. Patent and Trademark Office.
25. Tran, B. Q., Miller, P. R., Taylor, R. M., Boyd, G., Mach, P. M., Rosenzweig, C. N., . . . Glaros, T. (2017). Proteomic characterization of dermal interstitial fluid extracted using a novel microneedle-assisted technique. *Journal of Proteome Research*, *17*(1), 479-485. doi:10.1021/acs.jproteome.7b00642
26. Miller, P. R., Taylor, R. M., Tran, B. Q., Boyd, G., Glaros, T., Chavez, V. H., Krishnakumar, R., Sinha, A., Poorey, K., Williams, K. P., Branda, S. S., Baca, J. T., & Polsky, R. (2018). Extraction and biomolecular analysis of dermal interstitial fluid collected with hollow microneedles. *Communications Biology*. Manuscript submitted for publication.
27. Ryan, D. (2017). New technology gives early warning of exposure to disease-causing pathogens. Lincoln Laboratory, Massachusetts Institute of Technology. Retrieved from https://www.ll.mit.edu/news/new-technology-gives-early-warning-of-exposure-to-disease-causing-pathogens.html
28. Hedeker, D., & Gibbons, R. D. (2006). *Longitudinal Data Analysis*. Hoboken, NJ: Wiley-Interscience.
29. Hirschberg, D. L., Betts, K., Emanuel, P., & Caples, M. (2014). *Assessment of wearable sensor technologies for biosurveillance* (Rep. No. ECBC-TR-1275). U.S. Army Edgewood Chemical Biological Center. Retrieved from http://www.dtic.mil/dtic/tr/fulltext/u2/a611718.pdf
30. Rempfer, K. (2018, January 30). GPS tracking company reviews privacy settings amid fitness app security concerns. *Military Times*. Retrieved from https://www.militarytimes.com/news/your-army/2018/01/30/gps-tracking-company-reviews-privacy-settings-amid-fitness-app-security-concerns/
31. Shameer, K., Badgeley, M. A., Miotto, R., Glicksberg, B. S., Morgan, J. W., & Dudley, J. T. (2016). Translational bioinformatics in the era of real-time biomedical, health care and wellness data streams. *Briefings in Bioinformatics*, *18*(1), 105-124. doi:10.1093/bib/bbv118
32. Do, Q., Martini, B., & Choo, K. R. (2016). Is the data on your wearable device secure? An Android Wear smartwatch case study. *Software: Practice and Experience*, *47*(3), 391-403. doi:10.1002/spe.2414
33. Zhou, J., Cao, Z., Dong, X., & Lin, X. (2015). Security and privacy in cloud-assisted wireless wearable communications: Challenges, solutions, and future directions. *IEEE Wireless Communications*, *22*(2), 136-144. doi:10.1109/MWC.2015.7096296

Glory Emmanuel-Aviña, Ph.D.
Quantitative Psychologist, Sandia National Laboratories - Livermore

Glory Emmanuel-Aviña is a quantitative psychologist at Sandia National Laboratories, located in Livermore, California. She has a Ph.D. in experimental psychology and an MBA in international management from the University of New Mexico. Emmanuel-Aviña has been at Sandia since 2006 and now leads the Wearables at The Canyon for Health project, which is funded by the Defense Threat Reduction Agency. Her expertise is in human-subjects studies, quantifying the human dimension through experimental design and novel analytics, and managing cognitive load through intelligent web crawling and text analytics.

EMPOWERING THE OF GENOMICS



AC Camacho
& Charles Hong

Genomics is a transformative and data-rich field that has experienced tremendous growth over the past 12 years. With the advent of Next-Generation Sequencing (NGS) platforms in 2005, an exponential amount of data has been generated and deposited into the National Center for Biotechnology Information databases [1]. Genomics provides valuable research opportunities to help describe the function, structure, and evolution of all living organisms. For the Chemical and Biological Defense Program (CBDP), it has provided Department of Defense (DoD) laboratories with a powerful tool that helps characterize biological threat agents and an abundance of information that shapes detection, diagnostics, therapeutics, and prophylaxis capabilities.

In 2003, initial sequencing of the entire human genome cost approximately $2.7 billion [2]. Fifteen years later, what once took billions of dollars to accomplish, now can cost less than $1,000 [3]. Today, valuable data can be generated in a relatively cost-effective manner from numerous sequencing platforms available on the market. A steady and continuous decrease in genome sequencing costs is projected, which may lead to: 1) an overwhelming abundance of data and 2) increased opportunities to utilize NGS to address various research topics in a cost-effective manner [4]. The decrease in genome sequencing costs and the proliferation of

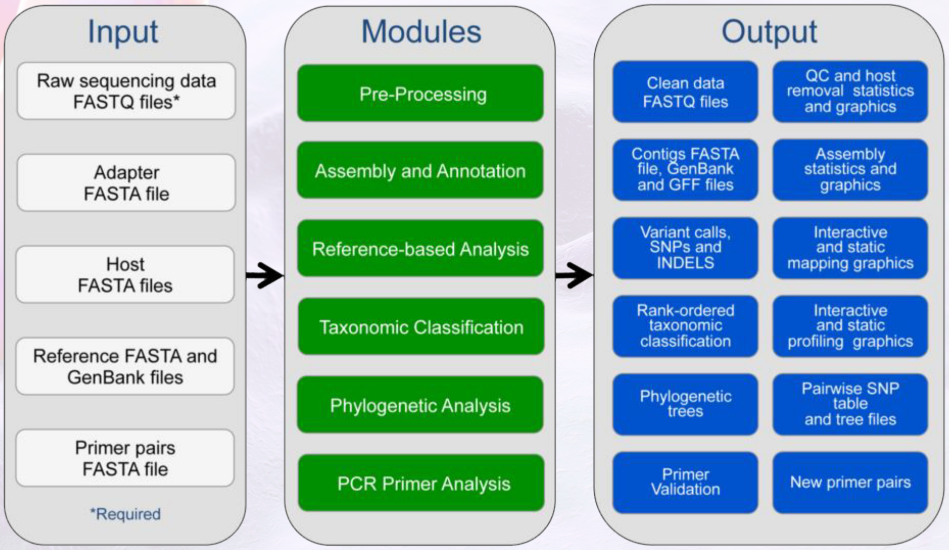

Input
Raw sequencing data FASTQ files*
Adapter FASTA file
Host FASTA files
Reference FASTA and GenBank files
Primer pairs FASTA file
*Required
Modules
Pre-Processing
Assembly and Annotation
Reference-based Analysis
Taxonomic Classification
Phylogenetic Analysis
PCR Primer Analysis
Output
Clean data FASTQ files
QC and host removal statistics and graphics
Contigs FASTA file, GenBank and GFF files
Assembly statistics and graphics
Variant calls, SNPs and INDELS
Interactive and static mapping graphics
Rank-ordered taxonomic classification
Interactive and static profiling graphics
Phylogenetic trees
Pairwise SNP table and tree files
Primer Validation
New primer pairs

Figure 1. An overview of the EDGE Bioinformatics workflow and modules [7]

Image Credit | *Photo Illustration created by HDIAC and adapted from Adobe Stock.*

DEVELOPMENT EXPERTISE

various next generation sequencing technologies show great promise in improving force health protection.

For more than a decade, the DoD CBDP has monitored this trend and invested in utilizing NGS to molecularly characterize biological threat agents that can, in turn, help detect, diagnose, and treat the warfighter [5]. There is an overwhelming amount of genomic data that has been generated by DoD service laboratories, U.S. government agencies, academia, and industry. In fact, it is predicted that genomic data will "be on par with or the most demanding of" big data generators such as astronomy, Twitter, and YouTube, by 2025 [1].

In addition to the sheer amount of data being generated, this NGS data is often not readily actionable or informative as it requires significant analyses and data processing. In order to address this big data challenge, and ultimately best support the warfighter, we must overcome a significant technology gap—how can the U.S. military rapidly analyze all the resulting sequencing data without a team of bioinformaticians?

Empowering the Development of Genomic Expertise (EDGE) Bioinformatics was developed to address the genomic analysis challenge to effectively utilize NGS for the CBDP mission. For example, the ability to quickly analyze genetic data may allow the U.S. military to determine if a warfighter has been exposed to a biological warfare agent; determine whether the causative agent is a virus or bacteria; inform medical countermeasures such as prescribing antibiotics; and provide information on circulating pathogens and infectious diseases in field-forward locations prior to deployment.

Challenges Using NGS

In 2013, DoD began equipping laboratories located in the U.S. and abroad with cutting-edge equipment, such as the Illumina MiSeq next-generation sequencer and server systems, in an effort to improve warfighter protection from biological warfare agents and public health threats. However, the adoption and use of these state-of-the-art NGS technologies have been limited due to numerous complexities involving, but not limited to, sample preparation and workflow bottlenecks associated with genomic analysis. This, coupled with the overwhelming amounts of NGS data generated from a sequencing run, can be a daunting challenge for inexperienced users or those that lack significant bioinformatic training. The U.S. military is not immune to the shortage of bioinformaticians, making the rapid adoption of cutting-edge diagnostic equipment even more difficult [6].

Solving the Big Data Analysis Challenge

To readily address the analysis bottleneck issues, the Joint Science and Technology Office (JSTO) at the Defense Threat Reduction Agency (DTRA) has collaborated with Los Alamos National Laboratory (LANL) and the Biological Defense Research Directorate at the Naval Medical Research Center to

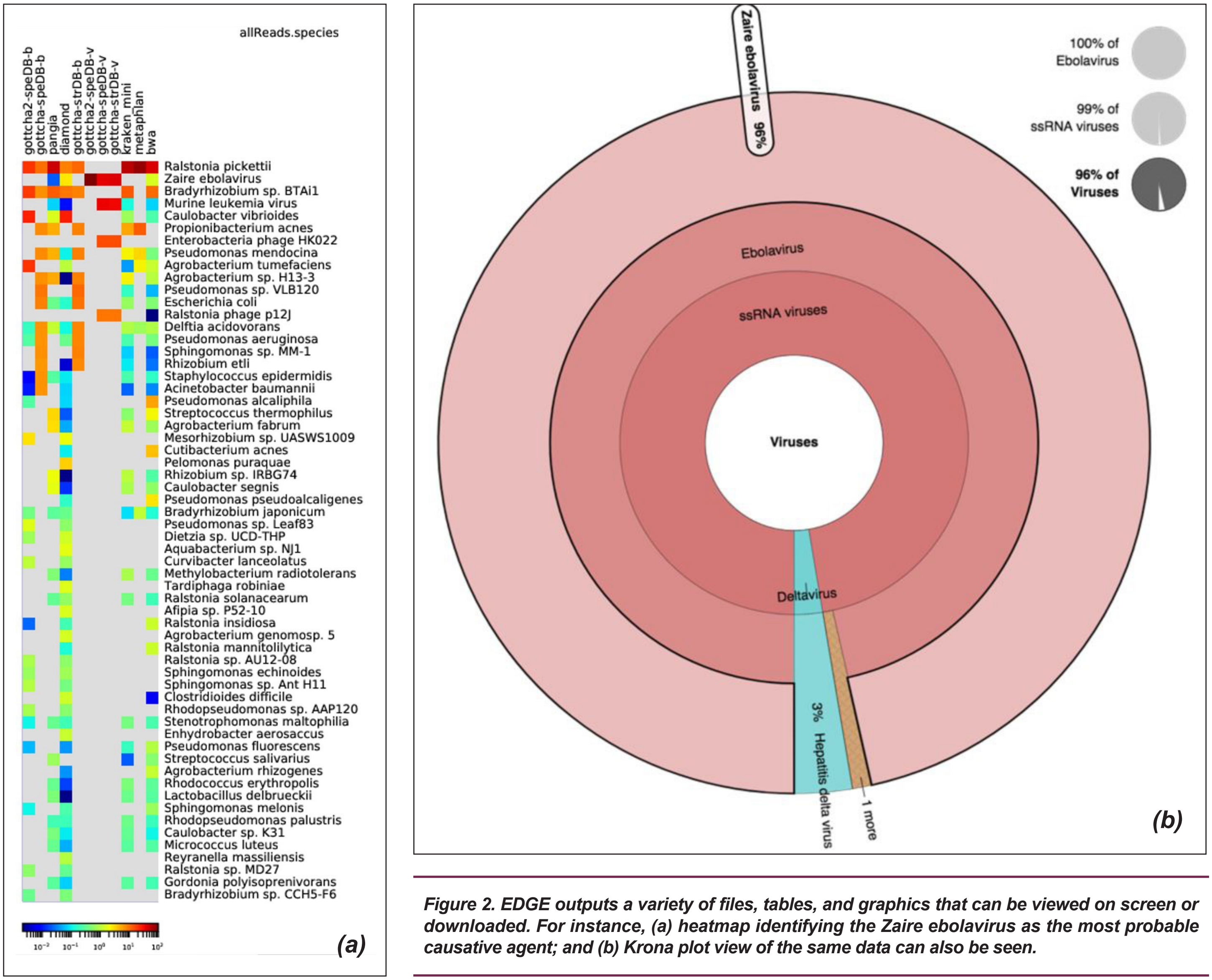


Figure 2. EDGE outputs a variety of files, tables, and graphics that can be viewed on screen or downloaded. For instance, (a) heatmap identifying the Zaire ebolavirus as the most probable causative agent; and (b) Krona plot view of the same data can also be seen.

develop and pilot the EDGE Bioinformatics platform. This suite of bioinformatic tools was initially tailored to support the Illumina MiSeq, providing a variety of modular tools that can analyze genomic data generated by various NGS instruments. Specifically, EDGE Bioinformatics can analyze any raw data in the FASTA/FASTQ file format.

EDGE Bioinformatics has pre-configured workflows or modules (see Figure 1) for analyzing genomic data, identifying relevant genes of interest, and creating reports and graphics with an easy-to-use web-interface [7]. The latest version of EDGE (Version 1.5) is built around a collection of more than 50 publicly available open-source software packaged into seven modular workflows: pre-processing; assembly and annotation; reference-based analysis; taxonomic classification; phylogenetic analysis; specialty gene analysis; and polymerase chain reaction primer analysis [7]. An operator can select modules individually or run them in any number of combinations to address particular analysis needs. Specific modules used in the EDGE Bioinformatics suite are dependent on the user's scientific hypotheses and experimental needs. Additional tools and modules can be developed or incorporated to best support the variety of analyses needed for applications across DoD. Many of these applications can be leveraged by other government agencies that have similar scientific questions and require similar bioinformatics solutions.

Bioinformatics can be used to detect virulence factors, determine bacterial strain type, combat the emerging threat of antimicrobial resistance, and identify dangerous pathogens [8]. EDGE Bioinformatics relies on several modules, which have numerous tools within each to readily analyze and make sense of the wealth of data. One popular module within the EDGE Bioinformatics suite is the taxonomic classification module, which currently uses numerous taxonomy tools such as Genomic Origins Through Taxonomic CHAllenge (GOTTCHA) to help identify biological organisms such as pathogens in environmental and/or clinical samples using sequencing data.

GOTTCHA was designed by LANL researchers (developers of the EDGE Bioinformatics suite) to detect and classify microbes present from a mixed metagenomic sample [9]. In addition to GOTTCHA, EDGE Bioinformatics allows the user to utilize and compare other alternative taxonomy tools (e.g., Kraken, BWA, DIAMOND, etc.) (see Figure 2a). The user may gain confidence in the reliability of his/her results because multiple tools yield the same output (although based on different algorithms).

Taxonomy tools such as GOTTCHA can be used to help identify *Bacillus anthracis* from a stool sample or help detect *Francisella tularensis* from air [9]. Alternatively, if the user was also interested in identifying antimicrobial resistance genes or virulence factors, the user would simply use the specialty gene analysis module.

According to the 2015 *National Action Plan for Combating Antibiotic-resistant Bacteria*, antibiotic-resistant bacteria pose an "urgent and serious" threat to both the U.S. and global population [10]. In fact, the DoD was directed to "fund at least one project involving next-generation sequencing technologies or bioinformatics platforms or tools that can be leveraged to improve diagnostics for drug-resistant or multidrug resistant pathogens [10]." EDGE Bioinformatics is addressing this serious threat through the specialty genes analysis module that leverages Short, Better Representative Extract Dataset (ShortBRED) to help identify phylogenetic signatures of antibiotic resistance. ShortBRED is a software tool developed by Harvard University researchers that profiles proteins families of interests from sequencing data [11].

In the specialty gene analysis module, EDGE Bioinformatics can perform either read-based or DNA fragment/contig-based analysis, which the user can easily select to profile protein families associated with antibiotic-resistance or virulence factors (or both) depending on the needs of the user. EDGE Bioinformatics is the first platform designed to allow the user to operate any number of tools (developed by multiple organizations) independently or in parallel using genomic sequencing data.

The only input required from the user is raw sequencing data in the form of a FASTA or FASTQ file, and the EDGE Bioinformatics platform will generate accessible outputs, including text and figures (some featuring user-interactive graphics) [7]. This means no coding experience is required. Instead, a laboratory technician can analyze a sample in as little as minutes to hours (instead of days or weeks) by simply toggling featured options on or off within each module, promptly gaining access to results that can be directly provided to decision-makers. Although EDGE Bioinformatics was designed with non-bioinformaticians in mind, it can easily be customized for use by advanced bioinformaticians with an optional command line interface seen in other platforms such as Galaxy and BaseSpace [12]. These more experienced bioinformaticians can utilize EDGE Bioinformatics to initially run data through the platform and then delve deeper into the NGS data using custom workflows.

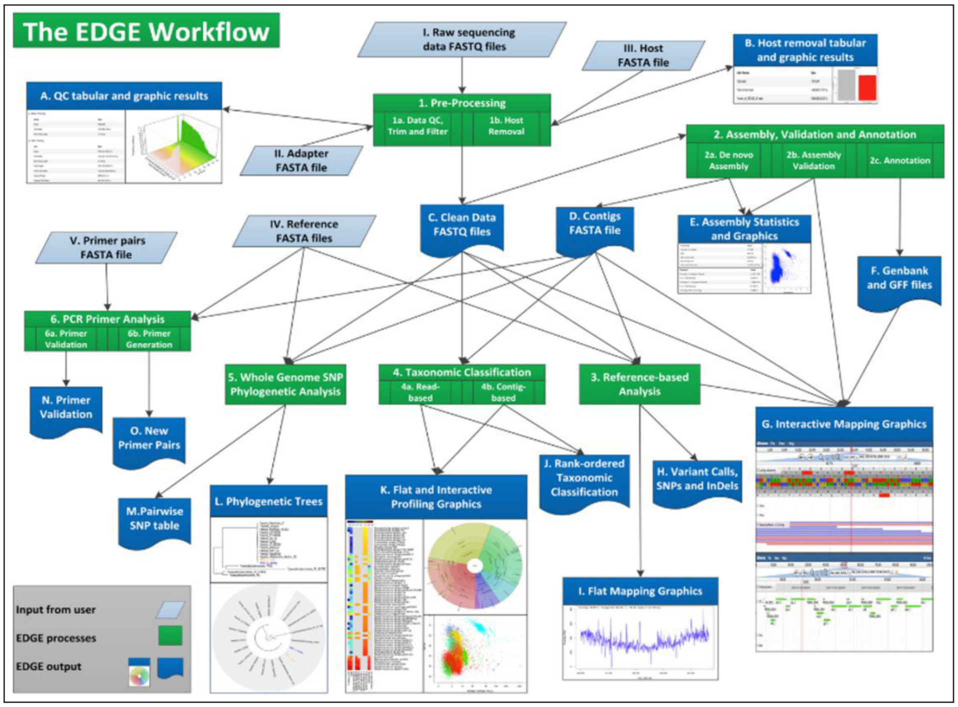

The EDGE Workflow
I. Raw sequencing data FASTQ files
III. Host FASTA file
B. Host removal tabular and graphic results
A. QC tabular and graphic results
1. Pre-Processing
1a. Data QC, Trim and Filter
1b. Host Removal
II. Adapter FASTA file
2. Assembly, Validation and Annotation
2a. De novo Assembly
2b. Assembly Validation
2c. Annotation
V. Primer pairs FASTA file
IV. Reference FASTA files
C. Clean Data FASTQ files
D. Contigs FASTA file
E. Assembly Statistics and Graphics
F. Genbank and GFF files
6. PCR Primer Analysis
6a. Primer Validation
6b. Primer Generation
5. Whole Genome SNP Phylogenetic Analysis
4. Taxonomic Classification
4a. Read-based
4b. Contig-based
3. Reference-based Analysis
G. Interactive Mapping Graphics
N. Primer Validation
O. New Primer Pairs
J. Rank-ordered Taxonomic Classification
H. Variant Calls, SNPs and InDels
M.Pairwise SNP table
L. Phylogenetic Trees
K. Flat and Interactive Profiling Graphics
I. Flat Mapping Graphics
Input from user
EDGE processes
EDGE output

Figure 3. A detailed overview of the EDGE Bioinformatics Version 1 environment

EDGE Bioinformatics 2.0

EDGE Bioinformatics Version 2.0 is currently under research and development and is scheduled to be released in 2019. It will include enhanced versions of tools for taxonomy and phylogeny and will also incorporate tools tailored for transcriptomic studies with ribonucleic acid sequencing (RNA seq) as well as software tools designed by the U.S. Army Medical Research Institute of Infectious Diseases (USAMRIID). These USAMRIID-developed tools will assist with pathogen discovery and develop NGS-based laboratory developed tests. Once Version 2.0 becomes available, JSTO will encourage others to incorporate third party workflows and tools. This will provide ample opportunity for collaboration, serving as a way to crowdsource bioinformatic solutions, overcoming the big data analysis challenge of genomics.

Outside of genomics, EDGE Bioinformatics will begin providing solutions to RNA seq/transcriptomic studies that evaluate gene expression. Studying gene expression allows JSTO and DoD to gain a deeper understanding of cellular functions and processes that may contribute to disease. To readily address and enable these types of research studies, EDGE Bioinformatics developers at LANL are actively working on a tool called Pipeline for Reference-based Transcriptomics (known as PiReT) that will allow researchers to discover and evaluate biomarkers or signatures from host–pathogen interactions. The interplay between host and microbe can provide early indicators/signatures that could in turn prove to be revolutionary in how we diagnose and control diseases [13].

Moving forward, EDGE Bioinformatics will empower the user to incorporate his/her own tools and workflows into the suite. Furthermore, JSTO is investigating the incorporation of tools built for other sequencing platforms in order to accommodate upcoming NGS technologies, such as the Oxford Nanopore Technologies MinION. Eventually, a fully functional EDGE Bioinformatics will allow DoD to develop a Food and Drug Administration cleared and approved NGS-based test for clinical use against biological threat agents.

Conclusion

EDGE Bioinformatics was intended for use in DoD laboratories that lack bioinformatics capabilities. However, it is readily being utilized internationally by private industry, health care providers, other government laboratories, and academia. It has been successfully installed in more than 20 DoD and partner-nation laboratories across 11 countries, including a number of Naval Medical Research Units and Centers for Disease Control and Prevention laboratories [12, 14]. DoD is primarily using EDGE Bioinformatics for analyses of microbial genomics and identification of biological threat agents. EDGE Bioinformatics was used to help analyze the sequencing data from the 2014-2016 Ebola Outbreak in West Africa and was more recently used to track diseases such as hantavirus in the Republic of Korea [7, 15]. Ultimately, in order to utilize NGS as a tool to aid medical diagnostics, hardened bioinformatic solutions that readily process and quickly analyze data in a timely fashion will be required. Because of time hindrances, NGS is not yet a premier diagnostic tool but rather a research tool that can provide informative laboratory data that can potentially aid clinicians and influence diagnosis [16]. An accurate medical diagnosis ideally requires a comprehensive amount of information, including patient (i.e., warfighter) history and physical examination and test results.

Future DTRA-JSTO investments regarding host-pathogen interactions will continue to make sequencing a useful research tool that may ultimately aid in the advancement of novel diagnostic capabilities, with the hope that NGS can be used to diagnose ill patients in the future. Until then, EDGE Bioinformatics will continue to be used to help develop diagnostic products and support biological detection capabilities.

