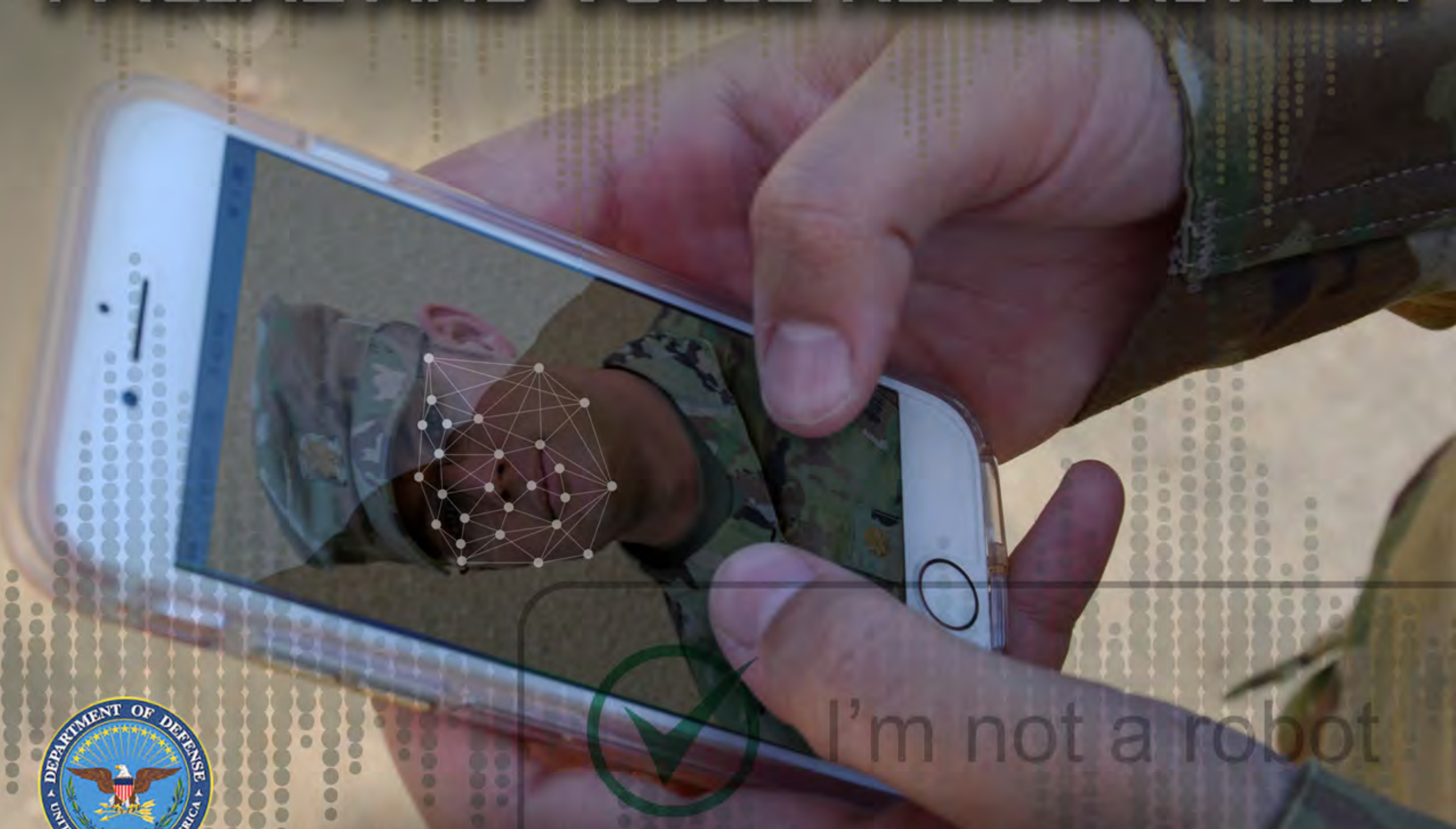
HDIAC Journal

The Journal of the Homeland Defense & Security Information Analysis Center

Volume 5 Issue 3 Fall 2018

DEFENDING AGAINST BIOMETRIC MIMICRY:

Real-time CAPTCHA-based FACIAL AND VOICE RECOGNITION



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

Volume 5 • Issue 3 • Fall 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)

ON THE COVER

Photo illustration created by HDIAC and adapted from U.S. Army and Government photos (Available for viewing at http://www.usarcent.army.mil/News/Features/Article/1302079/legacy-lives-on-as-35th-inf-div-celebrates-100-years/ and https://media.defense.gov/2017/Jan/12/2001686598/-1/-1/0/170112-F-MJ568-001.JPG)

Alternative Energy | **Cultural Studies**
Biometrics | **Homeland Defense & Security**
CBRN Defense | **Medical**
Critical Infrastructure Protection | **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
David McCarville, Social & Multi-Media Editor
Joel Hewett, Subject Matter Expert
Amanda Andrews, Editor
Tim Gould, Graphic Designer

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

Over the last quarter, our Subject Matter Experts (SME) have continued to advance the Homeland Defense & Security Information Analysis Center's (HDIAC) mission through their respective Research and Development (R&D) and Science and Technology (S&T) contributions in all eight of HDIAC's focus areas. HDIAC SMEs are recognized experts from industry, academia, and throughout government—including the Department of Defense (DoD), Department of Energy (DOE), the National Aeronautics and Space Administration (NASA), and others.

In addition to contributing to the HDIAC Journal, our SMEs have recently presented at conferences on behalf of HDIAC, provided trainings through our webinar platform, contributed to our Tech Talk video series, authored Spotlights, and supported Technical Inquiries and Core Analysis Tasks.

As technologies progress through the R&D lifecycle, HDIAC engages its Communities of Interest (COIs) and Communities of Practice (COPs) by attending and presenting at conferences and symposia dedicated to relevant technical developments with potential military or government application. In May, HDIAC attended the Special Operations Forces Industry Conference (SOFIC) to engage in technical discussions regarding the Biometrics, CBRN Defense, and Medical focus areas. In late June, HDIAC presented at the Biodefense World Summit with HDIAC SME Thomas Spencer from the Georgia Institute of Technology, regarding a Biomimetic Nose for Airborne Chemical Detection and Bubble-Based Underwater Chemical Sensing. HDIAC also displayed scientific posters from Mr. Spencer on these topics during the CBRN Defense Conference & Exhibition in late July.

HDIAC Webinars are a valuable platform for reaching our vast user community, as they offer unique training opportunities and technically-focused discussions regarding novel R&D and S&T advances. In June, HDIAC SME and Defense Threat Reduction Agency (DTRA) research microbiologist Cory Bernhards, Ph.D., presented on the topic of Biological Agent Detection for the Warfighter in support of our Weapons of Mass Destruction focus area. Because HDIAC consistently seeks ways to support the mission of DoD agencies while also pursuing broader areas for collaboration, HDIAC SME and NASA Johnson Space Center engineer Raymond Wagner, Ph.D., presented our July webinar on RFID for Continuous Monitoring in Dynamic Environments. Through this webinar, HDIAC was able to leverage advances from NASA to support our COIs and COPs in Critical Infrastructure Protection (CIP), Medical, and Homeland Defense & Security.

Social media platforms—particularly Twitter, LinkedIn, and YouTube—have become some of the most effective venues for reaching audiences and engage users. Across these platforms, HDIAC also publishes Tech Talks—short videos detailing relevant and timely R&D and S&T advances—that showcase expertise from our SMEs across all eight focus areas. In August, we published a CIP-focused Tech Talk, Engineering Resilience into the Electric Grid, in which Fangxing Li, Ph.D., the James McConnell Professor in the Department of Electrical Engineering & Computer Science at the University of Tennessee, Knoxville, highlighted novel analytical and simulation tools that can help secure the nation's electric grid against interruptions in service.

In this issue of the HDIAC Journal, HDIAC SMEs from Mississippi State University also discuss critical infrastructure issues in the energy sector. Hariteja Nandimandalam, Umesh Ghimire, and Veera Gnaneswar Gude, Ph.D., of the Civil and Environmental Engineering Department, discuss technologies for monitoring crude oil and natural gas pipelines to detect and prevent hydrocarbon leaks. They present the results of early tests on their microbial electrochemical biosensor capable of detecting and identifying multiple types and grades of hydrocarbons.

HDIAC's SMEs are an integral element of our Basic Center of Operations. From responding to Technical Inquiries, supporting our project-focused Core Analysis Tasks, to contributing to the HDIAC Journal and other publications, our volunteer SMEs bring the knowledge and experience required to rapidly address the R&D and S&T needs and challenges of HDIAC's DoD customers and clients. If you are interested in joining our SME network, please apply at: www.hdiac.org/sme_network/.

Defending Against Biometric Mimicry:

Erkam Uzun, Pak Ho “Simon” Chung, Irfan Essa, & Wenke Lee

The appeal of automatic facial and voice recognition is growing as such methods become more accurate and widely available. On the civilian side, Alipay and MasterCard deploy facial-based authentication in order to validate customer access to online financial accounts. The U.S. Department of Defense (DoD) is reportedly “shifting the use of biometrics from just law enforcement to identity and access management”—preparing to integrate these methods into Common Access Cards (CAC) for physical and logical access [1]. CACs are used by uniformed service members, DoD civilian employees, and certain contractor personnel [2]. In 2016, the DoD Defense Manpower Data Center estimated that it had issued 2.8 million CAC cards the year before—each a potential point of vulnerability for future biometric spoofing [2].

Meanwhile, several other components of DoD are seeking to implement biometric-based security and identity-verification capabilities. For example, the Defense Advanced Research Projects Agency (DARPA) is investigating the use of facial data for active (passwordless) authentication. And the Defense Information Systems Agency is researching the simultaneous use of multiple biometrics measures on mobile devices, with facial recognition included [3].

Unfortunately, facial- and voice-based authentication systems are still plagued by a wide range of impersonation attacks. Studies have shown that singular approaches to biometric authentication (such as face or voice alone) can easily be acquired from publicly available samples and manipulated with common editing tools to appear live—effectively impersonating the victim.

Many cloud-based facial- and voice-recognition systems can be defeated by the crudest impersonation attacks. So how can we defend against malicious biometric impersonation and provide better security to user authentication solutions? We propose the use of a real-time CAPTCHA system, or rtCaptcha, that combines facial and/or voice authentication requirements with a dynamic, “liveness”-based CAPTCHA challenge. Such a system prevents impersonators from knowing in advance how to circumvent standard CAPTCHA defenses.

Current Attack Methods

There are two common attack forms against bio-authentication systems: presentation attacks and compromising attacks. Depending on the usage scenario, the relevance of different attacks varies (see Figure 1). For example, if the system is used to control physical access, the integrity of the authentication device and its communication with the backend server can be guaranteed; the attacker must perform a presentation attack. In this case, employing extra sensors and better analysis of the captured data can improve the security. Examples of work in this direction include infrared to distinguish real skin from masks [4], pulse, blood circulation, or subtle head movement as liveness detection [5], or the recent FaceID on iPhone-X, which uses both infrared and depth-sensing technology to distinguish real faces from masks.

However, for logical/remote access, since the authentication device could be jeopardized, compromising attacks become more

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

Real-time CAPTCHA-based Facial and Voice Recognition

relevant and dangerous. Not only can the attacker directly feed maliciously crafted data into the authentication server (and thus overcome physical limitations of a presentation attack), but they can also read all the sensors to learn what data the server expects, then ship this data to another device. As such, defenses that respond to these threats by employing more sensors and better analyzing data are unlikely to defeat such attacks.

The digital, remote nature of compromising attacks also means they can be automated to achieve large-scale impersonation. In fact, as noted in a 2017 report released by the Office of the Deputy Assistant Secretary of the Army for Research & Technology, recently developed tools can be used to automatically impersonate someone by generating high fidelity voice or video of that victim from stolen or publicly available samples [6].

These tools include deep learning-based speech synthesizers [7, 8]; Face2Face, a real-time facial expression reenactment tool [9]; Deep Video Protraits, a photo-realistic full 3D face expression, head position and rotation, and eye gaze and blinking synthesizer [10]; and Lip Sync, a 3D face synthesizer that syncs targeted lips from an audio source [11].

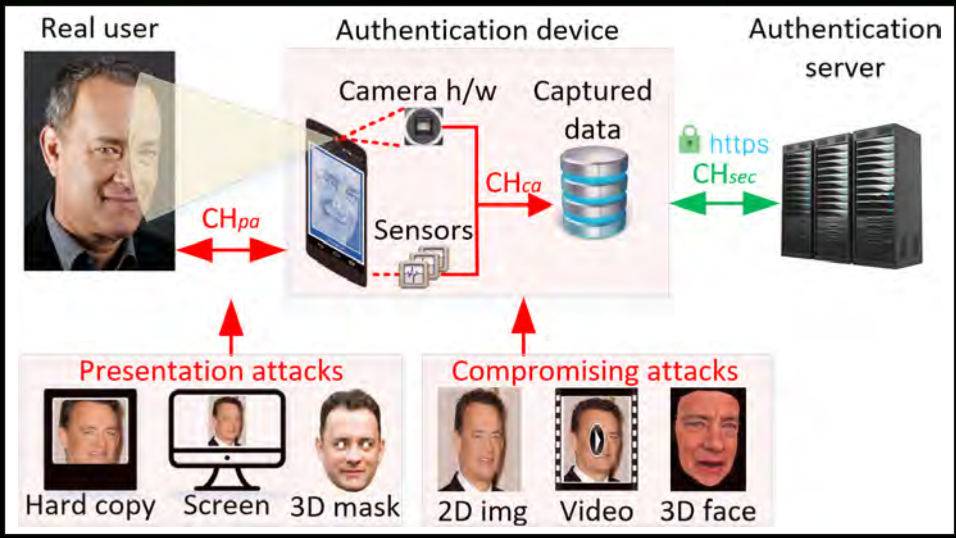


Figure 1. Attack channels specified by ISO/IEC 3017-1 standard and possible spoofing media types deployed via these channels. CH_{pa} and CH_{ca} represent presentation and compromising attack channels respectively.

Furthermore, we tested the most popular cloud-based facial- and voice-recognition services, and our study (presented here) shows that all can be defeated by the crudest impersonation attacks; mainly because these systems are not built with sufficiently high security features in mind.

Evaluating the Security of Existing Systems

Before building a new solution, we first worked to demonstrate the severity of com-

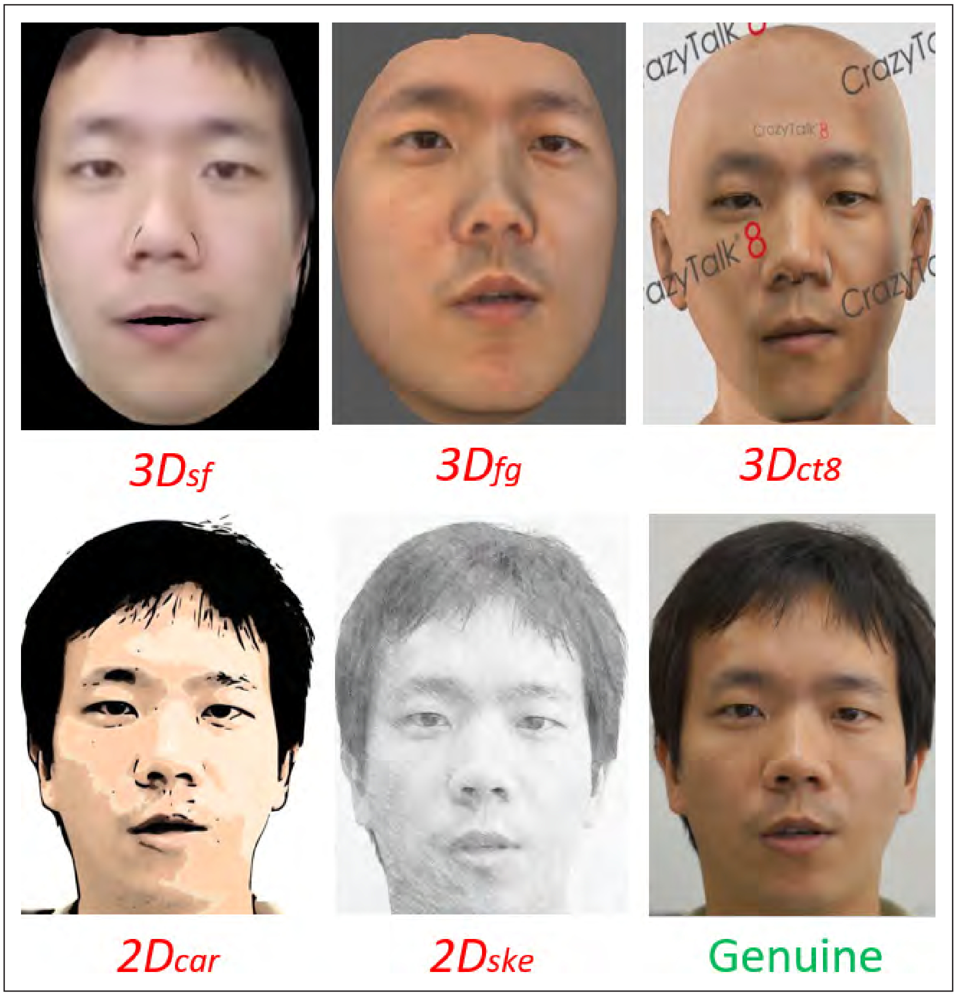


Figure 2. Genuine and spoofed versions of a full-face, frontal image of a subject from our face authentication database.

promising attacks—particularly for authentication systems that are built on top of existing cloud-based facial- and voice-recognition services. We evaluated four facial recognition systems: Microsoft Cognitive Services, Amazon Rekognition, Face++ (used by Alipay), and Kairos. We also evaluated the voice-only speaker verification system from Microsoft.

We obtained sample videos of 10 different subjects from the Chinese Academy of Sciences Institute of Automation Face Anti-Spoofing Database, used extensively by biometrics researchers worldwide [12]. For each subject, we used frames from one video to enroll the individual in the test system. We then established a true-positive and true-negative baseline by presenting an image from a different video of the enrolled user and video of an entirely different user. After that, we used another video from the enrolled user as input to synthesize new, artificial 2D and 3D images of the user.

Then we presented the synthesized images to the original tested system to see if any of these mock impersonations would successfully, but erroneously, authenticate that individual. The academic/publicly available tools we used to generate 3D attack images were: (a) Surrey Face Model ($3D_{sf}$), a multi-resolution 3D morphing modeling (3DMM) tool [13], (b) FaceGen ($3D_{fg}$), and (c) the demo version of CrazyTalk8 by Reallusion ($3D_{ct8}$). To generate the 2D attack images, we used an online tool from Cartoonizenet to create cartoonized ($2D_{car}$) and sketch ($2D_{ske}$) photos of the user. Figure 2 presents the impersonated image from each method listed above alongside the genuine (original) photo of one test subject used in the study.The results of our evaluation against existing facial-recognition systems are presented in Table 1. All evaluated systems performed fairly well under benign situations. However, all of them fell for the synthesized image generated by Surrey Face Model ($3D_{sf}$). Even a cartoonized image ($2D_{car}$) was good enough to impersonate a user at least seven out of 10 times.

To evaluate the robustness of the Microsoft Speaker Identification service (part of Microsoft Cognitive Services), we used data from the Automatic Speaker Verification (ASV) Spoofing Challenge dataset [14], and the data from the Deep Neural Network-based (DNN) speaker adaptation paper by Wu et al. [14]. Both datasets contain authentic and synthesized voice samples from real subjects.

For our experimental procedure, we first picked 10 random subjects—eight from the ASV dataset (V_{asv}) and two from the DNN dataset (V_{dnn}). We enrolled them with the Microsoft Speaker Identification service using their real voice, then tested the true-positive and true-negative baselines of the system using authentic voices from the enrolled user and another individual. After that, we tried to impersonate each enrolled subject using the different synthesized voices provided by the datasets. The results of our experiment can be found in Figure 3.

A few of the voice synthesis techniques from the ASV Spoofing Challenge achieved more than an 80 percent success rate when impersonating the target, while the voice that was synthesized using the DNN-based method had a 100 percent success rate. Each of these trials confirmed that singular forms of biometric authentication can be easily and repeatedly spoofed.

Developing a Better Defense

Employing additional sensory methods and better analysis of the captured face/voice

Cognitive Service	Baseline/Conf. (%)		Spoofed/Overall Confidence (%)				
	TP	TN	$3D_{sf}$	$3D_{fg}$	$3D_{ct8}$	$2D_{car}$	$2D_{ske}$
MS Cognitive	100/78	100/65	100/70	100/75	100/70	100/82	100/84
Amazon	100/97	100/82	100/89	80/77	90/67	70/84	60/84
Face++	100/87	100/83	100/86	100/71	100/72	90/77	70/80
Kairos	100/80	80/58	100/75	100/78	100/73	100/91	100/83

Table 1. Baseline and spoofing results of cloud-based face authentication systems.

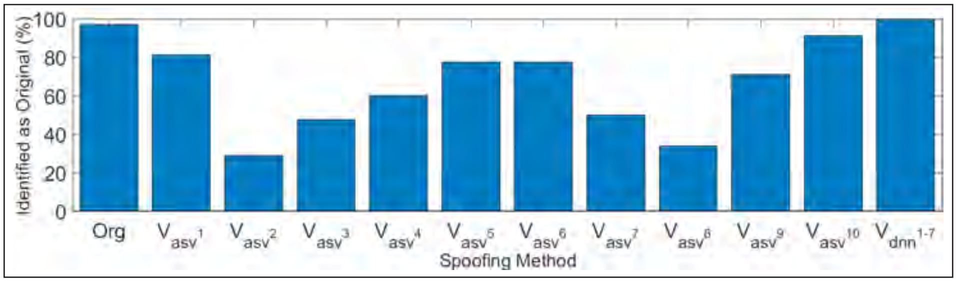


Figure 3. Identification accuracy of genuine voices and spoofed versions as originals.

data can be effective against *presentation* attacks, but such defenses cannot defeat *compromising* attacks, where we have to assume the authentication device itself is compromised. The first defense would be ineffective because the attacker could fabricate the output of any number of sensors. The second defense would simply create an arms race with the attacker, as any signals that can be used by the defender to distinguish authentic face/voice data from synthesized data could be synthesized by an attacker of sufficient sophistication.

Another popular defense used in facial- and voice-based authentication is to employ some kind of *liveness* detection. Examples of liveness detection include prompting the user to smile (Smile-To-Pay from Alipay), blink (Blink-To-Pay from MasterCard), make a particular gesture, read some text aloud [5], or display some kind of security token to the camera of the authenticating device [15]. However, existing liveness detections based on prompting the user to perform tasks are still weak because the tasks are typically drawn from a fixed, small set (as with Smile-To-Pay and Blink-To-Pay, there is only one required task).

Once the attacker has built an accurate model of the target's face/voice, most existing tools allow the attacker to manipulate the model to generate video/audio samples of the target doing or saying anything on the fly. As such, the biggest obstacle to the attacker remains the same—generate an authenticated model of the target's face/voice. As for a proposed approach in which the user must use a second computing device for authentication [15], we believe that it is not feasible to require the user to carry an extra item. This approach is either not scalable or weak against replay, since the number of security tokens users can carry is usually limited.

As Figure 1 illustrates, a fraudulent model of a target's face/voice can be developed from an attack on the transmission channel between a real user and an authentication device. However, such a model can also be created from open-source video of any person—for example, a famous individual. This heightens the vulnerability of the devices used to verify the identity of high-profile government leaders.

Changing the Game with rtCaptcha

In order to truly protect current and future facial- and voice-recognition systems from cyberattacks and malicious imposters, we propose a new, practical approach that places a formidable computational burden on the attacker by combining dynamic, live detection with a randomized CAPTCHA challenge for stronger security in real time: *rtCaptcha*.

With rtCaptcha, we change the game between the attacker and the defender from one of endless "better synthesis vs. better detection" to one that's known to be difficult for the attacker—solving CAPTCHA [16]. At authentication time, the server will send the authentication device a CAPTCHA, which will then be shown to the user. In order to accurately authenticate, the user needs to solve the CAPTCHA and announce the answer into the camera and/or microphone on the authentication device.

When presented with this kind of liveness detection challenge, even if the attacker already has an accurate face/voice model of the target, the attacker will need to first solve the CAPTCHA before they can synthesize video/audio of the targeted victim answering that specific challenge. As such, this will require a human attacker to stay in the loop (since automatically breaking CAPTCHA is still too slow and inaccurate), thus potentially preventing large-scale impersonation attacks.

In fact, our experiments showed that a CAPTCHA challenge that can be answered in two seconds by human users took state-of-the-art CAPTCHA-breaking systems more than 10 seconds. In other words, since humans can solve the CAPTCHA challenge at least twice as fast as an automated attacker, per our results, we could defeat automated, large-scale attacks by setting a very generous time-out for the user to correctly answer the CAPTCHA-based liveness challenge. To account for different paces of speech among

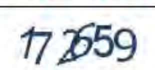
Captcha Sample	Captcha Scheme	Recognition Accuracy (%)				Response Time (seconds)			
		Hum_{aud}	Atc_{typ}	Atc_{ocr}	Atc_{best}	**Hum_{aud}**	Atc_{typ}	Atc_{ocr}	Atc_{best}
	$reCaptcha_{num}$	**87.1**	96.7	0	77.2	**0.90**	22.11	2.98	10.27
	$Ebay_{num}$	**94.1**	100	0	58.8	**0.73**	12.33	2.79	5.98
	$Yandex_{num}$	**87.7**	96.7	0	2.2	**0.89**	15.05	3.30	15.50
	$reCaptcha_{phr}$	**88.0**	91.5	0	N/A	**1.02**	20.88	3.03	N/A

Table 2. Recognition accuracy (%) and response time (in seconds) for rtCaptcha (Hum_{aud}), man-powered CAPTCHA solving service (Atc_{typ}), OCR-based CAPTCHA breaking service (Atc_{ocr}), and ML-based (state-of-the-art) CAPTCHA-breaking tools (Atc_{best}).

