CYBORG INSECT DRONES: RESEARCH, RISKS, AND GOVERNANCE

By: Heraclio Pimentel Jr.

12/01/2017

TABLE OF CONTENTS

INTRODUCTION

For at least a decade, curiosity and innovation have driven humans to combine the natural with the technical to create Hybrid Insect Micro-Electro-Mechanical Systems ("HI-MEMS"[1] or "cyborg insect drones").[2] Originally fueled by the Defense Advanced Research Projects Agency ("DARPA"), humans are exploiting insects' natural abilities to achieve feats that are not currently available with purely mechanical technology such as drones.[3] The potential uses of this HI-MEMS technology include: mapping difficult to explore environments, search and rescue operations, environmental rehabilitation and monitoring, and even counter-terrorism. With these beneficial uses also come certain obvious risks such as surveillance concerns.[4] Further, as the technology advances,[5] the "dual-use" applications of HI-MEMS create the potential for nefarious actors to invade personal privacy and endanger national security.

This article will provide an introduction to cyborg insect drone research and discuss some of the benefits and risks presented by HI-MEMS. Part I provides a background into HI-MEMS research. It discusses the current state of the technology and its anticipated applications. Part II discusses some of the risks associated with this dual-use technology. This part focuses on the

---

[1] To avoid confusion, this article uses HI-MEMS as both a singular and plural acronym.

[2] *See* Emily Anthes, *The Race to Create 'Insect Cyborgs'*, GUARDIAN (Feb. 16, 2013) https://www.theguardian.com/science/2013/feb/17/race-to-create-insect-cyborgs ("In 2006 the US Defense Advanced Research Projects Agency (Darpa) asked America's scientists to submit 'innovative proposals to develop technology to create insect-cyborgs'[.]").

[3] For simplicity, "drones" as used in this article includes Unmanned Aerial Systems (UAS), Unmanned Aerial Vehicles (UAV), drones, and HI-MEMS that do not possess flight abilities. *See* NILS RODDAY, RAS CONFERENCE 2016, HACKING A PROFESSIONAL DRONE (2016), https://www.rsaconference.com/writable/presentations/file_upload/ht-w03-hacking_a_professional_police_drone.pdf.

[4] See George Dery, *Cyborg Moth's War on Terror: The Fourth Amendment Implications of One of the Federal Government's Emerging Surveillance Technologies*, 11 SMU SCI. & TECH. L. REV. 227, 228 (2008) ("Combining such powerful technology with common bugs could potentially implicate privacy and search and seizure issues under the Fourth Amendment.").

[5] For example, more recently some scientists have moved beyond simply "hacking" natural insects to creating and hacking genetically modified dragonflies. Max Toomey, *Scientists Attached an Electronic Backpack to a Genetically Modified Dragonfly and Turned It Into a Drone*, QUARTZ (June 15, 2017) https://qz.com/1000011/scientists-attached-an-electronic-backpack-to-a-genetically-modified-dragonfly-and-turned-it-into-a-drone/.

risks HI-MEMS pose to national security, personal privacy, and cyber security. Part III of the article will discuss potential governance regimes. This part will analyze these governance regimes and evaluate their effectiveness at mitigating the risks associated with HI-MEMS. Finally, Part IV makes some suggestions for governance based on the discussion in Part III.

I. BACKGROUND: THE RESEARCH

A. *Emergence of HI-MEMS*

Research into HI-MEMS started in 2006 when the Defense Advanced Research Projects Agency ("DARPA")[6] requested proposals from researchers to create cyborg insect drones.[7] "Hybrid insect" drones would be created using live insects, electronic circuitry, and other technologies.[8] These HI-MEMS could then be equipped with sensors to conduct military and civilian missions.[9] Not surprisingly, the interest in commandeering insects' bodies to create HI-MEMS came at a time when DARPA was troubleshooting issues with its research into micro-sized mechanical surveillance drones or Micro Air Vehicles (MAVs).[10]

For various reasons, hijacking insects' bodies may be a reasonable solution to the problems inherent in creating miniature drones for various applications. First, insects are naturally self-powered. This means that HI-MEMS can operate for longer periods of time than

---

[6] DARPA is the United States Military research and development arm. Its primary purpose is "to make pivotal investments in breakthrough technologies for national security." *About DARPA*, DEFENSE ADVANCED RESEARCH PROJECTS AGENCY (DARPA), https://www.darpa.mil/about-us/about-darpa (last visited Nov. 26, 2017).