References

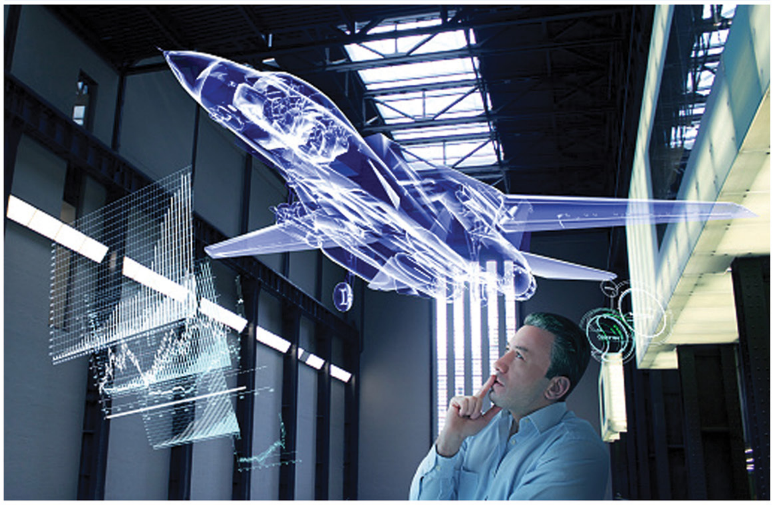
1. Stephens, Z. D., Lee, S. Y., Faghri, F., Campbell, R. H., Zhai, C., Efron, M. J., . . . Robinson, G. E. (2015). Big data: Astronomical or genomical? *PLOS Biology*, *13*(7). doi:10.1371/journal.pbio.1002195
2. Voelkerding, K. V., Dames, S. A., & Durtschi, J. D. (2009). Next-generation sequencing: From basic research to diagnostics. *Clinical Chemistry*, *55*(4), 641-658. doi:10.1373/clinchem.2008.112789
3. van Dijk, E. L., Auger, H., Jaszczyszyn, Y., & Thermes, C. (2014). Ten years of next-generation sequencing technology. *Trends in Genetics*, *30*(9), 418-426. doi:10.1016/j.tig.2014.07.001
4. Buermans, H. P., & den Dunnen, J. T. (2014). Next generation sequencing technology: Advances and applications. *Biochimica et Biophysica Acta (BBA) - Molecular Basis of Disease*, *1842*(10), 1932–1941. doi:10.1016/j.bbadis.2014.06.015
5. Deurenberg, R. H., Bathoorn, E., Chlebowicz, M. A., Couto, N., Ferdous, M., García-Cobos, S., . . . Rossen, J. W. (2017). Application of next generation sequencing in clinical microbiology and infection prevention. *Journal of Biotechnology*, *243*(10), 16-24. doi:10.1016/j.jbiotec.2016.12.022
6. Chang, J. (2015). Core services: Reward bioinformaticians. *Nature*, *520*(7546), 151-152. doi:10.1038/520151a
7. Li, P., Lo, C., Anderson, J. J., Davenport, K. W., Bishop-Lilly, K. A., Xu, Y., . . . Chain, P. S. (2016). Enabling the democratization of the genomics revolution with a fully integrated web-based bioinformatics platform. *Nucleic Acids Research*, *45*(1), 67-80. doi:10.1093/nar/gkw1027
8. Saeb, A. T. (2018). Current bioinformatics resources in combating infectious diseases. *Bioinformation*, *14*(1), 31-35. doi:10.6026/97320630014031
9. Freitas, T. K., Li, P., Scholz, M. B., & Chain, P. S. (2015). Accurate read-based metagenome characterization using a hierarchical suite of unique signatures. *Nucleic Acids Research*, *43*(10). doi:10.1093/nar/gkv180
10. The White House. (2015). National Action Plan for Combating Antibiotic-Resistant Bacteria. Retrieved from https://obamawhitehouse.archives.gov/sites/default/files/docs/-national_action_plan_for_combating_antibotic-resistant_bacteria.pdf
11. Kaminski, J., Gibson, M. K., Franzosa, E. A., Segata, N., Dantas, G., & Huttenhower, C. (2015). High-specificity targeted functional profiling in microbial communities with ShortBRED. *PLoS Computational Biology*, *11*(12). doi:10.1371/journal.pcbi.1004557
12. Perkel, J. M. (2017). How bioinformatics tools are brining genetic analysis to the masses. *Nature*, *543*(7643), 137-138. doi:10.1038/543137a
13. Knights, D., Parfrey, L. W., Zaneveld, J., Lozupone, C., & Knight, R. (2011). Human-associated microbial signatures: Examining their predictive value. *Cell Host Microbe*, *10*(4), 292-296. doi:10.1016/j.chom.2011.09.003
14. Mokashi, V. (2014, March 31). Navy researchers demonstrate bioinformatics capability in Thailand [Web log post]. Retrieved from http://navymedicine.navylive.dodlive.mil/archives/6168
15. Kim, W., No, J. S., Lee, S., Song, D. H., Lee, D., Kim, J., . . . Song, J. (2018). Multiplex PCR−based next-generation sequencing and global diversity of Seoul Virus in humans and rats. *Emerging Infectious Diseases*, *24*(2), 249-257. doi:10.3201/eid2402.171216
16. Lefterova, M. I., Suarez, C. J., Banaei, N., & Pinsky, B. A. (2015). Next-generation sequencing for infectious disease diagnosis and management: A report of the Association for Molecular Pathology. *The Journal of Molecular Diagnostics*, *17*(6), 623-634. doi:10.1016/j.jmoldx.2015.07.004

AC Camacho
Scientist, Engility

AC Camacho is a scientific and technical advisor for Engility supporting the Department of Defense.

Charles Hong
Science and Technology Manager, Defense Threat Reduction Agency

Charles Hong serves as a science and technology manager for the Defense Threat Reduction Agency and Joint Science and Technology Office.



Fungi-Mediated Self-Healing Concrete for Sustainable & Resilient Infrastructure

Congrui Jin, Ph.D.
& Ning Zhang, Ph.D.

Sustainability (durability and reliability that can be affordably maintained) and resiliency (withstanding and rapidly recovering from hazards) are two key characteristics of the American infrastructure system. However, the U.S. is facing critical challenges associated with progressively aging infrastructure. The *2017 Infrastructure Report Card* issued a grade of D+ to the overall condition of the U.S. infrastructure [1].

Bridges are illustrative of poorly maintained infrastructure. Out of the 600,000 bridges in the U.S., 40 percent are 50 years or older and 9 percent were structurally deficient in 2016, but, on average, 188 million trips were made across a structurally deficient bridge each day [1]. Long-term aging and deterioration of structures is not only a sustainability issue but also poses a significant threat to structural resiliency in the event of natural and man-made hazards, such as earthquakes, explosions, and hurricanes.

Recent structural failures and collapses illustrate that the current infrastructure cannot adequately face the broadening range of threats to public structures and facilities. For example, according to the Association of State and Dam Safety Officials, from 2005 to 2013, state dam safety programs reported 173 dam failures and 587 incidents that, without intervention, would likely have resulted in dam failure [2].

In 2013 the White House issued Presidential Policy Directive on Critical Infrastructure Security and Resilience (PPD-21) to advance a national effort to strengthen resilient critical infrastructure [3]. It directed the Department of Homeland Security, Department of Defense (DoD), and other federal agencies to focus research and development activities on maintaining the reliability and resilience of critical infrastructure. Since then, mitigating disasters caused by aging and

Image Credit | *Photo Illustration created by HDIAC and adapted from Adobe Stock.*

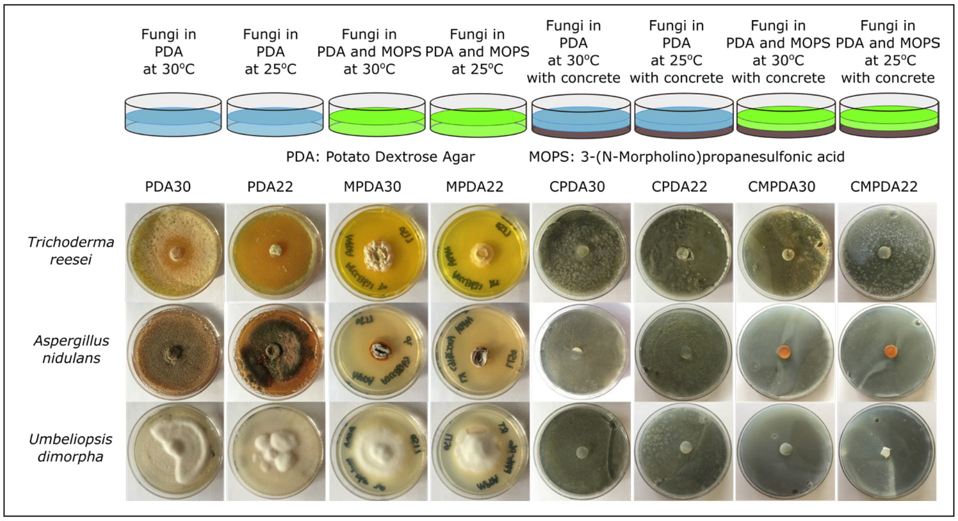

Fungi in PDA at 30°C
Fungi in PDA at 25°C
Fungi in PDA and MOPS at 30°C
Fungi in PDA and MOPS at 25°C
Fungi in PDA at 30°C with concrete
Fungi in PDA at 25°C with concrete
Fungi in PDA and MOPS at 30°C with concrete
Fungi in PDA and MOPS at 25°C with concrete
PDA: Potato Dextrose Agar
MOPS: 3-(N-Morpholino)propanesulfonic acid
PDA30
PDA22
MPDA30
MPDA22
CPDA30
CPDA22
CMPDA30
CMPDA22
Trichoderma reesei
Aspergillus nidulans
Umbeliopsis dimorpha

Figure 1. **T. reesei** ***spores germinated on concrete into hyphal mycelium and grew equally well with or without concrete. In comparison, neither*** **A. nidulans** ***nor*** **U. dimorpha** ***germinates on concrete. Adapted from [9].***

declining infrastructure has become a focus of several federal agencies, including agencies within DoD. For example, the U.S. Army Corps of Engineers (USACE) launched an updated version of its *Resilience Initiative Roadmap* in 2016, which identifies three strategies to evolve resilience, including Strategy 1 that, in part, aims to identify/develop resilience standards and best practices for resilience. Major areas of this strategy aim to ensure reliability, minimize failure, and preserve functionality when conditions change [4].

Concrete infrastructure suffers from significant deterioration and has been a major focus of federal agencies. Concrete is the most widely used construction material, and cracking is very common owing to the effect of various chemical and physical phenomena, including drying shrinkage, alkali-silica reaction, freeze-thaw cycles, reinforcement corrosion, and fatigue. Cracks themselves may not significantly affect the load-carrying capacity of concrete in the short term, but cracks significantly impair durability, as they provide an easy path for the ingress of liquids and gasses that may potentially contain corrosive agents that can degrade steel reinforcements.

A key way to bolster concrete-based critical infrastructure is through the use of state-of-the-art technology, as evidenced by the USACE *Civil Works Strategic Plan 2014-2018*, which supports an "invest[ment] in research that improves the resiliency of structures" [5]. Considering the significant number of concrete structures in the U.S. that require frequent inspection as well as the extensive amount of funding required to fix them, innovative ideas are urgently needed to tackle the concrete infrastructure challenge. Recently, the authors were part of a collaborative research team from Binghamton University and Rutgers University that published work on a new type of concrete that can automatically heal harmful cracks without human interference or intervention.

Background

The concept of self-healing concrete has already been investigated by the federal government for use in critical infrastructure. The Transportation Research Board reviewed uses of engineered nanomaterials in concrete and assessed the mentions of self-healing concrete mechanisms in the literature [6]. To date, self-healing mechanisms in concrete can be divided into three categories: autogenous healing, encapsulation of polymeric material, and microbial production of calcium carbonate precipitation. Autogenous healing is the natural process of concrete crack repair in the presence of water or humidity [7].

However, it is limited to small cracks less than 0.2 mm wide. Encapsulation of polymeric material can fill cracks in concrete by conversion of healing agent to foam in the presence of moisture. Although the chemicals released from incorporated hollow fibers inside concrete can fill the cracks, these materials are not usually compatible with concrete compositions. For example, the filler and the crack may have different mechanical properties and thermal expansion coefficients, and, in some cases, this incompatibility causes the existing cracks to propagate further [8].

Due to the aforementioned limitations, the biological repair technique based on the application of mineral-producing microorganisms has become a viable alternative. It has been demonstrated that in the presence of a calcium source, $CaCO_3$ (as one of the most suitable fillers for concrete cracks owing to the high compatibility with concrete compositions) can be precipitated by bacteria through biologically induced mineralization process. This microbial approach is advantageous over the other self-healing techniques due to superior microcrack-filling capacity, strong bonding between filler and crack, high compatibility with concrete compositions, favorable thermal expansion, and sustainability. It has been found that bacteria can precipitate $CaCO_3$ through many different pathways, such as urea hydrolysis [9], metabolic conversion of organic compound to $CaCO_3$ [10], and dissimilatory nitrate reduction [11]. While general research on bacteria-me-

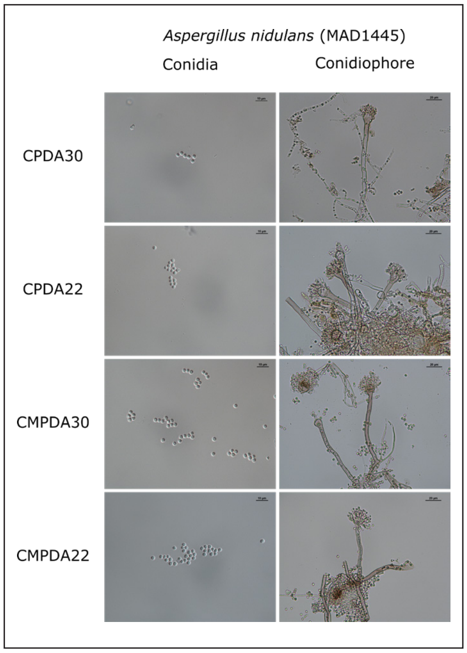
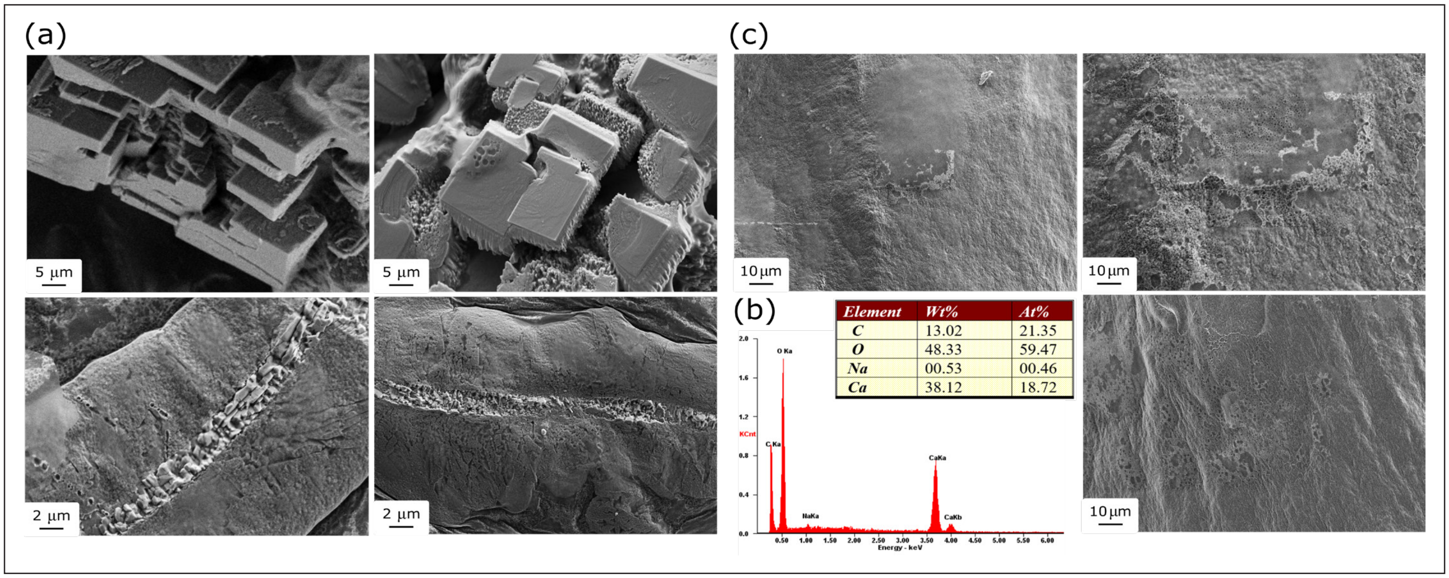


Figure 2. For the case of **A. nidulans** ***(MAD1445), abundant conidia were observed from the plates with concrete, which had similar morphology compared to those produced on the plates without concrete.***



Element	Wt%	At%
C	13.02	21.35
O	48.33	59.47
Na	00.53	00.46
Ca	38.12	18.72

Figure 3. SEM and EDS spectra of the calcium carbonate precipitation: (a) fungi-inoculated medium; (b) EDS spectra; and (c) fungi-free medium. Adapted from [9].

diated, self-healing concrete indeed achieved a certain level of success, there has been little progress in respect to the long-term healing efficacy and in-depth consolidation, mainly due to the limited survivability and calcinogenic ability of the bacteria. Concrete is considered an extreme environment for microbes mainly due to its high pH values. The matrix of young concrete is typically characterized by pH values between 11 and 13 due to the formation of $Ca(OH)_2$, which is, after calcium-silica-hydrate, quantitatively the most important hydration product. Other harsh conditions include severe moisture deficit, varied temperatures, and limited nutrient availability, which often dramatically influence the microbial metabolic activities that could lead to bacterial death. Further investigation into alternative microorganisms for the application of self-healing concrete is necessary.

Fungi-Mediated Self-Healing Concrete

The research team from Binghamton University and Rutgers University recently explored a revolutionary self-healing approach in which fungi are used to promote calcium mineral precipitation to heal cracks in concrete infrastructure [12]. It is widely believed that filamentous fungi possess distinct advantages over other microbial groups for use as biosorbent materials to attract and hold metal ions because of superior wall-binding capacity and extraordinary metal-uptake capability [13]. Although the exact mechanisms accounting for calcium mineralization by fungi are not completely understood, it has been concluded that fungal metabolic activities can influence two factors, carbonate alkalinity and Ca^{2+} concentration, which are critical for the precipitation of $CaCO_3$ [14].

Typical fungal metabolic activities that can decrease alkalinity are heterotrophic respiration leading to an increase in pCO_2, production of organic acids, and excretion of H^+ during fungal thigmotropism. On the contrary, water consumption, physicochemical degassing of fungal respired CO_2, organic acid oxidation, nitrate assimilation, and urea mineralization can increase alkalinity. Ca^{2+} concentration within metabolically active fungal cells should be under strict control. For example, Ca^{2+} must be concentrated at the apex for proper apical growth and instantly decreased in subapical regions. To keep Ca^{2+} concentration in the cytoplasm at low levels, fungi need to actively pump it out of the cell or bind it onto cytoplasmic proteins.

Fungi may also be used through organomineralization. Fungi have chitin in their cell walls, which is a substrate that significantly reduces the required activation energy for nucleus formation so that the interfacial energy between the fungi and the mineral crystal becomes lower than the one between the mineral crystal and the solution. Thus, cation binding by fungi can occur by means of metabolism-independent binding of ions onto cell walls, which is an important passive property of both living and dead fungal biomass, leading to nucleation and deposition of mineral phases. Bound Ca^{2+} can interact with soluble CO_3^{2-}, leading to $CaCO_3$ deposition on the fungal hyphae. High concentrations of Ca^{2+} and CO_3^{2-} in solution are likely to represent a stress for fungal cells owing to subsequent osmotic pressure and Ca^{2+} cytotoxicity. The formation of $CaCO_3$ has been suggested as a strategy to immobilize excessive Ca^{2+}. Excessive alkalinity could also represent a source of stress, and precipitation of $CaCO_3$ may be due to intracellular protection.

Methodology

The following three criteria were used by the researchers to select candidate fungi: 1) organisms should be eco-friendly and nonpathogenic (pose no risk to human health and be appropriate for use in concrete infrastructure), and 2) fungi added to the concrete mixture do not only have to resist mechanical stresses due to mixing but should also be able to withstand a high alkalinity for prolonged periods. Therefore, most promising fungal agents appear to be alkaliphilic spore-forming fungi. The fungal spores, together with nutrients, can be added into concrete during the mixing process. When cracks appear and water finds its way in, the dormant fungal spores will germinate, grow,

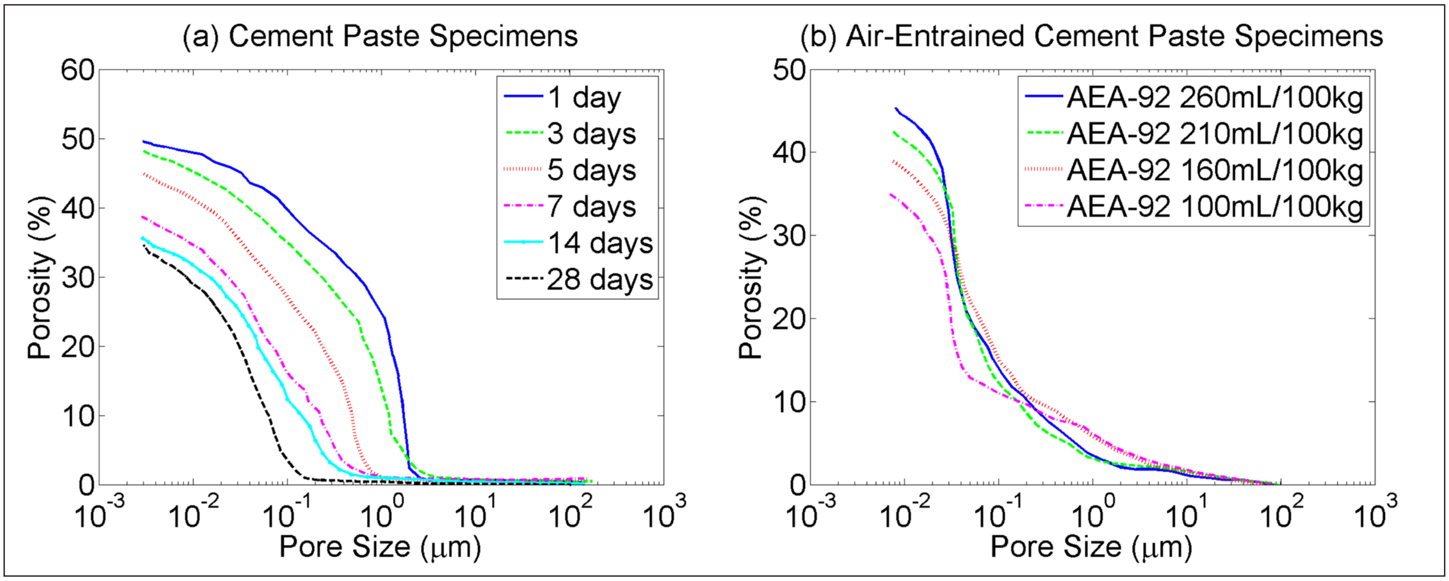


Figure 4. (a) Pore size of cement paste specimens with different curing time prepared with a water-to-cement weight ratio of 0.5 measured by MIP tests. (b) Effect of the amount of air-entraining agent on pore size of cement paste specimens prepared with a water-to-cement weight ratio of 0.5 cured for 28 days. Adapted from [9].

and precipitate $CaCO_3$ to *in situ* heal the cracks. When the cracks are completely filled and, ultimately, no more water can enter, the fungi will again form spores. As the environmental conditions become favorable in later stages, the spores could reawaken. 3) It is preferred that the genomes of the fungi have been sequenced and are publicly available so they can be genetically manipulated to enhance crack repair performance.

Along with the wild-type strains, a large range of mutants that are affected in a variety of metabolic pathways will also be tested. Because only a few fungi can handle the high pH of a concrete environment, pH regulatory mutants will be the focus. It is well known that many microorganisms can tailor gene expression to the pH of the growth environment if they are able to grow over a wide pH range [15]. Irrespective of ambient pH, a type of alkalinity-mimicking mutations believe they are always at alkaline pH and trigger a pattern of gene expression similar to that in the wild type grown under alkaline conditions [15], which is exactly what is needed for the application of self-healing concrete.

Besides genetically engineered fungi, alkaliphilic fungi is also found in nature. Through their evolution over millions of years, fungi have developed different primary strategies to survive and prosper in various environments. Many species of fungi can grow in alkaline environments where the pH value can often be 10 [16]. The research team conducted field collections at the New Jersey Pine Barrens and the Rocky Mountains of Alberta (Canada), as the soils in these regions are alkaline and have low nutrient-holding capacities. However, the habitats still support numerous species that have adapted to the harsh environment. The fungal species isolated from the roots of plants that grew in those regions were tested for the application of self-healing concrete.

A wide screening of different species of fungi has been conducted by the research team. *Pseudophialophora magnispora, Saccharomyces cerevisiae, Acidomelania panicicola, Trichoderma virens,* and *Umbeliopsis dimorpha* were isolated from natural low-nutrient harsh environments. *Rhizopus oryzae, Phanerochaete chrysosporium, Aspergillus nidulans, A. terreus, A. oryzae,* and *T. reesei* were purchased from the American Type Culture Collection, and three different types of alkalinity-mimicking mutants of *A. nidulans* (MAD1445, MAD0305, and MAD0306) were provided by Miguel Penalva's research group at the Biological Research Center of the Spanish National Research Council.

A series of mortar specimens were prepared and then poured into the petri dishes. Fungal spores suspended homogenously in growth medium were overlaid onto the cured concrete and incubated for three weeks. Results showed that, due to the leaching of $Ca(OH)_2$ from concrete, the pH of the growth medium increased dramatically from its original value of 6.5 to 13.0. Of all the fungi tested, only *T. reesei* (as shown in Figure 1) and the three alkalinity-mimicking mutants of *A. nidulans*, (shown in Figure 2) could survive this environment. Despite the pH increase, their spores germinated into hyphal mycelium and grew equally well with or without concrete.

The precipitation of crystalline calcite on the fungal hyphae was confirmed by X-ray diffraction (XRD) and scanning electron microscope (SEM). The SEM images are shown in Figure 3. A large amount of mineral crystals were observed in the fungi-inoculated medium. Wire-shaped traces having an average thickness of 2 μm were found on the surface of the minerals, which presumably occurred in the space occupied by the fungi. Energy-dispersive X-ray spectrometer (EDS) analysis demonstrated that the crystal is composed solely of calcium carbonate. In contrast to the fungi-inoculated medium, the amount of formed crystals in the fungi-free control medium was much less.

The research team proposed that air-entraining agents could be utilized to create extra air voids in the concrete matrix to facilitate the housing of the fungal spores. As measured by using the mercury intrusion porosimetry (MIP) method, the matrix pore diameter sizes in 28-day cured specimens decreased to less than 0.1 μm, as shown in Figure 4(a), which cannot accommodate fungal spores with typical diameters larger than 3 μm.

If the healing agents are put directly into cement paste specimens, the majority of spores will be squeezed and crushed due to the pore shrinkage during the hydration process, leading to loss of viability and decreased mineral-forming capacity. The matrix pore diameter sizes in 28-day cured air-entrained specimens are shown in Figure 4(b). As the amount of air-entrained agents increases, the amount of entrained air voids also increases.

Conclusion

The use of biological systems as self-healing materials is currently of key interest to DoD. The Defense Advanced Research Projects Agency launched the Engineered Living Materials program in 2016 to pursue research in this area, and the expectations of this program are "to develop design tools and methods that enable the engineering of structural features into cellular systems that function as living materials, thereby opening up a new design space for building technology [17]." Although the research is still in its initial stage, if successful, it will result in sustainable and resilient infrastructure that continually repairs itself eliminating the need for costly, onerous human labor.

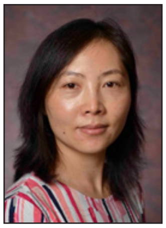
Recommendations for future research include: 1) a wider screening of different species of fungi in variable environmental conditions for biogenic crack repair (e.g., serpentine barrens, soda lakes, desert soils, and alkaline springs), 2) a series of modern micro-characterization techniques to study the fungi-mineral and concrete-precipitate interfaces at the micro-/nano-scale (to include SEM, traditional transmission electron microscope (TEM), Cryo-SEM, Cryo-TEM, liquid-cell TEM, *in situ* XRD, and atomic force microscope), 3) a wider screening of fungi-protecting materials, and 4) an evaluation of the self-healing capacity through standard mechanical and water permeability testing as well as high-resolution X-ray computed microtomography.