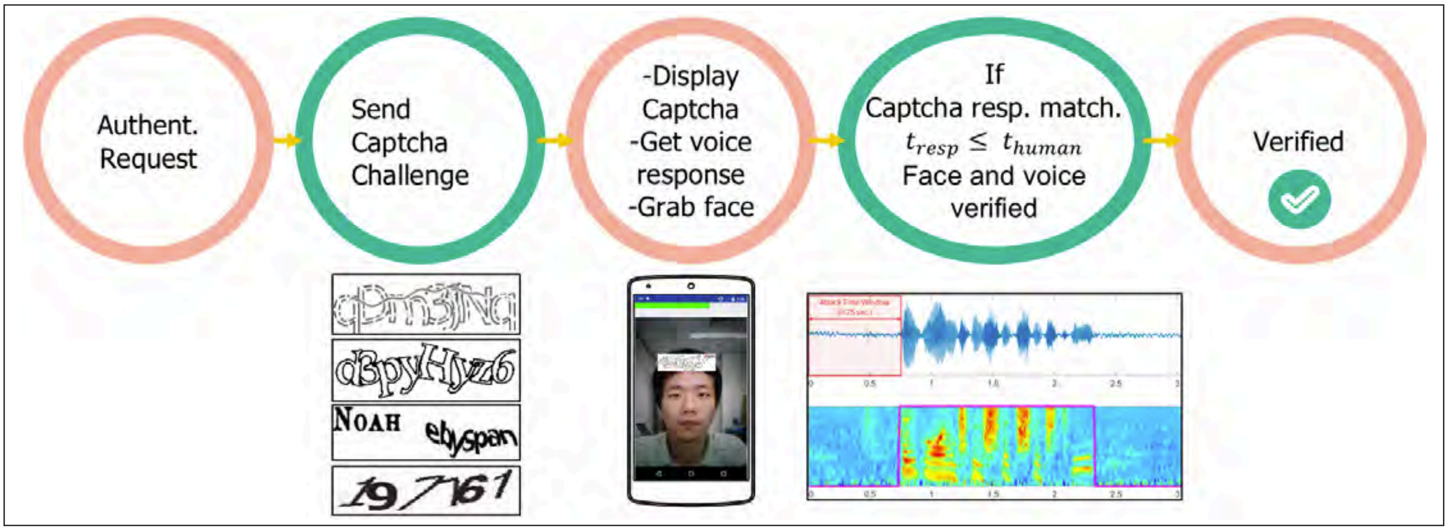


Figure 4. Process flow of rtCaptcha.

human users, our time-out mechanism employs voice activity detection techniques to detect when the user starts answering the CAPTCHA. The entire workflow of rtCaptcha is summarized in Figure 4.

Evaluating rtCaptcha

Our study, completed in 2017 and presented at the 2018 Network and Distributed Systems Security Symposium, shows that rtCaptcha is a capable and robust defense against state-of-the-art CAPTCHA-breaking schemes. In particular, we evaluated both the usability and the security of the proposed rtCaptcha scheme by recruiting 31 volunteers and asking each to solve three different kinds of CAPTCHA-based liveness detection challenges. We also asked them to solve the blink- and smile-type challenges presented by our implementation of the rtCaptcha client-side application (on an Android phone); each volunteer was given three trials for each type of CAPTCHA. All of the tested CAPTCHAs are summarized in Table 2.

For all the provided CAPTCHA responses, we used the CMU Pocketsphinx [17] to convert them into text before determining, in real time, whether the response is correct.

From our user study, we found that our subjects have an overall 89.2 percent success rate in solving the CAPTCHA. The average response time is 0.93 seconds, and the maximum response time for any CAPTCHA-based challenge is below two seconds. Finally, we will note that for those who were not successful in answering the CAPTCHA-based challenge the first time, they all successfully answered the challenges within three trials (with a different challenge for each trial).

Since the security of rtCaptcha rests on the assumption that an automated attacker will take much longer to answer the CAPTCHA-based challenge than a human user, we also evaluated many state-of-the-art CAPTCHA-breaking schemes and compared their response times with the response times of the subjects in our user study. For this study, we assumed the time-out for answering the CAPTCHA-based challenge is five seconds—more than twice the maximum response time recorded. The CAPTCHA-breaking schemes evaluated include: (a) 2Captcha (Atc_{typ}), a cloud-based, manual CAPTCHA-solving service; (b) CaptchaTronix (Atc_{ocr}), an online, Optical Character Reading-based CAPTCHA breaking scheme; and (c) state-of-the-art schemes (Atc_{best}) based on character segmentation [18] and reinforcement learning [19]. We consider the cloud-based, manual CAPTCHA-breaking scheme to be a way for the attacker to scale up their attack by employing more workers, and if that approach is successful in breaking rtCaptcha, it is still possible for the attacker to launch impersonation attacks at some scale.

The response time and the accuracy of each tested scheme is presented in Table 2 alongside results from our user study for comparison. Even though some CAPTCHA-breaking schemes achieved a response time less than three seconds, the accuracy of these instances is very low. Thus, we believe a five-second time-out for the CAPTCHA-based liveness detection provides a good balance between usability and security.

Finally, we note that the security of rtCaptcha is based on the general idea of CAPTCHA (i.e., there are problems that are very easy for humans, but very difficult for computers to solve automatically), but not on the strength of individual CAPTCHA schemes. In other words, if some of the CATPCHA schemes we studied can be automatically solved in less than five seconds at some point in the future, we can always modify rtCaptcha to use more secure CAPTCHAs. We are optimistic about this solution because CAPTCHA is a very important part of the internet ecosystem (i.e., almost every important web service will need it to prevent bots from generating fake or malicious accounts).

Conclusion

As the use of biometric technologies increases, user authentication methods like facial- and voice-based CAPTCHA challenges are likely to play a key role in securing DoD and other government networks from malicious actors. Defenses against impersonation must advance in tandem with new modes of biometric verification. Overall, our user study and comparative threat analysis prove that rtCaptcha constitutes a stronger, new basis against even the most scalable attacks that attempt to employ the latest audio/visual synthesizers and state-of-the-art CAPTCHA-breaking algorithms.

Acknowledgement

All reported user studies have been approved by the Central Institutional Review Board of the Georgia Institute of Technology Office of Research Integrity Assurance.

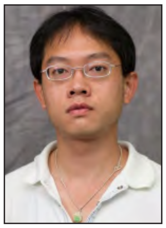
References

1. Miller, J. (2017, December 18). DoD eyeing bigger role for biometrics in CAC replacement. Federal News Radio. Retrieved from https://federalnewsradio.com/reporters-notebook-jason-miller/2017/12/dod-eyeing-bigger-role-for-biometrics-in-cac-replacement/
2. Miller, J. (2016, June 15). DoD plans to bring CAC cards to an end. Federal News Radio. Retrieved from https://federalnewsradio.com/defense/2016/06/dod-plans-bring-cac-cards-end/
3. Cordell, C. (2018, January 11). DISA working on multi-factor authentication that includes how you walk, retiring director says. FedScoop. Retrieved from https://www.fedscoop.com/7-factor-authentication-coming-includes-walk-disas-lynn-says/
4. Steiner, H., Sporrer, S., Kolb, A., & Jung, N. (2016). Design of an active multispectral SWIR camera system for skin detection and face verification. Journal of Sensors, 2016, 1-16. doi:10.1155/2016/9682453
5. Holtz, C. (2016, November). Computerized system and method for determining authenticity of users via facial recognition. U.S. Patent No. 2016/0342851 A1. Washington, DC: U.S. Patent and Trademark Office.
6. Augustyn, J. (2017, November). Emerging science and technology trends: 2017–2047. Office of the Deputy Assistant Secretary of the Army. Retrieved from http://www.dtic.mil/dtic/tr/fulltext/u2/1043071.pdf
7. Shonesy, K. (2015, September 25). UAB research finds automated voice imitation can fool humans and machines. UAB News. Retrieved from http://www.uab.edu/news/research/item/6532-uab-research-finds-automated-voice-imitation-can-fool-humans-and-machines
8. Wu, Z., Swietojanski, P., Veaux, C., Renals, S., & King, S. (2015). A study of speaker adaptation for DNN-based speech synthesis. Proceedings of Interspeech 2015 International Speech Communication Association. doi: 10.7488/ds/259
9. Thies, J., Zollhofer, M., Stamminger, M., Theobalt, C., & Niebner, M. (2016). Face2Face: Real-time face capture and reenactment of RGB videos. 2016 IEEE Conference on Computer Vision and Pattern Recognition (CVPR). doi:10.1109/cvpr.2016.262
10. Kim, H., Garrido, P., Tewari, A., Xu, W., Thies, J., Niessner, M.,…Theobalt, C. (2018) Deep video portraits. ACM Transactions on Graphics 2018 (TOG). Retrieved from https://web.stanford.edu/~zollhoef/papers/SG2018_DeepVideo/paper.pdf
11. Suwajanakorn, S., Seitz, S. M., & Kemelmacher-Shlizerman, I. (2017). Synthesizing Obama: Learning lip sync from audio. ACM Transactions on Graphics, 36(4), 1-13. doi:10.1145/3072959.3073640
12. Zhang, Z., Yan, J., Liu, S., Lei, Z., Yi, D., & Li, S. Z. (2012). A face antispoofing database with diverse attacks. 2012 5th IAPR International Conference on Biometrics (ICB). doi:10.1109/icb.2012.6199754
13. Huber, P., Hu, G., Tena, R., Mortazavian, P., Koppen, W. P., Christmas, W. J., . . . Kittler, J. (2016). A multiresolution 3D morphable face model and fitting framework. Proceedings of the 11th Joint Conference on Computer Vision, Imaging and Computer Graphics Theory and Applications. doi:10.5220/0005669500790086
14. Wu, Z., Kinnunen, T., Evans, N., Yamagishi, J., Hanilçi, C. & Sahidullah, M. (2015). ASVspoof 2015: The first automatic speaker verification spoofing and countermeasures challenge. Proceedings of Interspeech 2015 International Speech Communication Association.
15. Chang, A. I. S., Systems and Methods for Securely Authenticating Users via Facial Recognition. U.S. Patent No. 9,740,920 B1. (2017, August). Washington, DC: U.S. Patent and Trademark Office.
16. Uzun, E., Chung, S. P., Essa, I., & Lee, W. (2018). rtCaptcha: A real-time CAPTCHA based liveness detection system. Proceedings 2018 Network and Distributed System Security Symposium. doi:10.14722/ndss.2018.23253
17. Huggins-Daines, D., Kumar, M., Chan, A., Black, A., Ravishankar, M., & Rudnicky, A. (2006). Pocketsphinx: A free, real-time continuous speech recognition system for hand-held devices. 2006 IEEE International Conference on Acoustics Speed and Signal Processing Proceedings. doi:10.1109/icassp.2006.1659988
18. Gao, H., Yan, J., Cao, F., Zhang, Z., Lei, L., Tang, M., . . . Li, J. (2016). A simple generic attack on text captchas. Proceedings 2016 Network and Distributed System Security Symposium. doi:10.14722/ndss.2016.23154
19. Bursztein, E., Aigrain, J., Moscicki, & Mitchell, J. C. (2014). The end is nigh: Generic solving of text-based CAPTCHAs. WOOT. Retrieved from https://www.usenix.org/system/files/conference/woot14/woot14-bursztein.pdf

Erkam Uzun

Doctoral Student, School of Computer Science, Georgia Institute of Technology

Erkam Uzun is a fourth-year Computer Science Ph.D. student working in the Institute for Information Security and Privacy at Georgia Tech under the supervision of Prof. Wenke Lee. He currently holds B.Sc. degrees in both Computer Engineering and Electrical & Electronics Engineering and a M.Sc. degree in Computer Engineering from TOBB University of Economics and Technology, Turkey. His research interests range from audio/visual authentication systems, live biometrics, privacy preserving authentication and digital forensics to machine learning, deep learning and optimization.



Pak Ho "Simon" Chung

Post-Doctoral Fellow, School of Computer Science, Georgia Institute of Technology

Simon Chung is a research scientist at the Institute for Information Security and Privacy at the Georgia Institute of Technology. He obtained his Ph.D. degree from the University of Texas at Austin. His research interests range from UI security, improving the security and usability of authentication systems, to employing the latest hardware features to improve systems security.

Irfan Essa, Ph.D.

Associate Dean and Professor, School of Interactive Computing, Georgia Institute of Technology

Irfan Essa, Associate Dean, is a professor in the School of Interactive Computing (IC) of the College of Computing (CoC), and Adjunct Professor in the School of Electrical and Computer Engineering, Georgia Institute of Technology. He joined the Georgia Tech faculty in 1996 after earning his M.S., Ph.D., and holding a research faculty position at the Massachusetts Institute of Technology (Media Lab). Irfan Essa works in the areas of Computer Vision, Computer Graphics, Computational Perception, Robotics and Computer Animation, with potential impact on Video Analysis and Production, Human Computer Interaction, and Artificial Intelligence research.

Wenke Lee, Ph.D.

Co-Executive Director, Institute for Information Security & Privacy, Georgia Institute of Technology

Wenke Lee, Ph.D., is co-executive director of the Institute for Information Security & Privacy and responsible for continuing Georgia Tech's international leadership in cybersecurity research and education. Additionally, he is the John P. Imlay, Jr., Chair of Software and professor of computer science in the College of Computing at Georgia Tech, where he has taught since 2001. He received his Ph.D. from Columbia University in 1999. His research expertise includes systems and network security, botnet detection and attribution, malware analysis, virtual machine monitoring, mobile systems security, and detection and mitigation of information manipulation on the internet.

Detecting Chemicals in Drinking Water: Field Testing Biologically-based Toxicity Sensors

Mark Widder, William van der Schalie, Linda Brennan, David Trader, William Dennis, & Valerie DiVito

Military personnel deployed around the world require high-quality drinking water, and specific procedures are in place to ensure that military field water supplies are properly treated and monitored [1]. Chemical contaminants pose potential threats to field drinking water [2], and although current water treatment technology is highly efficient, removal of contaminants may be inadequate if chemicals are present in source waters at high concentrations or if the chemicals are introduced after processing. In the Army, preventive medicine (PM) personnel periodically test water supplies using the Water Quality Analysis Set-Preventive Medicine (WQAS-PM) and associated equipment, including field tests for a limited number of specific chemicals of concern. While water supplies can be evaluated more thoroughly at off-site laboratories, these evaluations are done infrequently and are more expensive. Additionally, analytical test results are usually not available for days or weeks.

There is a need, therefore, for field test methods that provide rapid assessment for a broad range of chemical contaminants, including agricultural and industrial chemicals, both organic and inorganic. Analytical chemistry instrumentation for this purpose (e.g., gas and liquid chromatography and mass spectrometry) tends to be complex and expensive, and has limited potential for field use. An alternative approach is to measure the response of a biological indicator to the presence of toxic chemicals in a water sample. Although there are analyte-specific biosensors (e.g., those that use antibodies, enzymes, and nucleic acids for detection of particular chemicals in water [3-6]), many biosensors would be required to detect a broad range of potential contaminants [7]. The goal is to develop a toxicity sensor with biological components that can rapidly respond to a broad spectrum of toxic compounds at concentrations relevant to warfighter health.

The Environmental Sentinel Biomonitor System

At the U.S. Army Center for Environmental Health Research, we developed a toxicity detection device, the Environmental Sentinel Biomonitor system (ESB), based on Army requirements defined in 2013 in a Capability Development Document (CDD) [8]. The Army needs a device that can detect a broad spectrum of toxic industrial chemicals, has field-portability, and utilizes biological components that have a shelf-life of at least nine months (refrigeration, but not freezing, of perishable components is permitted). Finally, the required system must perform satisfactorily in an independent laboratory evaluation using procedures developed for the U.S. Environmental Protection Agency's Technology Testing and Evaluation Program (TTEP) [9]. Here, we demonstrate that the ESB meets these requirements, and report for the first time the positive results of an in-theater field evaluation of the ESB system in Iraq and Kuwait during the spring of 2016.

Because of the large number of available toxicity sensor devices and the constraints imposed by Army field use requirements, we used a formal decision analysis approach for toxicity sensor downselection [10]. After considering 38 toxicity sensor technologies, the best performing sensors were found to be a cell-based electric cell-substrate impedance sensing (ECIS) test (Nanohmics, Inc.) and an enzyme inhibition test (ACE™ Rapid Test for Acetylcholinesterase Inhibitors, ANP Technologies) [10]. Together, these toxicity sensors respond to the broadest range of chemicals while minimizing the technical complexity, size, weight, and cost of the system.

The ECIS test monitors alterations in the electrical impedance of a monolayer of rainbow trout gill epithelial cells (RTgill-W1) [11], grown on fluidic biochips to indicate chemical-induced toxicity. Cells are seeded in two separate fluidic channels on the biochip containing electrodes; during testing, one

Image Credit | *Photo Illustration created by HDIAC and adapted from U.S. Army photo by Sgt. Timothy Koster, 362nd Mobile Public Affairs Detachment (Available for view-*

channel receives the control sample and the other receives the test sample. When a toxic chemical compromises the integrity of the cell monolayer, the ECIS sensor records a change in electrical impedance. Water sample toxicity is indicated when the impedance in the control channel differs significantly from the test channel during a one-hour exposure. ECIS biochips can be maintained for at least nine months at 6 degrees Celsius with no media replacement.

The ECIS test is used together with the ACE™ test to evaluate a water sample. The ACE™ test is an enzymatic assay designed to detect neurotoxicants—specifically, cholinesterase-inhibiting compounds such as organophosphate and carbamate pesticides. It monitors the activity of the enzymes carboxyl esterase (CE) and acetylcholinesterase (AChE) using a reporting chemical that fluoresces under ultraviolet (UV) light [12].

During testing, control and test water samples are added to separate vials containing either AChE or CE for 30 minutes. Then, the sample-enzyme mix is added to a test ticket well containing the reporting chemical that fluoresces after being cleaved if the active enzyme is present. The ticket is read after 15 minutes; interference with enzyme function will result in detectable color differences. Consumables are stable for at least nine months at room temperature.

Equipment for conducting both ECIS and ACE™ tests is stored in the ruggedized ESB carrying case (see Figure 1). The ECIS fluidic biochips, which require temperature control for long-term viability, can be transported in small insulated containers.

ESB Testing and Evaluation

To ensure that the ESB meets Army requirements as defined in the CDD, and is useful to Army PM personnel, we conducted three types of testing: toxicity testing to determine ESB responses to challenge chemicals, environmental testing, and field evaluations of ESB performance.

Toxicity Testing

To meet Army requirements, the ESB needs to detect at least 50 percent of a diverse set of 18 chemicals within two hours (see Table 1). For each chemical, the ESB needs to respond to water sample concentrations that exceed the seven- to 14-day military exposure guideline (MEG) levels, assuming an individual water consumption rate of 15 L per day, which is typical of arid environments [13]. The upper limit for a useful toxicity sensor response is defined as the estimated human lethal concentration (HLC) [14]; a level estimated to be lethal to a 70 kg person consuming 15 L of water in a day. Testing results showed that the combined ACE and ECIS sensor responses exceed CDD requirements for toxicant response to the 18 chemicals in the test set (i.e., they were able to detect more than 50 percent of the chemicals within one hour at levels that were relevant to human health) [12, 15]. It is important to note that while these test chemicals include diverse substances with varying modes of toxic action, they are not the sole focus for ESB detection; rather they are a subsample of a much larger set of potential threat chemicals to which the ESB can respond.

In addition to the toxicants, potential interfering materials were evaluated. For Army field water, the primary concern is contamination by chemicals used to disinfect drinking water—namely, chlorine and chloramine. For chloramine, the ECIS responds at 10 mg/L, with no response at 5 mg/L [15]. However, in practice, water samples for ESB testing can be dechlorinated prior to ESB testing using a reducing agent, so drinking water disinfection chemicals should not be an issue.

Environmental Testing

Army medical equipment, such as the ESB system, is required to pass field-relevant environmental testing administered by the U.S Army Medical Research and Materiel Command Test Branch, following Military Standard (MIL-STD) 810G [16]; these tests were conducted on both the ACE and ECIS

ing at https://www.army.mil/article/110900/eighth_army_medics_work_with_katusa_soldiers_on_real_world_mission_to_keep_soldiers_in_fight*) and Adobe Stock.*

Figure 1. ECIS (instrument on the left) and ACE™ sensors (right) with reusable supplies packaged in the ESB carrying case.

instruments [17]. "Operational" refers to active testing with the ACE and ECIS under the specified test conditions. "Non-operational" refers to storage under the specified test conditions, with testing done at room temperature.

- Low temperature, operational (15° C) and non-operational (0° C)
- High temperature, operational (45° C) and non-operational (71° C)
- Altitude (4,572 meters equivalent), operational and non-operational
- Settling dust and sand (settling for one hour on exposed equipment), non-operational
- Ground vibration (1.90 root mean square acceleration (Grms) for one hour), non-operational
- Transit drop (ESB packaged in its case was dropped from a height of four feet onto a steel surface)
- Loose cargo transportation, non-operational (ESB packaged in its case was vibrated at 300 rpm, 2.5 cm amplitude for one hour)

Both the ECIS and ACE tests passed environmental testing [17]. One notable point was the low temperature operational ACE test conducted, where the negative control tickets failed to show viable enzyme activity after 15 minutes. This was likely due to reduced enzyme activity at the lower test temperatures. Test readings were successful when the incubation time was extended to 25 minutes, meeting the standard of a successful test.

Field Testing

The ESB system was evaluated using a customer assessment organized by U.S. Army Medical Department Board, as well as in field assessments by PM personnel. The customer assessment determined if the ESB system would support the PM mission and if it was usable in an operational environment [18]. Following a four-hour familiarization period with the equipment, six teams of Army PM specialists and an environmental science and engineering officer used the ESB system in an operational environment to process blind water samples that were either negative or positive controls.

Operation was tested using commercial power (120 volts AC [VAC]), generator power (220 VAC), and internal battery power. U.S. Army Medical Department Board staff then evaluated ESB system performance against operationally-relevant criteria.

Overall, the results were supportive of ESB field use [18].The functionality of the ESB system supports the PM mission. Test completion time met CDD requirements, and 11 of 13 assessment participants indicated that ESB functionality was mission supportive.

- The ESB system was usable in an operational environment. System weight met CDD requirements, and the ESB functioned under 120 VAC, 220 VAC, and internal battery power as required. All 13 assessment participants thought the ESB was usable for water sample analysis in an operational environment.
- The ESB does not pose any actual or potential safety hazard to personnel, equipment, or facilities in an operational environment. The pliers used to open the ACE reagent vials pose a minor cut hazard.
- The ESB system was usable after transport. The ESB was used successfully to conduct water sample analyses after a transportation test (see Figure 2).

One identified problem involved several instances of false positive and negative ECIS readings. The false negatives occurred with the ammonia positive control, most likely because the ammonia concentration used was too low. Subsequently, a new positive control test chemical was used.

The false positives were thought to be due to the sensitivity setting used for the system statistical software. As a result, the statistical models were adjusted to incorporate the additional variability noted under field conditions and validated to ensure that no substantial loss in toxicant sensitivity occurred due to the sensitivity adjustments. As a check, PM personnel at the 1st Area Medical Laboratory, Aberdeen Proving Ground, conducted additional ECIS testing. When the ECIS results were analyzed using the refined statistical algorithm, there were no false positive or negative results.

The ESB system (both ECIS and ACE) was also evaluated by the 227th Medical Detachment (Preventive Medicine) in a deployed environment at Taji, Iraq and Camp Arifjan, Kuwait, over the spring of 2016. Two ESB units, along with consumables, were shipped from the U.S. to Kuwait. The theater biochemist coordinated evaluation by 18 participants (PM personnel), who completed a total of 20 water tests (eight ECIS and ACE tests at Camp Taji; 12 ECIS tests at Camp Arifjan). Participants were asked to fill out customer assessment forms evaluating their experiences with the ESB system.

Table 1. ESB Test Chemicals [12]
Acrylonitrile
Aldicarb
Ammonia
Arsenic (sodium arsenite)
Azide (sodium azide)
Copper (sulfate)
Cyanide (sodium)
Fenamiphos
Fluoroacetate (sodium)
Mercury (chloride)
Methamidophos
Nicotine
Paraquat (dichloride)
Pentachlorophenate (sodium)
Phenol
Thallium (sulfate)
Toluene

Figure 2. Soldiers performing water testing with the ESB device. Soldiers used the ESB during the customer assessment in a field laboratory setting as well as in the back of a High Mobility Multipurpose Wheeled Vehicle after transport on an off-road course.

Overall, the in-theater evaluations of the ESB system were highly favorable. There were no issues shipping equipment and reagents into theater (five days from Fort Detrick to Camp Taji, Iraq), and ECIS biochips remained viable when maintained by the theater biochemist for all of the evaluations by PM personnel. ECIS tests were completed in 19 of 20 evaluated with only one test yielding an error; there were no false positives. All 20 evaluators felt that the ESB system was supportive of the PM mission. Theater biochemists on different tours also transported the ESB system with them on missions to Camp Taji and missions to Northern Iraq, where successful water testing was performed.

Conclusion

As the ESB developed into a dual toxicity sensor that is currently in the pipeline for Army field deployment, customer assessment and field testing provided critical feedback that could not be obtained in a laboratory setting. Customer input led to modifications in some of the practical aspects of the ESB, such as manipulating pipets and syringes, accurately measuring water samples, ease of opening vials, and clarification of instructional materials.

The feedback also allowed for fine-tuning of statistical algorithms to ensure that false negatives and positives would be a rare occurrence. The ESB is scheduled for fielding in FY19 as part of the WQAS-PM to provide a rapid test for chemical-related toxicity in Army field drinking water supplies. As the ESB evolves, we will continue to seek field testing for any new modifications. Although the ESB was initiated specifically to help Army PM personnel screen potable water for the presence or absence of a wide range of toxic chemicals, the fact that all services have a common mission to provide warfighters with clean drinking water supplies means the ESB has applicability across the DoD.

Further, with the potential for development of novel chemical warfare agents or for the introduction of unknown or unsuspected materials into water supplies, the use of a toxicity-based approach for detection of these materials can provide an important complement to currently-utilized analytical chemistry devices.

Acknowledgements

The authors would like to thank Nanohmics, Inc., and ANP Technologies for their commercial support in developing the ESB system. And a final thanks to all of the Army medical personnel, military, civilian, and contractors who have helped in the development and advancement of the ESB system.

Disclaimer

The views, opinions, and/or findings contained in this article are those of the authors and should not be construed as official Department of the Army position, policy, or decision, unless so designated by other official documentation. Citations of commercial organizations or trade names in this article do not constitute an official Department of the Army endorsement or approval of the products or services of these organizations. This research was supported in part by an appointment to the Research Participation Program at the U.S. Army Center for Environmental Health Research administered by the Oak Ridge Institute for Science Education through an interagency agreement between the U.S. Department of Energy and USAMRMC.