[7] EMILY ANTHES, FRANKENSTEIN'S CAT: CUDDLING UP TO BIOTECHS BRAVE NEW BEASTS 148–49 (2013); JEFFREY H. LANG ET AL., ELECTROMECHANICS & MEMS, MIT 14-1 through 14-3, http://www.rle.mit.edu/media/pr152/14_PR152.pdf (last visited Nov. 4, 2017); Charles Q. Choi, *Military Developing Robot-Insect Cyborgs*, NBC NEWS (July 14, 2009), http://www.nbcnews.com/id/31906641/ns/technology_and_science-science/t/military-developing-robot-insect-cyborgs/#.Wf7H9xSnPzK; Sally Adee, *Research Reported This Week Advances the Goal of Turning Insects into Unmanned Aerial Vehicles*, IEEE SPECTRUM (Feb. 10, 2009), https://spectrum.ieee.org/robotics/military-robots/cyborg-moth-gets-a-new-radio; *see also* Mark Thompson, *Unleashing the Bugs of War*, TIME (Apr. 18, 2008), http://content.time.com/time/nation/article/0,8599,1732226,00.html; Dery, *supra* note 4, at 229.

[8] *See* Thompson, *supra* note 7.

[9] MARC J. MADOU, FUNDAMENTALS OF MICROFABRICATION AND NANOTECHNOLOGY: FROM MEMS TO BIO-MEMS AND BIO –NEMS 493–94 (3d Ed. 2011).

[10] ANTHES, *supra* note 7, at 144.

their mechanical counterparts[11] and do not always need to be controlled.[12] Also, insects have naturally evolved to survive harsh conditions and environments.[13] Furthermore, insects possess natural abilities that may be difficult to replicate in mechanical drones.[14] For example, locusts possess a strong sense of smell and can be trained to detect certain odors.[15]

Though flying insects have generally been targeted as host insects to date, future research may seek to exploit insects' other innate abilities such as swimming. Finally, insect drones are relatively less expensive compared to purely mechanical technologies that serve the same function, which means that the mass-production of HI-MEMS may be commercially feasible.[16]

B. *Technical Background*

Though the idea behind HI-MEMS seems at first glance highly technical, the science behind hybrid insect drones is surprisingly simple to understand. First, researchers select the host insect that they will try to manipulate.[17] In the past researchers have experimented with honeybees, beetles, cockroaches, moths, locusts and dragonflies.[18] Based on the insect selected, researchers then connect electrodes to the insect's muscles, nerves, antennae or brain to manipulate movement.[19] For example, researchers working with cockroaches clip the insect's