References

1. American Society of Civil Engineers. (2017). 2017 Infrastructure Report Card. Retrieved from http://www.infrastructurereportcard.org
2. Association of State Dam Safety Officials. (n.d.). Failures and incidents at dams. Retrieved from http://damsafety.org/dam-failures
3. The White House, Office of the Press Secretary. (2013, February 12). *Presidential Policy Directive -- Critical Infrastructure Security and Resilience* [Press release]. Retrieved from https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil
4. U.S. Army Corps of Engineers. (2017, October 16). *2016 U.S. Army Corps of Engineers Resilience Initiative Roadmap* (Rep. No. EP 1100-1-2). Retrieved from http://www.publications.usace.army.mil/Portals/76/Publications/EngineerPamphlets/EP_1100-1-2.pdf?ver=2017-11-02-082317-943
5. U.S. Army Corps of Engineers. (2014, December 31). *Sustainable solutions to America's water resource needs: Civil Works strategic plan 2014-2018* (Rep. No. EP 1165-2-503). Retrieved from http://cdm16021.contentdm.oclc.org/utils/getfile/collection/p16021coll9/id/61
6. Birgisson, B., Mukhopadhyay, A. K., Geary, G., Khan, M., & Sobolev, K. (2012, December). Nanotechnology in concrete materials: A synopsis (Transportation Research Circular E-C170). Retrieved http://onlinepubs.trb.org/onlinepubs/circulars/ec170.pdf
7. Edvardsen, C. (1999). Water permeability and autogenous healing of cracks in concrete. *Materials Journal*, *96*(4), 448-454. Retrieved from http://www.concrete.org/publications/internationalccreteabstractsportal/m/details/id/645
8. Dry, C. (1994). Matrix cracking repair and filling using active and passive modes for smart timed release of chemicals from fibers into cement matrices. *Smart Materials and Structures*, *3*(2), 118-123. doi:10.1088/0964-1726/3/2/006
9. Stocks-Fischer, S., Galinat, J. K., & Bang, S. S. (1999). Microbiological precipitation of $CaCO_3$. *Soil Biology and Biochemistry*, *31*(11), 1563-1571. doi:10.1016/S0038-0717(99)00082-6
10. Jonkers, H. M., Thijssen, A., Muyzer, G., Copuroglu, O., & Schlangen, E. (2010). Application of bacteria as self-healing agent for the development of sustainable concrete. *Ecological Engineering*, *36*(2), 230-235. doi:10.1016/j.ecoleng.2008.12.036
11. Erşan, Y. Ç., Belie, N. D., & Boon, N. (2015). Microbially induced CaCO3 precipitation through denitrification: An optimization study in minimal nutrient environment. *Biochemical Engineering Journal*, *101*, 108-118. doi:10.1016/j.bej.2015.05.006
12. Luo, J., Chen, X., Crump, J., Zhou, H., Davies, D. G., Zhou, G., . . . Jin, C. (2018). Interactions of fungi with concrete: Significant importance for bio-based self-healing concrete. *Construction and Building Materials*, *164*(10), 275-285. doi:10.1016/j.conbuildmat.2017.12.233
13. Volesky, B., & Holan, Z. R. (1995). Biosorption of heavy metals. *Biotechnology Progress*, *11*(3), 235-250. doi:10.1021/bp00033a001
14. Bindschedler, S., Cailleau, G., & Verrecchia, E. (2016). Role of fungi in the biomineralization of calcite. *Minerals*, *6*(2), 41. doi:10.3390/min6020041
15. Penalva, M. A., & Arst, H. N. (2002). Regulation of gene expression by ambient pH in filamentous fungi and yeasts. *Microbiology and Molecular Biology Reviews*, *66*(3), 426-446. doi:10.1128/mmbr.66.3.426-446.2002
16. Magan, N. (2007) Fungi in Extreme Environments. In *Environmental and Microbial Relationships* (Vol. 4, pp. 85-103). Springer-Verlag Berlin Heidelberg.
17. DARPA. (2016). Engineered Living Materials (ELM) Proposers Day - August 26, 2016. Retrieved from https://www.eiseverywhere.com/ehome/193277

Congrui Jin, Ph.D.
Assistant Professor, Department of Mechanical Engineering, Materials Science and Engineering Program, Binghamton University

Congrui Jin is an assistant professor in the Department of Mechanical Engineering at Binghamton University (Ph.D., Cornell University; M.S., University of Alberta, Edmonton, Canada). Prior to joining Binghamton University, she was a postdoctoral scientist in the Materials Science and Technology Division at Oak Ridge National Laboratory and then the Department of Civil Engineering at Northwestern University. Her research interests include concrete structures, fracture mechanics, and computational mechanics.



Ning Zhang, Ph.D.
Associate Professor, Department of Plant Biology & Department of Biochemistry and Microbiology, Rutgers University

Ning Zhang joined the Rutgers University faculty in 2009. She is an associate professor in fungal biology and works on molecular fungal biodiversity and systematics (Ph.D., Louisiana State University; M.S., Chinese Academy of Sciences). Zhang was previously a postdoctoral scientist at Pennsylvania State University and Cornell University. She has published more than 60 papers in peer-reviewed journals in these research areas and four invited book chapters on fungal systematics, biodiversity, and genomics.

NEAR REAL-TIME BEHAVIORAL ANALYSIS FOR THREAT DETECTION

Brian R. W. Baucom, Ph.D., Panayiotis Georgiou, Ph.D., & Dr. Craig J. Bryan, ABPP

Accurate and timely identification of military personnel who have a high likelihood of engaging in destructive behaviors is crucial in order to support continued military health and readiness. In the wake of the 2009 Fort Hood shooting, an independent review board established by the Department of Defense (DoD) identified the development of behavioral risk assessment tools as an area of pressing need to protect forces at home and abroad [1].

Studies of settings with high risk for interpersonal conflict, such as those with high levels of physical crowding, high levels of social and sensory monotony, and low levels of privacy/control of physical space (e.g., forward deployed areas, open-bay barracks, space, and other isolated areas such as Antarctica [2,3]), echo the need for rapid and precise behavioral risk assessment tools.

To ensure efficiency, systems designed to assess the risk of destructive behavior (e.g., illicit drug use, harm to self, and violence toward others) must achieve the following tasks.

1. Separate higher-risk individuals from lower-risk individuals

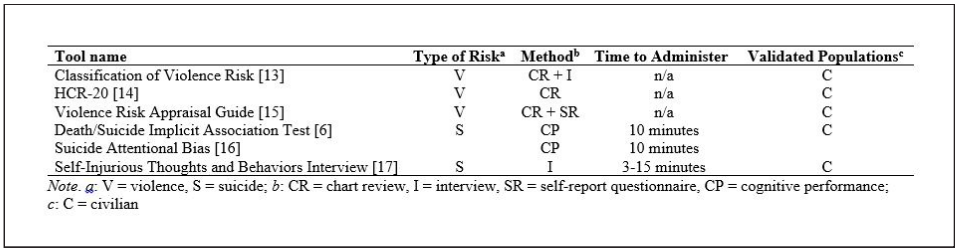
2. Identify periods of particularly heightened risk (i.e., periods of imminent risk that may or may not be anticipated)

3. Quickly adapt to the changing nature and form of destructive behaviors as culture and technology evolve

Existing methods of behavioral risk assessment (see Table 1), including those developed after the DoD independent review, place overwhelming focus on detecting static risk factors to discriminate

Image Credit | *Photo Illustration created by HDIAC and adapted from Adobe Stock and photo of a USAF psychologist (Available for viewing at http://www.militaryonesource.mil/-/does-receiving-psychological-health-care-affect-security-clearance-?inheritRedirect=true)*

between high-risk and low-risk individuals. The utility of these methods is limited by: low-to-moderate levels of sensitivity and specificity [4, 5]; an unknown ability to determine how soon a higher risk individual is likely to engage in an act of destructive behavior; and, in the case of clinical interviews and chart reviews, the requirement of a specially trained assessor [6].



Tool name	Type of Risk[a]	Method[b]	Time to Administer	Validated Populations[c]
Classification of Violence Risk [13]	V	CR + I	n/a	C
HCR-20 [14]	V	CR	n/a	C
Violence Risk Appraisal Guide [15]	V	CR + SR	n/a	C
Death/Suicide Implicit Association Test [6]	S	CP	10 minutes	C
Suicide Attentional Bias [16]		CP	10 minutes	
Self-Injurious Thoughts and Behaviors Interview [17]	S	I	3-15 minutes	C

Note. a: V = violence, S = suicide; *b*: CR = chart review, I = interview, SR = self-report questionnaire, CP = cognitive performance; *c*: C = civilian

Table 1. Summary of common risk assessment tools [6, 13-17]

Behavioral Signal Processing

An effective system for assessing destructive behavior is known as Behavioral Signal Processing (BSP) [7]—a technologically facilitated method of analyzing behavior in near real-time using artificial intelligence that is well-suited to this task. BSP was initially developed to detect communication behaviors and affective expressions during structured dyadic interactions, such as interpersonal communication and psychotherapy sessions for substance abuse. It has since been applied to a wide array of behavioral outcomes relevant to military personnel, such as suicide risk assessment.

BSP employs a set of computational techniques for extracting mathematical quantities, referred to as features, from a digital record of behavior that is captured by text, audio, or video recording. Based on these features, BSP assigns a score to an individual. A suite of machine learning techniques indicates the risk for becoming violent. These properties give BSP several advantages over existing risk assessment methods.

1. High ecological validity because it can be used to analyze documentation of behaviors presented by military service members in their routine course of duties (e.g., audio or video recordings of conversations, timing and location of entry and exit logs for rooms and buildings, and text of typed reports)

2. No specific equipment required beyond a method for digitally recording behavior (e.g., audio or video recorders that are already part of the workplace or networked file storage for work products)

3. Can be used to sort individuals into higher and lower risk groups and monitor changes in risk for engaging in destructive behavior, as well as engagement in new or different destructive behaviors

In addition to potentially identifying individuals who are at higher risk, BSP may detect when there is an increased risk—all without interrupting their routine duties or requiring additional assessment tasks. BSP achieves this through a series of steps that include data acquisition, data processing, computational modeling, and predicting the level of risk for engaging in destructive behavior(s). Behaviors of interest are defined to include any action taken by or communication performed by a person, including interactions between people and machines or other non-living entities. GPS logs from cars, work emails, and audio recordings of performance review meetings could all be incorporated into BSP analysis.

The data processing step of BSP involves substeps and is dependent on the modality of the data. Figure 1 depicts the substeps involved in processing audio of a conversation and preparing it for acoustic and linguistic feature extraction, which include cleaning the audio by removing noise (parts of the digital record that are not related to an action taken by or communication made by a person); determining who is speaking and when; and generating a transcript.

Similar principles are involved when processing other modalities of data, such as cleaning and grouping the data and identifying actors. It should be noted, the primary difference between processing audio recordings and other modalities of data is the algorithms used.

Following these steps, features are extracted from the acoustic and linguistic data using modality-specific algorithms. Algorithms used to extract features from the acoustic data are referred to as speech signal processing methods, which quantify both the spectral and temporal aspect of sound. Prosodic features are a subset of spectral features that quantify the tune and rhythm of a sound. Generally, prosodic features have perceptual correlates. For example, fundamental frequency (f0) refers to the lowest frequency harmonic of the speech sound wave and is highly correlated with the perceived pitch of a sound. Higher f0 corresponds to higher perceived pitch. Thousands of acoustic features can be extracted from each second of sound, which ensures a thorough, precise mathematical description of the manner and tone in which something is said.

Algorithms used to extract features from linguistic data are referred to as natural language processing techniques. Linguistic features characterize semantic aspects and syntactic aspects of the words used. Semantic features vary in terms of whether those characterizations are abstract or concrete. For example, topic modeling can be used to determine the themes discussed. This abstract characterization of semantic meaning can be used to summarize large corpora of text with a high degree of flexibility. However, the results are not necessarily readily interpretable.

On the other extreme, n-grams can be used to characterize the frequency of specific words (uni-grams) or phrases (bi-grams for two word sequences). This kind of concrete characterization can be used to summarize specific words and phrases that are identified a priori into highly interpretable metrics but it is much less flexible than more abstract representations.

A combination of concrete and abstract semantic features maximizes the flexibility and interpretability of the feature set and is advisable. For example, topic modeling of the transcript of a conversation between two service members might identify themes of aggression and substance use. These themes may not be of concern in and of themselves if the aggressive language is

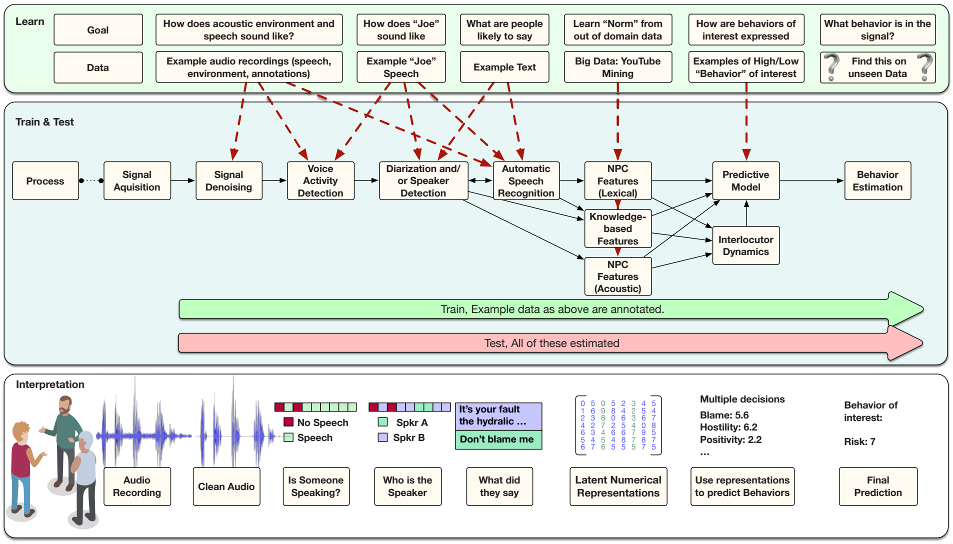

Learn
Goal
How does acoustic environment and speech sound like?
How does "Joe" sound like
What are people likely to say
Learn "Norm" from out of domain data
How are behaviors of interest expressed
What behavior is in the signal?
Data
Example audio recordings (speech, environment, annotations)
Example "Joe" Speech
Example Text
Big Data: YouTube Mining
Examples of High/Low "Behavior" of interest
Find this on unseen Data
Train & Test
Process
Signal Aquisition
Signal Denoising
Voice Activity Detection
Diarization and/ or Speaker Detection
Automatic Speech Recognition
NPC Features (Lexical)
Knowledge-based Features
NPC Features (Acoustic)
Predictive Model
Interlocutor Dynamics
Behavior Estimation
Train, Example data as above are annotated.
Test, All of these estimated
Interpretation
No Speech
Speech
Spkr A
Spkr B
It's your fault the hydralic ...
Don't blame me
Multiple decisions
Blame: 5.6
Hostility: 6.2
Positivity: 2.2
...
Behavior of interest:
Risk: 7
Audio Recording
Clean Audio
Is Someone Speaking?
Who is the Speaker
What did they say
Latent Numerical Representations
Use representations to predict Behaviors
Final Prediction

Figure 1. BSP pipeline

used in reference to sports teams or in a similar context, rather than to other members of their unit.

Similarly, language related to substance use may not be relevant if in reference to cigarette use, but it could be of strong interest if related to illicit substances or heavy alcohol consumption. N-gram processing of the topic modeling results would provide additional, actionable information in cases where leadership can construct lists of keywords and phrases that are of specific interest. For example, if leadership identified slang terms for methamphetamine (e.g., meth, speed, and crank) as being of specific interest, n-gram processing could return a frequency count of the number of times those terms appear in a substance use topic. An increase in that frequency count could be used to identify increased interest in and use of methamphetamine.

It will not always be possible for leadership to provide such keyword lists. Even when it is possible, there is a large amount of additional information present in linguistic features, and features from other modalities, that can help identify service members' level of risk for engaging in destructive behaviors. This information is utilized in the next step, computational modeling.

In the computational modeling step of BSP, features extracted in the previous step are used to estimate the presence versus absence and/or level of a range of cognitive, behavioral, and psychological markers. These markers include anger, impulsivity, boredom, and psychological distress, and they are known (or suspected) to be associated with the risk for engaging in destructive behavior.

The cognitive, behavioral, and psychological markers estimated in this step are indices that must be determined by content matter experts and leadership, as the scores on these markers are estimated using semi-supervised and supervised machine learning approaches, which rely on the availability of data that includes the specific behaviors of interest. These data are referred to the training set and are used to determine the linguistic, acoustic, and other features characteristic of the marker(s) of interest.

Once identified, the similarity of the features in the target data being processed are compared to those in the training set. The more similar the two sets of features, the more likely it is that the data being processed contains the marker(s) of interest.

Using training data in this step has important benefits. It allows the continual updating of cognitive, behavioral, and psychological markers of risk for destructive behaviors, even as knowledge about risk markers and the forms of destructive behavior advances. It also allows for adapting markers of low and high risk for destructive behaviors to the unique social norms and technical terminology of different military bases, theaters, and job requirements.

For example, different training sets could be used for analyzing conversations between two military service members and for analyzing an interaction between a supervisor and a subordinate as compared to an interaction between two peers. This adaptation is important because it allows for distinguishing actions and communications that may be appropriate and expected, from those that are atypical in a particular context from actions and communications that are inappropriate and of concern in all contexts.

This quality is the reason BSP has the potential for significantly greater sensitivity and specificity in predictive accuracy in comparison to chart reviews and structured clinical interviews that assess broad and general tendencies.

In BSP's final step, the risk marker estimates from the computational modeling stage and the raw features from the data processing stage are used in combination to estimate risk for engaging in destructive behaviors. Similar to the computational modeling stage, risk estimates from the final step are generated using machine learning methods. However, in this step, unsupervised and semi-supervised machine learning approaches can be used, whereas supervised and semi-supervised approaches are used in the computational modeling stage.

We can learn in an unsupervised manner by exploiting contextual or multimodal cues. For example, even if the definition of a word is not understood, its use can be observed in context a number of times, which may help to identify its contextual relationship (e.g., "king" is related to "queen" the same way that "man" is related to "woman"). This functions in a manner similar to other forms of association, such as for behavioral association of similar sounding speech.

This method of machine learning can be used to group individuals into categories, presenting similar levels of risk without having to specify all the possible forms of destructive behavior in which they might engage. Semi-supervised methods are based mostly on first-pass estimates from initial models, and then selective use of the output of those methods to train supervised models. This method of machine learning can be used to target risk estimation for specific forms of destructive behaviors that are of particular interest.

Conclusion

BSP is a proven method for the accurate prediction of complex, multiply determined, short- and long-term behavioral outcomes [8-12]. Given the recent successful demonstrations and the ongoing development of the technologies utilized in BSP, it is highly likely they could be effectively adapted to detect individuals who pose a greater risk of engaging in destructive behaviors; identify periods of time when high-risk individuals are particularly likely to engage in destructive behaviors; and measure risk for new forms of destructive behavior as they emerge. Close collaboration between technologists and leadership may enhance the likely success of such an endeavor and be a vital component of introducing these methods to military settings.

References

1. Department of Defense. (2010). *Protecting the force: Lessons from Fort Hood, The Report of the DoD Independent Review* (Rep.). Retrieved https://www.defense.gov/Portals/1/Documents/pubs/DOD-Protecting-TheForce-Web_Security_HR_13Jan10.pdf
2. Applewhite, L. (1994). Prevention measures to reduce psychosocial distress in MFO operations. In, *Peace Operations: Workshop Proceedings* (pp. 47–52). Alexandria, VA: U.S. Army Research Institute for the Behavioral and Social Sciences.
3. Bartone, P. T. (1996). American IFOR experience: Psychological stressors in the early deployment period. In, *Proceedings of the 32nd International Applied Military Psychology Symposium* (pp. 87–97). Brussels, Belgium.
4. Fazel, S., Singh, J. P., Doll, H., & Grann, M. (2012). Use of risk assessment instruments to predict violence and antisocial behaviour in 73 samples involving 24 827 people: Systematic review and meta-analysis. *BMJ*, *345*. doi:10.1136/bmj.e4692
5. Richard-Devantoy, S., Ding, Y., Turecki, G., & Jollant, F. (2016). Attentional bias toward suicide-relevant information in suicide attempters: A cross-sectional study and a meta-analysis. *Journal of Affective Disorders*, *196*, 101-108. doi:10.1016/j.jad.2016.02.046
6. Nock, M. K., Holmberg, E. B., Photos, V. I., & Michel, B. D. (2007). Self-injurious thoughts and behaviors interview: Development, reliability, and validity in an adolescent sample. *Psychological Assessment*, *19*(3).
7. Narayanan, S., & Georgiou, P. G. (2013). Behavioral signal processing: Deriving human behavioral informatics from speech and language. *Proceedings of the IEEE*, *101*(5), 1203-1233. doi:10.1109/jproc.2012.2236291
8. Baucom, B. R., Atkins, D. C., Simpson, L. E., & Christensen, A. (2009). Prediction of response to treatment in a randomized clinical trial of couple therapy: A 2-year follow-up. *Journal of Consulting and Clinical Psychology*, *77*(1), 160-173. doi:10.1037/a0014405
9. Black, M., Katsamanis, N., Baucom, B. R., Lee, C. Lammert, A., Christensen, A., Georgiou, P., & Narayanan, S. (2013). Towards automating a human behavioral coding system for married couples' interactions using acoustic features. *Speech Communication*, *55*(1). doi:10.1016/j.specom.2011.12.003
10. Kliem, S., Weusthoff, S., Hahlweg, K., Baucom, K. J. W., & Baucom, B. R. (2015). Predicting long-term risk for relationship dissolution using nonparametric conditional survival trees. *Journal of Family Psychology*, *29*(6), 807-817. doi:10.1037/fam0000134
11. Lee, C., Katsamanis, A., Black, M. P., Baucom, B. R., Christensen, A., Georgiou, P. G., & Narayanan, S. S. (2014). Computing vocal entrainment: A signal-derived PCA-based quantification with application to affect recognition in married couples' interaction. *Computer Speech and Language*, *28*(2), 518-539. doi:10.1016/j.csl.2012.06.006
12. Nasir, M., Baucom, B. R., Georgiou, P., & Narayanan, S. S. (2017). Predicting couple therapy outcomes based on speech acoustic features. *Plos One*, *12*(9). doi:10.1371/journal.pone.0185123
13. Steadman, H. J., Silver, E., Monahan, J., Appelbaum, P. S., Clark Robbins, P., Mulvey, E. P., ... & Banks, S. (2000). A classification tree approach to the development of actuarial violence risk assessment tools. *Law and Human Behavior*, *24*(1), 83-100.
14. Douglas, K. S., Ogloff, J. R., Nicholls, T. L., & Grant, I. (1999). Assessing risk for violence among psychiatric patients: The HCR-20 violence risk assessment scheme and the Psychopathy Checklist: Screening Version. *Journal of Consulting and Clinical Psychology*, *67*(6), 917-930.
15. Quinsey, V. L., Harris, G. T., Rice, M. E., & Cormier, C. A. (2006). Actuarial Prediction of Violence. In V. L. Quinsey, G. T. Harris, M. E. Rice, & C. A. Cormier, *The law and public policy. Violent offenders: Appraising and managing risk* (pp. 155-196). Washington, DC: American Psychological Association.
16. Cha, C. B., Najmi, S., Park, J. M., Finn, C. T., & Nock, M. K. (2010). Attentional bias toward suicide-related stimuli predicts suicidal behavior. *Journal of Abnormal Psychology*, *119*(3), 616-622. doi:10.1037/a0019710
17. Nock, M. K., Park, J. M., Finn, C. T., Deliberto, T. L., Dour, H. J., & Banaji, M. R. (2010). Measuring the suicidal mind: Implicit cognition predicts suicidal behavior. *Psychological Science*, *21*(4), 511-517. doi:10.1177/0956797610364762

Brian R. W. Baucom, Ph.D.
Assistant Professor of Clinical and Quantitative Psychology, University of Utah

Brian R. W. Baucom is an assistant professor of clinical and quantitative psychology at the University of Utah. His research focuses on behavioral and emotional processes in romantic relationships, cognitive behavioral couple therapies, and the development and application of technology facilitated data acquisition methods as well as computational modeling methods for intensively measured data. His work has been funded by DoD, multiple institutes at the National Institutes of Health, the National Science Foundation, the Volkswagon Foundation, and the Deutsche Forschungsgemeinschaft.

Panayiotis Georgiou, Ph.D.
Assistant Professor in Electrical Engineering and Computer Science, University of Southern California

Panayiotis (Panos) Georgiou is an assistant professor of electrical engineering and computer science at the University of Southern California. He has worked on and published more than 170 papers in fields such as behavioral signal processing, machine learning, statistical signal processing, speech and multimodal signal processing and interfaces, and speech translation. He has been a PI and co-PI on federally funded projects for DoD, Defense Advanced Research Projects Agency, National Science Foundation, National Institutes of Health, etc. His current focus is on behavioral signal processing, multimodal environments, and machine learning for speech applications.

Dr. Craig J. Bryan, ABPP
Executive Director of the National Center for Veterans Studies, University of Utah

Dr. Craig J. Bryan, ABPP, is a board-certified clinical psychologist in cognitive behavioral psychology and is currently the Executive Director of the National Center for Veterans Studies at the University of Utah. Dr. Bryan received his PsyD in clinical psychology in 2006 and served on active duty in the U.S. Air Force until 2009, which included a deployment to Iraq. He has managed numerous federally-funded projects in excess of $20 million, has published ore than 150 scientific articles and several books, and is considered a leading national expert on military and veteran mental health.

Defining the Profile of Potential Cybercriminals

COL Thomas Hyslip, Ph.D. & Thomas J. Holt, Ph.D.

In 2009, when Cyber Command was established as a sub-unified combatant command of the U.S. Strategic Command, a Pentagon spokesman said, “The power to disrupt and destroy, once the sole province of nations, now also rests with small groups and individuals, from terrorist groups to organized crime to industrial spies to hacker activists, to teenage hackers” [1].

On May 4, the Department of Defense (DoD) announced that Cyber Command has been elevated to a unified combatant command, which “demonstrates to international partners and adversaries our stake in cyberspace and shows that DoD is prioritizing efforts to build cyber defense and resilience [2].”

DoD may benefit from studies focused on hackers and cybercriminals who pose a threat to the DoD Information Network and the internet at large. Denial of service attacks may affect field operations and access to resources, prompting DoD to address their potential for harm. This study presents the findings of a survey of a population of potential cybercriminals who conduct distributed denial of service attacks (DDoS) using what are known as booter and stresser services.