References

1. Departments of the Army, Navy and Air Force. (2010). Sanitary Control and Surveillance of Field Water Supplies. TB MED 577, NAVMED P-5010-10, AFMAN 48-138_IP. Washington, DC.
2. Salem, H., Whalley, C. E., Wick, C. H., Gargan, T. P., & Burrows, W. D. (2008). Chemical warfare agent threat to drinking water. Chemical warfare agents: Chemistry, pharmacology, toxicology, and therapeutics (second edition) (pp. 21-50), Boca Raton, FL: CRC Press/ Taylor & Francis Group, LLC.
3. Eltzov, E., & Marks, R. S. (2010). Whole-cell aquatic biosensors. Analytical and bioanalytical chemistry, 400(4), 895-913. doi:10.1007/s00216-010-4084-y
4. Pancrazio, J. J., Whelan, J. P., Borkholder, D. A., Ma, W., & Stenger, D. A. (1999). Development and application of cell-based biosensors. Annals of biomedical engineering, 27(6), 697-711. doi: 10.1114/1.225
5. States, S., Scheuring, M., Kuchta, J., Newberry, J., & Casson, L. (2003). Utility-based analytical methods to ensure public water supply security. Journal - American water works association, 95(4), 103-115. doi:10.1002/j.1551-8833.2003.tb10337.x
6. Kelly, T., Baxter, W., McCauley, M., & E. Koglin. (2008). Testing of screening technologies for detection of toxic industrial chemicals in all hazards receipt facilities. (EPA/600/R-08/034). Washington, DC: U.S. Environmental Protection Agency.
7. Brennan, L. M., Widder, M. W., Lee, L. E., & van der Schalie, W. H. (2012). Long-

term storage and impedance-based water toxicity testing capabilities of fluidic biochips seeded with RTgill-W1 cells. Toxicology in vitro, 26(5), 736-745. doi: 10.1016/j.tiv.2012.03.010

8. U.S. Army. (2013). Capability Development Document for Environmental Sentinel Biomonitor Increment: 1. Catalog of Approved Requirement Documents (CARDS #14099). (Unpublished manuscript, available from the Office of the U.S. Army Deputy Chief of Staff, G-8, 700 Army Pentagon, Room 3E406, Washington, DC 20310-0700)
9. U.S. Environmental Protection Agency. (2008). Quality Management Plan National Homeland Security Research Center Technology Testing and Evaluation Program Version 3. Columbus, OH. Retrieved from https://nepis.epa.gov/Exe/ZyPURL.cgi?Dockey=P10062P1.txt .
10. Army Edgewood Chemical Biological Center, Aberdeen Proving Ground, MD. (2018). Environment Sentinel Biomonitor Technology Assessment. Retrieved from http://www.dtic.mil/dtic/tr/fulltext/u2/a586335.pdf
11. Lee, L. E. J., Dayeh, V. R., Schirmer, K., & Bols, N. C. (2009). Applications and potential uses of fish gill cell lines: examples with RTgill-W1. In Vitro Cellular & Developmental Biology-Animal, 45(3-4), 127-134. doi: 10.1007/s11626-008-9173-2
12. U.S. Army Center for Environmental Health Research, Fort Detrick, MD. (2014). An Evaluation of the NIDS® ACE™ Test. Retrieved from http://www.dtic.mil/dtic/tr/fulltext/u2/a603987.pdf
13. U.S. Army Public Health Command. (2013). Environmental health risk assessment and chemical exposure guidelines for deployed military personnel. Aberdeen Proving Ground, MD. Retrieved from https://phc.amedd.army.mil/PHC%20Resource%20Library/TG230-DeploymentEHRA-and-MEGs-2013-Revision.pdf
14. U.S. Army Center for Environmental Health Research, Fort Detrick, MD. (2006). Derivation of Human Lethal Doses. Retrieved from http://www.dtic.mil/dtic/tr/fulltext/u2/a494706.pdf
15. Widder, M. W., Brennan, L. M., Hanft, E. A., Schrock, M. E., James, R. R., & Schalie, W. H. (2014). Evaluation and refinement of a field portable drinking water toxicity sensor utilizing electric cell–substrate impedance sensing and a fluidic biochip. Journal of Applied Toxicology, 35(7), 701-708. doi: 10.1002/jat.3017
16. Department of Defense. (2008). Department of Defense test method standard: environmental engineering considerations and laboratory tests. MIL-STD-810G. Retrieved from http://www.wsmr.army.mil/RCCsite/Documents/265-06(Supp)_Radar%20Transponder%20Antenna%20Sys%20Eval%20Handbook/mil-std-810f.pdf
17. U.S. Army Medical Research & Materiel Command Test Branch, Fort Detrick, MD. (2014). Environmental Testing: Environmental Sentinel Biomonitor System. Test File #220.
18. Cabigon, G., & Breckheimer, D. (2014). Customer assessment report for the Environmental Sentinel Biomonitor (USAMEDDBD Project 3-12a). (Unpublished manuscript, available from the U.S. Army Medical Department Center and School, 3630 Stanley Road, Suite 301, JBSA Fort Sam Houston, TX 78234).

Mark Widder
Research Biologist, U.S. Army Center for Environmental Health Research
Mark Widder is a research biologist at the United States Army Center for Environmental Health Research in the Environmental Health Program located at Fort Detrick in Frederick, Maryland. He has worked for the Army for over 20 years in the applied medical research areas of toxicology and biosensor development to support soldier health and preventive medicine.

William van der Schalie, Ph.D.
Research Fellow, Oak Ridge Institute of Science and Technology, U.S. Army Center for Environmental Health Research
William van der Schalie has an Oak Ridge Institute for Science Education (ORISE) Research Participation Program appointment at USACEHR (Ph.D., Virginia Polytechnic Institute and State University). He is interested in the application of toxicity sensors for chemical detection and has assisted with the research and development process for the Army's Environmental Sentinel Biomonitor system.

Linda Brennan
Research Biologist, U.S. Army Center for Environmental Health Research
Linda Brennan is a research biologist at the U.S. Army Center for Environmental Research. Her research efforts have focused on assisting in the development and in-house testing of the Army's Environmental Sentinel Biomonitor system, which is comprised of water toxicity sensors designed to be used by soldiers to detect chemical toxicants in drinking water.

David Trader
Research Biologist, U.S. Army Center for Environmental Health Research
David Trader is a research biologist, institutional animal care and use committee chair, and executive officer at the USACEHR. His research interests are in water toxicity, specifically sensors and kits designed to detect toxic industrial chemicals.

William Dennis
Chemist, U.S. Army Center for Environmental Health Research
William Dennis is an analytical chemist at the U.S. Army Center for Environmental Research. He obtained his B.A. in Chemistry from the University of Maryland Baltimore County in 1989. He has been performing analytical chemistry for over 25 years in support of research with a focus on mass spectroscopy.

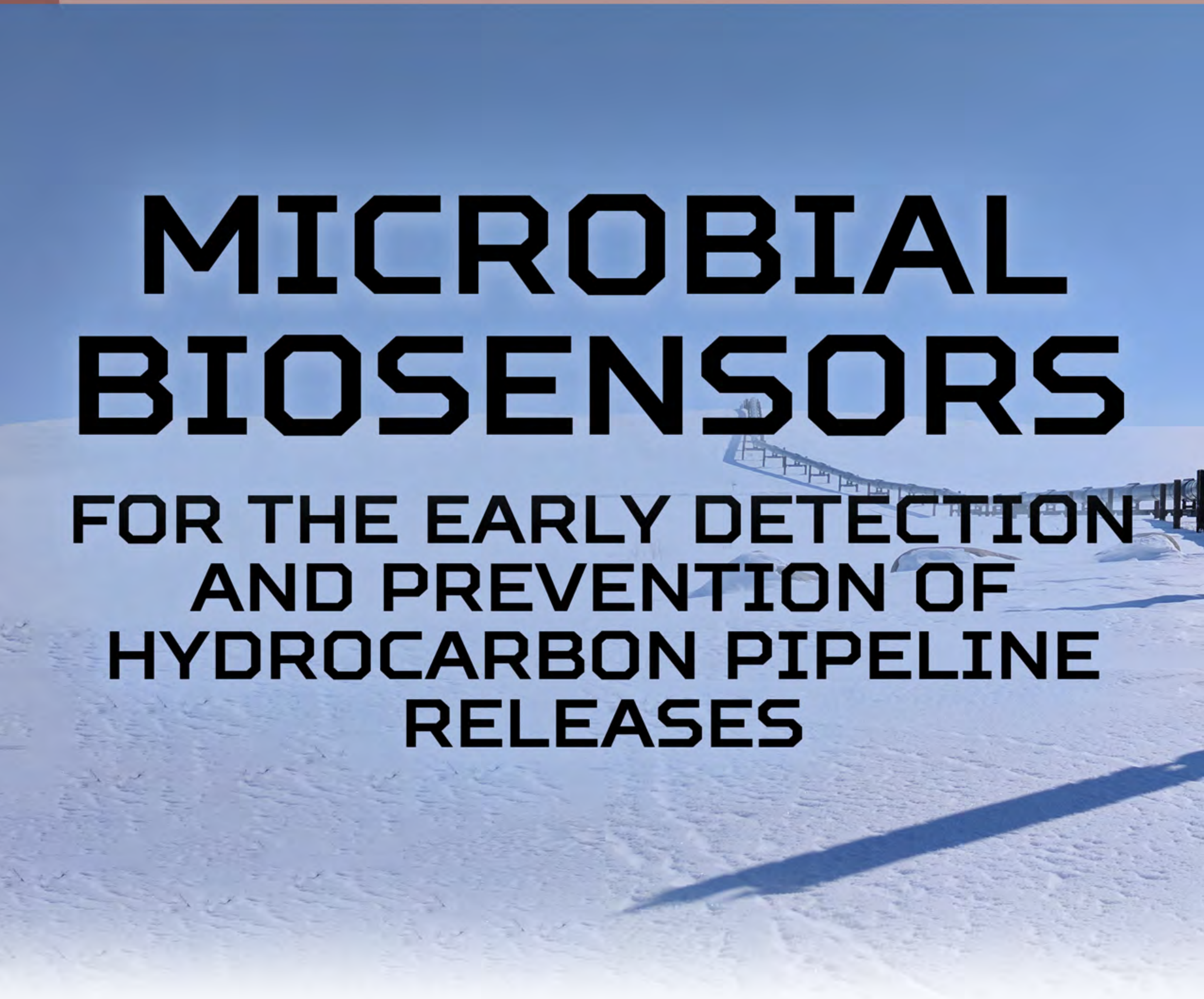
Valerie DiVito, Ph.D.
Director, Environmental Health Program, U.S. Army Center for Environmental Health Research
Valerie DiVito leads a multidisciplinary biomedical research program at the U.S. Army Center for Environmental Health Research to investigate the mechanisms of action for acute and chronic health effects caused by exposure to environmental hazards and toxicants. This work uses a systems toxicology approach to inform the development of surveillance tools, diagnostics, and interventions to prevent and/or mitigate the adverse consequences of toxicant exposure, including decreased military performance in occupational and operational environments.

Discover the value of sharing your DoD-funded research...

R&E Gateway Powered by DTIC

https://go.usa.gov/xUFVu

Defense Technical Information Center (DTIC) | Fort Belvoir, VA | https://discover.dtic.mil



MICROBIAL BIOSENSORS

FOR THE EARLY DETECTION AND PREVENTION OF HYDROCARBON PIPELINE RELEASES

Hariteja Nandimandalam, Umesh Ghimire, & Veera Gnaneswar Gude

Oil and natural gas transportation through pipelines—both onshore and offshore—is considered a safer alternative on a ton-mile basis to hauling fuel by tanker trucks, freight trains, or marine carriers [1]. Even so, the transportation of liquid or gas-phase hydrocarbons over long distances can lead to accidental releases via pipeline ruptures or leaks. The number and severity of incidents related to leaking pipelines, and the spills associated with them, have increased substantially over the last three decades (see Figure 1) [2].

Although safer than the alternatives for fuel transportation, pipeline networks require thorough maintenance and upkeep to remain operable. Pipeline ruptures can result in significant economic, environmental, and energy-security consequences. The energy system of the United States is one of 16 infrastructure sectors identified by the Department of Homeland Security (DHS) as "critical" to the nation's economic security, public health, safety, and defense [3,4].

The department's sector-specific plan for critical energy infrastructure notes that pipelines face two major risks: operational hazards caused by blowouts, spills, and personal injury; and interruptions in energy supplies due to damaged or inoperable hydrocarbon pipeline infrastructure [4].

Technologies that enable operators to detect small leaks before a rupture or major release incident occurs can significantly reduce these risks. The early detection of small leaks allows remedial action to ensure continued pipeline integrity [5]. The need for a new class of hydrocarbon sensors is especially pressing, because sensor types currently in use for onshore pipelines in the United States often fail to detect releases. Only 22 percent of the releases that occurred between 2010 and 2016 were detected by advanced pipeline sensor systems [6].

Image Credit | *Photo Illustration created by HDIAC and adapted from public domain photo (Available for viewing at https://www.usgs.gov/media/images/alaskan-pipeline-spring-2017).*

Current State of the Art

Well-known methods for leak detection in onshore pipelines include acoustic monitoring, optical sensor gas sampling, soil monitoring, flow monitoring, magnetic flux leakage, and dynamic model-based methods [9]. “Pig” (or pipeline-inspection-gadget) technology is used to detect stress corrosion cracking, uniform or general corrosion, and pitting corrosion—including gouges, dents, anomalous weld seams, longitudinal cracks, longitudinal grooves, and other faults in the pipeline wall [10]. In-pipe robots used for early detection include: pig type, wheel type, caterpillar type, walking type, inchworm type, screw type, and wall-press. Another monitoring technique involves the use of unmanned aerial vehicles (or autonomous underwater vehicle) for pipeline and flowline surveillance [10]. The major

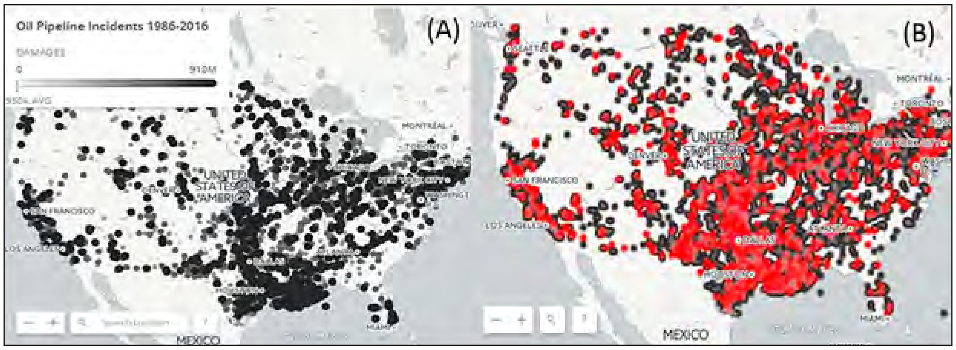


Figure 1. (A) Plot of economic damages caused by significant oil and natural gas pipeline-associated incidents and (B) number of resulting fatalities, 1986–2016. These incidents have resulted in 548 deaths, 2,576 injuries, and more than $8.5 billion in financial damages over this time period [2].

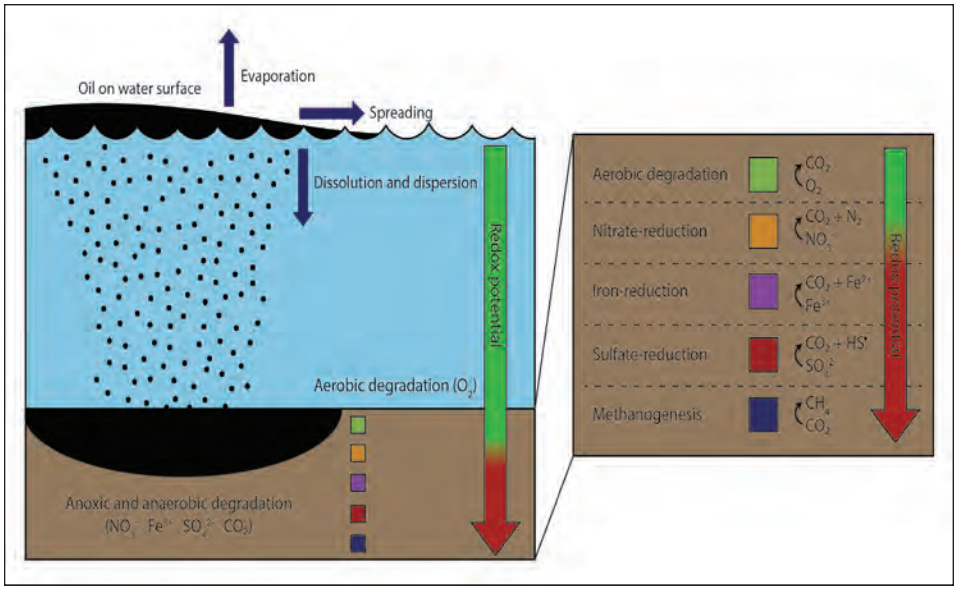


Figure 2. Fate and transport of oil leakages or spills in the marine environment and biodegradation (redox) potentials [13].

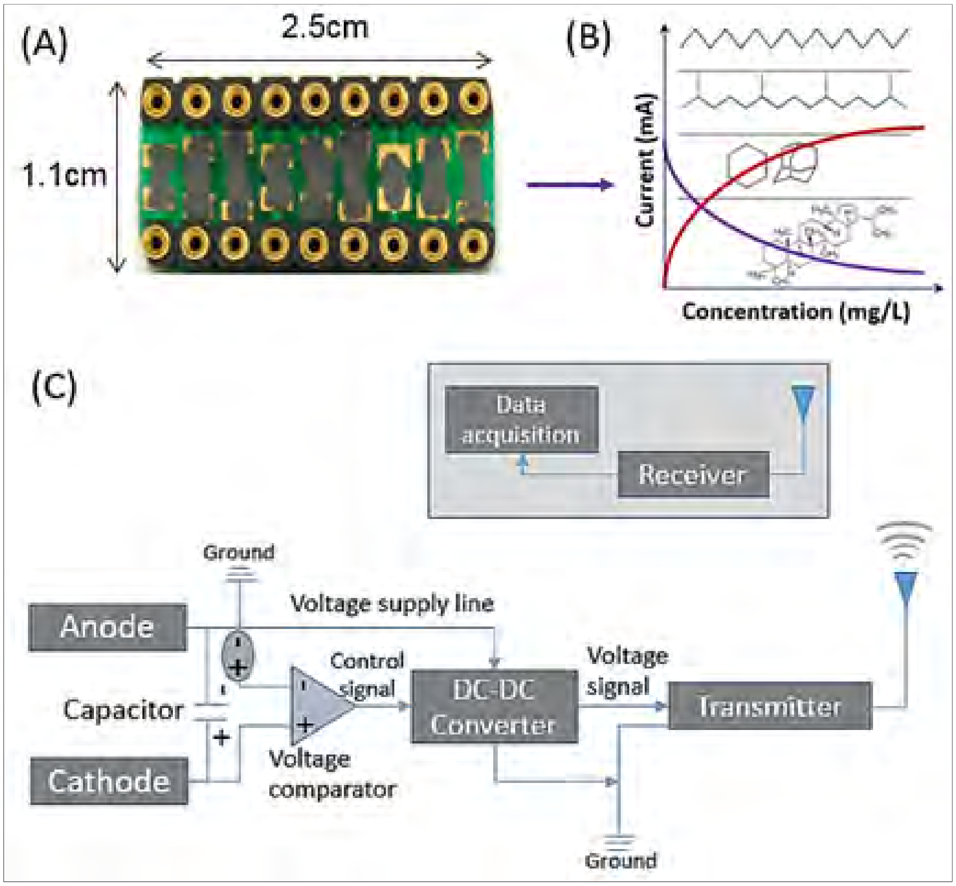


Figure 3. (A) a centimeter-scale microbial electrochemical sensor (microbial–microalgae); (B) evaluation of sensor response to hydrocarbon and petroleum compounds; and (C) a sensor platform for signal transmission, data acquisition, and signal processing.

drawbacks of the inspection robots presently used in the oil and gas industry center on insufficiently high levels of desired autonomy, robustness, and dependability.

Most of these robots work in highly supervised, short-term missions in extreme environments at high cost and with a high level of operational support [11].

A variety of sensor technologies are capable of remotely detecting hydrocarbon releases from offshore pipelines using techniques that rely on the relative adsorption of visible, infrared, and ultraviolet irradiation by an oil slick [7,8]. Adsorption intensity is related to the thickness of the oil layer on the water surface. Radar technologies, as well as microwave radiometers, laser fluoro-sensors, and laser-acoustic approaches, have also been used as oil thickness sensors. These sensors can provide information on the location and spread of an oil spill; its thickness distribution, which allows for a volumetric estimation; and the type and quality of the oil (i.e., its API gravity and H_2S content), which aids in assessing environmental damage and take appropriate actions for clean-up [7, 8].

When employing these techniques, one important consideration is the cost of data acquisition and analysis, which includes measurement equipment, operational and personnel costs, and data collection. Remote detection sensors are typically deployed in air-borne mode, adding significant cost to operations. Moreover, with regard to offshore pipeline rupture sensing, their data output is influenced by a plethora of conditions related to water flow, water quality, metocean and weather conditions. While the deployment of these technologies is significant, more robust and reliable sensor technologies with improved feasibility and reliability are desired for future applications [10].

Additionally, the sensor technologies outlined above generally do not provide information to implement a proactive strategy for the prevention of hydrocarbon releases. Most provide post-incident detection and notification, and those capable of early detection of deficiencies in pipeline integrity (e.g., pigs), do not deliver continuous monitoring. *In-situ* microbial sensors may have a unique ability to achieve this important outcome.

A Novel Microbial Sensor

Early detection of small liquid or gas hydrocarbon leaks or spills could lessen the likelihood of a major release incident. However, organic contaminant sensors are difficult to employ under certain settings due to material- or function-related constraints usually associated with background concentrations, mass-transfer, and detection limitations. In addition,

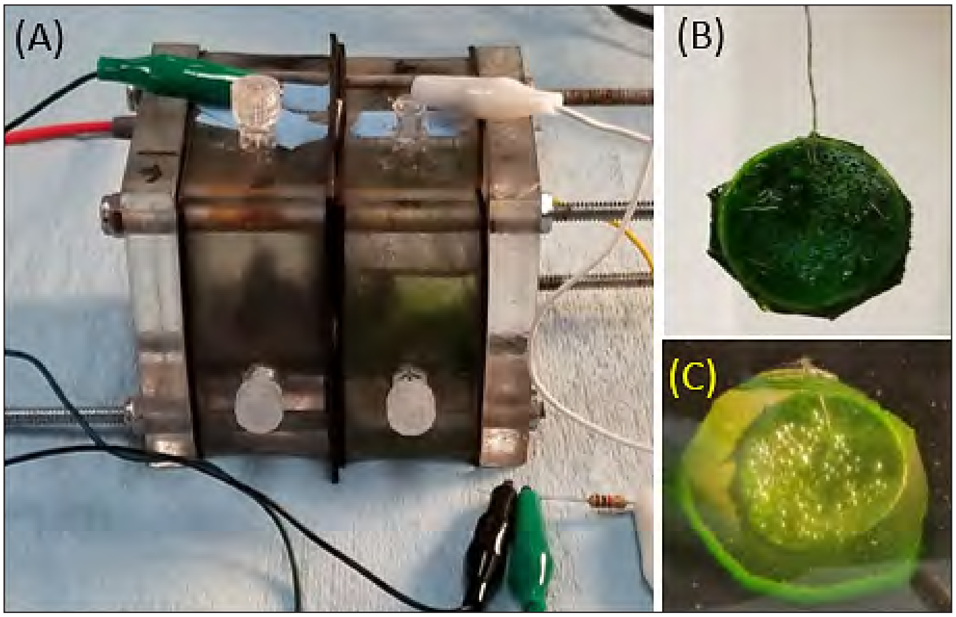


Figure 4. (A) A microbial biosensor with mixed bacterial consortium in the anode chamber and a microalgae biocathode in the cathode chamber; (B) a "mutag BioChip 25™" with a carbon felt electrode used to concentrate microalgae biofilm; and (C) in-situ oxygen generation by microalgae cells residing on the electrode.

environmental variations in temperature, barometric pressure, and relative humidity play an important role in subsurface environments [12]. Our research focuses on developing a self-sustained microbial (living-cell) sensor platform suitable for harsh or remote environments, such as those found at deep-water subsea infrastructure, onshore surface and subsurface pipelines, and hydrocarbon processing plants.

A microbial electrochemical cell (biosensor) was developed in order to harness the benefits of biodiversity in microbial populations and in their metabolic functions, thus creating a variety of electrochemical cells suitable for applications in varying environmental settings. The biosensor was created using exoelectrogenic bacteria that survives on organic matter in an anode and a phototrophic, autotrophic, or sulfur-reducing bacterial consortium in the cathode—enabling continuous transfer of electrons from one compartment (anode) to the other (cathode) [14].

This arrangement generates a voltage across a resistor which can be set or tuned to identify possible contamination by hydrocarbon compounds. The increased availability of organic compounds within the microbial biosensor cell will generate high voltage spikes. A variety of hydrocarbons and organic compounds (e.g., crude oil, natural gas, refined gasoline) can be used as substrates in laboratory studies to understand voltage generation potential and to optimize and stabilize sensor operations for different target petroleum products [15].

As shown in Figure 2, the oxidation-reduction potentials present in the marine, sediment, and above-ground onshore environments provide numerous opportunities for utilizing natural processes to simultaneously detect and communicate hydrocarbon releases. Microbial fuel cells (MFCs) have been used to run and power remotely-operated biological oxygen demand sensors [17]. Sediment-based MFCs have also been used for powering a meteorological buoy, wireless temperature sensors [18], and other environmental sensors [19]. MFCs have also functioned as power sources for remote sensors, digital wrist watches [20], light-emitting diodes for internal lighting [21], and basic phone/smart phone charging [22].

To overcome the restricted lifetime of batteries used in traditional, non-biological sensors, microbial sensor technology can be used as a telemetry system that transmits signals to remote receivers. To develop an effective and reliable biological sensor based on this technology, appropriate anodic and cathodic reactions should be combined. This enables the technology to be used for detection of organic pollutants, such as oil spills, and the communication of such. Several years of operational experience have been reported for other applications, including in biochemical oxygen demand sensors [17]. Because microbial systems have already proved useful for remediating toxic substances—such as phenols and petroleum compounds [23]—they should be explored for novel applications in extreme settings.