[11] *See* Sophie Weiner, *This Genetically-Modified Cyborg Dragonfly Is the Tiniest Drone*, POPULAR MECHANICS (June 1, 2017), http://www.popularmechanics.com/flight/drones/a26729/genetically-modified-cyborg-dragonfly/.
[12] *See* Stephen Cass, *Cyborg Cockroaches to the Rescue*, IEEE SPECTRUM (Dec. 5 2013), https://spectrum.ieee.org/podcast/biomedical/bionics/cyborg-cockroaches-to-the-rescue.
[13] *See id.*
[14] For example, DARPA's Biomimetics program's goal is "to extract and mimic design principles, materials, form, and function of biological systems in order to engineer new systems with enhanced structural and functional abilities." Statement by Frank Fernandez, Subcommittee on Emerging Threats and Capabilities, Armed Services Committee, U.S. Senate (March 21, 2000).
[15] Beth Miller, *Engineers To Use Cyborg Insects as Biorobotic Sensing Machines*, WUSTL.EDU (June 30, 2016), https://engineering.wustl.edu/news/Pages/WashU-engineers-to-use-cyborg-insects-as-biorobotic-sensing-machines.aspx.
[16] *See* Dery, *supra* note 4, at 229.
[17] ANTHES, *supra* note 7, at 148–49.
[18] *See id.* at 149 (2013); Sarah Yang, *Cyborg Beetle Research Allows Free-Flight Study of Insects*, BERKELEY NEWS (Mar. 16, 2015), http://news.berkeley.edu/2015/03/16/beetle-backpack-steering-muscle/; Cass, *supra* note 12; Miller, *supra* note 15.
[19] Yang, *supra* note 18.

antennae and attach electrodes to direct their movement.[20] In experiments using other insects, researchers pierce the creature's exoskeleton and implant electrodes in the desired location.[21] Further, researchers have successfully introduced electrodes into a moth's pupa stage, allowing the insect's exoskeleton to envelope the electrodes.[22] Next, researchers attach a circuit board—called a backpack—to the electrodes to control the insect's movement.[23] The backpack may be equipped with wireless capabilities, navigational systems, and custom software.[24] Finally, an external power source provides the energy needed to power the backpack.[25]

Currently, public and private actors are conducting research on various types of insects with different goals in mind. For these reasons, research has developed in ways that deviate from the basic model above. For example, some researchers have created genetically modified insects that can be controlled by light rather than electrical stimulation.[26] Other researchers have created "tattoos" that attach to insects' wings and direct movement through heat.[27] Researchers have also found ways to power the electronic backpacks using an insect's own natural vibrations[28] and solar energy.[29] Eventually, researchers hope to equip HI-MEMS with sensors to transmit audio and video data, detect gases, transmit heat signatures, and even map environments.[30]

---

[20] Cass, *supra* note 12.
[21] ANTHES, *supra* note 7, at 147.
[22] *Id.* at 150–51.
[23] Yang, *supra* note 18.
[24] ANTHES, *supra* note 7, at 148.
[25] *Id.* at 151.
[26] Gail Overton, *DragonflEye Backpack Turns Actual Insect Into Optogenetically Steered Drone*, LASERFOCUSWORLD (Sept. 13, 2017), http://www.laserfocusworld.com/articles/print/volume-53/issue-09/newsbreaks/dragonfleye-backpack-turns-actual-insect-into-optogenetically-steered-drone.html; MINDY Weisberger, *This Cyborg Insect Could Bring Big Advances in Medical Care*, NBC NEWS (Feb. 03, 2017), https://www.nbcnews.com/mach/technology/cyborg-insect-could-bring-big-advances-medical-care-n716391; *Equipping Insects for Special Service*, *supra* note 26.
[27] Miller, *supra* note 15
[28] ANTHES, *supra* note 7, at 151.
[29] Overton, *supra* note 26.
[30] *See* Thompson, *supra* note 7.

C. *The State of the Technology*

HI-MEMS technology has come a long way in the decade since DARPA initiated the race to create cyborg insects. Since then, some researchers have customized self-powered backpacks to fit different insects. Others have exploited insects' natural sensing abilities to detect odors and direct movement. Still, the best example of the state of the technology comes from Charles Stark Draper Laboratory ("Draper").