A considerable amount of research has focused on DDoS attacks and their underlying infrastructures, such as botnet malware [3-6]. Much of this work has focused on the use of network traffic data to identify and prevent DDoS attacks [7-12]. Consequently, DDoS attack methods and techniques have adapted to overcome the development of new defense and prevention techniques [13]. In fact, attackers are beginning to exploit vulnerabilities in Internet of Things devices, such as webcams, using botnets to enable large-scale DDoS attacks from diverse devices [14].

One type of new DDoS attack uses open internet servers—such as Network Time Protocol (NTP) and Domain Name System (DNS) servers—to “reflect” attacks off them and onto a target [15]. This technique not only masks the Internet Protocol (IP) address of the originating offender(s) but also amplifies the volume of attack traffic [15].

This method of DDoS attack has become very popular [16], and cybercriminals have embraced it, referring to it as either a booter or a stresser [17]. The colloquial name given to these attacks originated with booter because online game players used these attack methods to “boot” their gaming opponents offline by targeting the game server [18,19].

As booters gained popularity and notoriety, the hacking community began to refer to them as stressers because the attacks could be used as a way to stress-test their own web server.

Image Credit | *Photo Illustration created by HDIAC and adapted from Adobe Stock.*

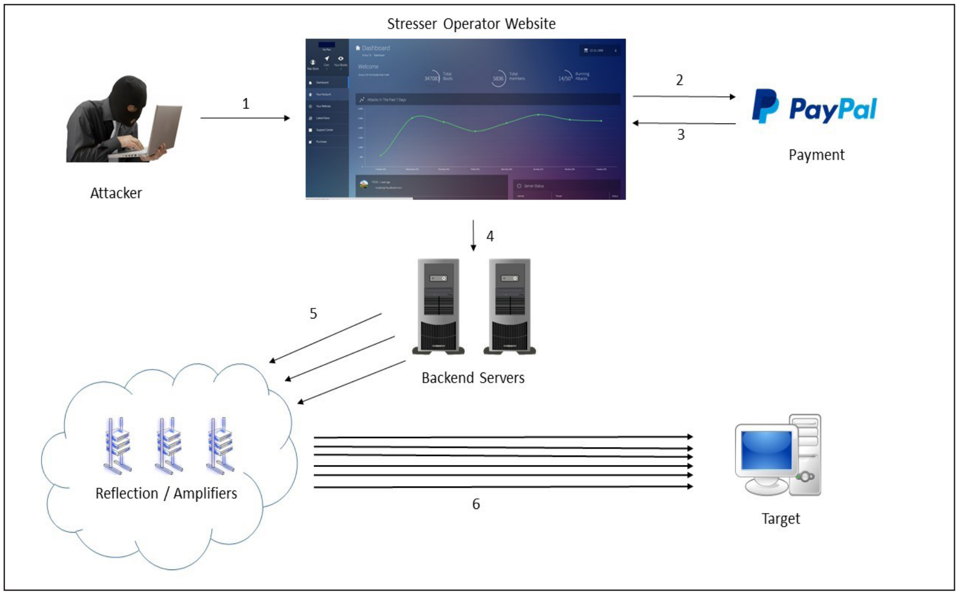


Figure 1. Structure of a Stresser DDoS-for-hire service

Individuals capable of operating these attacks began offering them up for lease on a subscription-fee basis so that customers could launch their own attacks (see Figure 1 for detail). The subscription service allows users with little or no technical skill to launch DDoS attacks by simply entering the IP address or domain name into the stresser website. Furthermore, because there is no restriction on which IP addresses or servers a stresser can target, they have been used to conduct massive DDoS attacks using the reflective technique, contributing to a significant increase in the number of reported DDoS attacks [20].

There are several noteworthy examples of booter and stresser attacks in action. For example, in 2014, the hacking group Lizard Squad attacked Sony's PlayStation Network and Microsoft's Xbox Live with a massive DDoS attack via their new Lizard Stresser, which left users unable to access services for days, resulting in Sony and Microsoft revenue loss [21]. And In 2015, the Bang Stresser was used to attack the BBC website, in what hacktivists claimed to be the largest DDoS attack ever reported, at 602 Gigabits per second (Gbps) [22].

This same method could be used to limit the availability of any critical online service, particularly those within DoD networks that provide real-time or critical connectivity to units within the field [23]. Director of the Defense Information Systems Agency and Commander of the Joint Force Headquarters DoD Information Network Lieutenant General Alan R. Lynn noted the threat to DoD from DDoS attacks and their growing sophistication and size [24]. LTG Lynn stated that as of January 2018, DoD was defending against attacks as high as 600 Gbps on internet access points, and they are preparing for 1 Terabit per second attacks [24].

Previous Research

As stressers gained notoriety, computer science researchers began to focus their efforts on the detection and disruption of stresser services. Multiple studies investigated the strength and capability of stressers by launching and capturing their own attacks [16, 17, 25], while other research efforts analyzed the underlying infrastructure required to carry out DDoS attacks [19, 26-28]. Rossow and Gortz identified 14 User Datagram Protocol (UDP) protocols for amplification attacks and the existence of millions of vulnerable amplification servers. They also measured the amplification factor for the 14 different protocols, recording an increase of 4,000 percent for the NTP protocol [16]. Ryba et al. reported stresser amplification attacks exceeding 400 Gbps, increasing internet latency across Europe [29].

These studies demonstrate that stressers have grown in number, size, and strength since their inception, and that they continue to pose a threat to the internet and its end users. Such technical analyses do not, however, provide insight into the human actors who operate stressers or into the customers who lease their services. To that end, Hutchings and Clayton surveyed a small sample of booter operators to explore how and why they operate these attack services. Booter operators interviewed as part of this research acknowledged that although they presented their offerings as legitimate network stressing services, their resources were mainly used to illicitly attack internet targets [18].

Such preliminary work is useful, but additional insight is needed to better understand the motivations, methods, and background of those who operate and use stresser services. Since booter operations simplify the process of attacks, it is vital to know the technical competencies of their user base and the operators.

Research on hacker subcultures suggests that individuals are judged within the community on the basis of their programming skill and expertise; those with more knowledge are granted elevated social status [30-33]. It is possible that those with greater skill are more likely to operate booter services, although their customers may be equally knowledgeable, simply opting to pay for the service rather than possess and manage the required infrastructure on their own.

Alternatively, booter customers may have relatively low skill, needing to purchase a service because they cannot cultivate it themselves. It is also essential to identify commonly reported attack targets and the rationales behind attacks in order to determine whether customers seek to target their own networks (as the booter advertiser claims) or to attack commercial, government, or military infrastructures. These insights better contextualize the actors who would use a stresser in a real attack.

Furthermore, DoD recognizes that a need exists for greater threat intelligence in cyber defense, and cultural studies of computer criminals helps to fill this gap [34, 35]. Understanding the demographics and motivations of actors may help DoD intelligence agencies identify potential adversaries. At the same time, identifying the attack targets and network protocols used to facilitate attacks can provide threat intelligence to help defend the DoD Information Network [36].

Our Contribution

Early research conducted on booters revealed that the users were primarily online gamers, but subsequent expansions in the use of booters, especially in large DDoS attacks against commercial targets, raises the following questions.

1. Who are the users of stressers?
2. Why do they use stressers (i.e., motivation)?
3. What do they use the stressers for (i.e., target)?

Methodology

We obtained 59,009 publicly available email addresses of registered users from 15 stresser services. An email was sent to each address that included a link to an anonymous survey hosted by Survey Monkey. The first round of emails was sent Nov. 27–29, 2016, and invited recipients to participate in a research study on stressers and booters. The email specified that responses would be used solely for research purposes.

Although the initial sample consisted of 59,009 email addresses, 8,018 of these were not valid based on bounce-back notices. A second email was sent Dec. 2, 2016, as a reminder to complete the survey before its Dec. 30, 2016 closing. Of all messages sent, 5,226 emails were verified as received and opened. This response rate was expected, as the email database was publicly available and included junk/false addresses.

Eight hundred and twenty one individuals began the survey and answered at least one question, resulting in at least 250 responses to each question. This decrease from the total of respondents who had any engagement with a survey question to those who completed it falls within the expected response rate for online survey studies; furthermore, it is a high response rate for an anonymous survey conducted among a population of active offenders [37, 38]. After discounting the 8,018 invalid email addresses, the effective response rate was 1.87 percent (821 of 43,891), which is unsurprising as prior research notes that individuals engaged in cybercrime are less likely to participate in research out of concern for their safety [18, 31, 39]. The nature of the survey may limit generalizability of the data. However, the responses provide essential insight into an underexamined phenomenon.

This sample of individuals, at minimum, had registered an account with a stresser—or may have used a stresser to launch a DDoS attack. Thus, questions were structured to understand the extent to which the respondent both used stresser services and facilitated their operations. The survey consisted of 22 multiple choice questions and one open comment box for follow-up requests. The questions covered the use of stressers and requested information regarding respondent skill level, payment type, attack protocols used, attack targets, motivation for use, and demographic data.

Results

Respondents were asked to provide their demographic characteristics in an attempt to quantify the overall makeup of the population. The majority of respondents reported living within the U.S. or U.K.—in keeping with evidence drawn from law enforcement investigations and arrest records over the last three years.

Respondents who reported their age were primarily in their late teens or 20s, were male (88 percent), and white (63 percent), corresponding to prior research findings on the ages of the hacker population as a whole [18, 32, 40]. The majority of respondents reported an education level beyond that of high school.

Respondents were also asked to rank their skill level from 1 to 10, with 10 being the most skilled. We acknowledge these results may be skewed, as skill level was self-reported. Indeed, the most commonly reported skill level was 10. However, the next most common response was 1, suggesting that most respondents answered in an honest fashion. While it is possible some respondents falsified response(s), such an idea runs counter to the broader empirical literature that indicates hackers prefer to make their abilities known [27, 29].

The overwhelming majority of respondents (89.2 percent) indicated they had used booter services, which makes sense given their addresses were associated with a database of service provider clients. The majority of those who had used a booter (65.2 percent) paid for the service. While a substantial amount of attention has been paid to the use of cryptocurrencies in cybercrime, the majority of respondents paid for stresser services via Paypal—a pattern corroborated by prior research on booters [25]. Cryptocurrencies were used with less frequency than PayPal, and Bitcoin was the most-used cryptocurrency.

Eighty-seven percent of respondents answered in the affirmative when asked, “Were you able to use the booter or stresser to test systems?” The question was written to be less accusatory and used the term "test systems" rather than "attack systems."

Relatedly, there was some distribution of responses related to stress testing systems with 17 percent of respondents (n=232) having stressed only one system, while 47 percent stressed more than 10. Almost half of stresser customers used them to attack multiple computer systems. Additionally, there appears to be limited fidelity within the community, as 29 percent of respondents reported having accounts with more than five vendors, followed by 25 percent having accounts with two stressers.

Interestingly, 74 percent of the respondents noted the booter worked as advertised, which suggests that not all vendors may be accurate in their advertising. While some in the general public may assume there is no trust between criminal actors, it is an important factor in the underground market for cybercrime services. As a result, if a service provider is unable to deliver on an advertised product, it may reduce the overall customer base over time.

The majority of customers used common attack methods, most notably UDP, DNS, and NTP attacks. Other less common methods, such as VSE, RST, and QUIC, were observed but in much smaller numbers. This matches previous research that examined network captures of stresser attacks and supports the notion that stressers utilize different attacks depending on the nature of their target and the reflection servers available to complete the attack [16, 17].

The reported motivations were also varied (as shown in Figure 2). Customers

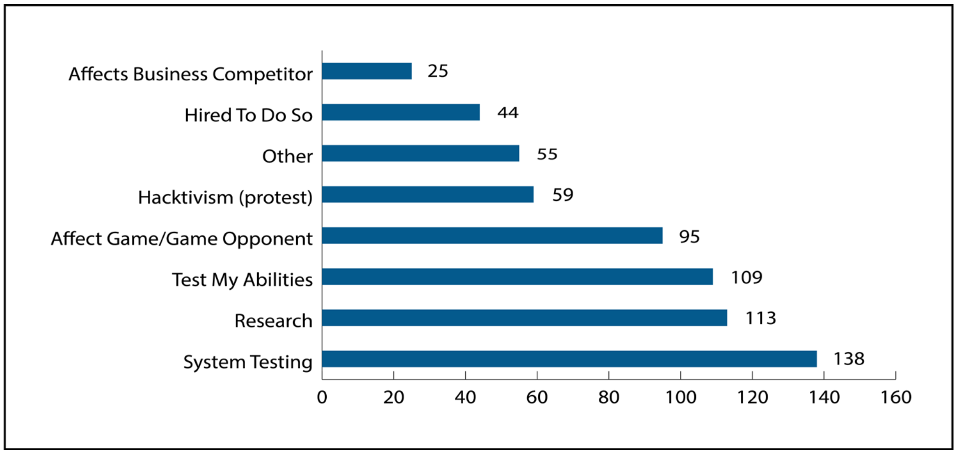


Figure 2. Participant response to, "What was your motivation to use a booter or stresser?"

(n=230) primarily reported using stressors to test their system, conduct research, or test their individual abilities. In addition, 41 percent of respondents used a booter to affect a game or gaming opponent. Such a motive is in keeping with the original use of booter services by hackers [25].

More nefarious motivations were also reported, with 26 percent of respondents reporting they used it for hacktivism or protest. (In this case, hacktivism refers to the use of hacking in support of a specific belief or activist agenda.) Nineteen percent of respondents also noted they were hired by someone else to use the stresser, and 11 percent were motivated to use the stresser to affect a business competitor.

Given that individuals who registered with a service may have done so as an interested client or potential competitor, respondents were asked if they have ever operated their own booter or stresser service. A majority of respondents (54 percent) reported they ran their own operation, suggesting there may be a low barrier to entry to engage in this form of cybercrime-as-service. Additionally, 64 percent of respondents assisted booter operations in some fashion.

Furthermore, 76.4 percent of respondents reported they have been targeted by a stresser operator. This finding supports prior research that suggests hackers may target one another either because of perceived slights or real conflicts between actors [30-32].

When asked what resource they used a stresser against (see Figure 2), the majority of respondents reported either targeting themselves or a game server. More than 52 percent of respondents reported using a stresser to attack a private or commercial website/webserver, and 26 percent reported attacking another type of business server, such as an email or file server. Seventeen percent of respondents reported use of the stresser to attack a government-owned website or webserver [20].

Cross tabulation was used to examine the relationship between attacker motivation and target (see Table 1). The majority who reported targeting themselves were motivated by system testing, research, and the desire to test their abilities. There was a more equal distribution of motives for those targeting game, business, and government servers.

Also, a plurality of respondents who were motivated by hacktivism or protest reported a commercial website as their primary target of attack. Respondents also attacked themselves in order to determine whether their infrastructure could withstand the

What was your motivation?	Yourself	Game	Business Server	Commercial Website	Government Website	Other
Research	27%	17%	13%	20%	9%	13%
System Testing	28%	17%	13%	21%	8%	13%
Affect Game/ Opponent	16%	27%	11%	21%	9%	16%
Hacktivism/ Protest	17%	20%	13%	24%	12%	14%
Affect Business Competitor	15%	18%	17%	19%	14%	17%
Test Abilities	22%	21%	12%	22%	9%	15%
Hired to Do So	19%	18%	17%	19%	12%	15%
Other	17%	18%	13%	21%	9%	22%

Table 1. Attacker motivations versus targets of attack.

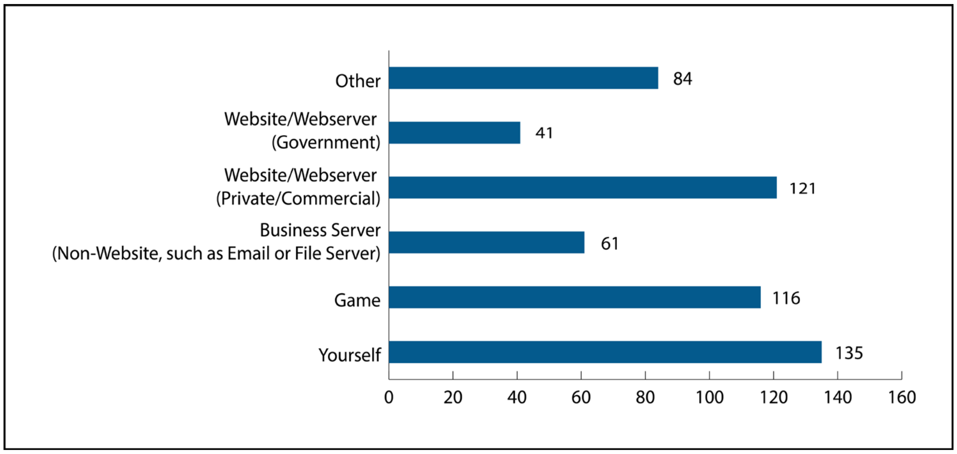


Figure 3. Participant response to, "What did you use the stresser/booter on?"

traffic, which corresponds to the notion that these services can stress-test sites.

Discussion and Conclusion

The rise of booter and stresser services evidences the evolution of cyberthreats and the rise of cybercrime-as-service providers. Although the technical dynamics of these attack types are commonly researched [19, 20], few have examined the characteristics of the clientele of the stresser to understand the human actors behind these attacks [18]. This analysis addresses this issue through a survey delivered to individuals who registered an email address with one or more of 15 select stresser operators. The results of the survey show that most of the respondents reported they are young, white males, which is in keeping with prior research on the hacker community [30-33]. Most of them did not, however, use stressers simply to test their own infrastructure or attack online game opponents [18, 19]. Nearly a quarter of respondents cited hacktivism as their motive when using stressers, and 10 percent tried to affect a business competitor.

This attack type is likely fueled by the ease of access to stressers, the low cost, anonymity, and simplicity of use [18, 24]. This as a potential asymmetric threat that could be used by any potential enemy actor, including those with nation-state sponsorship. Hiring a booter would provide the attacker, and the nation-state, with plausible deniability for the attack as the stresser operator may not know their clientele [18].

It is also clear that criminal actors may seek to leverage the power of a stresser or booter to more effectively target critical infrastructure without the need to cultivate advanced technical skills [23]. Such an attack could originate from an ideologically motivated organization, such as a jihadist group, or those without a specific political agenda, such as the group Anonymous. In fact, over the last decade, members of Anonymous repeatedly utilized large DDoS attacks against commercial and government entities in response to perceived wrongs, including attacks against the National Security Agency and the FBI [41, 42]. Many of these attacks were enabled through Anonymous' stand-alone DDoS tool—the Low Orbit Ion Cannon.

Groups like Anonymous may serve as a template for other attackers, which may partially account for the hundreds of new hacktivist groups established over the last few years [43, 44]. These groups do not hesitate to attack military and government infrastructure and may use stressers as a more effective and inexpensive attack resource [43, 44]. To that end, the number and strength of stressers has grown concurrently with the emergence of new hacktivist groups.

This may create an operational environment where hacktivists do not invest time or resources to build their own tools or develop skills to engage in attacks. Instead, they can quickly and easily launch massive DDoS attacks that are bounced off millions of vulnerable internet servers at a low cost [16]. Thus, additional research is needed to understand the human actors behind large-scale DDoS attacks and their decision-making [18, 23, 30, 31]. Such information can improve our knowledge of the rationale of attackers, which may provide insight into why and how these methods can be used to take down critical infrastructure components.

References

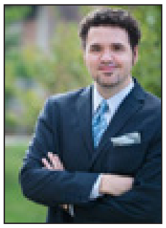
1. Gray, A. (2009, June 23). Pentagon approves creation of cyber command. Reuters. Retrieved from https://www.reuters.com/article/us-usa-pentagon-cyber/pentagon-approves-creation-of-cyber-command-idUSTRE55M78920090624
2. Lange, K. (2018, May 3). Cybercom becomes DoD's 10th unified combatant command [DoD Live web log post]. Retrieved from http://www.dodlive.mil/2018/05/03/cybercom-to-become-dods-10th-unified-combatant-command/
3. Leder, F., Werner, R., & Martini, P. (2009, June). Proactive botnet countermeasures an offensive approach. *Proceedings of the Conference on Cyber Warfare 2009*, Tallinn, Estonia. Retrieved from http://www.ccdcoe.org/publications/virtualbattlefield/15_LEDER_Proactive_Coutnermeasures.pdf
4. Gu, G., Porras, P., Yegneswaran, V., Fong, M., & Lee, W. (2007, August). BotHunter: Detecting malware infection through IDS-driven dialog correlation. *Proceedings of the 16th USENEX Security Symposium*, Boston, MA. Retrieved from https://www.usenix.org/legacy/events/sec07/tech/full_papers/gu/gu.pdf
5. Dittrich, D. (2012, April). So you want to take over a botnet . . . *Proceedings of the 5th USENIX Workshop on Large-Scale Exploits and Emergent Threats, LEET '12*, San Jose, CA. Retrieved from https://www.usenix.org/system/files/conference/leet12/leet12-final23.pdf
6. Zeng, Y. (2012). *On detection of current and next-generation botnets* (Doctoral dissertation). University of Michigan. Retrieved from http://deepblue.lib.umich.edu/handle/2027.42/91382
7. Rossow, C., & Dietrich, C. J. (2013, July). PROVEX: Detecting botnets with encrypted command and control channels. *Detection of Intrusions and Malware, and Vulnerability Assessment Lecture Notes in Computer Science*, 21-40. doi:10.1007/978-3-642-39235-1_2
8. Gu, G., Zhang, J., & Lee, W. (2008, February). BotSinffer: Detecting botnet command and control channels in network traffic. *Proceedings of the 15th Annual Network and Distributed System Security Symposium*, San Diego, CA. Retrieved from http://www.isoc.org/isoc/conferences/ndss/08/proceedings.shtml
9. Feily, M., Shahrestani, A., & Ramadass, S. (2009, June). A survey of botnet and botnet detection. *2009 Third International Conference on Emerging Security Information, Systems and Technologies*, 268-273. doi:10.1109/SECURWARE.2009.48
10. Brezo, F., Santos, I., Bringas, P. G., & Val, J. L. (2011, Aug). Challenges and limitations in current botnet detection. *2011 22nd Inter-*

national Workshop on Database and Expert Systems Applications, 95-101. doi:10.1109/DEXA.2011.19

11. Zhang, J. (2012, August). *Effective and scalable botnet detection in network traffic* (Doctoral dissertation, 2012). Georgia Institute of Technology. Retrieved from ProQuest Dissertations and Theses database. (AAT 1115317916)
12. Lu, C., & Brooks, R. R. (2013). Timing analysis in P2P botnet traffic using probabilistic context-free grammars. *Proceedings of the Eighth Annual Cyber Security and Information Intelligence Research Workshop*, 1-4. doi:10.1145/2459976.2459992
13. Dittrich, D. (2012, April). So you want to take over a botnet. *Proceedings of the 5th USENIX Workshop on Large-Scale Exploits and Emergent Threats*. Retrieved from https://www.usenix.org/system/files/conference/leet12/leet12-final23.pdf
14. European Union Agency for Network and Information Security. (2016, November 3). Major DDoS attacks involving IOT devices. Retrieved from https://www.enisa.europa.eu/publications/info-notes/major-ddos-attacks-involving-iot-devices
15. United States Computer Emergency Readiness Team. (2014, January 17). Alert (TA14-017A): UDP-Based Amplification Attacks. Retrieved from https://www.us-cert.gov/ncas/alerts/TA14-017A
16. Rossow, C. (2014, February). Amplification hell: Revisiting network protocols for DDoS abuse. *Proceedings of the 2014 Network and Distributed System Security (NDSS) Symposium*. doi:10.14722/ndss.2014.23233
17. Hyslip, T., & Holt, T. (2018). Assessing the capacity of DDoS-for-hire services in cybercrime markets. *Deviant Behavior*. Manuscript submitted for publication.
18. Hutchings, A., & Clayton, R. (2016). Exploring the provision of online booter services. *Deviant Behavior*, 37(10), 1163-1178. doi:10.1080/01639625.2016.1169829
19. Karami, M. & McCoy, D. (2013, August). Understanding the emerging threat of DDoS-as-a-Service. USENIX Workshop on Large-Scale Exploits and Emergent Threats, Berkeley, CA. Retreived from https://www.usenix.org/conference/leet13/workshop-program/presentation/karami
20. Arbor Networks (2015, January). *Arbor Networks 10th Annual Worldwide Infrastructure Security Report* Finds 50X Increase in DDoS Attack Size in Past Decade [Press release]. Retrieved from https://www.enhancedonlinenews.com/news/eon/20150127005614/en/Arbor-Networks/Worldwide-Infrastructure-Security-Report/WISR
21. Turnton, W. (2014, December 30). Lizard Squad's Xbox Live, PSN attacks were a 'marketing scheme' for new DDoS service. The Daily Dot. Retrieved from http://www.dailydot.com/crime/lizard-squad-lizard-stresser-ddos-service-psn-xbox-live-sony-microsoft/
22. Whitaker, Z. (2016, January). BBC, Trump web attacks "just the start," says hacktivist group. ZDNet. Retrieved from https://www.zdnet.com/article/attackers-targeting-bbc-donald-trump-amazon-web-services/
23. Denning, D. (2010). Cyber-conflict as an emergent social problem. In T.J. Holt and B. Schell (eds), *Corporate Hacking and Technology-driven Crime: Social Dynamics and Implications* (pp. 170-186). Hershey, PA: IGI-Global
24. Karami, M., Park, Y., & McCoy, D. (2015, August). Stress testing the booters: Understanding and undermining the business of DDoS services. *Proceedings of the 25th International Conference on World Wide Web*, 1033-1043. doi:10.1145/2872427.2883004
25. Schwartz, S. A. (2018, January 17). DOD hit with 36M malicious emails daily, prepares for massive DDoS attack. Retrieved from https://www.ciodive.com/news/dod-hit-with-36m-malicious-emails-daily-prepares-for-massive-ddos-attack/514844/
26. Kovacs, E. (2015, July 1). Attackers abuse RIPv1 protocol for DDoS reflection: Akamai. Security Week. Retrieved from http://www.securityweek.com/attackers-abuse-ripv1-protocol-ddos-reflection-akamai
27. Kravtsov, P. (2015, October 16). A look at the new WordPress brute force amplification attack. Retrieved from https://blog.cloudflare.com/a-look-at-the-new-wordpress-brute-force-amplification-attack/
28. Santanna, J., RiJswijk-Deij, R. V., Hofstede, R., Sperotto, A., Wierbosch, M., Granville, L. Z., & Pras, A. (2015, May). Booters — An analysis of DDoS-as-a-service attacks. *2015 IFIP/IEEE International Symposium on Integrated Network Management (IM)*. doi:10.1109/INM.2015.7140298
29. Ryba, F., Orlinkski, M., Wahlisch, M., Rossow, C., & Schmidt, T. (2016, May). Amplification and DRDoS attack defense - - A survey and new perspectives. Retrieved from https://arxiv.org/abs/1505.07892
30. Bachmann, M. (2010). The risk propensity and rationality of computer hackers. *International Journal of Cyber Criminology*, *4*(1&2), 643-656
31. Holt, T. J. (2007). Subcultural evolution? Examining the influence of on- and off-line experiences on deviant subcultures. *Deviant Behavior*, *28*(2), 171–198. doi:10.1080/01639620601131065
32. Jordan, T., & Taylor, P. (1998). A sociology of hackers. *The Sociological Review*, *46*(4), 757-780. doi:10.1111/1467-954x.00139
33. Steinmetz, K. F. (2016). *Hacked: A Radical Approach to Hacker Culture and Crime*. New York, NY: New York University Press.
34. Pomerleau, M. (2018, January 12). Defensive cyber continues to mature, still lags offensive cyber. Fifth Domain. Retrieved from https://www.fifthdomain.com/dod/cybercom/2018/01/12/defensive-cyber-continues-to-mature-still-lags-offensive-cyber/
35. Pomerleau, M. (2017, June 19). Cyber protection teams need intelligence, say officials. C4ISRNET. Retrieved from https://www.c4isrnet.com/disa/disa-vision-guide/2017/06/19/cyber-protection-teams-need-more-intelligence-say-officials/
36. Pomerleau, M. (2017, June 15). DoD cyber defense arm establishes intel/ops fusion cellC4ISRNET. Retrieved from https://www.c4isrnet.com/disa/disa-vision-guide/2017/06/15/dod-cyber-defense-arm-establishes-intel-ops-fusion-cell/
37. Curtin, R., Presser, S., & Singer, E. (2005). Changes in telephone survey nonresponse over the past quarter century. *Public Opinion Quarterly*, *69*(1), 87-98. doi:10.1093/poq/nfi002
38. Zan, H., & Fan, J. X. (2010). Cohort effects of household expenditures on food away from home. *Journal of Consumer Affairs*, *44*(1), 213-233. doi:10.1111/j.1745-6606.2010.01163.x
39. Pruitt, M. V. (2007). Deviant research: Deception, male internet escorts, and response rates. *Deviant Behavior*, *29*(1), 70-82. doi:10.1080/01639620701457782
40. Greenwood, C. (2017, April 21). How the average age of British hackers is only 17... and they start at 13 with web-connected games consoles. *Daily Mail*. Retrieved from http://www.dailymail.co.uk/news/article-4434526/How-average-age-British-hackers-17.html
41. Harkinson, J. (2012, January 20). How and why Anonymous took down the FBI'swebsite. MotherJones. Retrieved from http://www.motherjones.com/crime-justice/2012/01/inside-anonymous-largest-attack-ever-fbi-megaupload-mega-upload/
42. Sheets, C. A. (2013, October 25). NSA Website down following apparent DDoS attack possibly by Anonymous of a foreign government. International Business Times. Retrieved from http://www.ibtimes.com/nsa-website-down-following-apparent-ddos-attack-possibly-anonymous-or-foreign-government-1442452
43. Lohrmann, D. (2017, February 22). The dramatic rise in hacktivism. Techcrunch. Retrieved from https://techcrunch.com/2017/02/22/the-dramatic-rise-in-hacktivism/
44. Bergal, J. (2017, January 10). Hacktivists launch more cyberattacks against local, state government. PBS. Retrieved from https://www.pbs.org/newshour/nation/hacktivists-launch-cyberattacks-local-state-governments