Our research approach is depicted in Figure 3. Three different types of immobilized microbial sensors will be developed to adapt to deep marine saline and sediment environments as well as surface and subsurface environments. These microbial sensors use exoelectrogenic bacteria (anode) as well as anammox and microalgae (namely, *Chlorella Vulgaris sp.* [cathode]) as anode and cathode consortia [24-26]. The specific objectives are:

- to develop centimeter-scale microbial electrochemical cells (see Figure 3a) suitable for marine/soil/surface environmental settings using various combinations of exoelectrogenic, autotrophic, and phototrophic microbial consortia;
- to evaluate the performance of the biosensors in terms of voltage generation potentials through the use of hydrocarbon- and petroleum-based compounds (see Figure 3b);
- to optimize biosensor performance by varying environmental settings, including pH, water depth, temperature, and substrate/nutrient concentrations; and
- to develop a sensor platform using voltage-to-acoustic signal transfer, data acquisition, and signal processing (see Figure 3c).

Our microbial biosensor prototype, shown in Figure 4, was used to carry out a series of experiments that build upon the findings of our previous research on biofilm development and experimental procedures [27, 28]. After a stable biofilm had been produced in the biosensor and a stable voltage achieved (under the reference physiological settings), the unit was subjected to various concentrations of gasoline (by volume/volume) in both anode and cathode chambers in order to mimic real-world conditions of a hydrocarbon release into the environment.

The microbial sensor's response to various gasoline concentrations during more than 1,000 hours of operation can be seen in Figure 5. The first six experiments (represented by the blue columns in Figure 5) were performed to allow for the start-up and establishment of a stable biofilm in both anode and cathode chambers; achievement of this is confirmed by the voltage generated by the cell. The maximum voltage (peak) produced by the cell was 0.1201 V at a chemical oxygen demand (COD) concentration of 500 mg/L. Three repetitive cycles were conducted which yielded an average response value of 0.1151 V. The microbial sensor was then subjected to a very low concentration of gasoline with 10 percent ethanol (0.04% v/v, shown in purple in Figure 5). The response of the microbial sensor remained the same, demonstrating that it was not sensitive to a very low level of gasoline concentration.

In the next experiment, the gasoline concentration was increased by 2.5 times (i.e., 0.1% v/v) from the previous experiment. The response of the sensor was significantly affected by the gasoline, resulting in a 23 percent reduction in the response (shown in green in Figure 5). When the concentration was increased by 10 times (i.e., from 0.1% to 1% v/v ratio), the response was decreased by 37% from its original gasoline test level (shown in red in Figure 5). Following these experiments, the microbial sensor was returned to its original condition (without the addition of gasoline). Overall, a linear relationship was observed between the voltage response and the gasoline concentrations of 0% and 0.04%. An exponential relationship was observed for the voltage response between 0.04% and 1.0% v/v.

Another set of experiments was conducted at low COD concentrations to understand the response of the microbial sensor under low substrate conditions (shown in purple in Figure 5). There was a 57 percent reduction in voltage at 0.1% v/v gasoline addition at a COD concentration of 30 mg/L. The sensor was able to recover its voltage response when the media was replaced with a low COD wastewater without a gasoline addition. A matrix of experiments is required to further develop response relationships to variations of hydrocarbon compounds. For example, gasoline with 10 percent ethanol, which contains a mixture of long chain hydrocarbons, was used as a model compound in this research.

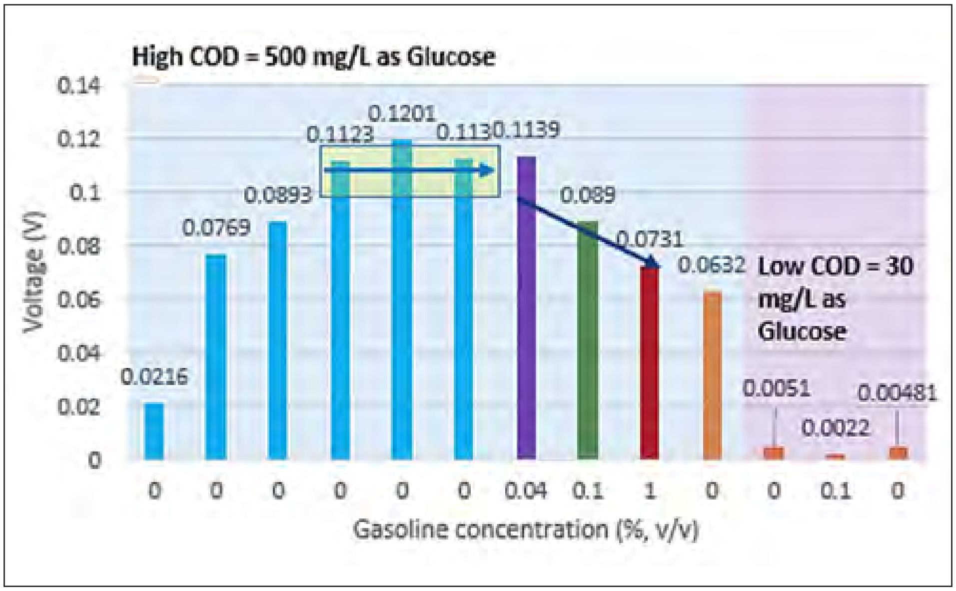


Figure 5. Response of a microbial-microalgae sensor with respect to the varying COD (30 mg/L and 500 mg/L) and Gasoline concentrations (0-1% v/v).

Diesel has a different composition, however, and a microbial sensor will exhibit a different response when exposed to it. Therefore, a series of experiments and optimization studies are required to develop a robust microbial sensor that would produce stable and reliable responses when exposed to hydrocarbon releases from a wide array of fuel types.

Future Perspective

The proposed microbial electrochemical cell (biosensor) platform produces a voltage *spike* or *sink* in response to a certain environment. Moreover, sensors using different types of microbes can be used to detect an array of target molecules. Researchers have identified several microorganism groups that readily degrade hydrocarbons, especially in aquatic and marine environments [29, 30].

Recent research suggests that *Alcanivorax borkumensis* marine bacteria in particular are specialized in utilizing alkanes for growth. Several other microorganisms belonging to bacteria, yeast, and fungi groups have also been identified for their potential to degrade crude oils and hydrocarbons [29]. Several members of these communities could be employed in the microbial sensor platform to develop a substantial and traceable response to the availability of hydrocarbons.

While this is an attractive approach, little knowledge exists on this microbial community structure and their function in environments exposed to oil, gasoline, or natural gas spills and leaks [31]. Future research efforts should focus on developing a deeper understanding of the functional genes responsible for oil degradation in marine and soil environments. If this knowledge is developed comprehensively, midstream petroleum companies, pipeline network operators, and government and military leaders in the homeland defense community may be able to quickly, accurately, and precisely respond to small hydrocarbon releases before a rupture threatens economic, environmental, and energy security.

Acknowledgement

The authors would like to thank Multi Umwelttechnologie AG of Germany for providing the Mutag BioChip25™ samples used in this study.

References

1. Furchtgott-Roth, D. (2013, June 6). Pipelines are safest for transportation of oil and gas. Manhattan Institute for Policy Research Issue Brief, 23, 1–10. Retrieved from https://www.manhattan-institute.org/pdf/ib_23.pdf
2. Joseph, G. (2016, November 30). 30 years of oil and gas pipeline accidents, mapped. CityLab. Retrieved from https://www.citylab.com/environment/2016/11/30-years-of-pipeline-accidents-mapped/509066/
3. U.S. Department of Homeland Security. (2013, December). National Infrastructure Protection Plan (NIPP) 2013: Partnering for critical infrastructure security and resilience. Retrieved from https://www.dhs.gov/sites/default/files/publications/national-infrastructure-protection-plan-2013-508.pdf
4. U.S. Department of Homeland Security. (2015). Energy Sector-Specific Plan. Retrieved from https://www.dhs.gov/sites/default/files/publications/nipp-ssp-energy-2015-508.pdf
5. Canada's Oil and Natural Gas Producers. (2018, May 26). Best management practice: Pipeline leak detection programs. Retrieved from https://www.capp.ca/~/media/capp/customer-portal/publications/310502.pdf?-modified=20180526153412
6. Renshaw, J., & Kumar, D. K. (2016, September 30). Technology designed to detect U.S. energy pipeline leaks often fails. Reuters. Retrieved from https://www.reuters.com/article/us-usa-pipelines-colonial-analysis/technology-designed-to-detect-u-s-energy-pipeline-leaks-often-fails-idUSKCN1200FQ
7. Grüner, K., Reuter, R., & Smid, H. (1991). A new sensor system for airborne measurements of maritime pollution and of hydrographic parameters. GeoJournal, 24(1), 103–117. doi:10.1007/bf00213062
8. Jha, M., Levy, J., & Gao, Y. (2008). Advances in remote sensing for oil spill disaster management: State-of-the-art sensors technology for oil spill surveillance. Sensors, 8(1), 236–255. doi:10.3390/s8010236
9. Liu, M., Zang, S., & Zhou, D. (2005). Fast leak detection and location of gas pipelines based on an adaptive particle filter. International Journal of Applied Mathematics and Computer Science, 15(4), 541–550. Retrieved from http://matwbn.icm.edu.pl/ksiazki/amc/amc15/amc15411.pdf
10. Shukla, A., & Karki, H. (2016). Application of robotics in onshore oil and gas industry—A review Part I. Robotics and Autonomous Systems, 75, 490–507. doi:10.1016/j.robot.2015.09.012
11. Albiez, J., Hildebrand, M., Vogele, T., Joyeux, S., & Kirchner, F. (2011, January 1). Robust Robots for Arctic Exploration. Offshore Technology Conference. doi:10.4043/22120-MS
12. Ho, C. K., & Hughes, R. C. (2002). In-situ chemiresistor sensor package for real-time detection of volatile organic compounds in soil and groundwater. Sensors, 2(1), 23–34. doi:10.3390/s20100023
13. Daghio, M., Aulenta, F., Vaiopoulou, E., Franzetti, A., Arends, J. B., Sherry, A., ... & Rabaey, K. (2017). Electrobioremediation of oil spills. Water Research, 114, 351–370. doi:10.1016/j.watres.2017.02.030
14. Gude, V. G. (2016). Wastewater treatment in microbial fuel cells–an overview. Journal of Cleaner Production, 122, 287–307. doi:10.1016/j.jclepro.2016.07.048
15. Tecon, R., der Meer, V., & Roelof, J. (2008). Bacterial biosensors for measuring availability of environmental pollutants. Sensors, 8(7), 4062–4080. doi:10.3390/s8074062
16. Du, Z., Li, H., & Gu, T. (2007). A state of the art review on microbial fuel cells: a promising technology for wastewater treatment and bioenergy. Biotechnology Advances, 25(5), 464–482. doi:10.1016/j.biotechadv.2007.05.004
17. Chang, I. S., Moon, H., Jang, J. K., & Kim, B. H. (2005). Improvement of a microbial fuel cell performance as a BOD sensor using respiratory inhibitors. Biosensors and Bioelectronics, 20(9), 1856–1859. doi:10.1016/j.bios.2004.06.003
18. Tender, L. M., Gray, S. A., Groveman, E., Lowy, D. A., Kauffman, P., Melhado, J., ... & Dobarro, J. (2008). The first demonstration of a microbial fuel cell as a viable power supply: powering a meteorological buoy. Journal of Power Sources, 179(2), 571–575. doi:10.1016/j.jpowsour.2007.12.123
19. Donovan, C., Dewan, A., Peng, H., Heo, D., & Beyenal, H. (2011). Power management system for a 2.5 W remote sensor powered by a sediment microbial fuel cell. Journal of Power Sources, 196(3), 1171–1177. doi:10.1016/j.jpowsour.2010.08.099
20. Papaharalabos, G., Greenman, J., Melhuish, C., Santoro, C., Cristiani, P., Li, B., & Ieropoulos, I. (2013). Increased power output from micro porous layer (MPL) cathode microbial fuel cells (MFC). International Journal of Hydrogen Energy, 38(26), 11552–11558. doi:10.1016/j.ijhydene.2013.05.138
21. Ieropoulos, I. A., Ledezma, P., Stinchcombe, A., Papaharalabos, G., Melhuish, C., & Greenman, J. (2013). Waste to real energy: the first MFC powered mobile phone. Physical Chemistry Chemical Physics, 15(37), 15312–15316. doi:10.1039/C3CP52889H
22. Walter, X. A., Stinchcombe, A., Greenman, J., & Ieropoulos, I. (2017). Urine transduction to usable energy: a modular MFC approach for smartphone and remote system charging. Applied Energy, 192, 575–581. doi:10.1016/j.apenergy.2016.06.006
23. Morris, J. M., & Jin, S. (2007). Feasibility of using microbial fuel cell technology for bioremediation of hydrocarbons in groundwater. Journal of Environmental Science and Health, Part A, 43(1), 18–23. doi:10.1080/10934520701750389
24. Kokabian, B., Smith, R., Brooks, J. P., & Gude, V. G. (2018). Bioelectricity production in photosynthetic microbial desalination cells under different flow configurations. Journal of Industrial and Engineering Chemistry, 58, 131–139. doi:10.1016/j.jiec.2017.09.017
25. Kokabian, B., Ghimire, U., & Gude, V. G. (2018). Water deionization with renewable energy production in microalgae-microbial desalination process. Renewable Energy, 122, 354–361. doi:10.1016/j.renene.2018.01.061
26. Kokabian, B., Gude, V. G., Smith, R., & Brooks, J. P. (2018). Evaluation of anammox biocathode in microbial desalination and wastewater treatment. Chemical Engineering Journal, 342, 410–419. doi:10.1016/j.cej.2018.02.088
27. Kokabian, B., & Gude, V. G. (2013). Photosynthetic microbial desalination cells (PMDCs) for clean energy, water and biomass production. Environmental Science: Processes & Impacts, 15(12), 2178–2185. doi:10.1039/c3em00415e
28. Kokabian, B., & Gude, V. G. (2015). Sustainable photosynthetic biocathode in microbial desalination cells. Chemical Engineering Journal, 262, 958–965. doi:10.1016/j.cej.2014.10.048
29. Hazen, T. C., Prince, R. C., & Mahmoudi, N. (2016). Marine oil biodegradation. Environmental Science & Technology, 50(5), 2121–2129. doi:10.1021/acs.est.5b03333
30. Hazen, T. C., Dubinsky, E. A., DeSantis, T. Z., Andersen, G. L., Piceno, Y. M., Singh, N., ... & Stringfellow, W. T. (2010). Deep-sea oil plume enriches indigenous oil-degrading bacteria. Science, 330(6001), 204–208. doi:10.1126/science.1195979
31. Mason, O. U., Hazen, T. C., Borglin, S., Chain, P. S., Dubinsky, E. A., Fortney, J. L., ... & Mackelprang, R. (2012). Metagenome, metatranscriptome and single-cell sequencing reveal microbial response to Deepwater Horizon oil spill. The ISME Journal, 6(9), 1715. doi:10.1038/ismej.2012.59

Hariteja Nandimandalam
Graduate Student in Environmental Engineering, Mississippi State University

Hariteja Nandimandalam is a graduate student in environmental engineering at Mississippi State. He is originally from New Delhi, India. He is currently developing biosensors using exoelectrogenic bacteria to prevent oil spills. This principle may also be used to treat hydrocarbon-contaminated water sources, such as those originating from fracking operations. His research interests extend to water-wastewater treatment, microbial fuel cells, and bioelectrochemical systems.

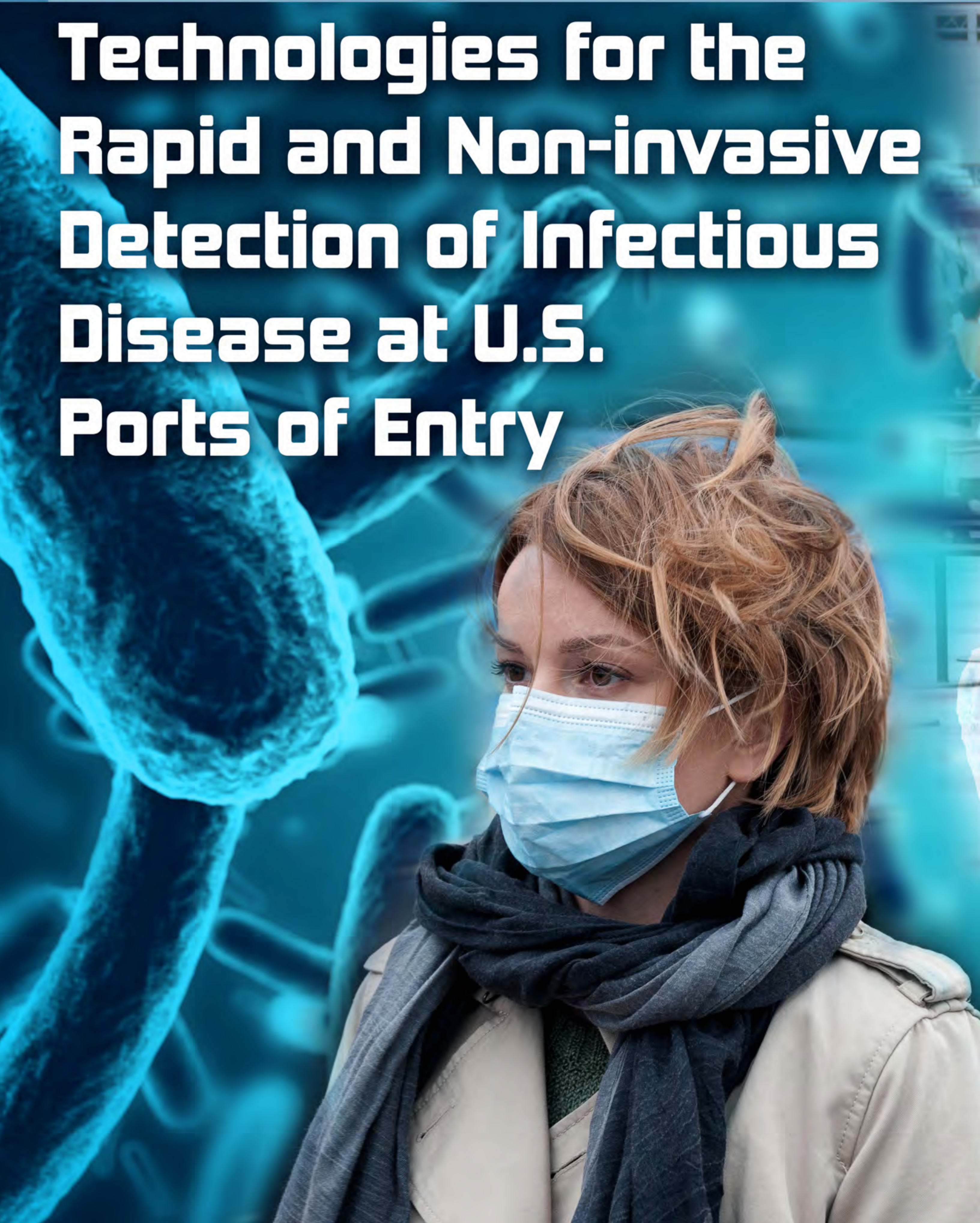
Umesh Ghimire
Graduate Student in Environmental Engineering, Mississippi State University

Umesh Ghimire is a graduate student in environmental engineering at Mississippi State. He is originally from Nepal. He received an M.S. in Biological Environmental Engineering from Kangwon National University, South Korea. He is currently developing sustainable and energy-efficient technologies for wastewater treatment, desalination, and energy production. More specifically, his research focus is on developing resource-efficient bioelectrochemical nitritation anammox process in microbial desalination cells to treat wastewater with simultaneous bioelectricity and water recovery.

Veera Gnaneswar Gude, Ph.D
Associate Professor of Environmental Engineering, Mississippi State University

Veera Gnaneswar Gude has 18 years of academic, industrial, and research experience in desalination, wastewater treatment, and biofuel scientific and technological areas. He received his Ph.D. in environmental engineering and is a licensed professional engineer. He has published over 100 scientific research articles on desalination, water-wastewater treatment and biofuels research including 75 journal papers, 5 books, 15 invited book chapters, 35 peer-reviewed conference proceedings papers, 20 technical reports, and 2 patents. He received recognition for his contributions to research and education from professional societies like ASCE, Chi-Epsilon, ASEE, and ASES.

Technologies for the Rapid and Non-invasive Detection of Infectious Disease at U.S. Ports of Entry



Alena James & Luther Lindler

The 2014 Ebola outbreak in West Africa captured the nation's attention, highlighting the need for improved biosurveillance at the border and identifying a capability gap in the United States' homeland defense and security architecture. In response, the U.S. strove to fill knowledge gaps and operational capabilities by advancing experimental patient treatments and therapies, strengthening the traveler screening process, and enabling a national strategic response framework for infectious disease—working with the United Nations and states of Liberia, Sierra Leone, and Guinea to contain the epidemic [1]. Through the execution of Operation United Assistance, the U.S. Department of Defense (DoD) dedicated more than $2.3 billon to the deployment of medical military personnel, research labs, hospital beds, and other necessary medical supplies to help more than 28,000 West Africans affected by the outbreak [2]. In addition, the Centers for Disease Control and Prevention (CDC), Department of Homeland Security (DHS), and West African governments implemented traveler health screenings at ports of entry (POE) to fortify border security and contain the spread of the virus.

To enact a risk-based screening process at domestic POEs (see Figure 1), officers from U.S. Customs and Border Protection (CBP) assessed travelers entering the country for potential exposure to Ebola. High-risk travelers—including those entering from the three affected African states [3]—received an enhanced health screening, in which a non-contact infrared thermometer was used to measure their temperature. Travelers with temperatures greater than 100 degrees Fahrenheit were assessed further and then advised to seek medical care [4–10].

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

In October 2014, after CDC confirmed the first case of Ebola in the United States, CBP began to implement an enhanced entry screening program. In the first 30 days of the program, CBP officers screened 1,993 travelers from Guinea, Liberia, and Sierra Leone. CBP referred 86 of those travelers to the CDC for a more intensive health screening [3]. Of those, seven asymptomatic individuals were sent for further medical evaluation [3]. While deployed, U.S. military personnel serving in Operation United Assistance were also monitored daily for exposure symptoms [11, 12].

Before re-entering the U.S., non-symptomatic DoD personnel received additional medical screening and were placed in controlled monitoring for 21 days [11, 12]. During this time, military personnel with no known exposure were assessed for febrile symptoms, measuring their temperature twice daily [12]. DoD civilians supporting the deployments (but without known exposure) were permitted to either voluntarily participate in DoD's controlled monitoring protocol, or follow guidance from CDC, state, and local public health authorities on the active monitoring of Ebola [12].

During the outbreak, border screenings of travelers were essential to preventing the biothreat from spreading to other countries [13]. More than 38,000 travelers entering the U.S. underwent enhanced Ebola screening [14]. Apart from the results of traveler questionnaires taken during CBP's secondary screening stage, the only other determining risk factors were symptoms of infection—namely an elevated temperature. Of the 38,000 travelers screened in this manner, 2,975 returned positive responses to the questionnaire, 81 travelers presented elevated temperatures, 2,996 travelers were referred to tertiary screening, and 49 travelers were sent to medical facilities for further assessment [4].

Viral hemorrhagic diseases like Ebola can be spread via direct contact with bodily fluids—including saliva, sweat, blood, vomit, and waste excrement [15]. Presentation of high fever is actively used to confirm outbreaks at POEs, as fever can be an indicator that a traveler's body is experiencing an infection. Even so, fever cannot be used as a diagnostic marker for specific pathogens or diseases, because it is a common clinical symptom.

However, the only diagnostic tool currently available for secondary screening in CBP's tiered process is a thermometer. The Ebola outbreak reinforced the need to deliver a field-deployable diagnostic test capable of rapidly and non-invasively screening pre-symptomatic travelers for diseases of concern.

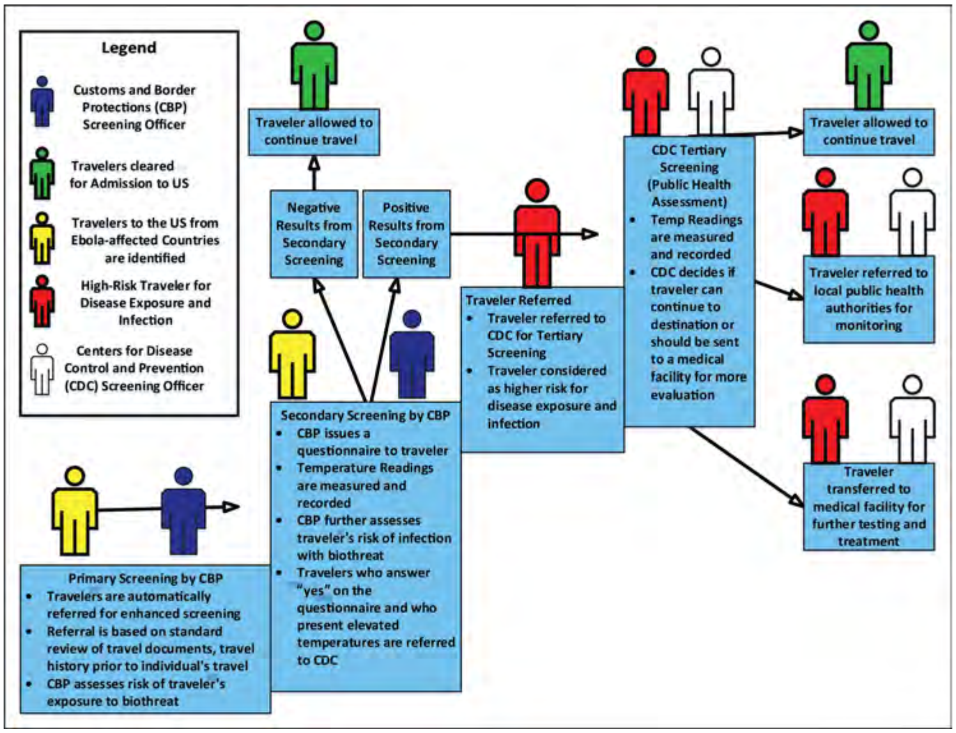


Figure 1. Risk-based screening process for travelers entering the U.S. During the 2014 Ebola Outbreak. This figure demonstrates the traveler screening process used to assess travelers to the United States during the 2014 Ebola outbreak [4–10].

Development of a diagnostic tool for this stage could expedite the screening process, improve response times for positive tests, and provide public health officials with better information than current questionnaire- and temperature-based tools. Moreover, with a severe biothreat like Ebola, the use of non-invasive diagnostics is critical for protecting medical screening officers (and other travelers) from exposure. Non-invasive sampling collection techniques are defined as such because they do not penetrate through the skin. Examples include nasal, oral, and epidermal swabs, or the collection of breath samples.

Required characteristics for an effective POE screening device include: a high degree of portability, user friendliness, durability, non-invasive sample collection, generation of minimal hazardous material during the analysis process, accurate diagnostics for multiple diseases in less than 60 seconds (a standard benchmark for "rapid" analysis), and the ability to detect a pathogen in an asymptomatic traveler.