Draper is a private "not-for-profit" corporation founded in 1932.[31] Draper specializes in positioning, navigation, and autonomous systems, and microelectronic components in the fields of security and space exploration.[32] Draper provides research and development ("R&D") assistance to large "for-profit" contractors, government agencies (e.g., military agencies), and universities.[33] Recently, Draper secured a $36.9 million dollar contract from the Missile Defense Agency to work on "sensors . . . precision targeting and missile avionics development."[34]

Draper's research into HI-MEMS has resulted in the creation of DragonflEye.[35] DragonflEye is a hybrid insect drone that uses a light-emitting backpack to steer a dragonfly genetically modified to respond to pulses of light.[36] According to Draper, DragonflEye incorporates miniaturized navigation, synthetic biology, neurotechnology, and positioning and autonomous systems that "push[] the boundaries of energy harvesting, miniaturization and optogenetics."[37] In addition, Draper has managed to incorporate all this technology onto a dragonfly—an insect that is much smaller and more agile than the insects (e.g., beetles and

---

[31] *Aerospace and Defense: Company Overview of The Charles Start Draper Laboratory, Inc.*, BLOOMBERG.COM, https://www.bloomberg.com/research/stocks/private/snapshot.asp?privcapid=24792126 (last visited Nov. 26, 2017).
[32] *Id.*
[33] *Working with Draper*, DRAPER, http://www.draper.com/working-with-draper (last visited Nov. 26, 2017).
[34] *Draper Awarded $36M for Guidance, Navigation & Control Technology*, Draper (Sept. 7 2017), http://www.draper.com/news/draper-awarded-36m-guidance-navigation-control-technology.
[35] *Equipping Insects for Special Service*, *supra* note 26.
[36] *Id.*
[37] *Id.*

cockroaches) used in other research.[38] As a final cherry on top, DragonflEye's electronics are solar powered, meaning it can "operate indefinitely."[39]

Despite DragonflEye's many technological advancements, Draper is still in the R&D phase of its cybernetic insect research.[40] Currently, Draper is working on making its electronics smaller and hopes to eventually fit its "backpacks" on other insects such as bees.[41] Draper predicts its research could eventually lead to numerous applications such as guided pollination, payload delivery, reconnaissance, and precision medicine and diagnostics.[42] Though it may be some time before the technology is available for commercial implementation, Draper's work represents a great advancement for cybernetic insect research.[43]

D. *Intended Applications of HI-MEMS*

As previously discussed, DARPA and other military agencies have been the main drivers of HI-MEMS technology. As a result, much of the research has focused on the military applications of this technology. For example, researchers at the Washington University in St. Louis, funded by the Office of Naval Research,[44] have focused on using cybernetic backpacks to exploit a locust's sense of smell.[45] These locusts are trained to detect explosives and may eventually replace explosive-sniffing dogs.[46] In addition to their sense of smell, locusts small size and ability to fly makes them superior to their canine counterparts because they can access

---

[38] Evan Ackerman, *DragonflEye Project Wants to Turn Insects Into Cyborg Drones*, IEEE SPECTRUM (Jan. 25, 2017), https://spectrum.ieee.org/automaton/robotics/industrial-robots/draper-dragonfleye-project.
[39] *Id.*
[40] *Id.*
[41] *Equipping Insects for Special Service*, *supra* note 26.
[42] *Id.*
[43] Ackerman, *supra* note 38.
[44] Travis M. Andrews, *Navy Grants $750,000 to Develop Bomb-Snigging Locusts*, WASH. POST (July 6, 2016), https://www.washingtonpost.com/news/morning-mix/wp/2016/07/06/navy-grants-750000-to-develop-cyborg-locusts-to-sniff-out-bombs/?utm_term=.96741473c88d.
[45] Miller, *supra* note 15. (explaining that "the difficulty and time necessary to train and condition [dogs]" and the difficulty in processing the information perceived by them makes it difficult to use dogs in more situations).
[46] *See id.*

more areas without setting off explosives.[47] Meanwhile, at North Carolina State University, researchers are equipping cockroaches with custom software that allows them to map hard to access areas.[48] Researchers envision using a group of cockroaches to map disaster sites during search and rescue operations.[49] In the future, they expect to equip the cockroaches with microphones and speakers to communicate with survivors.[50]

In addition to these applications, advances in HI-MEMS technology may allow for application in environmental conservation, research, and agriculture. For example, many people are aware that bee populations have declined over the past decade.[51] Observers have noted that bee loss places global agriculture production at a risk[52] and predict that hundreds of bee species may soon become extinct.[53] In economic terms, the potential financial loss associated with the declining bee species is in the billions.[54] However, application of HI-MEMS technology may soon play a role in countering some of the problems associated with bee loss. For example, Draper has stated that one future application of its DragonflEye technology is guided pollination.