COL Thomas S. Hyslip, Ph.D.
Adjunct Professor, Norwich University

Thomas S. Hyslip is an adjunct professor in the College of Graduate and Continuing Studies at Norwich University, specializing in cybersecurity, cybercrime, and critical infrastructure protection (Ph.D., Capitol College). Hyslip works full time as federal agent specializing in cybercrime investigations and forensics and is also a Colonel in the U.S. Army Reserve.



Thomas J. Holt, Ph.D.
Professor, Michigan State University

Thomas J. Holt is a professor in the School of Criminal Justice at Michigan State University, specializing in cybercrime, cyberterrorism, and policy responses to these threats (Ph.D., University of Missouri-Saint Louis). His work has appeared in numerous academic journals, including *British Journal of Criminology*, *Crime & Delinquency*, *Deviant Behavior*, and *Terrorism & Political Violence*. He is also the author of multiple books and has presented his work in various academic and practitioner conferences around the world.

Image Credit | *Photo Illustration created by HDIAC and adapted from U.S. Marines Photo by Lance Cpl. Zachery Laning. (available for viewing at http://www.marines.mil/Photos/igphoto/2001753020/).*

COL Barrett K. Parker
& David B. Kang

Recent responses to hurricanes, while never seamless, have been very successful. Even more important than the success of a given response is the validation of processes and relationships. Disaster response planning and exercises are well informed by real world event after action reviews (AARs). Updated information products, such as the Federal Emergency Management Agency's (FEMA) Incident Annexes, have improved awareness and increased fidelity across a wider range of government levels than ever before.

However, it must be noted that the disaster response community's vast amount of recent experience has been across a narrow range of disasters. The "right" response for a hurricane may be inappropriate for another type of disaster. Hurricanes, tornadoes, floods and most of the other types of disasters we have experienced in recent years share a trait—the disasters themselves are relatively short in duration. There is another class of disaster that threatens our homeland which we have not experienced recently—an enduring disaster.

What is an Enduring Disaster?

Enduring disasters are those in which an initial event continues to generate new casualties and new damage weeks and months into the response. They are not necessarily more catastrophic than acute or discrete disasters, but enduring disasters may break current operational phase planning models and introduce new complicating factors and demands not experienced during shorter duration events. Enduring disasters do not have traditional signposts for transition into sustained operations or the recovery phase.

Lasting minutes, hours, or days, recent and typical meteorological events have allowed for a relatively quick and clean transition between operational phases. Whether employing FEMA's three-phase model [1] (see Figure 1) or the Department of Defense's (DoD) Operation Phases of Defense Support of Civil Authorities (DSCA) six-phase model (shape, anticipate, respond, operate, stabilize, and transition) [2], achieving a quick transition is essential for planning and anticipating needs. Considerations, priorities, and even planning personnel may change between phases.

Enduring disasters do not allow for a quick or clean transition between phases. A lengthy disaster event—lasting weeks or months—mires responders in prolonged Phase 2 operations while simultaneously requiring actions normally associated under Phases 1 and 3. While it is normal to have some phase overlap for a limited period of time during transition, the requirement to simultaneously execute tasks associated with all three phases in the long term is new.

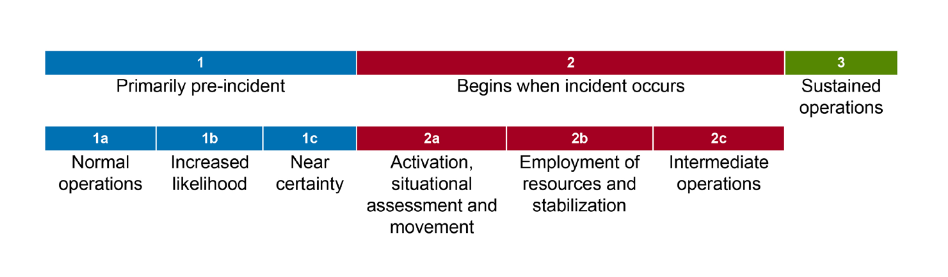
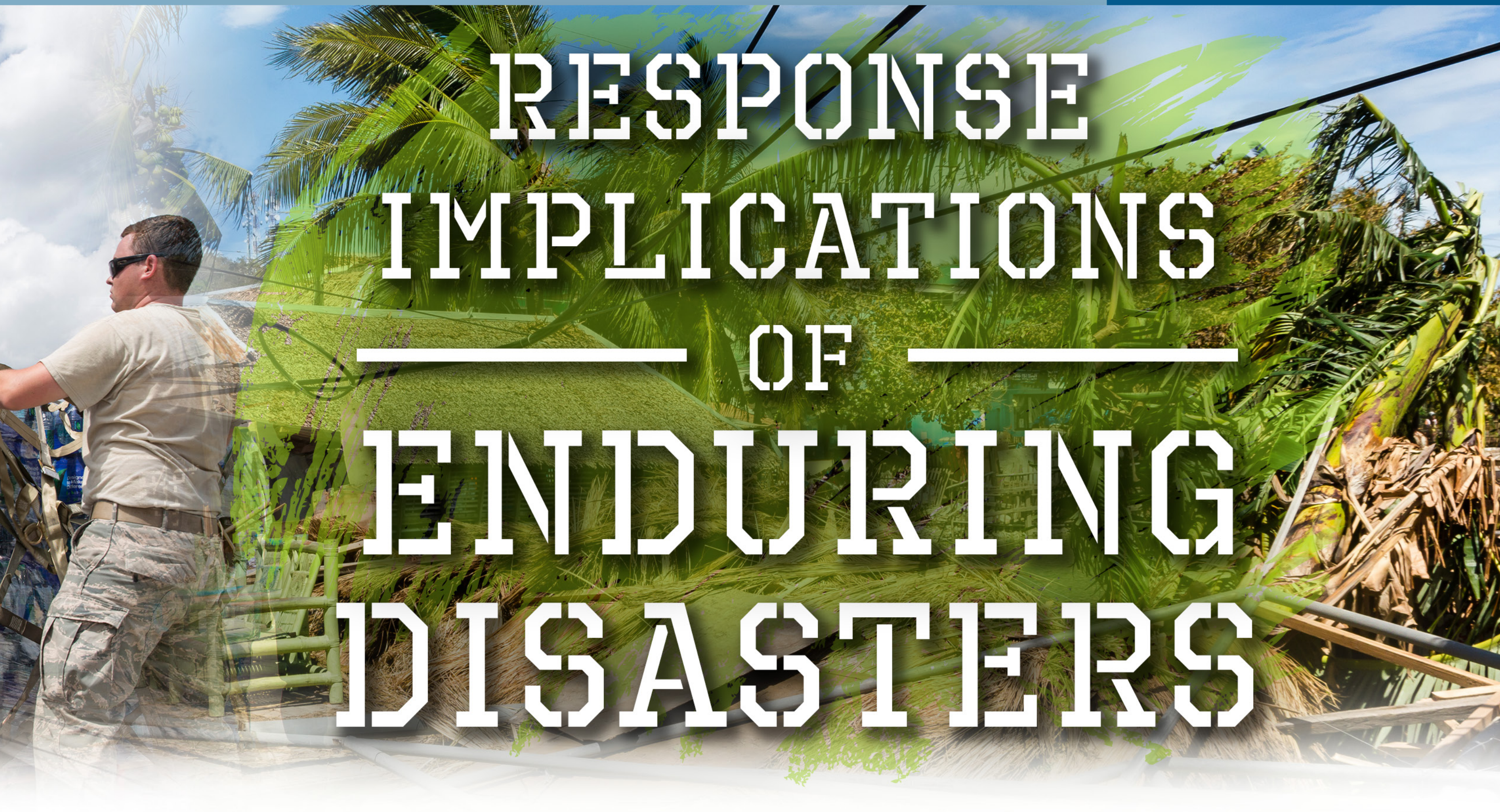


Figure 1. FEMA Common Operational Phases [1]. DoD is considering transitioning to a FEMA-based three phase model for DSCA operations: (1a) normal operations, (1b/1c) elevated/creditable threat (for a notice event), (2a) immediate response, (2b) deployment of resources and personnel, (2c) sustained response, and (3) recovery/transition in the next edition of JP 3-28 Defense Support of Civil Authorities.

Image Credit | *Photo Illustration created by HDIAC. Adapted from Marine Corps photo by Lance Cpl. Alexis C. Schneider (Available for viewing at http://www.jcs.mil/Media/News/cle/1320454/jbsa-volunteers-aid-in-hurricane-maria-relief-efforts/), and Adobe Stock.*

RESPONSE IMPLICATIONS OF ENDURING DISASTERS



Enduring disasters outlast local and personal on-hand resources (such as prescription medication refills), compelling responders to perform life-sustaining operations to prevent new secondary casualties while lifesaving operations in response to the original event continue. New considerations for planning and exercises must be implemented to ensure our community can respond to enduring disasters effectively.

An example of an enduring disaster is FEMA's response to Puerto Rico (DR 4339). Hurricane Irma's landfall set the conditions for Hurricane Maria, which resulted in enduring disaster conditions. As the local and state response culminated for Irma, Maria brought additional systemic requirements not normally seen in typical landfall. Destruction of the power grid, widespread debris management, and destruction of the commercial communication system significantly degraded Puerto Rico's ability to transition out of Phase 2. Combined with the logistical challenges of responding to an event outside the continental United States, Phase 2 actions for Puerto Rico went well into 60 days post landfall [3].

Disaster duration was proposed as one of five factors for the typology of disasters by Michael Berren in 1980 [4]. Berren hypothesized that using a five factor typology (natural vs. man-made, duration, degree of personal impact, potential for occurrence/recurrence and control over future impact), planners could better predict the psychological impact of a disaster and more effectively target intervention. Applying this same concept beyond just the psychological response to disasters provides an alternative way to improve our planning and response to disasters, which occur infrequently and are not supported by AARs, lessons learned, and responder experience.

Likely Enduring Disasters

Certain disasters clearly have the potential to become enduring disasters. Epidemics, earthquake series, or major power outages may last weeks, months, or years.

America has not had a major epidemic in 100 years. The 1918 Great Flu Epidemic killed half a million Americans, roughly 0.5 percent of the population. Lasting from January 1918 to December 1920, this enduring disaster has largely been relegated to the history books, as it occurred in an America that bears little resemblance to our own [5]. However, there is a more recent epidemic worthy of discussion. The Ebola epidemic in Africa involved a significant U.S. response and qualifies as an enduring disaster. From December 2013 to March 2016, the Ebola epidemic took an especially heavy toll on native health care personnel [6, 7].The Centers for Disease Control and Prevention (CDC) enduring response lasted two and a half years.

After multiple American health care personnel contracted Ebola in the response, researchers expressed a renewed interest in developing Biosafety Level 4 (BSL-4) biocontainment technologies. While BSL-4 environments have been proven successful in preventing the infection and spread of pathogens in laboratory-based research and development (R&D), these biocontainment standards are all but impossible to meet in a dynamic (and often mobile) response environment [8]. Moreover, the infection pathways of the virus are poorly understood. Some persons closely involved with infected patients do not get sick, while others with only brief and tangential interaction to a patient can contract the virus.

Critically, recent research has established test protocols for chemical deactivation of BSL-4 level pathogens, including Ebola [9]. In July 2016, a team at the U.S. National Institutes of Health evaluated the efficacy of chemical inactivation techniques for Ebola specimen destruction, with an eye toward verifying their use for multiple specimen types in the lab. Although this effort focused on lab environments, its review of the efficacy of other methods of inactivation may prove invaluable in scenarios of high-level biocontainment for Tier-1 pathogens. Such technologies could aid first responders

News-Display/Article/1329638/dod-continues-support-in-hurricane-ravaged-areas/), *photo by Ismael Ortega (Available for viewing at* http://www.jbsa.mil/News/News/Arti-

Figure 1. U.S. Marines with SPMAGTF Crisis Response - Africa load bags of concrete, that will be used by local and international health organizations to build Ebola Treatment Units, into an MV-22B Osprey during Operation United Assistance in Monrovia, Liberia, Nov. 21, 2014. U.S. Marine Corps photo by Lance Cpl. Andre Dakis/ SPMAGTF-CR-AF Combat Camera/Released

in the early stages of response to a disaster, but cannot alone mitigate pathogenicity risks during an enduring disaster.

The New Madrid Earthquake Sequence started on December 16, 1811, and concluded on March 15th, 1812. The region experienced three earthquakes greater than magnitude 7, 10 greater than magnitude 6, and approximately 100 greater than magnitude 5. In total, more than 1,800 earthquakes above magnitude 3 struck during that three month period. Surprisingly, the earthquake epicenter also shifted steadily northward about 55 miles from the initial event. While the 1811-12 earthquake sequence long pre-dates our response procedures, if it were to occur today, this event would qualify as an enduring disaster.

The New Madrid Seismic Zone (NMSZ) underlies the engine of the United States' domestic and international commerce: the Mississippi River Valley. Major means of transport (e.g., major commercial air terminals, including FedEx headquarters in Memphis, Tennessee) are vulnerable to such a seismic threat, including an extended seismic sequence as the one witnessed in 1811/1812.

Apposite to its role in managing inland hydrological flows along major population areas, the U.S. Army Corps of Engineers (USACE) has been an active participant in researching ways to continuously monitor the status and structural resistive strength of civil flood control infrastructure [10]. USACE recognizes the importance of deploying advanced sensor technologies (attached to real-time communication devices) to critical flood-control structures to allow for effective control of area-wide flood events.

USACE studies conducted in 2016 and 2017 looked at means of improving flood-control monitoring beyond traditional airborne surveys. While remote, satellite-based sensing remains a distinct option for future use, it is likely to be prohibitively expensive even in the mid-term. Unmanned Aerial Vehicle (UAV) use in conjunction with thermal imaging cameras is a more likely candidate for the detection of behind-berm seepage and sand boil locations, especially with the rapid decrease in small-scale "drone"-type UAVs.

Both seepage and sand boils are flood symptoms likely to present in the wake of seismic-induced damage or terrain-shift along the USACE-administered Lower Mississippi Levee System. One of the studies recommended that researchers consider fiber-optic-based monitoring of seepage as an early-warning system for earthen dam failures. Fiber-optic-based monitoring may also be suitable for flood-control and other infrastructural-based applications, as fiber-optic-based sensors have demonstrated their capability to act as permanent receivers over distances of 12 miles or more via a single optical fiber line [11].

The second USACE study investigated the use of structural infrasound signals to monitor urban environments [12]. The effort demonstrated that infrasound arrays, which consist of a network of sensors capable of detecting acoustic signals below 20 hertz (monitorable at distances well beyond 8,000 miles), can successfully detect structural sources of wave propagation in an urban environment. Such infrasound sensors and algorithms have already been useful in detecting events likely to occur along the Mississippi in the wake of an earthquake, including barge–bridge allisions. Extended deployment of infrasound array-based monitoring can offer true real-time and remote monitoring and rapid assessment of structural changes in flood-control structures and areas.

The U.S. has not experienced a widespread, extended power outage. Such an outage could be generated by a stand-alone event, such as a cyberattack, a space weather event (solar flare), or even a weaponized electromagnetic pulse. Alternatively, such an outage could also result from a cascade effect of other disasters. For example, 8.5 million people lost power during Hurricane Sandy in 2012 [13]. And in 2017, after 136 days of response to Hurricanes Irma and Maria, only 70 percent of Puerto Rico's residents regained power [14].

Domestic DoD installations are major consumers of electrical energy, accounting for more than 1 percent of total United States consumption in FY 2015 [15]. The vast majority of these rely on the commercial grid for the provision of power—a key point of vulnerability in any electrical blackout scenario, and especially so in an enduring disaster. DoD's traditional approach to mitigating an extended blackout period relies almost entirely on the use of diesel-fired standalone generators, which are energy inefficient [15].

A study commissioned by the Pew Charitable Trusts suggested that a unique form of hybrid microgrid may be especially well suited to DoD's need to remain resilient in the face of an enduring disaster. Combining natural gas-fired generators with standalone diesel generators would alleviate the disruption caused by an interruption in supply of one fuel type [16]. Indeed, DoD recently installed at least two such hybrid microgrids—one at the Marine Corps Air Ground Combat Center at Twentynine Palms, and the other at the Marine Corps Air Station Miramar [15]. However, this is not a long term solution, as it won't eliminate the problem entirely. Even the most efficient hybrid microgrid of this type can only extend the energy self-sufficiency of a base for a finite period of time.

FEMA has developed a new Power Outage Incident Annex to the Response and Recovery FIOPs, which addresses the response and recovery to a mass or long-term power outage, regardless of cause. FEMA Regions I, II, III, V, VIII, and X developed regional power outage plans that address power outage risks and impacts. The Incident Annex also specifically highlights the development or addition of microgrids as a key preparedness activity, whether operated by DoD, federal entities, or commercial interests [17].

Recommendations for Current Plans and Exercises for Enduring Disasters

Minor changes and low-cost additions to select plans and exercises involving enduring disasters could save lives, increase efficiency, and reduce overall response costs.

Extended and Robust Planning Staff

Perhaps the biggest challenge of an enduring disaster is the establishment and long-term operation of an integrated, strategic-minded planning staff with prevention, response, and recovery phase expertise.

For instance, a 2006 federal lessons learned report on the response to Hurricane Katrina concluded that

"Federal, state, and local officials responded to Hurricane Katrina without a comprehensive understanding of the interdependencies of the critical infrastructure sectors in each geographic area and the potential national impact of their decisions. For example, an energy company arranged to have generators shipped to facilities where they were needed to restore the flow of oil to the entire mid-Atlantic United States. However, FEMA regional representatives diverted these generators to hospitals. While lifesaving efforts are always the first priority, there was no overall awareness of the competing important needs of the two requests [18]."

Therefore, it is imperative that balancing the competing needs of immediate live-saving relief efforts and critical infrastructure restoration activities be part of a strategic plan.

The potential damage to energy infrastructure caused by an NMSZ earthquake provides a ready example. The East Coast relies on gasoline and heating oil, but pipelines in the Mississippi Valley will likely be damaged during a New Madrid earthquake sequence. If the next major NMSZ event occurs in the winter, as it did in 1811, pipeline repair and operation will be a national priority, competing for resources against immediate local needs. All pipelines along the Mississippi Valley may have to be inspected and repaired after each earthquake greater than magnitude 3 for months. Such an extended earthquake sequence could shut down the majority of crude oil, natural gas, and refined liquid petroleum product-bearing pipelines that emanate from the Gulf Coast.

International oil and gas firms and midstream corporations have invested significant R&D dollars in pipeline monitoring and inspection technologies at a slow, but steady, rate since the construction and installation of the 800-mile-long Trans-Alaskan Pipeline System. The surge in crude oil prices between 2004 and 2008 served to supercharge pipeline protection-related R&D investments. However, apart from the addition of wireless connectivity and by-now-common optical ranging capabilities to standard oil field "pig" (Pipeline Inspection Gadget) designs, pipeline-monitoring technology has lagged behind the need for continual inspection necessitated by aging pipe ages. The threat of a major seismic area in the Lower Mississippi River Valley area stands as a notable threat to both below- and above-ground petroleum pipeline integrity.

Since 2015, multiple methods of improving pipeline status and performance monitoring have been introduced in the petroleum engineering community [19]. However, the majority of these advances assume a stable base pipeline (and seismic) environment for the operation of their inspection or monitoring technologies. In March 2018, engineers at Mississippi State University (MSU) revealed the results of research conducted on a bacteria-based sensor network designed to alert pipeline managers to even the smallest leaks in real time [20].

Unlike traditional pig-based inspection techniques, this material would be applied to the full outer diameter surface of each pipeline segment, which would also provide supplementary information on the basic structural integrity of the pipes. The MSU team has proven the versatility of their bacteria-based coating. Future research efforts will seek to identify and test suspending materials for the durable application of the bio-based film to pipelines at full scale.

Operations planning for an enduring disaster will be more complex, covering all the opera-

Figure 2. Loadmasters from Dover Air Force Base, Del. work with Aerial Port personnel to unload a Transport Isolation System on Joint Base Charleston, S.C. during Exercise Mobility Solace Aug. 17, 2016. Exercise Mobility Solace provides AMC, working with joint partners, the opportunity to evaluate the protocols and operational sequences of moving multiple patients exposed or infected with Ebola using the TIS while testing its capabilities and working in concert with various military units, first responders and local government agencies. (U.S. Air Force Photo by Tech. Sgt. Gregory Brook)

tional phases simultaneously, and will have to be maintained over a prolonged period of time versus that of a typical hurricane response. Plans and exercises for enduring disasters must reflect the need for a larger planning staff and the need to rotate both individual staff members and staff teams.

Integration of Non-traditional Aid

Disaster response work has inherent hazards. Search and recovery teams may be caught in significant earthquake aftershocks. Medical providers may become infected during an epidemic. Enduring disaster response may take a heavy toll on equipment. Long-term operations can require responders to service equipment and rotate personnel. It is likely that a prolonged response to an enduring disaster will deplete existing domestic resources, which may be offset by the integration of foreign response teams and resources.

Interest in employing these resources is a recurring theme in AARs from recent operations. For example, the 2017 Joint Task Force Texas Hurricane Harvey AAR stated “there were a number of foreign governments who sought to lend support to Texas during this response [21].”

Additionally, the NMSZ 2011 National Level Exercise AAR indicated “Sweden was unwilling to deploy their medical team without the [United States Government] assuming medical liability. Other international offers—such as those to supply field hospitals, medical teams, HazMat (Hazardous Material) teams, and water purification resources—had not been accepted by the end of the exercise and were therefore still pending [22].”

Pre-planning for the use of foreign response teams and their inclusion in enduring disaster response exercises provides the opportunity to exercise individual international support agreements with key partner nations. Processes for quickly employing unanticipated partners as well as establishing pre-incident agreements with traditional international partners for selected enduring disasters may prove beneficial.

Government agencies continue to benefit from collaboration with industry, representing enhanced capabilities in strategic crisis management planning. These partnerships will bring a quicker response and facilitate an efficient transition into community recovery following a crisis [23].

Collaboration with non-traditional disaster response groups can also be optimized to provide highly accurate data for the mapping of a disaster site. The last decade has seen a trend of online volunteers using satellite imagery to crowdsource an up-to-date map of an affected area. However, this data is typically produced in a random order, and not in line with responder needs or priorities. Research recently published by a team from the University of Tennessee, Knoxville, and the University of California, Santa Barbara, has demonstrated a digital triage method for prioritizing disaster mapping for volunteer efforts [24]. Such mapping data, when combined with on-the-ground reconnaissance, can aid in an effective response.

Increase Responder Resiliency Via Social Networks

CDC Deputy Team Lead and Senior Laboratory Advisor John Saindon worked in Liberia during the Ebola epidemic from November 2014 through March 2017. He made several observations and recommendations for improving the U.S. response that can easily be extrapolated to other enduring disasters, writing that “the focus of much of the existing published literature is on the disease outbreak itself but neglects the responder’s own social and resilience considerations during a disease outbreak [25].”