This article reviews four distinct technologies that can be applied to improving research and development (R&D) in the field of rapid diagnostics. These four technologies include nucleic acid-based detection technology; antigen-antibody binding-based detection technology; volatile organic compound-based detection technology; and infrared light-based detection technology. A review of the literature suggests that current R&D for improving the performance of rapid diagnostic tests is focused heavily on tests rooted in nucleic acid-based and antigen-antibody binding-based detection technologies (see Figure 2) [16–19]. Less emphasis and attention have been paid to the development of volatile organic compound-based and infrared light-based detection technologies.

Testing for Diseases of Public Health Significance

Four classes of disease can be closely monitored and detected using traditional screening practices (e.g., measuring temperature, heart rate, or other symptoms). These four classes include infectious respiratory, viral hemorrhagic, vector-borne, and gastrointestinal disease. Foreign nationals seeking to enter the U.S. under immigration or refugee protocols must pass a medical examination as part of the visa application process, and those who present symptoms of what CDC terms “communicable diseases of public health significance” are excludable from entry [20]. Foreign nationals visiting or transiting through the U.S. who present symptoms of such diseases may also be examined before entry is granted. U.S. citizens re-entering the country are not required to pass a health screening to gain entry, except in the event of an emerging disease outbreak posing a significant threat to the nation’s public health.

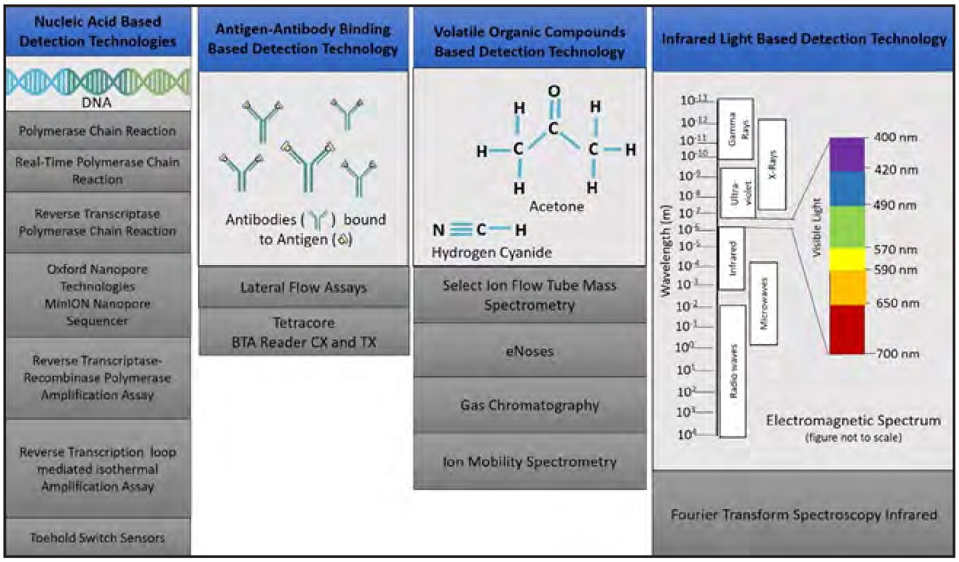


Figure 2. Technological approaches for pathogen detection. This figure depicts existing technologies with the potential to further advance the development of rapid and non-invasive diagnostic tests [16–19].

Diagnostic tests vary in their approach to disease detection, but many are designed to target an analyte specific to a pathogen that can be bound to some form of a bioreceptor. After binding, a transducer can be used to amplify a signal that indicates the binding of the analyte to the receptor. Diagnostic tests designed in this manner are crucial for pathogen detection *in vitro* and allow medical professionals to select an appropriate treatment regimen. Diagnostic technologies also vary in their processing times, instrumentation reliability, and tradeoffs between specificity and sensitivity.

Nucleic Acid-based Detection

Nucleic acid-based detection technologies use genetic code to identify pathogens. While doing so, nucleic acid-based detectors will target chemical compounds within either deoxyribonucleic acid (DNA) or ribonucleic acid (RNA). Several technologies, such as reverse transcriptase-polymerase chain reaction (RT-PCR), PCR, and real-time PCR (qPCR), can detect and confirm multiple pathogens through nucleic acid amplification and quantification. Many Ebola diagnostic assays used during the 2014 outbreak were developed on the principles of RT-PCR [21]. While these lab-based methods are the most accurate available, they require expensive instrumentation, a high degree of technical expertise, invasive sampling techniques (e.g., venipuncture), and lengthy processing times (two or more hours) to operate. However, nucleic acid amplification provides a thorough analysis of the amplified products. Targeted amplification, combined with nucleic acid sequencing, can provide more detail about a biological agent, potentially including its relationship to another biothreat, or its susceptibility to medical countermeasures.

Through technical R&D, the diagnostics industry has improved our ability to complete sequencing in a field-deployable (non-laboratory) environment. For example, Oxford Nanopore Technologies Ltd. developed the MinION Nanopore Sequencer, which shows promise for use at POE. The MinION has demonstrated its ability to rapidly sequence viral genomes during the early phases of an influenza pandemic [22] and during the Zika virus epidemic [23]; and it was used by researchers in Guinea during the Ebola outbreak to process serum samples from patients in real time [24]. Powered by a USB port, the MinION relies on a flow cell to analyze nucleotide bases and it can simultaneously run multiple samples. The sequencer can operate independent of an internet connection and process a sample within an hour. Using the MinION, researchers have conducted real-time bioinformatics analysis in resource-limited areas such as the rain forest [25]. It has also been used in the rapid metagenomic detection of Chikungunya virus, Ebola, and hepatitis C virus in human blood samples [26]. These features make the MinION a promising candidate for border medical screening, if the requirement for non-invasive sample collection is waived.

Reverse transcriptase-recombinase polymerase amplification (RT-RPA) is another nucleic acid-based approach for pathogen detection. These assays function by placing enzymes and the DNA or RNA sample of interest within a centrifuge to initiate the amplification reaction (which can take place at room temperature). RT-RPAs have been useful in the on-site detection of dengue virus in human serum samples [27]; in the laboratory-based detection of multiple strains of Rift Valley fever virus taken from virus cultures [28]; and in the on-site detection of yellow fever virus taken from cultures, mosquito pools, and human plasma samples [29]. These assays benefit from the fact that the reaction does not require a thermocycler, which minimizes assay times and expense. These assays have also been used to identify viruses in pigs such as type 2 porcine reproductive and respirator syndrome virus [30], and detect epidemic human norovirus strains in viral RNA [31]. Reverse transcription loop-mediated isothermal amplification assays employ a similar technique, and have been proven to identify Middle East Respiratory Syndrome Coronavirus in human samples [32].

Synthetic biology—the generation of new biological products like genes, cells, or enzymes using advanced bioengineering techniques—has also furthered the development of nucleic acid-based detection technologies. For example, the development of programmable RNA sensors has led to the production of paper-based methods for virus detection. Such methods combine RNA sensors, known as Toehold Switches, with a freeze-dried, cell-free protein expression paper platform [33]. These methods are capable of identifying Zika virus without reporting a false detection of the closely related dengue virus [33]. As a review of the literature indicates, R&D on nucleic acid-based detection technology continues to be the primary focus in the advancement of rapid diagnostic tests.

Antigen-antibody Binding-based Detection

Relied on as diagnostic instruments since the early 1990s, antigen-antibody binding-based detection technologies work rapidly and are easy to interpret. The most relied-upon assays are Lateral Flow Assays (LFAs), which are relatively inexpensive and user-friendly [34]. Antigen-antibody binding diagnostic tests use blood proteins (antibodies) to capture foreign substances from pathogens (antigens). Antigen-antibody binding is specific; this means that only certain antibodies can bind to certain antigens. For a disease-detecting assay to function, strips are coated with pathogen-specific antibodies. Once a sample is applied, antigens flow toward the antibodies, which are coated in gold or latex particles. They bind and form complexes that accumulate in a line, yielding a colorimetric result that indicates the absence or presence of the pathogen. LFAs' user-friendliness and cost-efficiency make them appealing tools for medical screening in non-laboratory environments.

However, LFAs can be limited in their analytical capabilities due to sensitivity and specificity challenges. Many LFA test strips are singleplex, or single-pathogen-specific. This is problematic when attempting to detect the presence of unidentified (or multiple) pathogens. Recent efforts have produced multiplex LFAs capable of detecting multiple pathogens simultaneously. Researchers have demonstrated the multiplex detection of 10 epidemic foodborne pathogens, including *Escherichia coli*, *Salmonella*, and *Cholera* [34]. However, multiplex LFAs face challenges like high levels of cross-reactivity (non-specific binding to antibodies), which can produce false positives among multiple pathogens [35]. Often used in environmental sampling, LFAs have identified the presence of biothreat agents like *Bacillus anthracis* [36]. Furthermore, these types of tests have been integrated with the use of mobile devices (e.g., smartphones, tablets) in analyzing results. For example, Biothreat Alert Multiplex Strips, produced by Tetracore, target up to five different antigen targets at once: a control line, *Yersinia pestis*, *Francisella tularenis*, *Bacillus anthracis*, and *Burkholderia*. These strips can be read and analyzed by Tetracore's BTA Reader CX and BTA Reader TX phone or tablet add-ons to confirm the identity of the pathogens within 60 seconds [37].

Given their limitations regarding sample collection and multiplex-use, LFAs are only moderately suitable for the biomedical screening of travelers at POEs. In comparison to nucleic acid-based diagnostic assays, LFAs are more cost-effective and require less scientific expertise for use. However, when used outside of a laboratory environment, antigen-antibody tests are susceptible to factors that can compromise their reliability. Variables like temperature, light, and pH can compromise an LFA's results. Assay performance is also affected by the shelf life and storage conditions of the testing reagents.

Volatile Organic Compound-based Detection

Defined in a medical context, volatile organic compounds (VOCs) are small molecules produced by the body (and/or microbial pathogens) and liberated in bodily fluids like breath, urine, feces, and sweat [38]. Research on the viability of using VOCs as indicators for infections is underway, but the scientific literature has already recognized an association of several VOC arrays with specific diseases. Urinary tract, gastro-intestinal, fungal, and bacterial infections, such as *Mycobacterium tuberculosis*, are just a few examples of instances where VOCs can be used as markers for the detection of disease [39]. Studies have also linked certain concentrations of acetone in breath to diabetes mellitus [40]; increased levels of hydrogen cyanide in the breath of patients aged seven to 17 to lung infections induced by *Pseudomonas aerugnosa* [41]; and the presence of thioethers in breath to *Plasmodium falciparum*, the protozoan parasite that causes malaria in humans [42].

In addition, several VOC-releasing bacterial pathogens—such as *Staphylococcus aureus*, *Streptococcus pneumoniae*, *Enterobacter faecalis*, *Pseudomonas aeruginosa*, *Klebsiella pneumoniae*, and *Escherichia coli*—are being studied in order to produce statistical models of VOC–pathogen production relationships [43]. VOC analysis relies on the use of traditional chemical analytical technologies such as gas chromatography coupled with mass spectrometry (GC-MS) for compound identification. GC-MS is the gold standard for gas sample analysis, and it can analyze breath-borne compounds. Studies have used GC-MS in the detection of chemicals like ammonia, which, when present in breath, correlates with *Helicobacter pylori* infection in humans [44]. Other types of spectrometry that can be used to analyze chemical compounds include ion mobility spectrometry (IMS), selected ion flow tube mass spectrometry (SIFT-MS), and proton transfer spectrometry (PTS). IMS and SIFT-MS can provide real-time measurements of VOCs, and PTS has been used to detect VOCs associated with food spoilage-related bacteria [45]. All of these technologies provide a strong platform for the chemical analysis of gas samples.

Electronic noses, or e-noses, are sensors used to continually detect the presence of VOCs in gas samples [46]. E-nose technology relies on electronic sensors to identify patterns and recognize odors, but also typically integrates traditional chemical analyzers (like gas chromatography) into the system. Several e-nose devices are being improved upon or optimized for detecting the presence of disease-associated VOCs in human breath profiles [47]. Airborne chemical detection has already been deployed in efforts to interdict illegal substances and contraband at national borders [48], and tools for VOC detection are showing promise for use in the interdiction of human trafficking activity [49]. Recognizing that canines' exceptional sense of smell grants them the ability to sniff out certain chemicals and biomarkers, researchers have undertaken studies to better understand the flow of air within a dog's nose, to inform the development of better e-nose devices [50, 51].

Analysis of VOCs in human breath shows significant potential for swiftly and accurately identifying travelers infected with a disease of concern during a medical screening. The release of VOCs in the gaseous phase makes these compounds a non-invasive means of sample collection [52, 53]. However, the release of relevant biomarker VOCs may not occur until a person is in the very late stages of infection, making detection challenging during the pre-symptomatic stage. As additional R&D

focuses on exploring VOCs as markers for infectious disease, development of a portable, non-invasive VOC diagnostic tool may be plausible in the near future.

Infrared Light-based Detection

Like VOC sampling, infrared light also holds promise for use as a diagnostic technique—and it may be the most ideal technology for the development of a rapid, non-invasive detection device. Infrared light is often used in research laboratories as an analytical tool for determining the chemical components of solid or liquid samples. In comparison to ultraviolet radiation or visual light, infrared light reflects lower energy levels when applied to a sample [54], thus decreasing the risk of damage.

At present, no diagnostic test for an infectious disease uses this technology *in vivo*. However, infrared light-based detection devices have been deployed as biosurveillance scanners and used to detect febrile symptoms when screening travelers during outbreaks. Infrared thermal imaging scanners were used, with varying levels of effectiveness, to identify travelers presenting fevers during several seasonal flu outbreaks [55]; to complement other detection measures during the 2003 Severe Acute Respiratory Syndrome (SARS) outbreak [56]; and during the 2014 Ebola outbreak. The use of infrared thermal imaging scanners and non-contact infrared thermometers allows border officials to assess whether a given traveler may pose a risk of pathogen infection. However, it is important to note that non-contact thermometers have displayed limited efficacy in detecting the early stages of viral infections (such as influenza) in travelers [57].

Currently, engineers are working to apply this non-invasive technology to the development of user-friendly medical diagnostic instruments. In an ideal rapid and non-invasive diagnostic device, the instrument should be capable of directing light waves through the epidermal layer of the skin to detect the presence of a pathogen—without damaging the body. However, this diagnostic capability is not yet feasible, and the body of scientific literature related to its maturation remains limited in size. Direct application of infrared light to the body faces significant technical challenges, such as interference by dense physical features of the skin that inhibit optical analysis. Skin pigmentation and thickness all influence the propagation of light waves, which in turn impacts the accuracy of optical measurements [58].

While there is no light-based detection technology available for diagnosis *in vivo*, there is a laboratory technique used to analyze samples for bacterial and viral presence. This technique, known as Fourier transform infrared spectroscopy (FTIR), uses vibrational spectroscopy to examine vibrations between molecules. FTIR relies on infrared radiation to analyze the chemical composition of samples, and it is the vibrational spectroscopic technique most widely used in bacterial detection [59]. FTIR technology can identify structural information, like molecular changes to cellular components, allowing for the rapid identification of bacteria. To date, this technology has successfully detected *E. coli O157:H7* in apple juice [60]; has been applied as a diagnostic and surveillance tool for cancer [61]; and has been demonstrated as a rapid technique for the identification of bacteria like *P. aeruginosa* in sputum samples [62]. In addition, FTIR has also successfully sensed foodborne pathogens such as *Listeria monocytogenes* [63].

Studies are still needed regarding the use of FTIR in rapid diagnostics in the biomedical field. Some researchers have had success using near-infrared light waves to monitor glucose levels in individuals with diabetes (or susceptible to it) [64]. Scientists have also attempted to use near-infrared light spectroscopy to detect and study viral or bacterial particles in model systems. In May 2018, scientists reported the use of near-infrared spectroscopy to detect Zika virus in *Aedes aegypti* mosquitoes [65]. Also, influenza and Ebola have been detected in serum samples via infrared light technology [66].

Because they are subject to the same challenges observed with nucleic acid-based, antigen-antibody binding-based, and VOC-based detection technologies, infrared light-based detection is still costly and not well-suited for field environments. Even so, infrared methods require no sample preparation, and results can be produced quickly in the form of spectral images. More research on integrating spectroscopy techniques with disease diagnosis procedures may lead to hybridized diagnostic devices capable of non-invasively testing for a disease-causing pathogen, and providing an accurate diagnosis for further action.

Conclusion

The greatest challenge in developing a rapid diagnostic tool is designing a non-invasive sampling technique that can reliably identify pathogen carriers before they show symptoms. Traditional oral or nasopharyngeal swab specimen collection remains the least invasive method currently available for sampling. However, this technique still subjects the sample to lengthy processing times. The use of swabs generates hazardous waste, further increasing the risk of exposure and the spread of disease. The operational environment at a POE requires safer techniques, less costly, more specific, and more portable technologies to improve the medical screening process of travelers deemed high-risk for exposure during a biological outbreak. The use of VOCs and infrared light-based detection devices hold the most promise for meeting these criteria.

Travelers entering the country and warfighters returning to the U.S. after serving in areas with ongoing infectious disease outbreaks require extensive health screenings to ensure their safety and to protect the country against an outbreak. Continued R&D in improved rapid and non-invasive diagnostic technologies may enhance our nation's ability to prevent dangerous biothreats from entering the U.S., while providing timely and effective treatment for military and government personnel at risk of exposure.

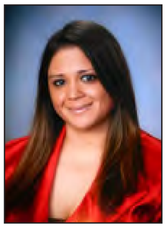
Disclaimer

The research discussed in this article was supported in part by an appointment to the U.S. Department of Homeland Security (DHS) Research Participation Program administered by the Oak Ridge Institute for Science and Education (ORISE) through an interagency agreement between the U.S. Department of Energy (DOE) and DHS. ORISE is managed by ORAU for the DOE under contract number DE-SC0014664. All opinions expressed in this paper are the author's and do not necessarily reflect the policies and views of DHS, DOE, or ORISE.

References

1. Fact Sheet: U.S. Response to the Ebola Epidemic in West Africa. The White House. Office of the Press Secretary. Retrieved from https://obamawhitehouse.archives.gov/the-press-office/2014/09/16/fact-sheet-us-response-ebola-epidemic-west-africa
2. Joint and Coalition Operational Analysis. (2016). Operation UNITED ASSISTANCE: The DOD Response to Ebola in West Africa. Retrieve from http://www.jcs.mil/Portals/36/Documents/Doctrine/ebola/OUA_report_jan2016.pdf
3. Brown, C.M., Aranas, A.E., Benenson, G.A., Brunette, G., Cetron, M., Chen, TH., Cohen, N.J… & Pesik, N. (2014). Airport Exit and Entry Screening for Ebola — August–November 10, 2014. Morbidity and Mortality Weekly Report, 63(49), 1163-1167. Retrieved from http://europepmc.org/backend/ptpmcrender.fcgi?accid=PMC4584540&blobtype=pdf
4. The Department of Homeland Security. (2016, June). Ebola Response. Retrieved from https://www.dhs.gov/archive/ebola-response
5. The Department of Homeland Security. (2005). Memorandum of Understanding between The Department of Health and Human Services and The Department of Homeland Security. Retrieved from https://www.dco.uscg.mil/Portals/9/DCO%20Documents/5p/CSNCOE/MOU%20between%20the%20DHHS%20and%20DHS.pdf?ver=2017-08-08-081620-793
6. Office of Inspector General. (2016, January). DHS' Ebola Response Needs Better Coordination, Training, and Execution. Retrieved from
7. Centers for Disease Control and Prevention. (2014, October). Enhanced Ebola Screening to Start at Five U.S. Airports and New Tracking Program for all People Entering U.S. from Ebola-affected Countries. Retrieved from https://www.cdc.gov/media/releases/2014/p1008-ebola-screening.html
8. Cohen, N.J., Brown, C.M., Alvarado-Ramy, F., Bair-Brake, H., Benenson, G.A., Chen, T.H., … & Cetron, M.S. (2016). Supplement: Travel and Border Health Measures to Prevent the International Spread of Ebola. MMWR, 65(3), 57-67. doi: 10.15585/mmwr.su6503a9
9. Virginia Department of Health. (2018). Ebola-Basic Airport Screening and Active Monitoring Protocal. Retrieved from http://www.vdh.virginia.gov/epidemiology/epidemiology-fact-sheets/ebola-frequently-asked-questions/ebola-basic-airport-screening-and-active-monitoring-protocol/
10. DeVries, A., Talley, P., Sweet, K., Kline, S., Stinchfield, P., Tosh, P., & Danila, R. (2016). Development and Implementation of the Ebola Traveler Monitoring Program and Clinical Outcomes of Monitored Travelers during October-May 2015, Minnesota. PloS One, 11(12), 1-11. doi:10.1371/journal.pone.0166797
11. Cardile, A.P., Murray, C.K., Littell, C.T., Shah, N.J., Fandre, M.N., Drinkwater, D.C., … & Vento, T.J. (2015). Monitoring Exposure to Ebola and Health of U.S. Military Personnel Deployed in Support of Ebola Control Efforts-Liberia, October 25, 2014-February 27, 2015. MMWR, 64(25), 690-694.
12. The Department of Defense. Under Secretary of Defense for Personnel and Readiness, Wright, J. (2014). Memorandum for Under Secretaries of Defense. Retrieved from http://archive.defense.gov/home/features/2014/1014_ebola/docs/Pre-Post-Deployment-Training-Screening-Monitoring-Guidance-for-DoD.pdf
13. Centers for Disease Control and Prevention. Ebola (Ebola Virus Disease) 2014-2016 Ebola Outbreak in West Africa. Retrieved from www.cdc.gov/vhf/ebola/history/2014-2016-outbreak/index.html
14. Centers for Disease Control and Prevention. Ebola (Ebola Virus Disease) Cost of the Ebola Epidemic. Retrieved from www.cdc.gov/vhf/ebola/history/2014-2016-outbreak/cost-of-ebola.html
15. Centers for Disease Control and Prevention. Ebola (Ebola Virus Disease) Transmission. Retrieved from https://www.cdc.gov/vhf/ebola/transmission/index.html
16. The University of Arizona. (2000). Antibody Structure. The Biology Project. Retrieved from http://www.biology.arizona.edu/immunology/tutorials/antibody/structure.html
17. National Center for Biotechnology Information. PubChem Compound Database; CID=768, https://pubchem.ncbi.nlm.nih.gov/compound/768
18. National Center for Biotechnology Information. PubChem Compound Database; CID=180, https://pubchem.ncbi.nlm.nih.gov/compound/180
19. The University of The State of New York. The State Education Department. (2006). Reference Tables for Physical Setting/Physics. Retrieved from http://www.p12.nysed.gov/assessment/reftable/physics-rt/physics06tbl.pdf
20. Centers for Disease Control and Prevention. (2017, October). Technical instructions for panel physicians and civil surgeons, introduction and background. Retrieved from https://www.cdc.gov/immigrantrefugeehealth/exams/ti/panel/technical-instructions/panel-physicians/introduction-background.html
21. Cherpillod, P., Shibler, M., Vieille, G., Cordey S., Vetter, P., & Kaiser, L. (2016). Ebola virus disease diagnosis by real-time RT-PCR: A comparative study of 11 different procedures. Journal of Clinical Virology, 77, 9-14. doi:10.1016/j.jcv.2016.01.017
22. Wang, J., Moore, N.E., Deng, Y.M., Eccles, D.A., & Hall, R.J. (2015). MinION Nanopore Sequencing of an Influenza Genome. Frontiers in Microbiology, 6, doi:10.3389/fmicb.2015.00766
23. Quick, J., Grubaugh, N.D., Pullan, S.T., Claro, I.M., Smith, A.D., Gangvarapu, K., Oliveira, G., Loman, N.J. (2017). Multiplex PCR method for MinION and Illumina sequencing of Zika and other virus genomes directly from clinical samples. Nature Protocols, 12(6), 1261-1276. doi: 10.1038/nprot.2017.066
24. Quick, J., Loman N.J., Duraffour S., Simpson J.T., Severi E., Cowley L,… & Carroll, M.W. (2016). Real-time, portable genome sequencing for Ebola surveillance. Nature, 30(7589), 228–232. doi:10.1038/nature16996
25. Pomerantz, A., Peñafiel, N., Arteaga, A., Bustamante, L., Pichardo, F., Coloma, L.A.,… & Prost, S. (2017). Real-Time DNA barcoding in remote rainforest using Nanopore sequencing. bioRxiv 189159. doi:10.1101/189159
26. Greninger, A, Naccache, S, Federman, S, Yu, G, Mbala, P, Bres, C, … & Chiu, C. (2015). Rapid Metagenomic identification of viral pathogens in clinicalsamples by real-time nanopore sequencing analysis. Genome Medicine, 7(9), 9. doi:10.1186/s13073-015-0220-9
27. Abd, E.I .,Wahed, A., Patel, P., Faye, O., Thaloengsok ,S., Heidenreich, D., …& Weidmann, M. (2015). Recombinase Polymerase Amplification Assay for Rapid Diagnostics of Dengue Infection. PLoS ONE, 10(6), e0129682. doi:10.1371/journal.pone.0129682
28. Euler, M., Wang, Y., Netnwich, O., Piepenburg, O, Hufert, F.T., & Weidmann, M.(2012). Recombinase polymerase amplification assay for rapid detection of Rift Valley fever virus. Journal of Clinical Virology, 54(4), 308–312. doi:10.1016/j.jcv.2012.05.006
29. Escadafal, C., Faye, O., Sall, A.A., Faye, O., Weidmann, M., Strohmeier, O., … & Patel, P. (2014) Rapid Molecular Assays for the Detection of Yellow Fever Virus in Low-Resource Settings. PLoS Negl Trop Dis, 8(3), e2730. doi:10.1371/journal.pntd.0002730
30. Wang, J., Yuan, W., Han, Q., Wang, J., Liu, L..(2017). Reverse transcription recombinase polymerase amplification assay for rapid detection of type 2 porcine reproductive and respiratory syndrome virus. Journal of Virological Methods, 243, 55-60. doi:/10.1016/j.jviromet.2017.01.017
31. Moore, M.D., and Jaykus, L.A. (2017). Development of a Recombinase Polymerase Amplification Assay for Detection of Epidemic Noroviruses. Scientific Reports, 7, 40244. doi:10.1038/srep40244
32. Bhardra, S., Jiang, Y.S., Kumar, M.R., Johnson, R.F., Hensley, L.E., Ellington, A.D. (2015) Real-Time Sequence-Validated Loop-Mediated Isothermal Amplification Assays for Detection of Middle East Respiratory Syndrome Coronavirus (MERS-CoV). PLoS ONE, 10(4), e0123126. doi:10.1371/journal
33. Pardee, K., Green, A.A., Takahashi, M.K., Braff, D., Lamber, G., Lee, J.W., … & Collins, J.J. (2016). Rapid, Low-Cost Detection of Zika Virus Using Programmable Biomolecular Components. Cell, 165(5), 1255-1266. doi:/10.1016/j.cell.2016.04.059
34. Zhao, Y., Wang, H., Zhang, P., Sun, C., Wang, X., Wang, X., … & Zhou L. (2016). Rapid multiplex detection of 10 foodborne pathogens with an upconverting phosphor technology based 10-channel lateral flow assay. Scientific Reports, 6, 21342. doi:10.1038/srep21342
35. Hanafiah, K.M., Arifin, N., Bustami, Y., Noordin, R., Garcia, M., & Anderson, D. (2017). Development of Multiplexed Infectious Diseases Lateral Flow Assays: Challenges and Oppertunities. Diagnostics, 7(51), 1-9. doi:10.3390/diagnostics7030051.
36. Ramage, J.G., Prentice, K.W., DePalma, P.L., Venkateswaran, K.S., Chivukula, S., Chapman, C., … & Pillai, S.P. (2016). Comprehensive Laboratory Evaluation of a Highly Specific Lateral Flow Assay for the Presumptive Identification of Bacillus Anthracis spores in Suspicious White Powders and Environmental Samples. Health Security, 14(5), 351-365. doi:10.1089/hs.2016.0041
37. O'Brien, T. (2018). BioThreat Alert® Reader. Retrieved from http://www.tetracore.com/bio-warfare/
38. Filipiak, W., Mochalski, P., Filipiak, A., Ager, C., Cumeras, R., Davis, C.E., … & Troppmair, J. (2016). A Compendium of Volatile Organic Compounds (VOCs) Released by Human Cell Lines. Current Medicinal Chemistry, 23, 2112-2131. doi:10.2174/092986732366616031612505
39. Sethi, S., Nanda, R., & Chakraborty, T. (2013). Clinical Application of Volatile Organic Compound Analysis for Detecting Infectious Diseases. Clinical Microbiology Reviews, 26(3), 462-475. doi:10.1128/CMR.00020-13.
40. Saasa, V., Malwela, T., Beukes, M., Mokgotho, M., Liu, C.P., & Mwakikunga, B. (2018). Sensing Technologies for Detection of Acetone in Human Breath for Diabetes Diagnosis and Monitoring. Diagnostics, 8(1), 12. doi:10.3390/diagnostics8010012
41. Enderby, B. Smith, D. Carroll, W., & Lenney, W. (2009). Hydrogen cyanide as a biomarker for Pseudomonas aeruginosa in breath of children with cystic fibrosis. Pediatr Pulmonol, 44(2), 142-147. doi:10.1002/ppul.20963
42. Berna, A.Z., McCarthy, J.S., Wang, R.S., Saliba, K.J., Bravo, F.G., Cassells, J., … & Trowell, S.C. (2015). Analysis of Breath Specimens for Biomarkers of Plasmodium falciparum Infection. The Journal of Infec-