---

[47] *See* Rob Crilly, *Engineers Develop Cyborg Locusts to Sniff Out Explosives*, TELEGRAPH (July 5, 2016), http://www.telegraph.co.uk/technology/2016/07/04/engineers-develop-cyborg-locusts-to-sniff-out-explosives/ ("But cyborg insects offer several advantages [to rats or dogs], flying to inaccessible locations and running far less risk of triggering explosions.").

[48] As of the writing of this article, researchers in Singapore have created a cyborg darkling beetle. The beetle, at only 2 to 2.5 centimeters, is much smaller than a cockroach. *See, e.g.*, Evan Ackerman, *Controllable Cyborg Beetles for Swarming Search and Rescue*, IEEE SPECTRUM (Nov. 28, 2017), https://spectrum.ieee.org/automaton/robotics/robotics-hardware/cyborg-beetles-for-swarming-search-and-rescue

[49] Matt Shipman, *Researchers Use Video Game Tech to Steer Roaches on Autopilot*, N. CAROLINA STATE NEWS (June 25, 2013), https://news.ncsu.edu/2013/06/wms-bozkurt-roach-autopilot/.

[50] *Id.*

[51] Elizabeth Grossman, *Declining Bee Populations Pose a Threat to Global Agriculture*, YALE ENV. 360 (Apr. 30, 2013), http://e360.yale.edu/features/declining_bee_populations_pose_a_threat_to_global_agriculture.

[52] *See, e.g.*, *id*. ("The danger that the decline of bees and other pollinators represents to the world's food supply was highlighted this week when the European Commission decide to ban a class of pesticides suspected of playing a role in so-called 'colony collapse disorder.'"); Justin Worland, *More than 700 North American Bee Species are Headed Toward Extinction*, TIME (March 2, 2017), http://time.com/4688417/north-american-bee-population-extinction/ ("Population levels of more than 700 North American bee species are declining as habitat loss and pesticide use continue to breakneck pace, according to a new [Center for Biological Diversity] report.").

[53] *See* Worland, *supra* note 52.

[54] *See* Justin Worland, *The White House Wants to Save the Bees*, TIME (June 20, 2014), http://time.com/2907230/the-white-house-wants-to-save-the-bees/ ("Pollinators also have profound economic impact: they contribute more than $24 Billion dollars to the U.S. economy.").

Such an application could potentially mitigate the loss in production associated with declining bee species by creating more efficient hybrid bee pollinators.[55] Additionally, fitting bees with Draper's backpack could aid researchers studying bee loss by "monitoring their flight patterns, migration and overall health."[56]

In addition to mitigating the loss of bee populations, HI-MEMS may be used to gather data about hard to reach ecosystems such as marshlands.[57] Additionally, HI-MEMS equipped with sensors may be useful in monitoring protected areas plagued by illegal poaching or mining.[58] They may even be useful in detecting violations of federal environmental statutes such as the Clean Water Act.[59] Many of these activities currently require the use of conventional drones or manned aircraft. However, using HI-MEMS would be superior to these technologies because insects are better suited to these environments, possess natural sensing abilities, and do not pose the same risk to sensitive habitats when they malfunction.[60]

II. RISKS: DUAL-USE APPLICATIONS OF HI-MEMS

As much as Draper's DragonflEye technology is representative of the potential benefits of cybernetic insect research, it equally represents the dangers posed by this type of "dual-use" technology. Dual-use technologies have both military and civilian applications.[61] This includes