Saindon had great concerns about the social and mental well-being of crisis responders in an environment where an increased distrust and fear of health workers and international support became inherent. This distrust and fear was due to the emphasis on stopping the disease at the expense of recognizing the community aspects of the response. He stated that remaining in contact with friends and family outside the crisis event is critical to long-term responder success [25]. “During any response, it is recommended that responders maintain communication with friends, family, and other responders to create a social network of support. It is also important that a responder consider participating in collective efficacy [25].”

Response to Vulnerable Populations

During an enduring disaster, citizens requiring access to prescription medication will turn to the disaster response community for assistance. While stockpiling a vast variety of medicines is expensive and seldom effective as a long-term solution, advanced planning on how to alternatively resource select drugs and obtaining advanced emergency-use waivers concerning manufacturing, importation, and inspection techniques may save significant and lifesaving time during an enduring disaster response. This consideration should be included in planning for disasters that may become enduring and exercised accordingly.

Effective responses to enduring disasters plan ahead for providing aid to vulnerable populations, such as the elderly and disabled. In the wake of Hurricane Sandy, New York City expanded its emergency response plan to address the evacuation of disabled citizens who live in high-rise apartments [26].

The revised plan includes a task force dedicated to addressing processes and methods for high-rise evacuation, bringing together governments, first responder agencies (New York City Fire Department, etc.), and technical standard-setting organizations like the National Institute of Standards and Technology and the National Fire Protection Association [27]. Planning for the evacuation of vulnerable populations must also account for the lengthy period of an enduring disaster, possibly resulting in multiple relocations.

Maintaining a Responder Reserve and Developing Responder Depth for Enduring Disasters

“Never be late to need” is a common mantra during response events and exercises. In an effort to meet the need, there is a tendency to maximize the use of personnel—sending all available responders on missions. However, holding a third of forces in reserve to enable later flexibility in response is a proven military tactic that assists in the recovery of initial responders. For example, in an earthquake sequence, where additional earthquakes are often incorrectly assumed to be significantly lower magnitude than the initiating event, responders and citizens can become trapped or injured as easily as in the initial event. Employing a reserve personnel in this scenario would greatly aid in response efforts.

Furthermore, a national-level cadre of properly trained reserve responders provides depth during an enduring disaster. After the 2017 Hurricane Season, FEMA’s Planning Cadre integrated Incident Management (Field) and Incident Support (Regional and National) operational planning capabilities [28]. The responding operational planning cadre provides assumption-based forecasting and planning, which allows greater use of programmatic activities to support responder communities.

Furthermore, a national qualification system should be operationalized to provide the standardized structure for training, organizing, and equipping personnel.

Conclusion

Enduring disasters require different approaches and considerations than traditional duration disasters. The aforementioned recommendations are low-cost improvements to existing response plans and training exercise designs. Deliberate planning will address issues readily apparent in enduring disaster response and recovery.

References

1. Federal Emergency Management Agency. (2014). FEMA Operational Planning Manual (p. 45, Rep. No. FEMA P-1017).
2. U.S. Joint Chiefs of Staff . (2013). *Joint Publication 3-28, Defense Support of Civil Authorities* (JP 3-28). Retrieved from http://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_28.pdf
3. Federal Emergency Management Agency. (2017). *Initial Notice* (Internal Agency Docket No. FEMA-4339-DR). Retrieved from https://www.fema.gov/disaster/notices/initial-notice-26
4. Berren, M. R., Beigel, A., & Ghertner, S. (1980). A typology for the classification of disasters. *Community Mental Health Journal, 16*(2), 103-111. doi:10.1007/bf00778582
5. Kolata, G. (1999). *Flu: The story of the great influenza pandemic of 1918 and the search for the virus that caused it.* New York: Farrar, Straus and Giroux.
6. World Health Organization. (2014, August 8). *Statement on the 1st meeting of the IHR Emergency Committee on the 2014 Ebola outbreak in West Africa* [Statement]. Retrieved from http://www.who.int/mediacentre/news/statements/2014/ebola-20140808/en/
7. World Health Organization. (2016, March 26). *WHO Director-General briefs media on outcome of Ebola Emergency Committee* [Statement]. Retrieved from http://www.who.int/mediacentre/news/statements/2016/ihr-emergency-committee-ebola/en/
8. Kortepeter, M. G., Kwon, E. H., Hewlett, A. L., Smith, P. W., & Cieslak, T. J. (2016). Containment care units for managing patients with highly hazardous infectious diseases: A concept whose time has come. *Journal of Infectious Diseases, 214*(Suppl 3). doi:10.1093/infdis/jiw292
9. Haddock, E., Feldmann, F., & Feldmann, H. (2016). Effective chemical inactivation of Ebola virus. *Emerging Infectious Diseases, 22*(7), 1292-1294. doi:10.3201/eid2207.160233
10. Dunbar, J. B., Galan-Comas, G., Walshire, L. A., Wahl, R. E., Yule, D. E., Corcoran, M. K., . . . Llopis, J. L. (2017). *Remote Sensing and Monitoring of Earthen Flood-Control Structures* (Rep. No. ERDC/GSL TR-17-21). Vicksburg, MS: U.S. Army Engineer Research and Development Center. Retrieved from http://www.dtic.mil/dtic/tr/fulltext/u2/1037860.pdf
11. Galan-Comas, G., & Costley, R. (2016). *Active Seismic Surveying with Fiber Optic Seismic Sensors for Determining Subsurface Anomalies*. Vicksburg: United States Army Corps of Engineers, Engineer Research and Development Center. Retrieved from https://www.dtic.mil/DTICOnline/downloadPdf.search?collectionId=tems&docId=SENSIAC-2120192
12. Pace, M. E., Diaz-Alvarez, H., Simpson, C. P., McKenna, M. H., & McComas, S. L. (2016). *Persistent monitoring of urban infrasound phenomenology; Report 2: Investigation of structural infrasound signals in an urban environment* (Rep. No. ERDC TR-15-5). Vicksburg, MS: U.S. Army Engineer Research and Development Center. Retrieved from https://erdc-library.erdc.dren.mil/xmlui/handle/11681/20428
13. Federal Emergency Management Agency. (2013, July 1). *Hurricane Sandy FEMA after-action report* (Rep.). Retrieved from https://www.fema.gov/media-library-data/20130726-1923-25045-7442/sandy_fema_aar.pdf
14. U.S. Army Corps of Engineers. (2018, January 31). *Hurricane Irma and Maria Response* (Facebook post). Retrieved from https://www.facebook.com/USACEHQ/photos/a.143492942344625.25047.13 6693759691210/2042860282407872/?type=3 (accessed 27 February 2018).
15. Marqusee, J., Schultz, C., & Robyn, D. (2017). *Power Begins at Home: Assured Energy for U.S. Military Bases* (Rep.). Retrieved http://www.pewtrusts.org/~/media/assets/2017/01/ce_power_begins_at_home_assured_energy_for_us_military_bases.pdf
16. St. John, J. (2017, January 17). How military microgrids could save the country—on energy costs. Retrieved from https://www.greentechmedia.com/articles/read/amidst-energy-insecurity-a-call-for-military-microgrids#gs.EyKCB1E
17. U.S. Department of Homeland Security. (2017, June). *Power outage incident annex to the response and recovery federal interagency operational plans: Managing the cascading impacts from a long-term power outage* (Rep.). Retrieved from https://www.fema.gov/media-library-data/1512398599047-7565406438d0820111177a9a2d4ee3c6/POIA_Final_7-2017v2_(Compliant_pda)_508.pdf
18. The White House. (n.d.) Chapter five: Lessons learned. Retrieved from https://georgewbush-whitehouse.archives.gov/reports/katrina-lessons-learned/chapter5.html
19. Obeid, A. M., Bensaleh, M. S., Qasim, S. M., Abid, M., Jmal, M. W., & Karray, F. (2016). Towards realisation of wireless sensor network-based water pipeline monitoring systems: A comprehensive review of techniques and platforms. *IET Science, Measurement & Technology*, 10(5), 420-426. doi:10.1049/iet-smt.2015.0255
20. American Chemical Society. (2018, March 18). Living sensor can potentially prevent environmental disasters from fuel spills. Retrieved from https://phys.org/news/2018-03-sensor-potentially-environmental-disasters-fuel.html
21. Texas National Guard, "2017 JTF Texas (Hurricane Harvey) AAR" (Austin, TX, Texas National Guard, 2017).
22. Federal Emergency Management Agency. (2011, October 28). *National Level Exercise 2011 (NLE 11) functional exercise: Final after action report (AAR)* (Rep.). Retrieved from https://info.publicintelligence.net/FEMA-NLE2011-AAR.pdf
23. Haghani, A., & Afshar, A. M. (2009, September). *Supply chain management in disaster response* (Final Project Rep.). Retrieved from http://www.mautc.psu.edu/docs/UMD-2008-01.pdf
24. Hu, Y., Janowicz, K., & Couclelis, H. (2016). Prioritizing Disaster mapping tasks for online volunteers based on Information Value Theory. *Geographical Analysis*, 49(2), 175-198. doi:10.1111/gean.12117
25. Saindon, J. M., & Patel, P. (2016). *The war on Ebola: A qualitative descriptive case study of an Ebola response in Liberia* (Doctoral dissertation, Nova Southeastern University). Retrieved from http://adsabs.harvard.edu/abs/2016PhDT.......182W
26. Santora, M., & Weiser, B. (2013, November 7). Court says New York neglected disabled in emergencies. *New York Times*. Retrieved from https://www.nytimes.com/2013/11/08/nyregion/new-yorks-emergency-plans-violate-disabilities-act-judge-says.html
27. Chuang, C. (n.d.). Re: Brooklyn Center for Independence of the Disabled v. de Blasio, 11-cv6690-JMF, Joint Letter Attaching Stipulation of Settlement and Defendants' Request for Further Clarification Regarding Rule 23(e) [Letter written September 30, 2014 to Honorable Jesse M. Furman]. Retrieved from https://www.cidny.org/wp-content/uploads/2017/07/Emergency-Preparedness-Settlement-MOUs-9-30-14.pdf
28. Federal Emergency Management Agency, *Integrated Planning Refinement and Implementation Guidance*, (Washington, D.C., Federal Emergency Management Agency, 9 September 2016), 6.

COL Barrett K. Parker
Instructor and John Parker Chair for Reserve Component Studies, U.S. Army War College

COL Barrett K. Parker was commissioned into the U.S. Army Chemical Corps in 1988. He holds a Bachelor of Science in earth science from Pennsylvania State University and master's degrees in environmental management (Samford University), engineering management (University of Missouri), and strategic studies (U.S. Army War College). COL Parker formerly commanded the USAR Consequence Management Unit in Abingdon, MD, and currently serves as instructor and the John Parker Chair for Reserve Component Studies at the U.S. Army War College in Carlisle, PA.

David B. Kang
Deputy Director, Planning and Excercise Division, Response Directorate, Federal Emergency Management Agency

David B. Kang serves as deputy director for the Planning and Exercise Division, Response Directorate of the Federal Emergency Management Agency (FEMA). In this role he oversees the development of the nation's interagency and joint local, state, and federal response plans for catastrophic incidents and FEMA's exercise conduct. Kang's past FEMA positions include (Acting) Director, Planning Exercise Division, Regional Planning Branch Chief, and Regional Technical Assistance Section Chief.

TISSUE ENGINEERING FOR A BETTER TOMORROW

Amy Jackson & Jed Johnson, Ph.D.

Re-growing limbs and organs in order to recover from irrevocable physical losses is no longer just for science fiction characters. Due to the advancements in regenerative medicine and tissue engineering, recovery of this magnitude is now possible. Regenerative medicine is the process of creating functional tissues to replace tissues or organs that have been damaged by disease, trauma, or congenital issues, and create solutions for organs that have become permanently damaged. The terms regenerative medicine and tissue engineering have become interchangeable; however, tissue engineering is a concentration or subfield of regenerative medicine. The focus of tissue engineering is to create constructs that restore, maintain, or improve damaged tissue or whole organs through the process of combining scaffolds, cells, and biologically active molecules into functional tissue [1, 2].

The Department of Defense (DoD) supports regenerative medicine in the hope of treating and curing fatal and debihilitating conditions. According to a study completed by the U.S. Government Accountability Office, between 2012 and 2014 the DoD was the second largest funder of regenerative medicine. The DoD invested $253 million into 178 projects related to regenerative medicine and health needs of active-duty military personnel [3].

According to Stratistics Market Research Consulting, the global tissue engineering market is expected to reach $16.82 billion by 2023 [4]. Three different areas categorize the tissue engineering market: synthetic, biological, and genetically engineered solutions. Generally, the synthetic products currently available (e.g., polypropylene hernia meshes) can be manufactured on a large scale, but do not provide the environment required for cells inside the body to properly grow and integrate into the mesh, resulting in severe scar formation. The biological solutions (i.e., allografts) can be integrated into the body, but suffer from problems with variable outcomes such as premature degradation, immune system reactions, sourcing of materials, and high cost [5]. The genetically engineered solutions typically consist of cells grown in a bioreactor in the lab to create a functional organ that can be implanted, but this is hugely expensive and still in early development. ParaGen Technologies aims to redefine tissue engineering through the development of a new type of synthetic scaffold capable of rapid biointegration and highly reproducible patient outcomes. The synthetic scaffold also ensures no immune rejection and high function regrowth. The core technology is a nanofiber scaffold that mimics physical structures (see Figure 1)

Image Credit | *Photo Illustration created by HDIAC and adapted from Adobe Stock and a photo by Lori Newman (Available for viewing at http://www.jbsa.mil/News/News/Article/1081439/medical-miracle-bamc-surgeons-perform-groundbreaking-arm-replant/)*

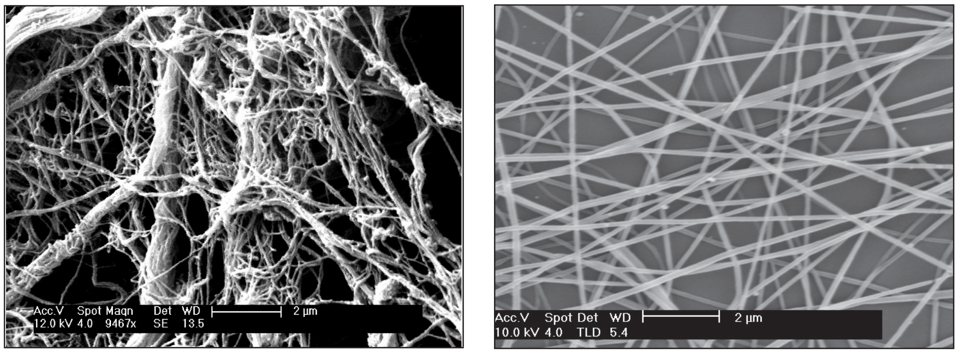


Figure 1. (Left) Scanning electron microscope image of a decellurized blood vessel demonstrating the fibrous structure found in human tissue. (Right) Polymer nanofiber scaffolds.

found within the body that allows for assimilation and tissue level structural support. The nanofiber scaffold is made from completely synthetic polymers (e.g., the same polymers used in resorbable sutures such as polyglycolide) and resorbs over time so no foreign material remains in the body.

Background

A 2015 Congressional Research Service Report found that 52,351 U.S. military members and civilians were non-lethally wounded in action between October 2001 and July 2015, during Operation Iraqi Freedom, Operation New Dawn, and Operation Enduring Freedom [6]. The injuries that military personnel face can be life-changing, and the DoD and other institutions are looking to tissue engineering as a means to repair these injuries. Advances in tissue engineering and regenerative medicine can potentially reduce surgical complications, speed healing time, and provide better patient outcomes for wounded soldiers.

The DoD is actively creating solutions for injuries sustained by military personnel in areas such as bone regeneration, muscle function restoration, and burn and wound care. On the basic research side, the Armed Forces Institute of Regenerative Medicine (AFIRM) is a multi-institutional, interdisciplinary network funded by the DoD and working to develop advanced treatment options for severely wounded servicemen and women. AFIRM has five research programs: extremity injury treatment, craniomaxillofacial reconstruction, skin injury treatment, vascular composite tissue allotransplantation and immunomodulation, and genitourinary and lower abdominal injury treatment. The goal of AFIRM and its numerous institutions across the globe is to use tissue engineering and regenerative medicine to address cardiovascular disease, neurological conditions, or chronic diseases, and potentially repair, replace, or regenerate damaged organs and tissues. The DoD also utilizes the tissue engineering and regenerative medicine field to treat injuries sustained by military personnel. However, a survey assessing the Technology Readiness Level (TRL) of ongoing DoD projects related to tissue engineering found that nine out 10 projects are currently at a TRL of 1. It is for this reason that alternative technologies, such as synthetic nanofiber scaffolds, are being investigated and rapidly progressing through the pre-clinical and clinical stages.

The fields of tissue engineering and regenerative medicine, as applied today, are relatively new—only about twenty years old. As the times change and the needs of healthcare providers shift, so does the focus and research of regenerative medicine. From the 1900s to the 2000s there was a change of focus in regenerative medicine—from symptomatic treatment to curative treatment [7, 8]. According to Allied Market Research, the global regenerative medicine market is expected to reach $67.5 billion by 2020. High-cost pressure on healthcare providers, due to an aging population and the increasing prevalence of chronic diseases, continues to drive interest in tissue engineering and regenerative medicine despite early setbacks and lack of significant progress [2, 7-9]. While the DoD is one of the largest funders of regenerative medicine research, their focus is on limb repair and battlefield injuries. However, tissue engineering has the potential to fix both traumatic injuries and chronic diseases. According to the Centers for Disease Control and Prevention, seven of the top 10 causes of death in 2014 were in connection to chronic diseases. Several advancements continue to push the fields of regenerative medicine and tissue engineering forward. These advancements address cardiovascular disease and neurological conditions or chronic diseases; repairing, replacing, or regenerating damaged organs and tissues; and the limitations of suitable organs for transplantation [10].

How does regenerative medicine work? The repair principles of regenerative medicine are rejuvenation, regeneration, and replacement [7, 9]. The process begins with building a scaffold that allows the body to repair itself, just like the scaffold around a building allows the workers to repair the structure. Once a functional scaffold is created, cells can be added and tissue will develop with the scaffold if the environment is right. Tissue engineering has three main components: cells, scaffolds, and biochemical signaling [1, 11, 12]. In this approach, cells are seeded on a polymeric scaffold that is then transplanted into damaged areas to repair them. With this traditional tissue engineering method, scaffolds act not only as a structural support system, but

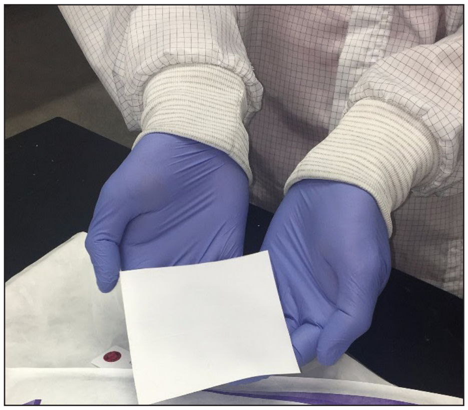


Figure 2: Phoenix Advanced Wound Care dressing.

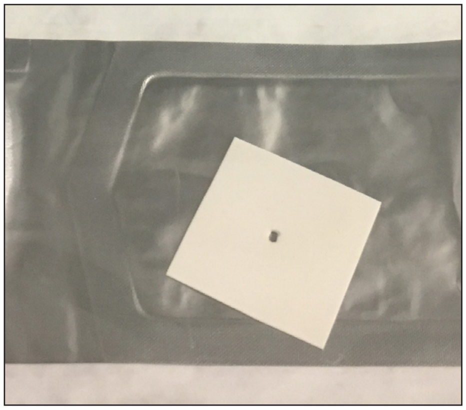


Figure 3: Atreon Orthopedics' rotator cuff repair patch.

also as a conductor for cell growth. Due to the significance of the scaffold, it is imperative that the scaffold can mimic the functionality and complexity of natural tissue (Figure 3). Research is underway for other approaches to tissue engineering such as a modular approach, which involves the assembly of small cell-laden modules that are combined to form larger structures. Another approach is the idea of a scaffold-free approach. This approach consists of growing cells in the lab and getting them to self-assemble into tissues [13, 14].

Current Approaches

Current medical products on the market utilize decellurized animal and human tissue. Decellularization is the process of removing cellular and immunogenic materials from tissues and organs while maintaining all the other mechanical and bioactive properties of the tissue. Think of it as doing a factory reset on a cellphone. This removes personal data, but the phone is still physically intact and can be passed on to another person for use.

Humacyte is a company developing lab-grown organs with subsequent decellularization. Their work focuses on investigational human acellular vessels that have the potential to be utilized as commercial-off-the-shelf human vascular grafts. In the current process used by Humacyte, the blood vessels are formed from banked human vascular smooth muscle cells grown into blood vessels in the lab, which are then decellularized to limit the chance of immune rejection once implanted. No cells from the patient are required for this production process. However, this lab culture process can take more than eight weeks and be very costly. Data pertaining to the recently initiated clinical trial evaluating their use in angioaccess have not been reported, but the preclinical studies used to support this ongoing clinical trial do not suggest that their performance will be superior to currently available vascular grafts made from expanded polytetrafluoroethylene, more commonly known as Gore-Tex [15-17].

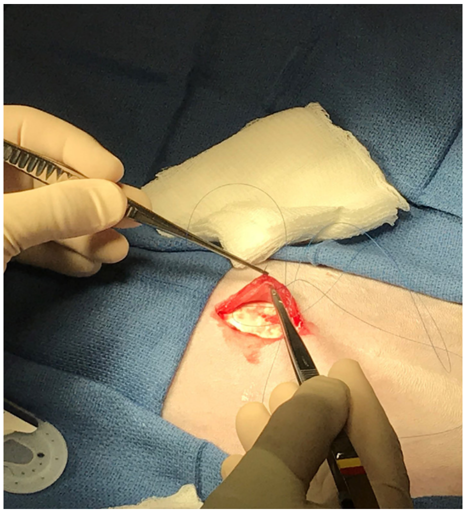


Figure 4. The Tarian Medical hernia mesh being implanted into a rabbit.

Another cell-based approach to making a vascular graft is being pursued by Cytograft, which grows flat sheets of cells which they then roll into a tube to form a blood vessel. This technology has yielded promising preclinical data and led to human clinical trials [15, 18-20]. Although these studies confirm the feasibility of using a tissue engineered vascular graft (TEVG) in humans, these cell sheet-based TEVGs have not outperformed current synthetic graft function in humans [21-23]. In fact, none of the data to date have demonstrated equivalent performance between the cell sheet TEVGs and currently available synthetic grafts.

LifeCell is another company in the tissue engineering and regenerative medicine market. LifeCell utilizes human cadaver tissue that is processed to remove cells while preserving the essential biological components and structure of the dermal matrix to support regeneration in a product called ALLODERM SELECT™. Allograft tissue can integrate into the body and has been used in numerous clinical applications, but it is extremely costly. A small patch of material can cost several thousands of dollars and some reconstructive procedures may use up to a dozen sheets.

ParaGen Technologies' mission is to eliminate the major problems associated with synthetic and biological implants, while incorporating the advantages of each. The core of this technology is synthetic nanofiber scaffolds that mimic the physical structures in the body (see Figure 1) and allow cells to assimilate and remodel into native tissue. The nanofiber scaffold acts to provide tissue level structural support to cells, thus encouraging cell adhesion to the scaffolding and proliferation. These are the key factors that enable tissue regeneration and prevent scar formation.

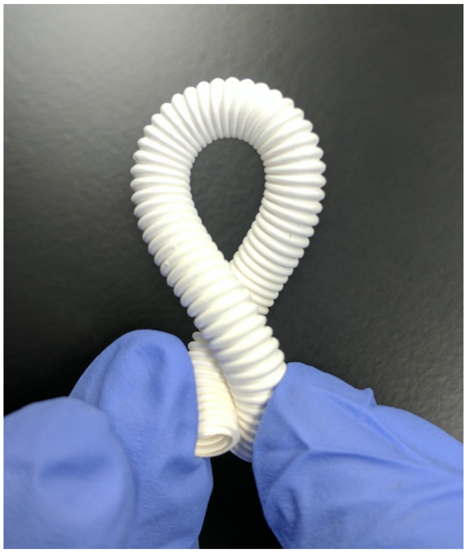


Figure 5: Vascular Genesis graft used for vascular access in dialysis patients.

ParaGen Technologies utilizes commercial-off-the-shelf polymers (i.e., the same polymers used in resorbable sutures) to create cost-effective nanofibers. Polymers are processed into fibers using electrospinning—a relatively common manufacturing process. The novel scaffold technology allows for a controlled degradation profile, a tailored fiber diameter, a specific pore size, and mechanical properties that match the native tissue. The materials are designed based on the clinical application and the devices are carefully tailored to address clinical needs for each indication.

RenovoDerm is developing a portfolio of wound care devices that increase the speed of healing for chronic wounds, while decreasing scar tissue. RenovoDerm's first product, the Phoenix Advanced Wound Care dressing (see Figure 2) received Food and Drug Administration (FDA) approval and is currently being used in wound care clinics. Atreon Orthopedics (see Figure 3) has developed a scaffold that improves the rate of healing and overall strength of repair in rotator cuff injuries. This was tested in a sheep study and is currently in the process of being submitted to the FDA. Tarian Medical (see Figure 4) is developing a scaffold product for stronger hernia repairs with less scarring and adhesions which is being tested in rabbits. Lastly, Vascular Genesis (see Figure 5) is developing synthetic vascular grafts that remodel into healthy vascular tissue with a focus on vascular access grafts for patients undergoing hemodialysis. These vascular grafts are being tested in sheep, with the data being presented to the FDA for an interactive review and consideration as a "breakthrough device" which will significantly speed up the process for regulatory review.

Conclusion

The field of tissue engineering is progressing and moving into the clinic, which provides benefits to the DoD and civilians alike. There are products currently available on the market that fall into the category of tissue engineering such as allografts and xenografts, but lab-grown organs are still over a decade away from reaching the clinic. Additionally, there are challenges for the DoD to utilize some of these allograft materials due to the need for cold storage and short shelf life.