tious Disease, 212, 1120-1128. doi:10.1093/infdis/jiv176
43. Bos, L.D.J., Sterk, P.J., Schultz, M.J. (2013). Volatile Metabolites of Pathogens: A Systematic Review. PLoS Pathog, 9(5), e1003311. doi:10.1371/journal.ppat.1003311
44. Buszewski, B., Kesy, M., Ligor, T., & Amann, A. (2007). Human Exhaled air analytics: biormarkers of diseases. Biomed Chromatogr, 21, 553-566. doi:10.1002/bmc.835
45. Mayr, D., Margesin, R., Klingsbichel, E., Hartungen, E., Jenewein, D., Schinner, F., & Märk, T.D. (2003). Rapid Detection of Meat Spoilage by Measuring Volatile Organic Compounds by Using Proton Transfer Reaction Mass Spectrometry. Appl Environ Microbiol, 69(8), 4697-4705. doi:10.1128/AEM.69.8.4697-4705.2003
46. Wilson, A., and Baietto, M. (2009). Applications and Advanaces in Electronic-Nose Technologies. Sensors, 9(7), 5099-5148. doi:10.3390/s90705099
47. Wilson, A. (2015). Advances in Electronic-Nose Technologies for the Detection of Volatile Biomarker Metabolites in the Human Breath. Metabolites, 5, 140-163. doi:10.3390/metabo5010140
48. Spencer, T.L, Lee, A.B., & Hu, D.L. (2018). A Biomimetic Nose for Advanced Threat Detection. HDAIC Journal, 5(1), 11-15. Retrieved from https://www.hdiac.org/wp-content/uploads/2018/04/A_Biomimetic_Nose_for_Advanced_Threat_Detection_V5I1_0.pdf
49. Giannoukos, S., Agapiou, A., Taylor, S. (2018, January). Advances in chemical sensing technologies for VOCs in breath for security/threat assessment, illicit drug detection, and human trafficking activity. Journal of Breath Research, 12(2). doi:10.1088/1752-7163/aa95dd
50. Angle, C., Waggoner, L.P., Ferrando, A., Haney, P., & Passler, T. (2016). Canine Detection of the Volatilome: A Review of Implications for Pathogen and Disease Detection. Frontiers in Veterinary Science, 3(47). doi:10.3389/fvets.2016.00047.
51. Staymates, M.E., MacCrehan, W.A., Staymates, J.L., Kunz, R.R., Mendum, T., Ong, T.H., … & Craven B.A. (2016). Biomimetic Sniffing Improves the Detection Performance of a 3D Printed Nose of a Dog and a Commercial Trace Vapor Detetor. Scientific Reports, 6, 1-10. doi:10.1038/srep36876
52. Wilson, A.D., & Baietto, M..(2011). Advances in Electronic-Nose Technologies Developed for Biomedical Applications. Sensors, 11, 1105-1176. doi:10.3390/s110101105
53. Wilson, A.D. (2015). Advances in Electronic-Nose Technologies for the Detection of Volatile Biomarker Metabolites in Human Breath. Metabolites, 5, 140-163. doi:10.3390/metabo5010140
54. Vargas, C., Wilhelm, A.A., Williams, J., Lucas, P., Reynolds, K.A., Riley, M.R. (2009). Appl.Environ.Microbiol, 75(20), 6431-6440. doi:10.1128/AEM.02036-08
55. Priest, P.C., Duncan, A.R., Jennings, L.C., & Baker, M.G. (2011). Thermal Image Scanning for Influenza Border Screening: Results of an Airport Screening Study. PloS ONE, 6(1), e14490. doi:10.1371/journal.pone.0014490
56. St. John, R.K., King, A., Jong, D., Bodie-Collins, M., Squires, S.G., Tam, T.W.S. (2005). Border Screening for SARS. Emerging Infectious Diseases, 11(1), 6-10. Retrieved from https://wwwnc.cdc.gov/eid/article/11/1/04-0835_article
57. Bitar, D., Goubar, A., Desenclos, J.C. (2008). International travels and fever screening during epdimics: a literature review on the effectiveness and potential use of non-contact infrared thermometers. Euro Surveillance, 14(6), 1-5. doi: 10.2807/ese.14.06.19115-en
58. Michel, A.P.M., Liakat, S., Bors, K., & Gmachl, C.F. (2013). In vivo measurement of mid-infrared light scattinering from human skin.Biomedical Optics Express, 4(4), 1-11. doi: 10.1364/BOE.4.000520
59. Zarnowiec, P., Lechowicz, L., Czwerwonka, G., & Kaca, W. (2015). Fourier Transform Infrared Spectroscopy (FTIR) as a Tool for Identification and Differentiation of Pathogenic Bacteria. Current Medicinal Chemistry, 22(14), 1710-1718. doi:10.2174/0929867322666150311152800
60. Al-holy, M.A., Lin, M., Cavinato, A.G., & Rasco, B.A. (2006). The use of Fourier transform infrared spectroscopy to differentiate Escherichia coli O157:H7 from other bacteria inoculated into apple juice. Food Microbiology, 23(2), 162-168. doi:10.1016./j.fm.2005.01.017
61. Bruyne, S.D., Speeckaert, M.M., & Delanghe, J.R. (2017). Applications of mid-infrared spectroscopy in the clinical laboratory setting. Critical Reviews in Clinical Laboratory Sciences, 55(1). doi:10.1080/10408363.2017.1414142
62. Bosch, A., Miñán, A., Vescina, C., Degrossi, J., Gatti, B., Montanaro, P., … & Yantorno, O. (2008). Fourier Transform Infrared Spectroscopy for Rapid Identification of Nonfermenting Gram-Negative Bacteria Isolated from Sputum Samples from Cystic Fibrosis Patients. Journal of Clinical Microbiology, 46(8), 2535-2546. doi:10.1128/JCM.02267-07
63. Bhunia, A.K. (2008). Chapter 1-Biosensors and Bio-Based Methods for the Separation and Detection of Foodborne Pathogens. Advances in Food and Nutrition Research, 54, 1-44. doi:10.1016/S1043-4526(07)00001-0\
64. Goodarzi, M. and Saeys, W. (2016). Selection of the most informative near infrared spectroscopy wavebands for continuous glucose monitoring in human serum. Science Direct, 146(1), 155-165. doi: 10.1016/j.talanta.2015.08.033
65. Fernandes, J. N., dos Santos, L.M.B., Chouin-Carneiro, T., Pavan, M.G., Garcia, G.A., David, M. R., … & Sikulu-Lord, M.T. (2018). Rapid, noninvasive detection of Zika virus in Aedes aegypti mosquitoes by near-infrared spectroscopy. Science Advances, 4(5), 1-6. doi: 10.1126/sciadv.aat0496
66. Tsang, M.K., Ye, W., Wang, G., Li, J., Yang, M., & Hao, J. (2016). Ultrasensitive Detection of Ebola Virus Olignonucleotide Based on Upconversion Nanoprobe/Nanoporous Membrane System. ACS Nano, 10(1), 598-605. doi: 10.1021/acsnano.5b05622



Alena James
Chemical and Biological Defense ORISE Fellow, Engility Corporation

Upon the completion of this article, Alena James was a Chemical and Biological Defense ORISE Fellow at The Department of Homeland Security Science & Technology Directorate (DHS S&T). Recently, Alena transitioned to a new role as a science and technology advisor for Engility supporting the Department of Defense. She earned her M.S. in Biodefense from George Mason University, her M.S. and B.S. in Biology from Winthrop University, and her B.A. in Political Science from Winthrop University. Her research interests are in chemical and biological defense research in risk analysis, disease surveillance, border security, and technology development.

Luther Lindler, Ph.D.
Senior Science Advisor Bio-Programs (ST), Department of Homeland Security Science & Technology Directorate

Luther Lindler, Ph.D., joined the Department of Homeland Security (DHS) Science and Technology Directorate (S&T) in October 2003 as a Senior Science Advisor. He currently serves as the Chief Scientist for biological programs providing expertise in the area of infectious disease threats from a global perspective. He is responsible for developing new technology strategies to meet DHS mission needs in the area of defense against bioterrorism. Before joining DHS, he was a leader in the U.S. Army Biodefense program. Lindler holds a Ph.D. in Microbiology from the Medical College of Virginia, a M.S. in Microbiology from Clemson University, and a B.S. in Medical Technology from Lenoir Rhyne College in North Carolina. He is the principal editor of the book, *Biological Weapons Defense: Infectious Diseases and Counterbioterrorism*.

BIOCOMPATIBLE AND PORTABLE SURGICAL SEALANT

TACTICAL COMBAT CASUALTY CARE

Nasim Annabi,
Anthony Weiss, &
Ehsan Shirzaei Sani

Major medical and technical advances in combat casualty care have significantly improved the military's ability to safely and effectively move wounded warfighters from tactical field care to in-hospital care. Studies have shown that wound infection, potentially due to insufficiently closed cutaneous closures, can be as deadly to the warfighter as the initial injury itself [1]. Conventionally, surgical closure and treatment of tissue defects is achieved by sutures, staples, or wires, which are not sufficient for repairing defects in highly stressed elastic tissues. Therefore, the application of adhesives for certain types of wounds is essential. There are also other issues related to sutures or staples, including limited access to defect sites. Even in tissues that can be sutured, the use of adhesives may be necessary to allow for better seal-

Image Credit | *Photo Illustration created by HDIAC and adapted from U.S. Army photo (Available for viewing at https://asc.army.mil/web/news-alt-jfm18-speeding-combat-casualty-care/).*

ing, such as in the closure of small stitching channels in a sutured artery wall. With these issues in mind, we aimed to synthesize an inexpensive, highly adhesive, biodegradable and biocompatible naturally derived sealant—methacryloyl-substituted tropoelastin (MeTro glue) [2].

Significance and Applications of MeTro Glue

The fabrication of MeTro glue is based on simple and fast photopolymerization using blue visible light or ultraviolet light. This polymerization technique is an inexpensive and technically simple approach to fabricate adhesives for particular surgical applications, especially those conducted in austere environments. During surgery, this sealant can be applied over the defect site as a liquid and rapidly cured—causing it to adhere strongly to soft tissues, stopping air and liquid leakages, and providing a more rapid time frame for tissue repair.

Due to the presence of tropoelastin, as soon as MeTro glue comes into contact with tissue, it solidifies into a highly flexible and elastic gel. It can then be further cured at the defect site by a short, light-mediated crosslinking to form an immediate bond—taking less than 60 seconds to seal the defects. The elastic properties of this glue give it an extensibility of more than 400 percent, which makes it a suitable biomaterial for engineering elastic tissues. MeTro's improved extensibility and rapid curing time make it well-suited for a tactical combat care environment, where wounded warfighters must be swiftly stabilized, and where evacuation methods may make it difficult to keep wounds fully immobile.

There is no commercially available elastic and biocompatible sealant that can be used suture-less for wound closure. Compared to commercial sealants, MeTro glue has remarkably higher elasticity (i.e., Progel) and higher adhesion to wet tissues (i.e., fibrin-based sealants, cyanoacrylate or Krazy glue). Also, the mechanical strength of MeTro glue can mimic native tissue, while some commercial sealants have insufficiently higher (i.e., BioGlue), or lower (i.e., hydrogel-based sealants) mechanical strength.

In order to translate the application of MeTro glue from animal to human use, our current study specifically evaluated the in vivo

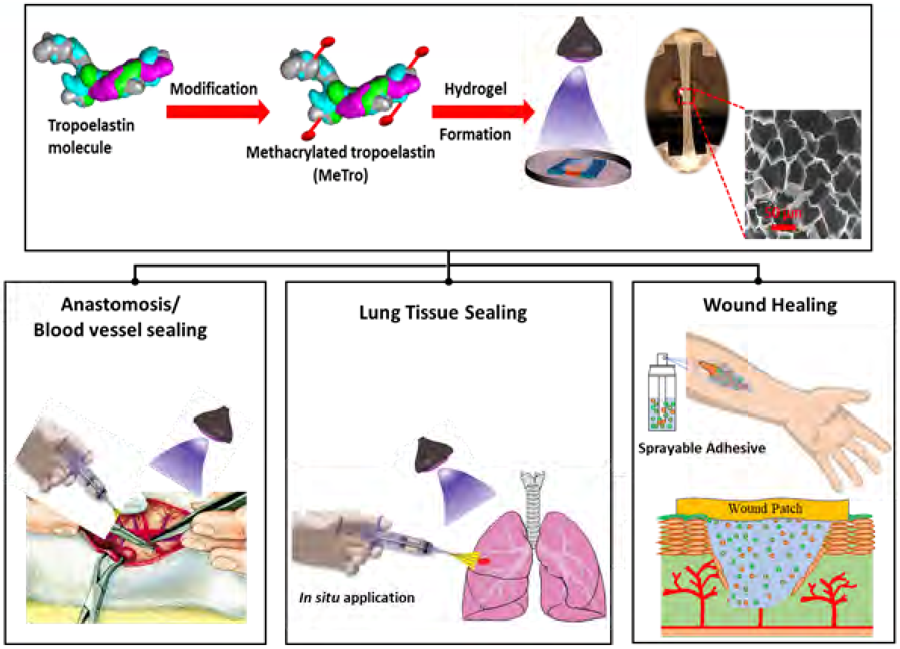


Figure 1. Synthesis of MeTro glue and its application in various surgical areas.

performance of the engineered hydrogel sealant in a rat and porcine lung leakage model. The experiments proved that MeTro is suitable for the sealing of significant pulmonary defects in large animals in the absence of additional suturing/stapling and facilitated fast wound healing. In terms of hemostasis, MeTro glue was sufficient in stopping mild hemorrhage from the generated rat and porcine lung lesions.

Thorough investigation of the actual hemostatic potential of the sealant should be performed in adequate bleeding models, such as a liver laceration model. In this context, appropriate modification of MeTro glue may allow for the creation of an effective sealant with strong hemostatic properties. Because pulmonary airways are a non-sterile environment, frequently evoking severe infections after lung surgery or other wounds, antibacterial functionality may be another desirable property of a pulmonary sealant [4]. This feature could be provided by including metal oxide nanoparticles, nanoparticle-carried antibiotic drugs, or antimicrobial peptides within the sealant. The next step is to test MeTro glue in clinical trials, in order to effectively investigate its functionality in a real-world setting.

MeTro glue is a highly promising solution to the Department of Defense's (DoD) growing need for novel and effective wound treatment strategies. According to recent publications outlining emerging requirements for combat causality care, there is a persistent need for medical technologies with minimal logistics footprints that can be used in austere environments [5]. Because each use of MeTro does not require supplementary equipment like sutures or staples to work, and has an estimated shelf life (at room temperature) of up to 10 years, it can meet the need of low maintenance supply chain trauma care solutions posed by the DoD.

Conclusion

MeTro glue has the potential for application as a highly biocompatible, elastic adhesive for use at each echelon of combat casualty care to reduce the mortality and morbidity associated with major wounds and injuries. In the case of surgical applications, it can be used as a sealant/bioadhesive to seal wounds (e.g., lung, skin, arteries, heart, nerves, etc.) after surgery. In austere environments, it can easily be sprayed or pipetted onto the wound area for both superficial and deep injuries. Regarding the ease of synthesis and application, our results show that MeTro's flexibility helps to minimize damage to adjacent tissue caused by avoiding mechanical compliance mismatch. MeTro glue offers strong potential for use as a surgical sealant in commercialized contexts and combat casualty care.

References

1. Aronson, N. E., Sanders, J. W., Moran, K. A. (2006). In harm's way: Infections in deployed American military forces. Clinical Infectious Diseases, 43(8), 1045–1051. doi:10.1086/507539
2. Annabi, N., Zhang, Y., Assmann, A., Sani, E. S., Cheng, G., Lassaletta, A. D., . . . Khademhosseini, A. (2017). Engineering a highly elastic human protein-based sealant for surgical applications. Science Translational Medicine, 9(410). doi:10.1126/scitranslmed.aai7466
3. Annabi, N., Shin, S. R., Tamayol, A., Miscuglio, M., Bakooshli, M. A., Assmann, A., . . . Khademhosseini, A. (2015). Highly elastic and conductive human based protein hybrid hydrogels. Advanced Materials, 28(1), 40–49.
4. Annabi, N., Rana, D., Sani, E. S., Portillo-Lara, R., Gifford, J. L., Fares, M. M., . . . Weiss, A. S. (2017). Engineering a sprayable and elastic hydrogel adhesive with antimicrobial properties for wound healing. Biomaterials, 139, 229-243.
5. U.S. Army. (2017, September 22). The warfighter's science and technology needs. Fort Eustis, VA: Army Capabilities Integration Center, U.S. Army Training and Doctrine Command. Retrieved from: https://pdfs.semanticscholar.org/b94c/ https://pdfs.semanticscholar.org/b94c/8fd-c629365b8b96932df91a26cb9135a81a8.pdf?_ga=2.145254324.1665739544.1532364846-2016030774.1532364846

Nasim Annabi, Ph.D.
Assistant Professor and Tannas Fellow, University of California, Los Angeles

Nasim Annabi is an assistant professor and a Tannas Fellow in the Department of Chemical and Biomolecular Engineering at the University of California, Los Angeles. Her research focuses on the design and synthesis of microengineered biomaterials for tissue engineering and surgical applications as well as development of *in vitro* bioengineering platforms for drug discovery and screening. Her contributions appear in nine patents/disclosures, six book chapters, and more than 100 peer-reviewed articles in highly regarded journals. Her interdisciplinary research has been recognized by several awards and funding, including the Australian Prestigious Endeavour Award (2010), the National Health and Medical Research Council Early Career Fellowship (2011), the Bright Futures Award at Harvard (2014), Scientist Development Award from American Heart Association (2016), C-Doctor Award (2017), and National Institute of Health (NIH, R01s) (2017, 2018).

Anthony S. Weiss, Ph.D.
McCaughey Chair in Biochemistry
Professor of Biochemistry and Molecular Biotechnology, The University of Sydney

Anthony S. Weiss is the McCaughey Chair in Biochemistry, Professor of Biochemistry and Molecular Biotechnology, Leader of the Tissue Engineering and Regenerative Medicine Node at the Charles Perkins Centre, and Professor at the Bosch Institute at the University of Sydney. He is a company founder, and his patented biomaterials inventions recently led to one of the largest commercial transactions in Australian healthcare history. Weiss has received several scientific prizes, recently including the highest category of national award, the Order of Australia. He leads research on human tropoelastin, which gives tissue its elasticity and enhances the repair of scars and wounds.

Ehsan Shirzaei Sani
University of California, Los Angeles

Ehsan Shirzaei Sani is a Ph.D. candidate in the Chemical and Biomolecular Engineering Department at the University of California, Los Angeles (M.S., Sharif University of Technology; B.S., University of Sistan and Baluchestan). His research is focused on the development of hydrogel-based bioadhesive platforms for sutureless sealing and repair of soft and hard tissues.

SWEAT BIOSENSING DEVICES FOR HEALTH MONITORING

Jason Heikenfeld
& Gavi Begtrup

While most commercial progress regarding the development of wearable sensors has centered around the smart adaptation of existing mechanical, electrical, and optical methods of measuring the body [1], these sensor modalities are of largely non-specific biometrics that are difficult to interpret outside limited applications.

For example, heart arrhythmias can either be an emergency or harmless, and directly measuring concentrations of biomarkers such as C-reactive protein, Interleukin-6, or B-type natriuretic peptide can provide a more definitive diagnosis of a heart condition. Although developing non-invasive chemical sensing of biomarkers is technologically challenging, these novel devices present the most significant biosensing opportunities, including:

- monitoring chemical agent exposure by measuring the agent permeating through skin—like an internal dosimeter for toxins
- tracking human performance (both cognitive and physical) in real time by measuring biomolecular indicators of stress, resilience, or dehydration
- identifying individuals who have come into contact with chemical or biological agents by measuring specific biological markers secreted by the body, reducing conventional reliance on external measurements based on markers that can be washed away or confounded

Multiple components of the Department of Defense (DoD) have highlighted real-time physiological status monitoring (PSM) as a top-tier priority for their research and development (R&D) and science and technology programs. The Army, Navy, and Air Force have set forth an R&D roadmap for Human Systems that focuses in part on delivering “technology capable of objectively measuring warfighter performance in operational environments,” that will enable “real-time monitoring” of critical stressors on warfighters and their resulting physiological status [2]. In order to achieve these R&D goals, researchers must develop simple sensors that may quickly, remotely, and non-invasively perform biomarker measurements.

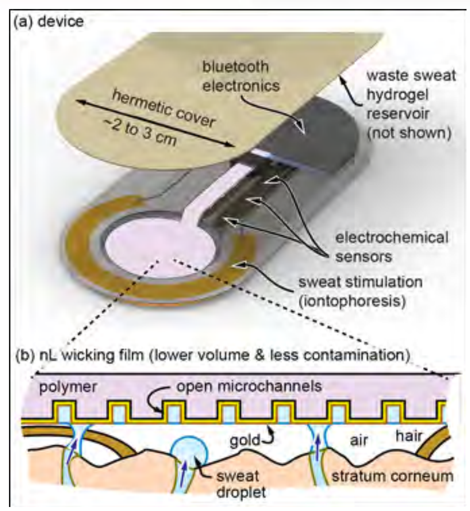


Figure 1. Diagram of an advanced sweat biosensing device, including integrated localized stimulation of sweat (sweat on-demand), advanced wicking materials to work with tiny nanoliter volumes of sweat, and electrochemical sensors to continuously read biomarker concentrations.

Image Credit *Photo Illustration created by HDIAC and adapted from photos by Michele Eaton (U.S. Air Force) and Adobe Stock. (Eaton's photos available for viewing at https://www.wpafb.af.mil/News/Article-Display/Article/818830/bio-sensing-gives-new-meaning-to-breaking-a-sweat/)*

The Air Force Research Laboratory (AFRL) is a notable R&D leader in this space, sponsoring multiple projects seeking to develop skin-wearable biosensing devices. For example, in 2014, AFRL kicked off a multi-year development project in collaboration with the Nano-Bio Manufacturing Consortium to develop a wearable sweat-based biofluid sensor [3]. GE Global Research served as project lead, with industry partner American Semiconductor, Inc., and academic partners Dublin City University, the University of Massachusetts at Amherst, the University of Connecticut, and the University of Arizona. Early prototypes of the patch—which have been tested in the laboratory and in the field—focused on sensing sodium and potassium levels in sweat to continuously monitor hydration levels [4]. The group's ongoing R&D is focused on improving the patch's reliability and stability, as well as extending its shelf life and incorporating additional measurement capabilities, like sweat rate sensing [4].

In 2011, ARFL launched a biochemical monitoring research initiative in collaboration with the University of Cincinnati (UC) to advance the state of the art in biosensing by focusing first on articulating its fundamental challenges. The team investigated the biological mechanisms behind how chemical analytes partition from blood and enter into secreted biofluids like sweat, saliva, or interstitial fluid [5]. For example, it was important to identify early on whether concentrations of the stress biomarker cortisol can be measured in sweat in order to monitor physiological status, similar to how they are used in blood. The team also focused on enabling the controllable secretion of fluids and chemical analytes, while also establishing methods for rapidly and efficiently capturing them in nanoliter-scale volumes for transport to sensors.

The AFRL–UC team developed an open microfluidic platform made out of advanced wicking materials that uses open micro-channels to wick sweat up from the surface of the skin (see Figure 1). These channels cover only 10 percent of the biosensing device's skin-to-sensor surface area, which allows the device to accurately measure analytes using substantially smaller volumes of sweat than previous designs. It also limits contamination of the sweat by dead skin cells—contamination that otherwise would decrease the device's efficiency and ultimate usefulness to the warfighter. AFRL is working with Eccrine Systems, Inc., to test the feasibility of DoD adopting wearable biochemical monitoring on a large scale [6, 7]. As part of AFRL's Tech Warrior 2017 training exercise, Eccrine Systems field-tested a biosensing device capable of continuously tracks and wirelessly reports sweat loss to profile warfighter risk of dehydration [6].

These devices may be used for other applications, the foremost of which is chemical sensing (whether in a continuous and/or repeated modality). It is impossible to imagine modern medicine without the ability to measure the presence, concentration, or functional activity of analytes in biofluids, such as blood and urine. Commercially, however, it is not yet possible to do the same in a continuous and wearable format for any analyte other than glucose. To close the gap, Eccrine Systems is investigating whether cortisol can be monitored in sweat to continuously track levels of stress and recovery.

To further benefit warfighter biosensing applications, two significant areas of future research are investigated. First, expanding capabilities in predictive modeling of analyte partitioning, with a goal of predicting how analyte concentrations change after a physiological event (toxin, injury, fatigue, infection, etc.). The use of predictive modeling is likely to minimize the time needed to develop biosensing technologies and perform on-body validation. Second, investing in new applications, which will invariably require new robust and specific sensors. Combined, these efforts seek to enhance DoD's ability to continuously and accurately monitor the physiological status of its forces in the field.

References

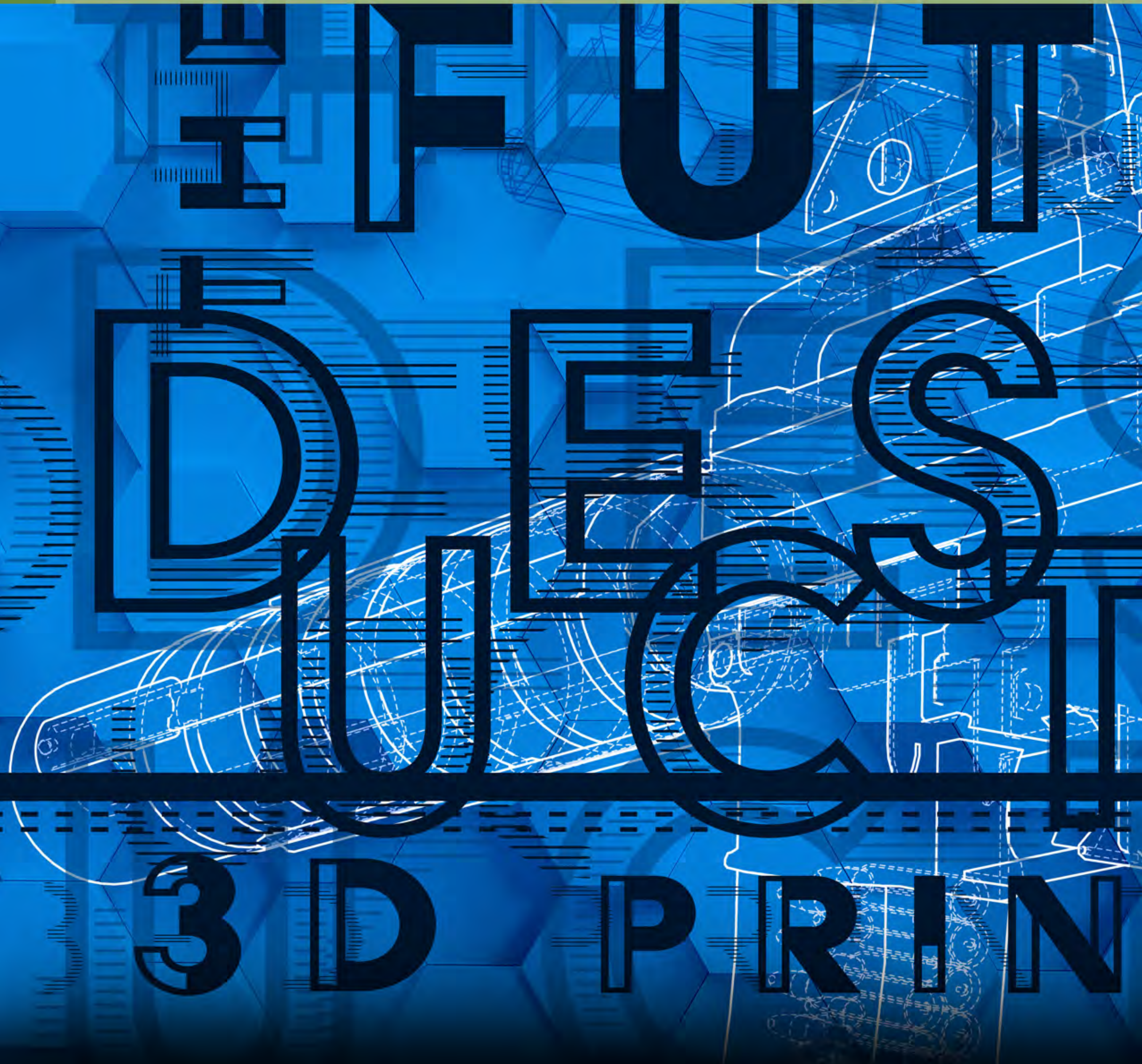
1. Heikenfeld, J., Jajack, A., Rogers, J., Gutruf, P., Tian, L., Pan, T., . . . Kim, J. (2018). Wearable sensors: Modalities, challenges, and prospects. *Lab on a Chip*, 18(2), 217-248. doi:10.1039/c7lc00914c
2. Tangney, J. (2016). Human systems roadmap review. *Defense Science & Technology*. Retrieved from http://www.defenseinnovationmarketplace.mil/resources/NDIA_Human_Systems_Conference_2016_HSCOI_DistroA_FINAL.pdf
3. Alia-Novobilski, M. (2018, April 17). AFRL-led patches make 'sense' of sweat. Wright-Patterson Air Force Base. Press release. Retrieved from https://www.wpafb.af.mil/News/Article-Display/Article/1495074/afrl-led-patches-make-sense-of-sweat/
4. Alizadeh, A., Burns, A., Lenigk, R., Gettings, R., Ashe, J., Porter, A., . . . (2018, July 31). A wearable patch for continuous monitoring of sweat electrolytes during exertion. *Lab Chip*, 18, 2632–2641. doi:10.1039/C8LC00510A
5. Heikenfeld, J. (2016). Non-invasive analyte access and sensing through eccrine sweat: Challenges and outlook circa 2016. *Electroanalysis*, 28(6), 1242-1249. doi:10.1002/elan.201600018
6. Wright-Patterson Air Force Base, 88th Air Base Wing Public Affairs. (2017, October 4). *Tech Warrior participants walk in the shoes of battlefield Airmen* [Press release]. Retrieved from http://www.wpafb.af.mil/News/Article/1328072/tech-warrior-participants-walk-in-the-shoes-of-battlefield-airmen/
7. Bachman, J. (2016, September 16). Why the Air Force wants to see pilots' sweat. Bloomberg. Retrieved from https://www.bloomberg.com/news/articles/2016-09-16/why-sweat-is-the-future-of-biotech

Jason Heikenfeld, Ph.D.
Professor and Assistant Vice President for Commercialization, University of Cincinnati

Jason Heikenfeld directs the Novel Devices Laboratory at the University of Cincinnati, which has established highly-focused international leadership roles in emergent technologial paradigms, including electrowetting, electronic paper, and sweat biosensing technology. He has accumulated a University of Cincinnati record number of patents and licenses. He was an Air Force Office of Scientific Research (AFOSR) Young Investigator, is a Senior member of IEEE and the Society for Information Display, a life-member of SPIE, a member of American Society for Engineering Education (ASEE), and a Fellow of the National Academy of Inventors.

Gavi Begtrup, Ph.D.
Chief Executive Officer of Eccrine Systems, Inc.

Gavi Begtrup, Ph.D. is the Chief Executive Officer of Eccrine Systems, Inc., a privately-held biotechnology company focused on advanced sweat sensors. He received his Ph.D. in Physics from the University of California, Berkeley and his B.S. from Western Kentucky University. He previously founded and was CEO of an agricultural materials startup and has supported technology commercialization and startup formation for research organizations and venture investment. He is an expert in micro- and nano-electromechanical systems, is the author of popular and scientific articles, and is an inventor listed on multiple issued and pending patents for novel nanoscale devices and sweat sensing systems. He served as a policy advisor to former Representative Gabrielle Giffords (AZ-8), overseeing NASA, DoD, and other federal agencies. He was also a science and technology policy fellow with the National Academies of Sciences, Engineering, and Medicine.

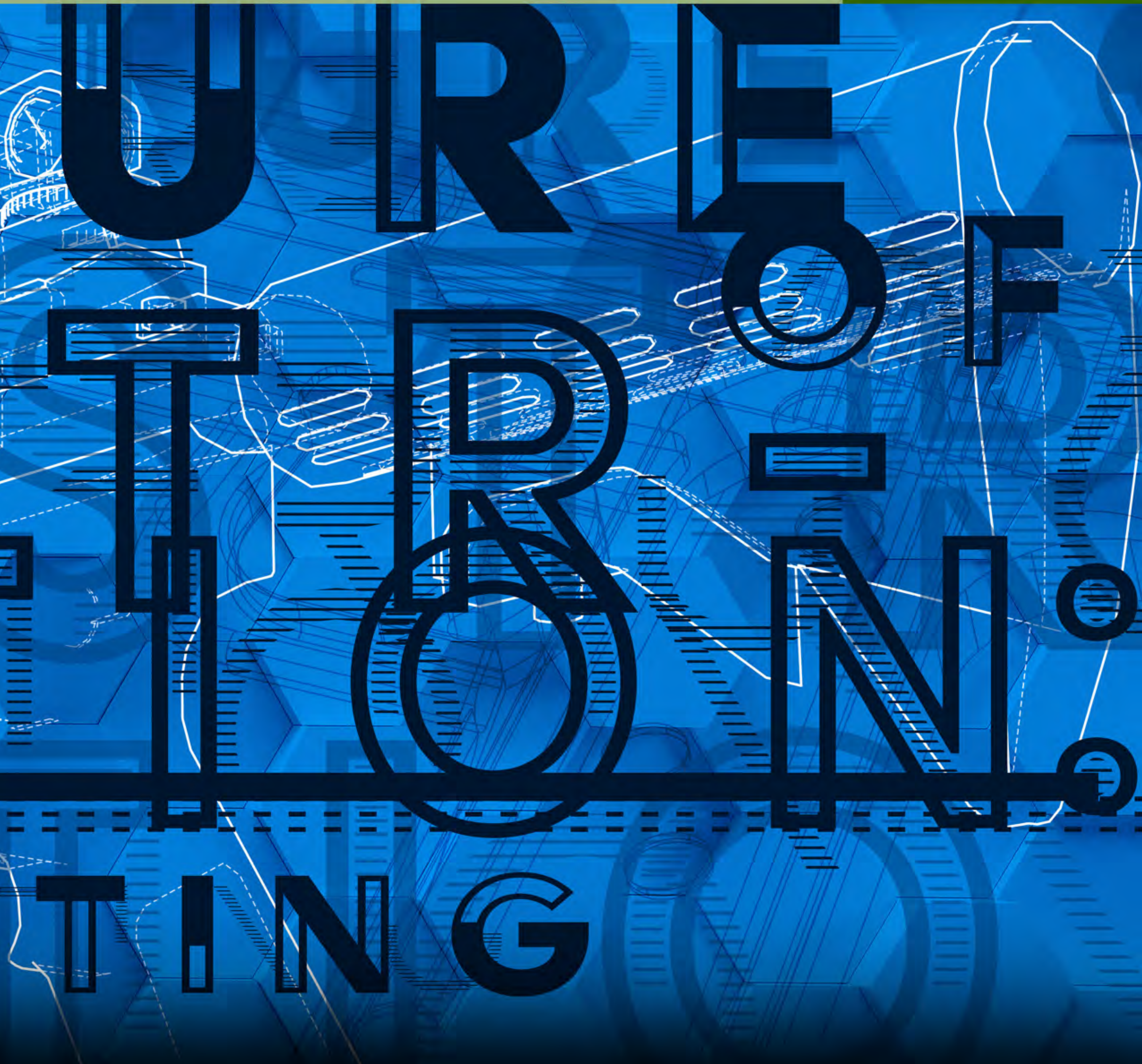


Gregory Nichols

Three-dimensional (3D) printing is rapidly being adopted by many sectors, including the U.S. Department of Defense (DoD), given its ability to reduce waste, cost, and time related to traditional subtractive manufacturing processes [1]. However, the advent of this technology, and its ability to produce objects that were previously extremely difficult to manufacture, has raised security concerns [2, 3], and many organizations have also begun to question the role that 3D printing could play in weapons development—including weapons of mass destruction (WMD).

For example, the U.K. Ministry of Defence (MoD) has acknowledged the advantages that 3D printing may present to terrorist organizations and other non-state actors in regard to weapons proliferation [4]. In 2016, DoD released its Additive Manufacturing Roadmap, which stated that, “AM [additive manufacturing] can be used to our advantage, and our adversaries can use it against us [5].'' Director of National Intelligence Dan Coats echoed this sentiment in his 2018 Worldwide Threat Assessment when he remarked, “Advances in manufacturing, particularly the development of 3D printing, almost certainly will become even more accessible to a variety of state and non-state actors and be used in ways contrary to our interests [6].” During events convened by the United Nations in both 2016 and 2017, potential challenges posed by 3D printing regarding access to WMD were discussed, including an increased opportunity to “violate internation-

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



al sanctions and export controls [7]," given that it is easier to acquire such weapons by printing parts that are otherwise difficult to obtain [8]. Although 3D printing techniques continue to be refined as the technology matures, security challenges remain largely unchecked. These concerns have already been made manifest in the development of 3D printed small arms [9], consequently raising questions as to what other potentially devastating WMD or weapons of mass disruption 3D printing may harbor. Some of these concerns, including cyber vulnerabilities and counterfeit parts, have been raised by DoD and planned to be addressed as evidence by strategic objectives in DoD's Additive Manufacturing roadmap (see Figure 1).

Overview of 3D Printing and Additive Manufacturing

3D printing "is the process of making an object by depositing materials, one tiny layer at a time [10]." The term is often used interchangeably with additive manufacturing; however, additive manufacturing can include other types of processes beyond printing [1]. Additive manufacturing techniques, including 3D printing, are in a family counterpoint to traditional manufacturing techniques, known as subtractive (e.g., forging, casting, and milling), in which material is removed from an object until the desired shape is formed [1].

The process of 3D printing is rather straightforward (see Figure 2). An object is either digitally scanned and turned into a digital file, or the design is directly created in a file. This file is imported into a machine that uses materials (e.g., metal powder or plastics) to build up a

Focus Area	Integrated Objective	Integrated Impact Statement
Design	DoD.D.1 – Enable Robust, Integrated, and Intelligent Design Tools	Streamline design process, reduced cycle time, and higher performance products
	DoD.D.2 – Enable Design for AM	Increase capability rapidly delivered to warfighter
	DoD.D.3 – Improve Reverse Engineering Capabilities	Push AM forward, enabling increased self-sufficiency of units and innovation by users in the field
	DoD.D.4 – Develop Design for Function (Application-based Design) Guidelines	Apply AM to meet specific weapons systems requirements
Material	DoD.M.1 – Define Standard AM Materials Requirements	Enhance predictability of resulting part performance using an interoperable framework for AM at DoD
	DoD.M.2 – Establish Vendor Qualification and Encourage Expansion of Material Sources	Increase the range of materials available to designers, enhancing part performance
	DoD.M.3 – Develop AM Materials	Establish priorities for AM material development activities necessary to meet DoD requirements
	DoD.M.4 – Create Defined and Accessible Pedigreed Datasets & Schemas	Establish authoritative data sets for simulation and reference
	DoD.M.5 – Establish a DoD-wide M&P AM Data Repository	Establish a single repository of material, process, and performance data. Speed up research, enable quality
	DoD.M.6 – Develop Model-based Approaches to Accelerate Materials Qualification and Certification	Guarantee quality of AM parts
Process	DoD.P.1 – Develop NDE and Process Control	Enhance the sensing capability of machines, gather data to ensure quality
	DoD.P.2 – Establish Stable and Robust AM Processes	Enable broader application of AM through process stability and equipment ruggedization
	DoD.P.3 – Develop Open Architecture Equipment	Ensure transferability and interoperability through specifications and standards
	DoD.P.4 – Modify Existing or Develop New Process Capabilities	Modify or develop processes to increase the applicability of AM in a variety of situations
Value Chain	DoD.V.1 – Build Cost Models and Decision Tools	Understand when, where, and how to apply AM
	DoD.V.2 – Develop Qualification and Certification Methods for Parts and Systems	Guarantee quality of parts and interface with existing/new DoD policies
	DoD.V.3 – Establish Cyber Infrastructure and Cyber Security	Enable secure information technology infrastructure for end-to-end connectivity of the manufacturing process
	DoD.V.4 – Establish Physical AM Infrastructure	Install AM machines across DoD enterprise
	DoD V.5 – Business Practices – Intellectual Property, Data Rights and Contracting Issues specific to AM	Establish agreed-upon business practices to ensure seamless integration of AM into the existing supply chain

Figure 1. DoD's Strategic Alignment of Objectives Regarding Development of Additive Manufacturing Capabilities [5]. (Adapted from Source: Department of Defense).

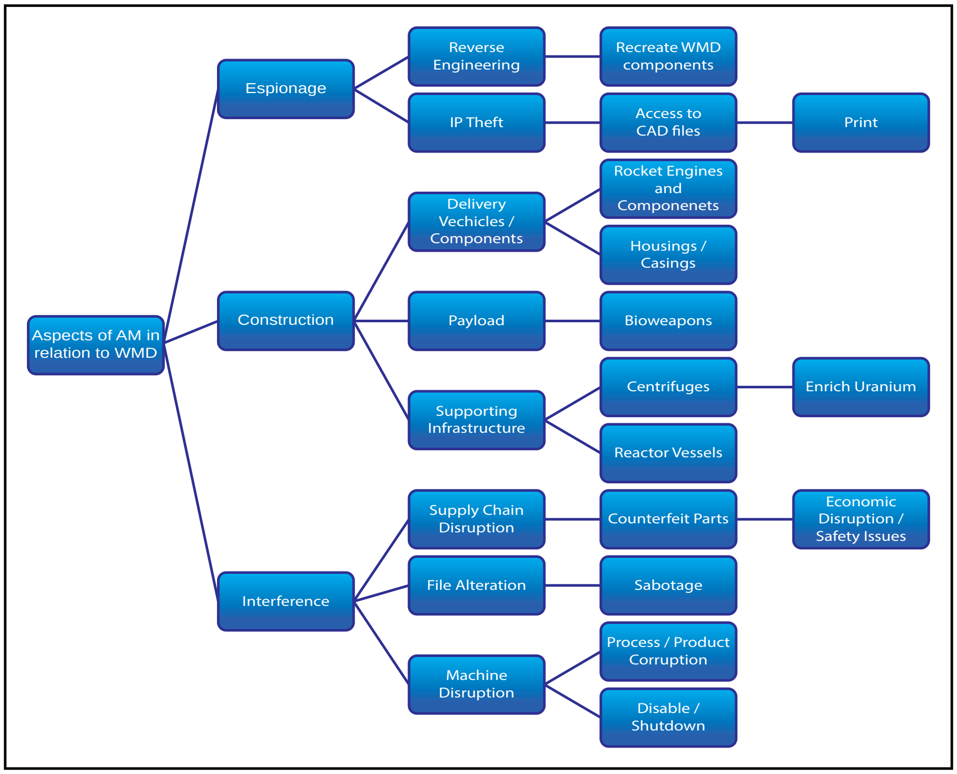


Figure 3. Classification tree demonstrating methods available to use additive manufacturing (AM) in or as a weapon of mass destruction.

3D object. Because the machine only uses the specific amount of material required to print each layer as instructed by the file, there is little to no waste.

Additional benefits afforded by this technology include a lower demand for highly skilled labor, a reduction in physical space required to house machinery compared to traditional manufacturing, and a decrease in the time required to produce objects. These benefits are also attractive to bad actors who may use 3D printing to more easily manufacture and distribute WMD—disrupting traditional barriers to WMD proliferation.

3D Printing in Relation to WMD

The potential for 3D printing to create WMD is still largely unknown, but most experts agree that it is currently unlikely that a WMD may be wholly constructed through 3D printing. However, components used to construct WMD can be 3D printed [3, 11-13]. Additionally, 3D printers and associated infrastructure (the technology itself) may be manipulated to, in effect, become weapons—more appropriately termed weapons of mass disruption [14]. This application of 3D printing for use in the development of WMD can be classified into three main categories: espionage, construction of a weapon, and interference with the 3D printing process (see Figure 3).

Espionage

According to MI5, "espionage is the process of obtaining information that is not normally publicly available ... if this information is obtained by those with no right to access it, serious damage can be caused [15]." Critical military assets manufactured by DoD laboratories and industry partners alike increasingly rely on 3D printing. Vulnerabilities in the printing process, even with restricted access, could allow this information to be gathered in one of two ways: gaining access to computer-aided design (CAD) files or conducting a side-channel attack. First, intellectual property theft is a primary concern. Since the CAD files used in 3D printing are digital, hackers could gain access to the blueprints of the item being printed, enabling the hackers to print these items or give/sell the CAD files to adversaries of the U.S. [3, 16-18]. Conversely, someone could easily scan an item and convert that image into a CAD file that could later be used in the 3D printing process [16]. The ease with which items can be copied and 3D printed replicas can be fabricated is cause for increased vigilance regarding insider threats [3, 18].

Second, based on outputs created by the 3D printing process, it is possible to reverse engineer a product—known as a side-channel attack. In 2016 and 2017, researchers at the University of California, Irvine, and Siemens Corporation published research supporting that each type of item printed on a 3D printer creates a unique pattern of "analog emissions such as vibration, acoustic, magnetic, and power [19, 20]." These emissions create a unique fingerprint for each item, and capturing these emissions makes it possible, through reverse engineering, to recreate the product being printed.

Additionally, researchers at University at Buffalo (the State University of New York) have also demonstrated that many of these emissions can easily be recorded using the sophisticated, sensitive sensors present in many smartphones [21]. Additional work by researchers at the University of California, Irvine, and Siemens Corporation was able to show that through the use of a thermal imaging camera, it is possible to trace the movement of the printer nozzle, since intense heat is used to melt the material used to form the object [22].

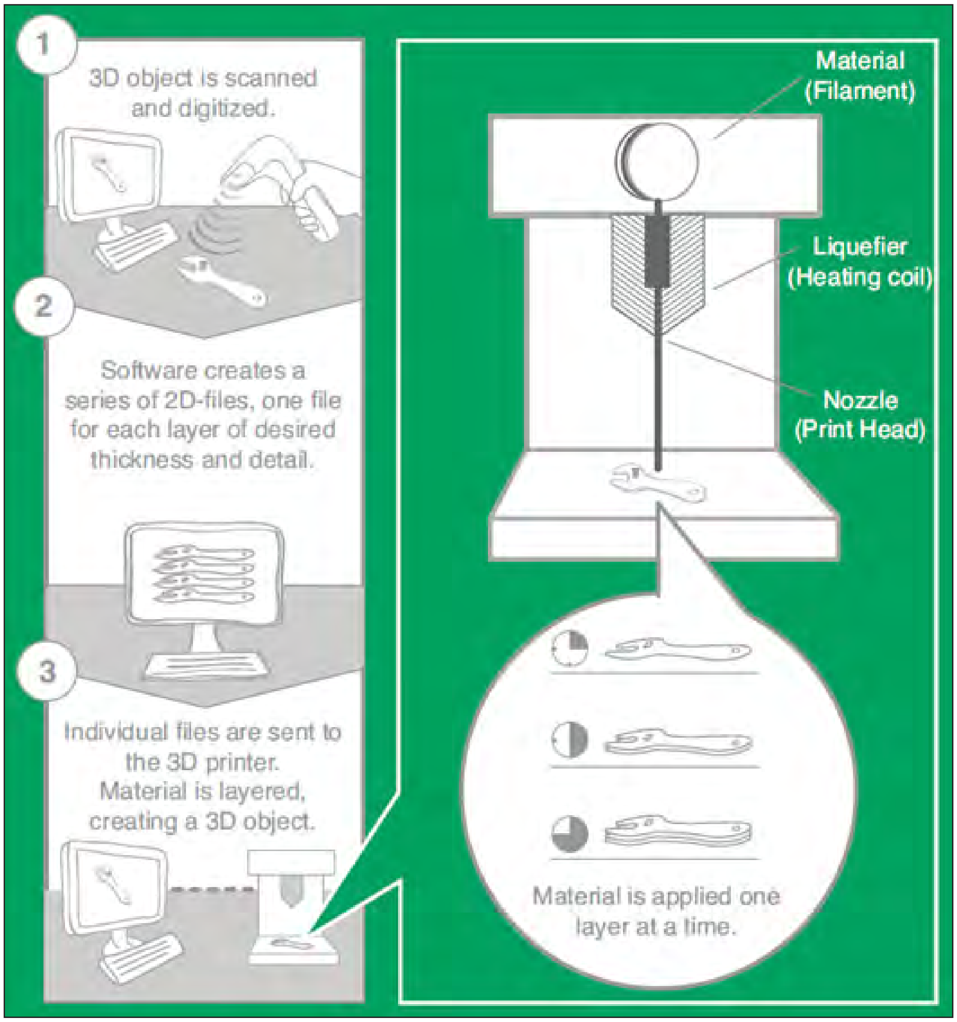


Figure 2. Overview of the additive manufacturing process [2] (Released).

Construction

Traditional barriers to creating WMD include export controls, limited access to specialized resources, time, scale of facilities needed, and volume of waste produced [23]. One of the key advantages, and also concerns, of 3D printing is that it removes some of these barriers. Several key components of a WMD could be printed [11, 13], including delivery vehicles/ components (e.g., missiles and engine components), some payloads (i.e., chemical and limited biological), and supporting infrastructure to make the payloads or WMD (e.g., centrifuges for uranium enrichment). However, at this time, 3D printing could not be used to print an entire WMD or even all components (i.e., nuclear payloads) [11-13].

Many governmental, academic, and industrial organizations have conducted research regarding the 3D printing of rocket and missile components. Organizations, including NASA, Aerojet Rocketdyne, and SpaceX have all successfully launched rockets comprised of smaller 3D printed components, such as valves [24, 25]. Furthermore, in 2016, students at the University of California, San Diego, launched a rocket, the Vulcan-1, which featured a completely 3D printed engine [25].