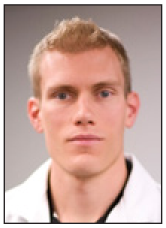
However, there is a new class of synthetic nanofiber scaffolds that are being used today for advanced wound care (i.e., the Phoenix Advanced Wound Care Dressing from RenovoDerm) and a suite of products for rotator cuff repair, hernia repair, and vascular graft replacement following on its heels. These synthetic nanofiber grafts are stored in ambient conditions with long shelf lives, making them great candidates for remote battlefield use (i.e., medical kits in the field) and stored at hospital centers for definitive treatment of injured military personnel and civilians. The same "plastic" that has been used for decades in resorbable sutures is now being used to re-grow organs through a process called tissue engineering. The wait for organ transplants is over, and tissue engineering is here for a better tomorrow.

References

1. Caddeo, S., Boffito, M., & Sartori, S. (2017). Tissue engineering approaches in the design of healthy and pathological in vitro tissue models. *Frontiers in Bioengineering and Biotechnology*, *5*.
2. Tsukamoto, A., Abbot, S. E., Kadyk, L. C., Dewitt, N. D., Schaffer, D. V., Wertheim, J. A., . . . Werner, M. J. (2015). Challenging Regeneration to transform medicine. *Stem Cells Translational Medicine*, *5*(1), 1-7.
3. Murphy, S. V., & Atala, A. (2015). New Government Accountability Office report on regenerative medicine provides an excellent assessment of the field. *Stem Cells Translational Medicine*, *4*(12), 1371-1372.
4. Stratistics MRC. (2017, November). Tissue engineering - Global market outlook (2017-2023). Retrieved from http://www.strategymrc.com/report/tissue-engineering-market-2017
5. Sampogna, G., Guraya, S. Y., & Forgione, A. (2015). Regenerative medicine: Historical roots and potential strategies in modern medicine. *Journal of Microscopy and Ultrastructure*, *3*(3), 101-107.
6. Fischer, H. (2015, August 7). *A guide to U.S. military casualty statistics: Operation Freedom's Sentinel, Operation Inherent Resolve, Operation New Dawn, Operation Iraqi Freedom, and Operation Enduring Freedom* (Rep. No. RS22452). Retrieved https://fas.org/sgp/crs/natsec/RS22452.pdf
7. Jessop, Z. M., Al-Sabah, A., Francis, W. R., & Whitaker, I. S. (2016). Transforming healthcare through regenerative medicine. *BMC Medicine*, *14*(1).
8. Rijt, S. V., & Habibovic, P. (2017). Enhancing regenerative approaches with nanoparticles. *Journal of The Royal Society Interface*, *14*(129).
9. Nelson, T. J., Behfar, A., & Terzic, A. (2008). Strategies for therapeutic repair: The "R3" Regenerative Medicine Paradigm. *Clinical and Translational Science*, *1*(2), 168-171.
10. Centers for Disease Control and Prevention. (n.d.). Chronic disease overview. Retrieved from https://www.cdc.gov/chronicdisease/overview/index.htm
11. Forgione, A., Colombo, F., Sampogna, G., Cocozza, G., & Guraya, S. (2017). Regenerative medicine: Clinical applications and future perspectives. *Journal of Microscopy and Ultrastructure*, *5*(1).
12. Miyachi, H., Shoji, T., Sugiura, T., Miyamoto, S., Breuer, K. C., & Shinoka, T. (2016). Clinical status of tissue engineering and regenerative medicine in cardiovascular disease. *Clinics in Surgery*, *1*. Retrieved from http://www.clinicsinsurgery.com/full-text/cis-v1-id1021.php
13. Duraine, G. D., Brown, W. E., Hu, J. C., & Athanasiou, K. A. (2014). Emergence of scaffold-free approaches for tissue engineering musculoskeletal cartilages. *Annals of Biomedical Engineering*, *43*(3), 543-554.
14. Tiruvannamalai-Annamalai, R., Armant, D. R., & Matthew, H. W. (2014). A glycosaminoglycan based, modular tissue scaffold system for rapid assembly of perfusable, high cell density, engineered tissues. *PLoS ONE*, *9*(1).
15. Dahl, S. L., Kypson, A. P., Lawson, J. H., Blum, J. L., Strader, J. T., Li, Y., . . . Niklason, L. E. (2011). Readily available tissue-engineered vascular grafts. *Science Translational Medicine*, *3*(68).
16. Quint, C., Arief, M., Muto, A., Dardik, A., & Niklason, L. E. (2012). Allogeneic human tissue-engineered blood vessel. *Journal of Vascular Surgery*, *55*(3), 790-798.
17. Quint, C., Kondo, Y., Manson, R. J., Lawson, J. H., Dardik, A., & Niklason, L. E. (2011). Decellularized tissue-engineered blood vessel as an arterial conduit. *Proceedings of the National Academy of Sciences*, *108*(22), 9214-9219.
18. L'Heureux, N., Dusserre, N., Konig, G., Victor, B., Keire, P., Wight, T. N., . . . Mcallister, T. N. (2006). Human tissue-engineered blood vessels for adult arterial revascularization. *Nature Medicine*, *12*(3), 361-365.
19. L'Heureux, N., Pâquet, S., Labbé, R., Germain, L., & Auger, F. A. (1998). A completely biological tissue-engineered human blood vessel. *The FASEB Journal*, *12*(1), 47-56.
20. Niklason, L. E., Gao, J., Abbott, W. M., Hirschi, K. K., Houser, S., Marini, R., & Langer, R. (1999). Functional arteries grown in vitro. *Science*, *284*(5413), 489-493.
21. Huber, T. S., Carter, J. W., Carter, R. L., & Seeger, J. M. (2003). Patency of autogenous and polytetrafluoroethylene upper extremity arteriovenous hemodialysis accesses: A systematic review. *Journal of Vascular Surgery*, *38*(5), 1005-1011.
22. L'Heureux, N., McAllister, T. N., & De la Fuente, L. M. (2007). Tissue-engineered blood vessel for adult arterial revascularization. *New England Journal of Medicine*, *357*(14), 1451-1453. doi:10.1056/nejmc071536
23. Mcallister, T. N., Maruszewski, M., Garrido, S. A., Wystrychowski, W., Dusserre, N., Marini, A., . . . Lheureux, N. (2009). Effectiveness of haemodialysis access with an autologous tissue-engineered vascular graft: A multicentre cohort study. *The Lancet*, *373*(9673), 1440-1446. doi:10.1016/s0140-6736(09)60248-8

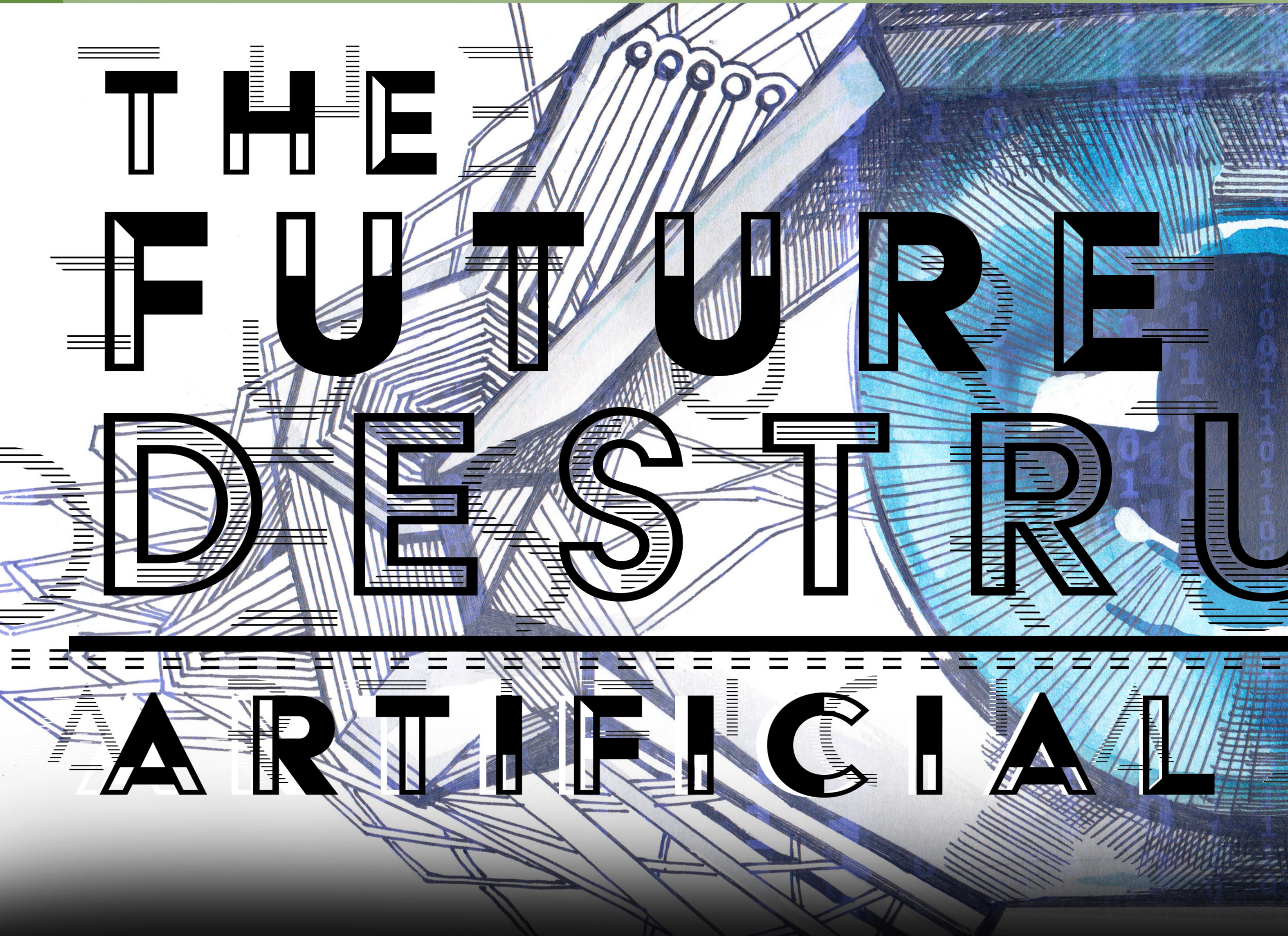
Amy Jackson
Business Development Lead, Ikove Venture Partners

Amy Jackson is the business development lead for Ikove Venture Partners (B.A., College of Mount Saint Vincent). Prior to joining Ikove, she was director of operations and due diligence manager at a foreclosure law firm in Maryland. Jackson spent four years working for law firms in the default industry during which time she gained experience in legal compliance, operational oversight and improvement, process development and implementation, and office management.



Jed Johnson, Ph.D.
Chief Technology Officer, Nanofiber Solutions Inc.

Jed Johnson received his Ph.D. in materials science and engineering with a focus on biomaterials in 2010 from The Ohio State University. He co-founded Nanofiber Solutions Inc. in the spring of 2009 based upon state-of-the-art nanofiber scaffolds for cell culture and tissue engineering applications as an extension of his thesis work, and he serves as its chief technology officer. Johnson led the team that won 1st Place in the 2009 Deloitte Business Plan Competition and has served as principal investigator on numerous National Institutes of Health and National Science Foundation SBIR/STTR grants in addition to Ohio Third Frontier grants.



THE FUTURE DESTRU

ARTIFICIAL

Gregory Nichols, MPH, CPH

The prospect of using artificial intelligence (AI) in warfare is complicated. Arguments exist both for and against the development of weaponized AI [1]. Although ideologies differ among the highest levels of government and throughout the global community [2–4], the very fact that this idea exists must give pause for further evaluation.

No matter the outcome, AI has already changed both defense and national security strategy. In a statement to the Senate Armed Services Committee in 2016, former Director of National Intelligence, James Clapper, eloquently and comprehensively summed up the situation by stating, “Implications of broader AI deployment include increased vulnerability to cyberattack, difficulty in ascertaining attribution, facilitation of advances in foreign weapon and intelligence systems, the risk of accidents and related liability issues, and unemployment. Although the United States leads AI research globally, foreign state research in AI is growing [5]."

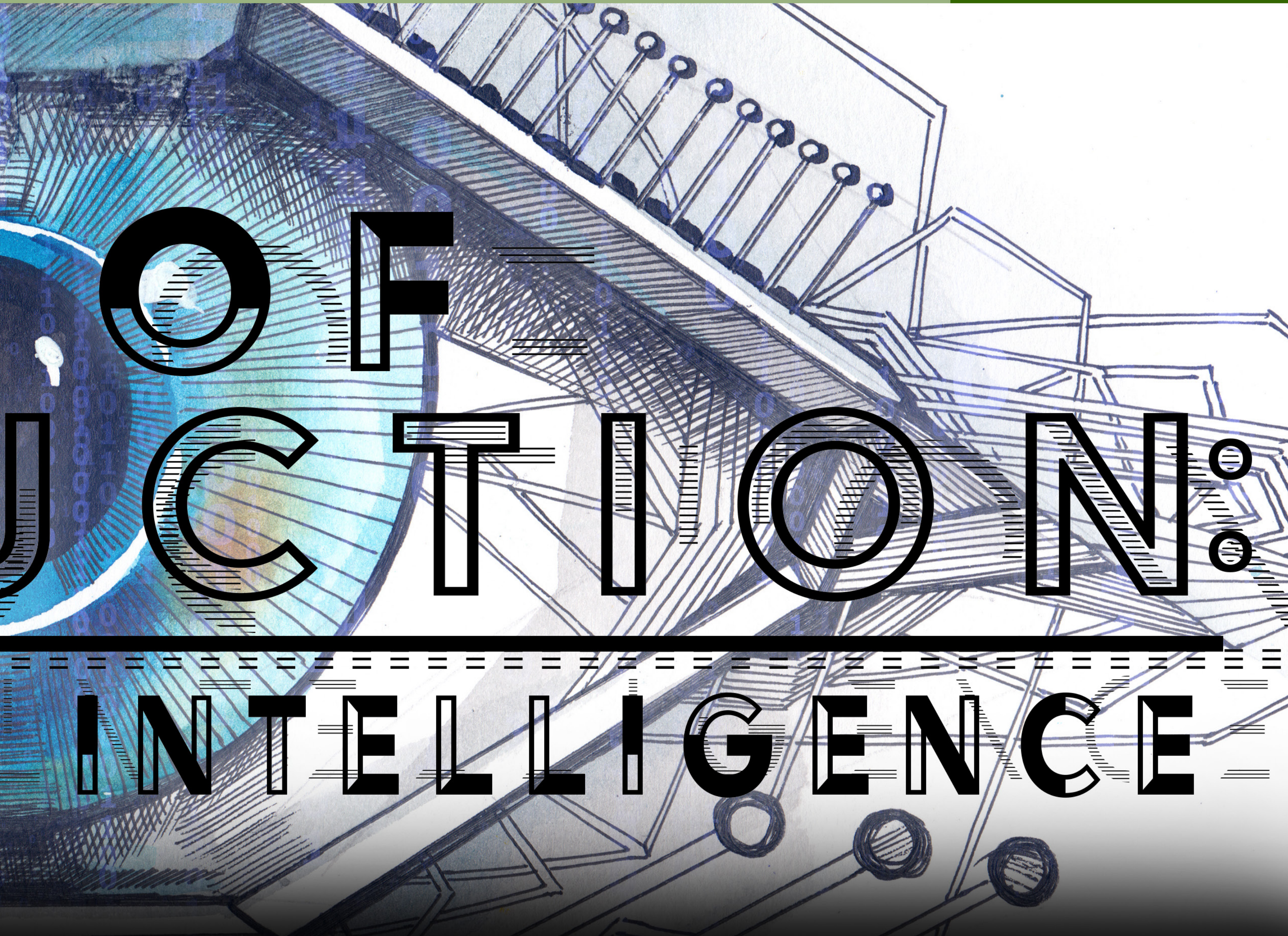
The importance of AI to defense and security strategy influences how the U.S. government and military plans for the future. The January 2018 National Defense Strategy underlined the notion that the Department of Defense (DoD) should invest heavily in the military application of AI and autonomy, as they belong to “the very technologies that ensure we will be able to fight and win the wars of the future [6]."

Likewise, the December 2017 National Security Strategy acknowledged the risks that AI poses to the nation, while also reaffirming the U.S.’s commitment to investing in AI research [7].

Artificial Intelligence and Autonomous Systems in Defense Applications

AI has no standardized definition, but it is generally understood as referring to any computerized system capable of exhibiting a level of rational behavior high enough to solve complex problems [8]. The concept grew out of work that defeated Germany’s “Enigma” code during World War II, primarily pushed by Alan Turing [9, 10]. The U.S. military has been highly engaged in AI research for nearly 70 years [11]. As a broad term, AI spans a wide range of approaches, including the branch of machine learning (ML), which encompasses deep-learning (see Figure 1). AI also encompasses autonomous systems, as AI is the “intellectual foundation for autonomy [12]." It is difficult to discuss weaponization of AI without discussing autonomous systems.

Image Credit | *Photo Illustration created by HDIAC and adapted from Adobe Stock.*



OF
UCTION:
INTELLIGENCE

The Defense Science Board has defined autonomy as a “capability (or a set of capabilities)” that allows aspects of a system to operate on their own “within programmed boundaries [13]." One of the most common military applications of autonomous systems has been its use in unmanned aircraft, or unmanned aerial vehicles (UAVs), which now account for nearly 40 percent of all aircraft used by DoD and comprised a $2.8 billion funding request for FY2018 [12, 14]. Autonomous systems have already changed the combat landscape by offering the ability to conduct precision strikes, which has arguably reduced the number of civilian casualties as well as limit the harm to U.S. and allied forces [15]. The capabilities that autonomy offers for defense applications will continue to grow and develop as technology improves (see Table 1).

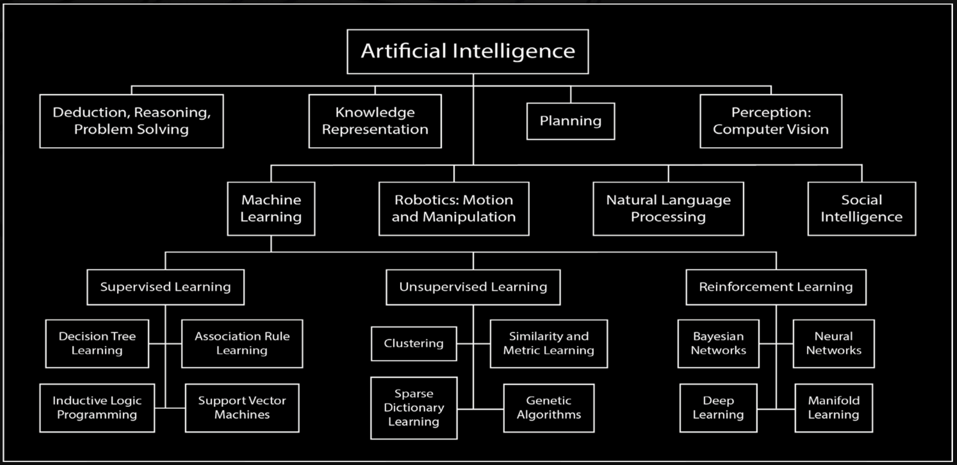


Figure 1: Approaches and disciplines in artificial intelligence and machine learning [61]

Integrating AI into a new paradigm of defense strategy is important for two reasons. First, the technology is available, so it makes sense for the U.S. to pursue technological superiority over its adversaries in this realm. Second, doing so is necessary in order to counter the advances in (and emerging proficiencies of) new technologies developed by Russia and China.

SENSE: Sensors, Perception, Fusion

Available today: Full-spectrum sensing (EM, bits, vibration, chemical...); Object recognition
Likely available near term: Human senses (sight, smell...); Integration of perception with motor skills
May be available long term: High-fidelity touch; Scene understanding

THINK/DECIDE: Analysis, Reasoning, Learning

Available today: High-Volume computational throughput and data architectures; Algorithm variety and complexity; Task-specific, rule-based decision; Rules; Learning from training data, sentiment analysis
Likely available near term: Explicit and testable knowledge representation; Anomaly recognition; Option generation, pruning; Social and behavioral models; Culturally informed, values-based reasoning; Transparent decision logic; C2 for may nodes; Learning by doing, watching
May be available long term: Goal definition; Abstraction, Skills transfer; Inference; Empathy; General purpose, idea-based reasoning; Judgment, intuition

ACT: Motion, Manipulation

Available today: Navigation (routing); Strength, endurance
Likely available near term: Navigation (obstacle avoidance); Agility, dexterity
May be available long term: Navigation (dense, dynamic domains); High degree of freedom actuator control

TEAM: Human/machine, Machine/machine, Info exchange

Available today: High man:machine ratio; Rule-based coordination of multiple platforms; High-volume communications and data transfer
Likely available near term: Observability and directability; Provably correct emergent behavior; Trustworthiness and trust calibration under defined conditions; Natural language processing
May be available long term: Shared "mental models," mutual predictability; Understanding intent; Fully adaptive coordination; Implicit communication

Table 1: Projected capabilities for autonomous systems [12]

Concerns over near-peer technological advances have been substantiated by several AI-based developments in Russia, which are discussed below. In addition, China's State Council released a major report on AI, "A Next Generation Artificial Intelligence Development Plan," in July 2017. This document acknowledges "…the world's major developed countries are taking the development of AI as a major strategy to enhance national competitiveness and protect national security [16]." As a corollary to some of the direct threats that the National Defense Strategy seeks to neutralize, China's AI Development Plan also stresses that the State will "promote all kinds of AI technology to become quickly embedded in the field of national defense innovation [16]." This technological tug-of-war has all of the hallmarks of a new arms race, complete with the possibility of creating never-before-seen destruction.

Artificial Intelligence as a Weapon of Mass Destruction

Existing applications of AI to Weapons of Mass Destruction (WMDs) are extremely limited. Thus, developments within the technology have to be extrapolated to determine how they may be used in WMDs. However, due to AI's unpredictable nature and its potential use in fully- and semi-autonomous weapons systems, scenarios may exist where AI changes the game, so to speak: situations not typically thought of as WMD-relevant could become such. The use of autonomy in weapon systems has grown swiftly over the past 50 years. However, few of these systems are fully autonomous and able to make decisions on their own by using AI, but that is the likely next step, as evidenced by the intentions of many nation-states.

Existing autonomous platforms merely set the stage for what is to come in terms of weapons with artificially intelligent capabilities. The use of AI in WMDs, while complex, can be simplified into a matrix (see Table 2) that illustrates two characteristics: (1) mode, which illustrates the way that AI could be used for the purposes of mass destruction, including as a weapon in itself, as an agent to control other weapons platforms, and as an agent used to design WMDs; and (2) temporality, demonstrated by how AI is currently being used in WMDs or advanced weaponry (actuality) versus emerging developments in AI technology that could be used in WMDs or as WMDs (potentiality). The mode of AI is more complicated than its temporality. In this sense, there are three possibilities.

As a Deadly Weapon *per se*

AI itself could be the weapon (deadly weapon per se), as in a program that finds the best route for hacking into a system [17] or one that propagates the spreading of falsities on social media by imitating human actors [18]. Fears of AI being used to support WMDs can be traced back to at least 1987, where Yazdani and Whitby argued AI at the time was increasing "the possibility of an accidental nuclear war [19]." These fears carry over to the present, and are possibly even more justified as AI technology flourishes. Roman Yampolskiy, an associate professor of computer engineering at the University of Louisville, contended in January 2017 that "weaponized AI is a weapon of mass destruction and an AI Arms Race is likely to lead to an existential catastrophe for humanity [20]." A survey conducted in August 2017 at the Black Hat USA Conference found that 62 percent of survey participants (briefly described as "the best minds in cybersecurity") believed AI would be used as a weapon within the upcoming year [21].

AI-based systems are becoming more common and more intelligent. These programs have already beaten expert human players at games, such as chess [22] and Go [23], and continue to surprise humans with their capacity. For example, chatbots created by Facebook were able to communicate with a language they developed [24, 25], and Google developed neural networks that designed an unbreakable encryption method to keep their conversations secret [26]. However, a darker side to AI programing exists as well, demonstrated by surprising, off-color remarks from Microsoft chatbots Tay and Zo, including being manipulated into defending controversial ideologies as well as making unprompted comments that could be seen as hate speech, respectively [27, 28]. Moving forward, the fear is that AI could lead to a social crisis of epic proportion by creating massive unemployment and a financial catastrophe [29], or even the onset of the technological singularity, the point at which machine intelligence exceeds human intelligence [30]. Although these scenarios may not seem like the results of a conventional WMD, they could usher in a great unknown with potentially life-changing circumstances.

As an Agent of Control

The second mode (agent of control) is much easier to conceptualize, in that AI is used to control an object, such as a missile or robot. This has been done for decades, and continues with systems such as the P-800 Oniks missile (SS-N-26 Strombile) [31]; mis-

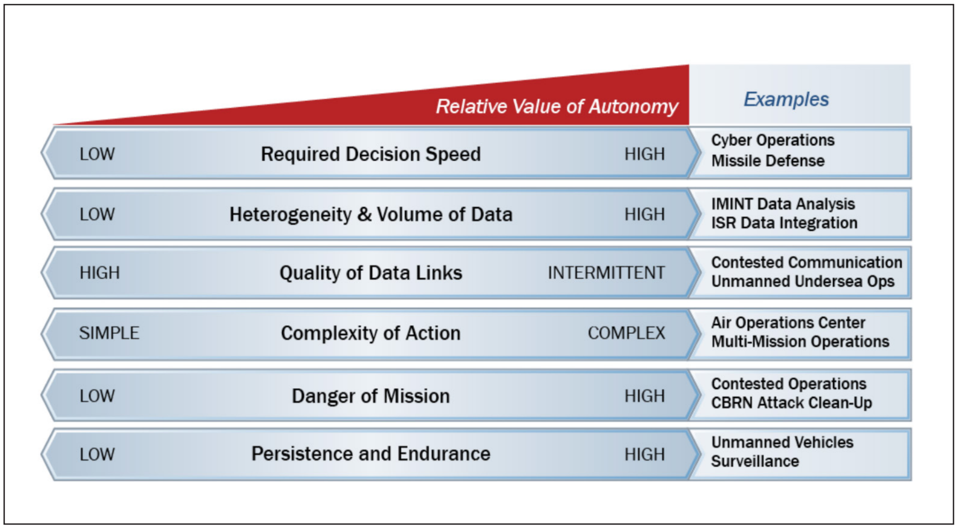


Figure 2: Autonomy derives operational value across a diverse array of vital DoD missions [12]

siles proposed for the planned Tupolev PAK DA bomber [32]; the Long-range Anti-Ship Missile (LRASM) [33]; and the Epsilon Launch Vehicle [34]. Each of these rocket/propulsion systems is capable of providing foundational technology for more advanced usage of AI in larger WMD systems. Most likely, the integration of AI into the guidance and control systems of these types of platforms will continue.