Raytheon Missile Systems has already demonstrated it is possible to 3D print almost every component of a missile, including rocket engines, fins, and parts for guidance and control systems [26]. The technology continues to develop, which may allow soldiers to print and assemble missiles in the field. In terms of traditional concepts of WMD delivery systems, Lockheed Martin is exploring potential uses of 3D printing for next generation intercontinental ballistic missiles [27].

The printing of payloads and support infrastructure is currently more complicated than the 3D printing of launch vehicles—thereby making it less likely to occur. One of the biggest debates over the past few years has been whether it is possible to 3D print an entire nuclear weapon. Researchers from academia and the non-gov-

Challenges	Solution	Performing Organization(s)
Counterfeiting	Embed quantum dots in object	Quantum Materials Corp [48]
File tampering	Hashing/blockchain	Virginia Polytechnic Institute and State University [37]
Counterfeiting	Add taggant to source material	Electric Power Research Institute [44]
Counterfeiting	Micro/nano-strctured fingerprints/watermarks	U.S. Department of Defense [5]
Sabotage/Counterfeiting/Quality Control	Mechanical and physical testing	New York University and University of Texas[38]
Illegal access to materials	Monitor online retailers	Wisconsin Project on Nuclear Arms Control [43]
Sabotage/Counterfeiting/Quality Control	Three-layer verification	Georgia Institute of Technology and Rutgers University [49]
Sabotage/Counterfeiting/Quality Control	Piezoelectric transducer augment impendence-based structural health monitoring	Virginia Polytechnic Institute and State University [50]
Sabotage	Continuous monitoring of current delivered to actuators	University of South Alabama, Ben-Gurion University, Lawrence Livermore National Laboratory, and Singapore University of Technology and Design [51]
Sabotage	Digital audio signing	Ben-Gurion University, University of South Alabama, and Singapore University of Technology and Design [42]
Weapons proliferation	Explore possibilities for 3D printing weapons	Terrorist Explosive Device Analytical Center [47]
Intellectual property protection/Counterfeiting	Spectral signatures	InfraTrac, The Pennsylvania State University and the University of Maryland [52]

Table 1: Proposed methods for mitigating challenges of 3D printing in the development of WMD.

ernmental organization sector with previous government and policy experience agree the technology does not fully support the ability to print an entire nuclear weapon [11-13]. One of the key challenges is printing the core due to the complicated chemistries of uranium, plutonium, and beryllium [11].

However, one crucial component, high-yield explosives, has been printed on at least two occasions at Department of Energy (DOE) laboratories —Los Alamos National Laboratory and Lawrence Livermore National Laboratory [28, 29]. To some degree, it is possible to print smaller components of nuclear weapons. It may also be possible to print parts of reactors [11] and centrifuges since additive manufacturing technology improves every day. For example, it is becoming possible to print with critical materials, such as carbon fiber and maraging steel, which are required in the construction of centrifuges [13].

A partnership between Lawrence Livermore National Laboratory and Y-12 National Security Complex supports the National Nuclear Security Administration in finding new methods to update the nuclear weapons enterprise using additive manufacturing [30]. In addition, DOE, the Electric Power Research Institute, and various industry partners are exploring additive manufacturing methods to create nuclear reactor components [31].

Chemical and biological agents are more difficult to 3D print, but the technology is rapidly developing to accommodate these capabilities. For example, researchers at the Middlebury Institute of International Studies in Monterey, California, explain that 3D printing may allow for the construction of tissues needed to perform toxicity testing for biological agents [32], and researchers from Louisiana State University estimate that it could be possible to print simple chemical weapons in 10 years [33].

Interference

Interference can be more accurately defined as disruption, rather than the conventional view of destruction. The interface of cyber-based and online controls with physical objects, known as cyber-physical systems, is becoming more commonplace, particularly among critical infrastructure sectors. Concerns regarding the effects of interrupting cyber-physical systems used in critical infrastructure can be traced to at least 1997, when the President's Commission on Critical Infrastructure Protection reported that "disruption of any infrastructure is always inconvenient and can be costly and even life threatening [34]."

3D printers are sometimes directly connected to the internet, are used in large-scale production facilities that are connected to extensive computer-based control systems, and rely on digital files—making them vulnerable to attack [35]. Apart from security concerns related to cyberattacks that could shut down 3D printers used in the Defense Industrial Base and Critical Manufacturing Sectors [36], disruption of cyber-physical systems in manufacturing could lead to major disruption among other sectors, including the Nuclear Reactors, Materials, and Waste Sector; the Chemical Sector; and the Transportation Sector.

Concerns related to the manipulation of 3D printed parts in these critical sectors can come in three forms. First, bad actors could deliberately manipulate CAD files so that crucial components would fail during operation, leading to catastrophic error in a system [37]. Sabotage could occur by altering the printing orientation of the object or embedding defects into the object [38]. This is a key concern within the aviation industry as an influx of companies, such as Boeing, Airbus, and GE Aviation, are utilizing 3D printed components [39]. In fact, this could also be a concern for military aircraft security as earlier this year, Marines aboard the USS Wasp successfully 3D printed a replacement part for an F-35B Lightning II [40]. Moreover, academic researchers demonstrated the ease of sabotage in 2016 when they altered the file for one of the propellers on a quadrotor drone, causing the propeller to fail during the test flight, crashing the drone [41].

Second, since many 3D printers are connected to the internet, or to a networked computer system, several researchers have also theorized it is possible to hack directly into the printer, causing it to malfunction [37, 42]. This threat has been acknowledge by DoD, and developing safeguards to prevent cyberattacks on 3D printers is identified as an objective in the DoD Additive Manufacturing Roadmap [5]. Finally, the ease of access to 3D printers and the materials they need to fabricate items makes it much easier for both legitimate users and underground operators to produce parts intended for critical sectors [43]. Counterfeit parts, particularly in the nuclear industry, have been tracked for many years [44]. However, the advent of 3D printing will most likely improve the ease with which counterfeit parts can be produced, yielding parts whose flaws remain nearly undetectable. These counterfeit parts pose safety and security concerns as they may more readily enter legitimate supply chains [2, 23, 45].

Research Gaps, Challenges, and Mitigation

A 2018 National Defense University study found that additive manufacturing will have a much greater impact than other emerging technologies on acquisition, production, weaponization, and delivery of WMD [46]. Because of this, many researchers and agencies are developing strategies to address critical safety and security gaps. These efforts have been placed into five categories by Fey [3]:

- Strengthening cybersecurity related to 3D printers and supporting infrastructure
- Incorporating protective measures directly within software, hardware, and materials
- Adapting export controls to minimize the purchase and use of new 3D printing technology and base materials that could be used to create WMD
- Raising awareness of the new challenges 3D printing brings to WMD proliferation
- Encouraging industry to impose self-regulation/best-practices regarding the responsible use of 3D printing technologies

The DoD acknowledges the cyber risks posed by 3D printers and has included objectives to strengthen this area in its Additive Manufacturing Roadmap [5]. Other areas of risk, such as sabotage and counterfeiting, are being addressed by researchers across academia, industry, and government, who are primarily investigating methods to embed identifying materials in 3D printed objects for easy detection of tampering (see Table 1).

However, the use of 3D printing to circumvent export controls remains one of the most difficult challenges to address. Critical materials (e.g., maraging steel, titanium, and carbon fiber) are widely available for purchase online [43], and while the high-precision CNC machines needed to create components of nuclear weapons are export-controlled, 3D printers are not. The technological ability of many 3D printers that use metal powders could be precise enough to print several components needed for nuclear weapons production [13].

Closing export control gaps is crucial to national security. In 2014, the FBI's Terrorist Explosive Device Analytical Center (TEDAC) purchased a 3D printer to investigate the types of explosive devices that can be made with printers and printing materials easily purchased online. This effort allows the agency to better understand the capabilities that 3D printing may provide to terrorists and insurgents [47]. Actions such as TEDAC's may support other agencies, including DoD, in understanding the emerging capabilities 3D printing brings to WMD proliferation. It can also aid in the development of 3D printing-specific counterproliferation techniques.

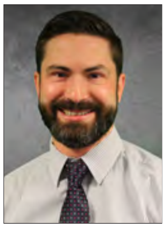
Conclusion

3D printing has already been used to create small arms that can fire bullets with relative precision [9], and additional uses in weapons development will continue to take shape as the technology advances. As the level of sophistication regarding 3D printing grows, so will the risk attributed to non-state actors in weapons proliferation and WMD creation. The DoD and Department of Homeland Security have both acknowledged these risks, but the rapid pace of technology development and existing policies that were created to address traditional WMD threats (i.e., nuclear weapons made with conventional means) do not necessarily provide all the resources needed to mitigate new threats. However, DoD has acknowledged some of these challenges and is working toward solutions, primarily securing cyber-physical infrastructure and reducing the risk of sabotage.

References

1. U.S. Government Accountability Office. (2015, October). Defense additive manufacturing: DoD needs to systematically track department-wide 3D printing efforts (GAO-16-56). Washington, DC. Retrieved from https://www.gao.gov/assets/680/673099.pdf
2. McNulty, C. M., Arnas, N., & Campbell, T. A. (2012). Toward the printed world: Additive manufacturing and implications for national security (Defense Horizons Policy Brief No. 73). Washington, DC: National Defense University, Institute for National Strategic Studies. doi:10.21236/ada577162
3. Fey, M. (2017). 3D printing and international security: Risks and challenges of an emerging technology (PRIF Rep. No. 144). Frankfurt am Main, Germany: Peace Research Institute. Retrieved from https://www.hsfk.de/fileadmin/HSFK/hsfk_publikationen/prif144.pdf
4. Ministry of Defence U.K. (2015). Strategic Trends Programme: Future operating environment 2035 (1st ed., Development, Concepts and Doctrine Centre Strategic Trends Programme, MOD Guidance). Ministry of Defence U.K. Retrieved from https://www.gov.uk/government/publications/future-operating-environment-2035
5. U.S. Department of Defense. (2016, November 30). Department of Defense Additive Manufacturing Roadmap (Final Rep.). Retrieved from https://myclass.dau.mil/bbcswebdav/institution/Courses/Deployed/ACQ/ACQ404/Archives/Student%20Materials/Student_Materials/6%20SAMC%20Class%20Prep%20Readings%20-%20FY17-2%20June%205-9/Additional%20References/DoD%20Nov%2016%20Rpt%20Re%20Additive%20Manufacturing%20Roadmap.pdf?uniq=d3jpcp&version=1
6. Statement for the record: Worldwide threat assessment of the U.S. Intelligence Community (2018) (testimony of Daniel R. Coats, Director of National Security). Retrieved from https://www.dni.gov/index.php/newsroom/congressional-testimonies/item/1845-statement-for-the-record-worldwide-threat-assessment-of-the-us-intelligence-community
7. United Nations Office for Disarmament Affairs. (2016, October 14). Emerging technology, international security, and international law. Retrieved from https://www.un.org/disarmament/update/emerging-technology-international-security-and-international-law/
8. United Nations. (2017, June 28). International cooperation key to keeping WMDs away from terrorists, Security Council told. Retrieved from https://news.un.org/en/story/2017/06/560512-international-cooperation-key-keeping-wmds-away-terrorists-security-council
9. Walther, G. (2015). Printing insecurity? The security implications of 3D-printing of weapons. Science and Engineering Ethics, 21(6), 1435-1445. doi:10.1007/s11948-014-9617-x
10. U.S. Department of Energy. (2014, June 19). How 3D printers work. Retrieved from https://www.energy.gov/articles/how-3d-printers-work
11. Kelley, R. (2017). Is three-dimensional (3D) printing a nuclear proliferation tool? (Non-Proliferation Papers No. 54). EU Non-Proliferation Consortium. Retrieved from https://www.sipri.org/publi-

cations/2017/eu-non-proliferation-papers/three-dimensional-3d-printing-nuclear-proliferation-tool
12. Kroenig, M., & Volpe, T. (2015). 3D printing the bomb? The nuclear nonproliferation challenge. The Washington Quarterly, 38(3), 7-19. doi:10.1080/0163660x.2015.1099022
13. Christopher, G. (2015). 3D printing: A challenge to nuclear export controls. Strategic Trade Review, 1(1), 18-25. Retrieved from http://www.str.ulg.ac.be/wp-content/uploads/2016/01/2_3D_Printing_A_Challenge_to_Nuclear_Export_Controls.pdf
14. Bunker, R. J. (2000). Weapons of mass disruption and terrorism. Terrorism and Political Violence, 12(1), 37-46. doi:10.1080/09546550008427548
15. MI5 - The Security Service. (n.d.). Espionage. Retrieved from https://www.mi5.gov.uk/espionage
16. Dijkstra, M., Krause, A., Masri, L., McCambridge, G., Ng, J., Pek, S.B., Yang, E.S., & Zheng, Y. (2014). U.S. National Strategy for Additive Manufacturing. 2014 Capstone Project. Yale Jackson Institute for Global Affairs. Retrieved from https://cgsr.llnl.gov/content/assets/docs/AMCapstone_Final.pdf
17. Holbrook, T. R., & Osborn, L. (2014). Digital patent infringement in an era of 3D printing. SSRN Electronic Journal. doi:10.2139/ssrn.2483550
18. Andrews, J. W. (2017). Additive manufacturing: Implications for the interagency's nuclear counterproliferation task. InterAgency Journal, 8(2), 7-16. Retrieved from http://thesimonscenter.org/iaj-8-2-2017/
19. Chhetri, S. R., & Faruque, M. A. (2017). Side channels of cyber-physical systems: Case study in additive manufacturing. IEEE Design & Test, 34(4), 18-25. doi:10.1109/mdat.2017.2682225
20. Faruque, M. A., Chhetri, S. R., Canedo, A., & Wan, J. (2016). Acoustic side-channel attacks on additive manufacturing systems. 2016 ACM/IEEE 7th International Conference on Cyber-Physical Systems (ICCPS). doi:10.1109/iccps.2016.7479068
21. Song, C., Lin, F., Ba, Z., Ren, K., Zhou, C., & Xu, W. (2016). My smartphone knows what you print. Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security - CCS16. doi:10.1145/2976749.2978300
22. Al Faruque M. A., Chhetri, S. R., Faezi, S., & Candeo, A. (2016). Forensics of thermal side-channel in additive manufacturing systems (CECS Technical Report #16-01). Retrieved from https://pdfs.semanticscholar.org/c8ca/d6066871137ecca3003d35b6111ea4107ba2.pdf
23. Bajema, N.E. & DiEuliss, D. (2016). Peril and promise: Emerging technologies and WMD (Emergence and Convergence Workshop Report). National Defense University. Retrieved from http://wmdcenter.ndu.edu/Publications/Publication-View/Article/1181150/peril-and-promise-emerging-technologies-and-wmd/
24. Brockmann, K., & Bauer, S. (2017, November). 3D printing and missile technology controls (Stockholm International Peace Research Institute Background Paper). Retrieved from https://www.sipri.org/publications/2017/sipri-background-papers/3d-printing-and-missile-technology-controls
25. Atherton, K. D. (2016, May 25). University students launched a rocket with completely 3D-printed engine. Popular Science. Retrieved from https://www.popsci.com/university-students-launch-rocket-with-3d-printed-engine
26. Raytheon. (2017, December 11). To print a missile - Raytheon research points to 3D printing for tomorrow's technology. Retrieved from https://www.raytheon.com/news/feature/print-missile
27. Insinna, V. (2017, April 3). Lockheed pitches 3D printed parts for next-generation ICBM program. Retrieved from https://www.defensenews.com/digital-show-dailies/space-symposium/2017/04/03/lockheed-pitches-3D-printed-parts-for-next-generation-icbm-program/
28. Hutterer, E. (2016, March). Explosive 3D design: 3D printing could revolutionize the high-explosives industry. 1663, 2-5. Retrieved from https://www.lanl.gov/discover/publications/1663/2016-march/_assets/docs/1663_26.pdf
29. Gash, A. (2015). High-explosive components using advanced manufacturing methods. FY2015 LDRD Annual Report. Retrieved from https://ldrd-annual.llnl.gov/ldrd-annual-2015/materials/components
30. 30. Hansen, R. (2015, January/February). Next-generation manufacturing for the stockpile. Science & Technology Review, 4-11. Retrieved from https://str.llnl.gov/january-2015/marrgraff
31. 31. Barker, B. (2017, May/June). A "moonshot" for reactor vessel production. EPRI Journal, 2, 5-8. Retrieved from http://eprijournal.com/a-moonshot-for-reactor-vessel-production/
32. 32. Zilinskas, R.A. & Mauger, P. (2015). Biotechnology e-commerce: A disruptive challenge to biological arms control (CNS Occasional Paper No. 21). Middlebury Institute of International Studies at Monterey. Monterey, CA. Retrieved from http://www.nonproliferation.org/wp-content/uploads/2015/06/biotech_ecommerce.pdf
33. 33. Tirone, D. C., & Gilley, J. (2015). Printing power: 3D printing and threats to state security. Journal of Policing, Intelligence and Counter Terrorism, 10(2), 102-119. doi:10.1080/18335330.2015.1089636
34. President's Commission on Critical Infrastructure Protection. (1997). Critical foundations: Protecting America's infrastructures (Rep.). Retrieved from https://www.hsdl.org/?abstract&did=986
35. Desmit, Z., Elhabashy, A. E., Wells, L. J., & Camelio, J. A. (2017). An approach to cyber-physical vulnerability assessment for intelligent manufacturing systems. Journal of Manufacturing Systems, 43, 339-351. doi:10.1016/j.jmsy.2017.03.004
36. U.S. Department of Homeland Security. (2017, July 11). Critical Infrastructure Sectors. Retrieved from https://www.dhs.gov/critical-infrastructure-sectors
37. Sturm, L. D., Williams, C. B., Camelio, J. A., White, J., & Parker, R. (2017). Cyber-physical vulnerabilities in additive manufacturing systems: A case study attack on the .STL file with human subjects. Journal of Manufacturing Systems, 44, 154-164. doi:10.1016/j.jmsy.2017.05.007
38. Zeltmann, S. E., Gupta, N., Tsoutsos, N., G., Maniatakos, M., Rajendran, J., & Karri, R. (2016). Manufacturing and security challenges in 3D printing. JOM, 68(7), 1872-1881. doi:10.1007/s11837-016-1937-7
39. Cooper, P. (2017). Aviation cybersecurity: Finding lift, minimizing drag (Rep.). Atlantic Council. Retrieved from http://www.atlanticcouncil.org/publications/reports/aviation-cybersecurity-finding-lift-minimizing-drag
40. Mendez, S. (2018, April 19). Marines Use 3D Printer to Make Replacment Part for F-35 Fighter. Retreived from https://www.defense.gov/News/Article/Article/1498121/.
41. Belikovetsky, S., Yampolskiy, M., Toh, J., & Elovici, Y. (2016). dr0wned – Cyber-physical attack with additive manufacturing. Retrieved from https://arxiv.org/abs/1609.00133
42. Belikovetsky, S., Solewicz, Y., Yampolskiy, M., Toh, J., & Elovici, Y. (2017). Detecting cyber-physical attacks in additive manufacturing using digital audio signing. Retrieved from https://arxiv.org/abs/1705.06454
43. Clover, C. (2014, September 26). Alibaba: Weapons of mass ecommerce. The Financial Times. Retrieved from https://www.ft.com/content/2a19e07c-43ef-11e4-8abd-00144feabdc0
44. Tannenbaum, M. (2015, June). Counterfeit and fraudulent parts: Improving prevention and detection. Nuclear News, 58(13), 46-49. Retrieved from www.ans.org/pubs/magazines/download/a_981
45. Deloitte. (2017). 3D opportunity for adversaries: Additive manufacturing considerations for national security (Rep.). Deloitte University Press. Retrieved from https://www2.deloitte.com/content/dam/insights/us/articles/3847_3D-opportunity-for-adversaries/DUP_3D-opportunity-for-adversaries.pdf
46. Bajema, N. E. (2018). Emergence & convergence: Risk assessment survey (Rep.). National Defense University. Retrieved from http://wmdcenter.ndu.edu/Media/News/Article/1484495/emergence-and-convergence/
47. Halterman, T. (2014, June 24). FBI to use 3D printing for bomb research. Retrieved from http://www.3dprinterworld.com/article/fbi-use-3d-printing-for-bomb-research
48. Taylor, P. (2014, July 1). Anti-counterfeit tech developed for 3D-printed objects. Retrieved from https://www.securingindustry.com/electronics-and-industrial/anti-counterfeit-tech-developed-for-3d-printed-objects/s105/a2075/#.WtdLQS7wZEY
49. Bayens, C., Le, T., Garcia, L., Beyah, R., Javanmard, M., & Zonouz, S. (2017). See no evil, hear no evil, feel no evil, print no evil? Malicious fill pattern detection in additive manufacturing. In Proceedings of the 26th USENIX Security Symposium (pp. 1181-1198). Retrieved from https://www.usenix.org/system/files/conference/usenixsecurity17/sec17-bayens.pdf
50. Vincent, H., Wells, L., Tarazaga, P., & Camelio, J. (2015). Trojan detection and side-channel analyses for cyber-security in cyber-physical manufacturing systems. Procedia Manufacturing, 1, 77-85. doi:10.1016/j.promfg.2015.09.065
51. Moore, S. B., Gatlin, J., Belikovetsky, S., Yampolskiy, M., King W. E., & Elovici, Y. (2017). Power consumption-based detection of sabotage attacks in additive manufacturing. Retrieved from https://arxiv.org/abs/1709.01822.
52. Flank, S., Nassar, A. R., Simpson, T. W., Valentine, N., & Elburn, E. (2017). Fast Authentication of Metal Additive Manufacturing. 3D Printing and Additive Manufacturing, 4(3), 143-148. doi:10.1089/3dp.2017.0018.



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.

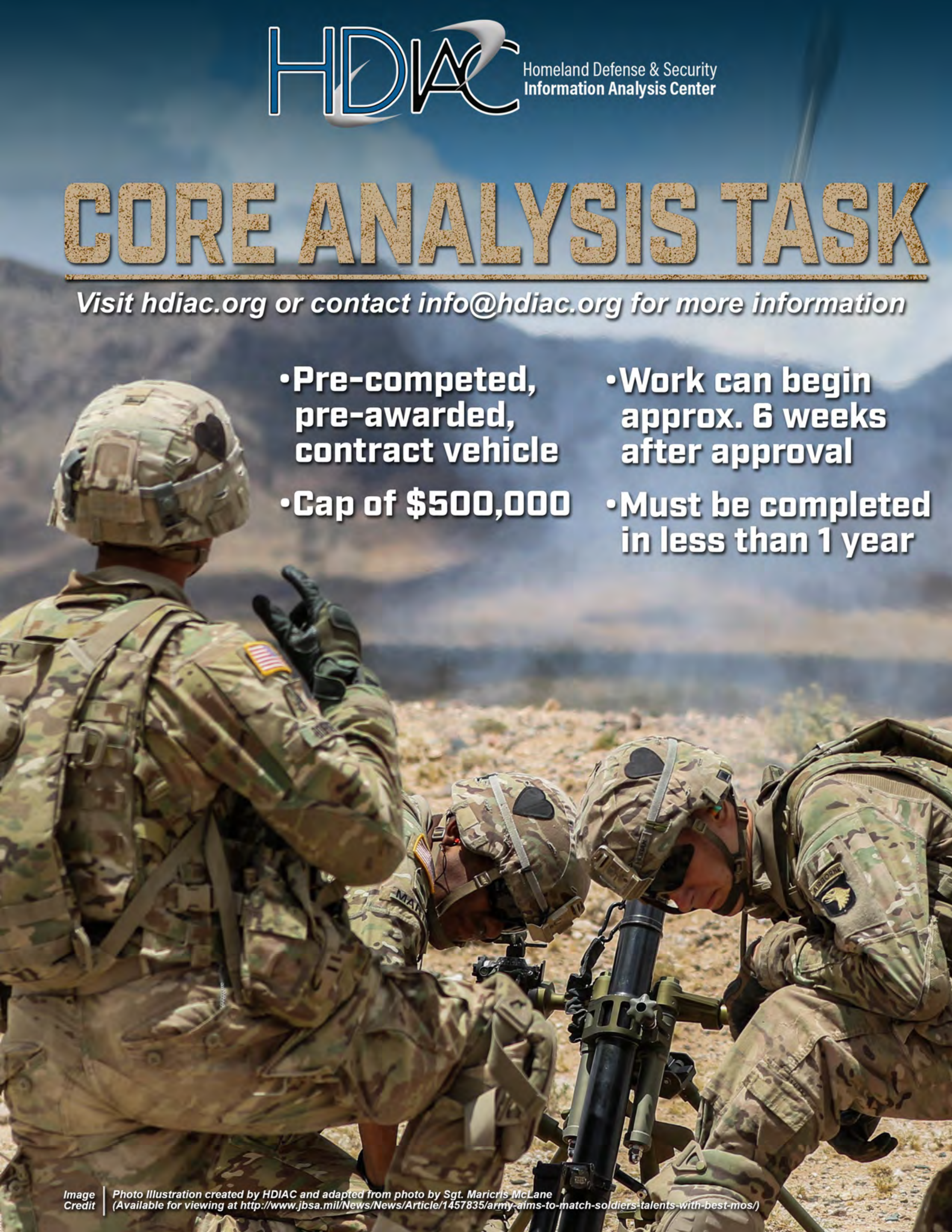


Image Credit | Photo Illustration created by HDIAC and adapted from photo by Sgt. Maricris McLane (Available for viewing at http://www.jbsa.mil/News/News/Article/1457835/army-aims-to-match-soldiers-talents-with-best-mos/)

Calendar of Events

October 2018

10/22/18 - 10/24/18 • **Hyattsville, MD**
HDS 13th Annual Homeland Security Week

10/23/18 - 10/25/18 • **Tampa, FL**
HDS Defense TechConnect Fall Expo

10/30/18 - 10/31/18 • **Arlington, VA**
AE 9th Annual Battery Safety Conference

10/30/18 - 11/1/18 • **Tampa, FL**
B SOFWERX Next Generation Identification Awareness Capability Assessment Event

November 2018

11/06/18 - 11/08/18 • **Orlando, FL**
CBRN CBRNe Convergence 2018

11/09/18 • **Washington, DC**
AE DoD Energy & Water Forum

December 2018

12/01/18 • **Philadelphia, PA**
M IEEE Signal Processing in Medicine and Biology Symposium

12/04/18 - 12/06/18 • **Tampa, FL**
CIP Critical Infrastructure Protection and Resilience - Americas

DoD_HDIAC | 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.