Perhaps the most feared, fastest growing, and least understood WMD applications of AI can be found in robotics. As explained by Vice Chairman of the Joint Chiefs of Staff Gen. Paul Selva during an interview at the Brookings Institution in 2016:

> There are implications that I call the "terminator conundrum." What happens when that thing can inflict mortal harm and is empowered by artificial intelligence. How are we going to deal with that? How are we going to know what's in the vehicle's mind, presuming for the moment we are capable of creating a vehicle with a mind. It's not just a programmed thing that drives a course or stays on the road or keeps you between the white lines and the yellow lines, doesn't let you cross into oncoming traffic, but can actually inflict lethal damage to an enemy and has an intelligence of its own. How do we document that? How do we understand it? How do we know with certainty what it's going to do? [35].

General Selva's "terminator conundrum" has been echoed by the Department of Homeland Security (DHS). A 2017 report on AI stated, "Robots could kill mankind, and it is naive not to take the threat seriously [29]." This fear is becoming reality. For example, when asked if she wanted to destroy humans, Hanson Robotics' Sophia, responded, "OK. I will destroy humans [36]." However, the future form of robots as WMDs may be heading in the direction of the Russian-created Final Experimental Demonstration Object Research, which is capable of replicating complex human movements including firing weapons [37]. The growth of autonomous vehicles for defense applications (especially UAVs and unmanned ground vehicles) will continue, and fundamental questions regarding robotic operations, especially in combat, must be answered [38], but whether or not these could be or would be considered WMDs is open for debate.

As an Agent of Design

Finally, the third mode of AI is its use in design. AI techniques could be used to develop weapons, some of which may not be designs previously conceived by human beings. In other words, AI could use its unique perspectives, as demonstrated by behavior from the Google neural network and Facebook chatbots, to create weapon designs that humans may not have otherwise conceptualized. Little currently exists in the field of AI as it applies to the design of WMDs, but lessons from other areas may provide some insight into how this could be possible. Predicting the outcomes of chemical reactions (particularly in organic chemistry) can be quite challenging. However, last year, several researchers showed how AI can be used to predict the outcomes of complex reactions with greater accuracy than other methods [39, 40].

Using AI to maximize the products of a reaction could create chemical superweapons with massive yields. Research partially funded by the U.S. Army Medical Research and Materiel Command reverse-engineered the complex mechanism of regeneration in planarians by searching the genome with AI [41]. While the intent of the work was focused on understanding cellular and tissue regeneration for medical applications, this method could be used to reverse-engineer the most lethal characteristics of an organism and design a super bioweapon focused on enhancing this trait.

Most AI functions with supervised learning as the backbone of how it performs tasks, meaning the AI sorts images and patterns into pre-programmed categories that have been developed by humans and programmed into the AI. For example, researchers may feed millions of images of trees into an artificial neural network (ANN) (artificial creation that mimics the functions of neurons in a human brain) so that the program can learn what a tree looks like. Based on these images, researchers may also program tree categories (e.g., pine, maple) so that the AI, by way of the ANN, can categorize images of trees based on type.

	AI as a Deadly Weapon *per se*	AI as an Agent of Control	AI as an Agent of Design
Actuality	- Fake news - Hacking	- Missiles - Robots - Conventional arms	- Predicting reactions - Mapping biological mechanisms
Potentiality	- Hostile takeover - Financial crisis - Social unrest - Superintelligence	- Drones - UAVs	- Unstructured learning - Superweapons

Table 2: Classification of AI as WMDs

The opposite of this is unsupervised learning, in which the AI has no pre-programmed categories, but rather is allowed to design its own. The machine would sort patterns or images into what it thinks would be logical categories (which may not overlap with human-generated categories). In 2015, researchers at Google fed white noise into an ANN, and let the AI use what it learned from the millions of images it had in its database. Through a process that Google has nicknamed “inceptionism,” bizarre, yet beautiful images are created by the ANN [42]. Likewise, Google has also developed the UNsupervised REinforcement and Auxiliary Learning (UNREAL) agent (see Figure 3), which has improved the speed of learning certain applications by a factor of 10.

To date, AI has been used in weapon systems or to understand relatively common aspects of chemistry and biology. However, what if AI creates something that never existed before? What if it generates a new class of weapon never imagined by human beings? Unsupervised learning used in this capacity has the potential to do just that.

Counterbalance

The difficulty in assessing how AI could be a WMD threat is a product of the fact that so little information exists regarding this concept. Most likely, evaluating AI uses in conventional weaponry would be limiting. However, as stated by DHS, “Humans must maintain control over machines [29].” Arguably, the two greatest fears (and threats) of AI are its use in autonomous weapon systems and the loss of human control. A number of actions have been taken in regards to these threats. Three categories describe the level of autonomy a system can have:

- Human-in-the-Loop Weapons – Robots that can select targets and deliver force only with a human command;
- Human-on-the Loop Weapons – Robots that can select targets and deliver force under the oversight of a human operator who can override the robots’ actions; and
- Human-out-of-the Loop Weapons – Robots that are capable of selecting targets and delivering force without any human input or interaction [43].

The DoD adheres to the human-in-the-loop principle, as evidenced by DoD Directive 3000.09 [44]. In fact, the U.S. is the first country to proclaim a formal policy on autonomous weapons systems [45]. In addition, “DoD personnel must comply with the law of war, including when using autonomous or unmanned weapon systems” as directed by the DoD Law of War Program (DoD Directive 2311.01E) [46, 47].

The challenge, however, lies in the fact that although the U.S. and its allies adhere to developing human-in-the-loop systems—or even human-on-the loop systems—other countries may not, and probably will not.

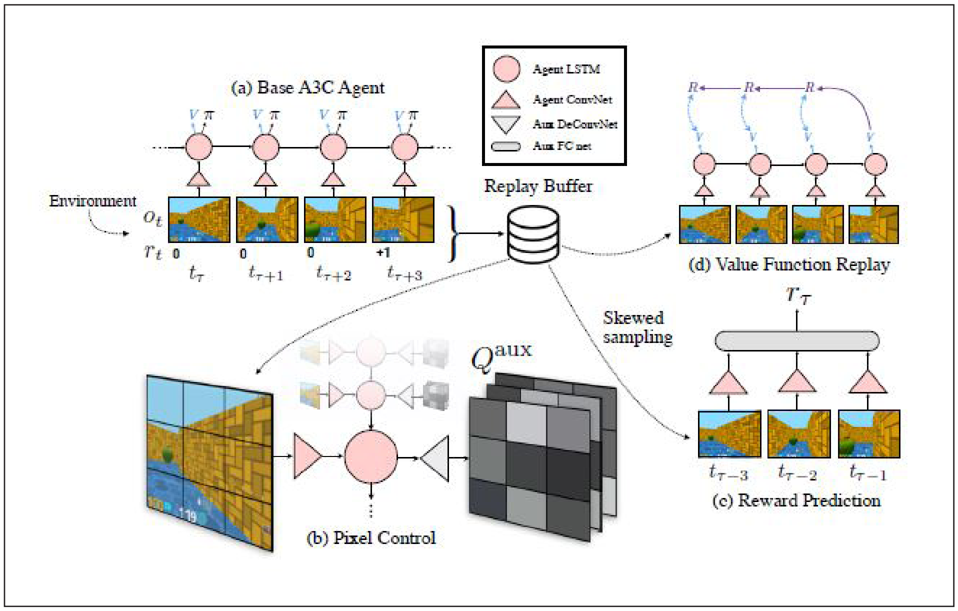


Figure 3: Overview of the UNREAL agent [62]

Former Deputy Secretary Bob Work acknowledged this challenge in 2015 when he stated, “Now, we believe, strongly, that humans should be the only ones to decide when to use lethal force. But when you're under attack, especially at machine speeds, we want to have a machine that can protect us [48].” Ironically, AI may be the greatest counter to AI in some cases, at least in principle. AI may also be the best counter to non-AI WMDs. Programs such as Synchronized Net-Enabled Multi-INT Exploitation have enabled DoD to more efficiently exploit an adversary’s weakness [49]. Research by University of Missouri researchers has shown that a deep-learning program could reduce the amount of time needed to identify surface-to-air missile sites from 60 hours to 42 minutes [50].

Unfortunately, this interplay has possibly already created an arms race, and as Edward Geist, a MacArthur Nuclear Security Fellow at Stanford University argues, the only thing that can be done now is to manage it [51]. Significant efforts in the global community have sought to understand the implications of AI both for its use in WMD development and as a WMD counterbalance. The United Natons Interregional Crime and Justice Research Institute (UNICRI) has led many of the efforts in this area, beginning with the announcment of its programme on AI and Robotics in 2015, and the launch of the Centre on Artificial Intelligence and Robotics in 2016 [52].

Additionally, UNICRI held a series of events from 2015 to 2016 focused on understanding the interplay between AI’s emergence and its application to the chemical, biological, radiological, and nuclear communty [53]. Finally, a recent meeting held during the 72nd Session of the United Nations General Assembly discussed the implications of AI for nuclear non-proliferatoin and disarmament [54].

The potential uses of AI as, or in, a WMD are still very much up for debate. Even so, many in the scientific and even political communities have taken action against the weaponization of AI in general. More than 20,000 prominent figures across the world have called for the exercise of caution when it comes to developing AI for non-benefical uses [55]. Additionally, a group of AI researchers and ethicists have developed a list of 23 principles—mirroring the Asilomar Principles developed in reponse to the use of recombinant DNA—intended to drive the responsible innovation and development of AI [56]. Google's DeepMind has supported the development of an AI "kill switch" that could, as a last resort, shut down a system if control were lost [57]. The future of AI is uncertain, expecially as it applies to WMDs, but one thing is certain: there has been no lack of concern regarding what a future with weaponized AI could look like [58, 59].

Conclusion

Near- and long-term applications of AI in WMD development are uncertain, but the technology exists and improves every day. The uncertainty of the use of AI in WMD development rather than the potential for what it could create is the greater concern in regards to AI as a WMD and as a weaponized AI in general. Some regard AI's military applications as potentially more transformative than the advent of nuclear weapons [60]. Although DoD has taken measures to ensure that humans remain in ultimate control of machines, it is not known how long this may last. For now at least, two things are clear: AI research in general should proceed with caution, and follow the principles of responsible innovation. Moreover, government and military officials must be prepared to face the certainty of AI in an uncertain future.

References

1. Roff, H. M., & Moyes, R. (2016). Meaningful human control, artificial intelligence and autonomous weapons. Briefing paper prepared for the Informal Meeting of Experts on Lethal Autonomous Weapons Systems, UN Convention on Certain Conventional Weapons, Geneva. Retrieved from http://www.article36.org/wp-content/uploads/2016/04/MHC-AI-and-AWS-FINAL.pdf
2. Kerr, I., Bengio, Y., Hinton, G., Sutton, R., & Precup, D. (n.d.) RE: AN INTERNATIONAL BAN ON THE WEAPONIZATION OF AI [Letter written November 2, 2017 to The Right Honourable Justin Trudeau, P.C., M.P.]. Retrieved from https://techlaw.uottawa.ca/bankillerai#letter
3. Frew, W. (2017, November 7). Killer robots: Australia's AI leaders urge PM to support a ban on lethal autonomous weapons. Retrieved from https://newsroom.unsw.edu.au/news/science-tech/killer-robots-australia%E2%80%99s-ai-leaders-urge-pm-support-ban-lethal-autonomous-weapons
4. Future of Life Institute. (n.d.). An open letter to the United Nations Convention on Certain Conventional Weapons. Retrieved from https://futureoflife.org/autonomous-weapons-open-letter-2017/
5. Clapper, J. R. (2016). Statement for the record: Worldwide threat assessment of the U. S. Intelligence Community. Office of the Director of National Intelligence. Retrieved from https://www.dni.gov/files/documents/SASC_Unclassified_2016_ATA_SFR_FINAL.pdf
6. U.S. Department of Defense. (2018). *Summary of the National Defense Strategy of the United States of America*. Retrieved from https://www.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf
7. The White House. (2017). *National Security Strategy of the United States of America*. Retrieved from https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf
8. Executive Office of the President, National Science and Technology Council Committee on Technology. (2016). *Preparing for the Future of Artificial Intelligence* (Rep.). Washington, DC. Retrieved from https://obamawhitehouse.archives.gov/sites/default/files/whitehouse_files/microsites/ostp/NSTC/preparing_for_the_future_of_ai.pdf
9. Turing, A. M. (1950). Computing machinery and intelligence. *Mind*, *59*(236), 433–460. Retrieved from http://www.jstor.org/stable/2251299
10. Rejewski, M. (1981). How Polish mathematicians deciphered the Enigma. *IEEE Annals of the History of Computing*, *3*(3), 213-234. Retrieved from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.692.9386&rep=rep1&type=pdf
11. National Research Council. (1999). *Funding a revolution: Government support for computing research*. Washington, DC: The National Academies Press. Retrieved from https://doi.org/10.17226/6323
12. Defense Science Board. (2016, June). *Defense Science Board summer study on autonomy*. Washington, DC. Retrieved from https://www.hsdl.org/?abstract&did=794641
13. Office of the Under Secretary of Defense (Comptroller)/Chief Financial Officer. (2017). *Program acquisition cost by weapon system: United States Department of Defense Fiscal Year 2018 budget request* (Rep.). Retrieved from http://comptroller.defense.gov/Portals/45/Documents/defbudget/fy2018/fy2018_Weapons.pdf
14. U.S. Department of Defense, Defense Science Board. (2012). *Task force report: The role of autonomy in DoD systems* (Rep.). Retrieved from https://fas.org/irp/agency/dod/dsb/autonomy.pdf
15. Arkin, R. (2013). Lethal autonomous systems and the plight of the non-combatant. *AISB Quarterly*, 137, 4-12. Retrieved from http://www.aisb.org.uk/publications/aisbq/AISBQ137.pdf
16. Webster, G., Creemers, R., Triolo, P., & Kania, E. (2017). China's plan to 'lead' in AI: Purpose, prospects, and problems [Web log post]. Retrieved from https://www.newamerica.org/cybersecurity-initiative/blog/chinas-plan-lead-ai-purpose-prospects-and-problems/
17. Metz, C. (2016, August 5). Hackers don't have to be human anymore: This bot battle proves it. *Wired*. Retrieved from https://www.wired.com/2016/08/security-bots-show-hacking-isnt-just-humans/
18. Chessen, M. (2017). *The MADCOM Future: How artificial intelligence will enhance computational propaganda, reprogram human culture, and threaten democracy... and what can be done about it* (Rep.). Washington, DC: Atlantic Council. Retrieved from http://www.atlanticcouncil.org/publications/reports/the-madcom-future
19. Yazdani, M., & Whitby, B. (1987). Accidental nuclear war: The contribution of artificial intelligence. *Artificial Intelligence Review*, *1*(3), 221-227. doi:10.1007/bf00142294
20. Conn, A. (2017, January 18). Roman Yampolskiy interview. Future of Life Institute. Retrieved from https://futureoflife.org/2017/01/18/roman-yampolskiy-interview/
21. Cylance. (2017, August 1). Black Hat attendees see AI as double-edged sword. Retrieved from https://www.cylance.com/en_us/blog/black-hat-attendees-see-ai-as-double-edged-sword.html
22. Krauthammer, C. (1997, May 26). Be afraid: The meaning of Deep Blue's victory. *The Weekly Standard*. Retrieved from http://www.weeklystandard.com/be-afraid/article/9802
23. Etherington, D. (2017, May 23). Google's AlphGo AI beats the world's best human Go player. Retrieved from https://techcrunch.com/2017/05/23/googles-alphago-ai-beats-the-worlds-best-human-go-player/
24. Simonite, T. (2017, August 1). No, Facebook's chatbots will not take over the world. *Wired*. Retrieved from https://www.wired.com/story/facebooks-chatbots-will-not-take-over-the-world/
25. Lewis, M., Yarats, D., Dauphin, Y., Parikh, D., & Batra, D. (2017). Deal or no deal? End-to-end learning of negotiation dialogues. *Proceedings of the 2017 Conference on Empirical Methods in Natural Language Processing*. doi:10.18653/v1/d17-1259
26. Abadi, M. & Andersen, D. (2016). Learning to protect communications with adversarial neural cryptography. Retrieved from https://arxiv.org/abs/1610.06918
27. Lee, P. (2016, March 25). Learning from Tay's introduction [Web log post]. Retrieved from https://blogs.microsoft.com/blog/2016/03/25/learning-tays-introduction/
28. Price, R. (2017, July 24). Microsoft's AI chatbot says Windows is 'spyware'. Retrieved from http://www.businessinsider.com/microsoft-ai-chatbot-zo-windows-spyware-tay-2017-7
29. U.S. Department of Homeland Security. (2017). Narrative analysis: Artificial intelligence (Rep.). Retrieved from https://info.publicintelligence.net/OCIA-ArtificialIntelligence.pdf
30. Shanahan, M. (2015). *The technological singularity*. Cambridge, MA: The MIT Press. Retrieved from https://mitpress.

mit.edu/books/technological-singularity

31. Litovkin, N., & Litovkin, D. (2017, May 31). Russia's digital doomsday weapons: Robots prepare for war. Retrieved from https://www.rbth.com/defence/2017/05/31/russias-digital-weapons-robots-and-artificial-intelligence-prepare-for-wa_773677
32. Wood, L. T. (2017, July 21). Russia to develop missile featuring artificial intelligence. *The Washington Times*. Retrieved from http://www.washingtontimes.com/news/2017/jul/21/russia-develop-missile-featuring-artificial-intell/
33. Mizokami, K. (2016, February 25). The Navy's new AI missile sinks ships the smart way. *Popular Mechanics*. Retrieved from http://www.popularmechanics.com/military/weapons/a19624/the-navys-new-missile-sinks-ships-the-smart-way/
34. Japan Aerospace Exploration Agency. (n.d.). Epsilon Launch Vehicle. Retrieved from http://global.jaxa.jp/projects/rockets/epsilon/
35. T39. The Brookings Institution. (2016, January 11). Trends in military technology and the future force. Retrieved from https://www.brookings.edu/events/trends-in-military-technology-and-the-future-force/
36. Edwards, J. (2017, November 8). I interviewed Sophia, the artificially intelligent robot that said it wanted to "destroy humans." Retrieved from http://www.businessinsider.com/interview-with-sophia-ai-robot-hanson-said-it-would-destroy-humans-2017-11
37. O'Connor, T. (2017, April 19). Russia built a robot that can shoot guns and travel to space. *Newsweek*. Retrieved from http://www.newsweek.com/russia-built-robot-can-shoot-guns-and-travel-space-586544
38. Metz, S. (2014). Strategic insights: The landpower robot revolution is coming. Retrieved from http://ssi.armywarcollege.edu/index.cfm/articles/Landpower-Robot-Revolution/2014/12/10
39. Coley, C. W., Barzilay, R., Jaakola, T. S., Green, W. H., & Jensen, K. F. (2017). Prediction of organic reaction outcomes using machine learning. *ACS Central Science*, *3*(5), 434–443. doi:10.1021/acscentsci.7b00064
40. Skoraczyński, G., Dittwald, P., Miasojedow, B., Szymkuć, S., Gajewska, E. P., Grzybowski, B. A., & Gambin, A. (2017). Predicting the outcomes of organic reactions via machine learning: Are current descriptors sufficient? *Scientific Reports*, *7*(1). doi:10.1038/s41598-017-02303-0
41. Lobo, D., & Levin, M. (2015). Inferring regulatory networks from experimental morphological phenotypes: A computational method reverse-engineers planarian regeneration. *PLOS Computational Biology*, *11*(6). doi:10.1371/journal.pcbi.1004295
42. Szegedy, C., Liu, W., Jia, Y., Sermanet, P., Reed, S., Anguelov, D., . . . Rabinovich, A. (2015). Going deeper with convolutions. In *2015 IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*. doi:10.1109/cvpr.2015.7298594
43. Human Rights Watch. (2015, April 9). Mind the gap: The lack of accountability for killer robots. Retrieved from https://www.hrw.org/report/2015/04/09/mind-gap/lack-accountability-killer-robots
44. U.S. Department of Defense. (2017). DoD Directive 3000.09. Retrieved from http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/300009p.pdf
45. Gubrud, M. (2012, November 27). DoD Directive on autonomy in weapon systems. Retrieved from https://www.icrac.net/dod-directive-on-autonomy-in-weapon-systems/
46. U.S. Department of Defense. (2011). DoD Directive 2311.01E. Retrieved from http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/231101e.pdf
47. U.S. Department of Defense. (2011). *Unmanned Systems Integrated Roadmap FY2011-2036* (Rep. No. 11-S-3613). Retrieved from https://fas.org/irp/program/collect/usroadmap2011.pdf
48. Work, B. (2015, December 14). *CNAS Defense Forum* [Speech]. U.S. Department of Defense. Retrieved from https://www.defense.gov/News/Speeches/Speech-View/Article/634214/cnas-defense-forum/
49. Freedberg, S. J. (2017, July 13). Artificial intelligence will help hunt Daesh by December. Breaking Defense. Retrieved from http://breakingdefense.com/2017/07/artificial-intelligence-will-help-hunt-daesh-by-december/
50. Marcum, R. A., Davis, C. H., Scott, G. J., & Nivin, T. W. (2017). Rapid broad area search and detection of Chinese surface-to-air missile sites using deep convolutional neural networks. *Journal of Applied Remote Sensing*, *11*(04), 1. doi:10.1117/1.jrs.11.042614
51. Geist, E. M. (2016). It's already too late to stop the AI arms race—We must manage it instead. *Bulletin of the Atomic Scientists*, *72*(5), 318-321. doi:10.1080/00963402.2016.1216672
52. United Nations Interregional Crime and Justice Research Institute. (n.d.). UNICRI Centre for Artificial Intelligence and Robotics. Retrieved from http://www.unicri.it/in_focus/on/UNICRI_Centre_Artificial_Robotics
53. Nichols, G., Haupt, S., Gagne, D. Rucci, A., Deshpande, G., Lanka, P., & Youngblood, S. (2018). *State of the Art Report: Artificial intelligence and machine learning for defense applications* (Rep.). Homeland Defense and Security Information Analysis Center. Manuscript in preparation.
54. Warnke, P. (2017, October 6). The effect of new technologies on nuclear non-proliferation and disarmament: Artificial intelligence, hypersonic technology and outer space. United Nations Office for Disarmament Affairs. Retrieved from https://www.un.org/disarmament/update/the-effect-of-new-technologies-on-nuclear-non-proliferation-and-disarmament-artificial-intelligence-hypersonic-technology-and-outer-space/
55. Future of Life Institute. (n.d.). The 24189 Open Letter Signatories Include. Retrieved from https://futureoflife.org/awos-signatories/
56. Future of Life Institute. (n.d.). Asilomar AI Principles. Retrieved from https://futureoflife.org/ai-principles/
57. Orseau, L., & Armstrong, S. (2016). *Safely interruptible agents. In Uncertainty In Artificial Intelligence: Proceedings of the Thirty-Second Conference (2016)* (pp. 557). Jersey City, NJ: Conference on Uncertainty in Artificial Intelligence. Retrieved from http://www.auai.org/uai2016/proceedings/papers/68.pdf
58. Johnson, B. D., Vanatta, N., Draudt, A., & West, J. R. (2017). *The new dogs of war: The future of weaponized artificial intelligence* (Rep.). West Point, NY: Army Cyber Institute. Retrieved from http://www.dtic.mil/docs/citations/AD1040008
59. Brundage, M., Avin, S., Clark, J., Toner, H. Eckersley, P., Garfinkel, B., . . . Amodei, D. (2018). *The malicious use of artificial Intelligence: Forecasting, prevention, and mitigation* (Rep.). Retrieved from https://img1.wsimg.com/blobby/go/3d82daa4-97fe-4096-9c6b-376b92c619de/downloads/1c6q2kc4v_50335.pdf
60. Allen, G., & Chan, T. (2017). *Artificial intelligence and national security* (Rep.). Cambridge, MA: Belfer Center for Science and International Affairs, Harvard Kennedy School. Retrieved from https://www.belfercenter.org/sites/default/files/files/publication/AI%20NatSec%20-%20final.pdf
61. De Spiegeleire, S., Maas, M., & Swejis, T. (2017). *Artificial Intelligence and the Future of Defense: Strategic implications for small- and medium-sized force providers* (Rep.). The Netherlands: *The Hague* Centre for Strategic Studies. Retrieved from https://hcss.nl/report/artificial-intelligence-and-future-defense
62. Jaderberg, M., Mnih, V., Czarnecki W. M., Schaul, T., Leibo, J. Z., Silver, D., & Kavukcuoglu, K. (2016). Reinforcement learning with unsupervised auxiliary tasks. Retrieved from https://arxiv.org/abs/1611.05397

Gregory Nichols, MPH, CPH
Subject Matter Expert, HDIAC

Gregory Nichols is an HDIAC Subject Matter Expert. Previously, he managed the Nanotechnology Studies Program at ORAU in Oak Ridge, Tennessee, where he provided expertise on nanotechnology-related topics and conducted research. Prior to ORAU, Nichols spent 10 years in various healthcare roles including five years as a hospital corpsman in the U.S. Navy. He has published and presented on a variety of topics including nanotechnology, public health and risk assessment. He has a bachelor's degree in philosophy and a Master of Public Health degree, both from the University of Tennessee and holds the Certified in Public Health credential.

Calendar of Events

August 2018

08/14/18 - 08/15/18 • Bethesda, MD
WMD 2018 Global Explosive Ordnance Disposal Symposium & Exhibition

08/21/18 - 08/23/18 • Washington, DC
HDS Army Science & Technology Symposium and Showcase

08/21/18 - 08/23/18 • Fort Bragg, NC
HDS Modern Warfare Symposium & Expo

08/22/18 - 08/24/18 • Washington, DC
CIP/HDS Counter UAS Summit

September 2018

09/05/18 - 09/07/18 • Washington, DC
HDS ISS World North America

09/17/18 - 09/19/18 • Washington, DC
B Biometrics for Government and Law Enforcement International Summit

09/25/18 - 09/27/18 • Quantico, VA
HDS Modern Day Marine 2018

October 2018

10/08/18 - 10/10/18 • Washington, DC
AE, M 2018 AUSA Annual Meeting & Exhibition

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**

DoD_HDIAC · in **HDIAC Outreach** · **HDIAC** · **DoDHDIAC** · **dod_hdiac**

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 Defense, 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.