---

[55] *See* Ackerman, *supra* note 38.
[56] *See Equipping Insects for Special Service*, *supra* note 26.
[57] *Cf.* Lindsey Blomberg*, How Can Drones Help Environmentalists?*, EARTHTALK.ORG (Aug. 17, 2015), https://earthtalk.org/how-can-drones-help-environmentalists.
[58] *Cf. id.*
[59] *See* David A. Fahrenthold, *Reigning in the Rumors About EPA 'Drones'*, WASH. POST (June 18, 2012), https://www.washingtonpost.com/politics/reining-in-the-rumors-about-epa-drones/2012/06/16/gJQAwWjkhV_story.html?utm_term=.6bc9e560e61f ("For more than a decade, EPA inspectors have flown over farmland in small private planes . . . . looking for clean-water violations.").
[60] *See* Peter Shadbolt, *The Flying Fungus: NASA's Biodegradable Drone that Flies and Dies*, CNN (Dec. 10, 2014), http://www.cnn.com/2014/12/10/tech/innovation/nasa-dissolving-drone/index.html ("Periodically UAVs [unmanned aerial vehicles] get lost – for example on coral reefs or in other sensitive habitats.").
[61] 15 C.F.R. § 730.3 (2017) ("A 'dual-use' item is one that has civil applications as well as terrorism and military or weapons of mass destruction (WMD)-related applications."); Gerald T. Nowak, *Above All, Do No Harm: The Application of the Exon-Florio Amendment To Dual-Use Technologies*, 13 MICH. J. INT'L L. 1002, 1004 (1992).

technologies that may be used for terrorism.[62] The dual-use nature of HI-MEMS technology becomes obvious when considering the two general functions they serve: payload delivery and information gathering.[63] These twin applications can be translated into entomological warfare and surveillance applications by governments, terrorist organizations, and private parties. Moreover, the integration of global positioning and autonomous navigation systems creates a danger that nefarious users could commandeer this technology.

A. *HI-MEMS Pose a Risk to National Security*

One of the nefarious uses of HI-MEMS that one can imagine is to deploy them as vectors to communicate deadly viruses and other pathogens. Insect vectors are capable of transmitting diseases between humans and animals.[64] Annually, vector-borne diseases cause more than 700,000 deaths around the world.[65] Given the potentially deadly consequences of insect vectors, various methods have been developed since the late 19th century and utilized to control the spread of vectors and the diseases they carry.[66]

Entomological warfare is the idea that insect vectors, such as mosquitoes, could be "weaponized" to transmit deadly pathogens or destroy resources.[67] Though Hi-MEMS are a relatively new concept, entomological warfare is not.[68] For example, evidence suggests that

---

[62] 15 C.F.R. § 730.3 (2017).

[63] *See Equipping Insects for Special Service*, *supra* note 26. ("Potential applications of the technologies underpinning DragonflEye include guided pollination, payload delivery, reconnaissance and even precision medicine and diagnostics.").

[64] *Vector-Borne Diseases: Fact Sheet*, WORLD HEALTH ORGANIZATION (2017), http://www.who.int/mediacentre/factsheets/fs387/en/.

[65] *Id.*

[66] *See generally* JAN A. ROZENDAAL, *Vector Control: Methods for Use by Individuals and Communities* (1997).

[67] Jeffrey A. Lockvvood, *Entomolgical Warfare: History of the Use of Insects as Weapons of War*, 33 BUL. OF THE ENTOMOLOGICAL SOC'TY OF AM. 76 (1987) ("[E]ntomological warfare (i.e., the use of insect and other arthropods to vector diseases or destroy resources [e.g., food supplies]) is a relatively new military concept.").

[68] *See* SLAVKO BOKAN, MINISTRY OF DEFENSE OF THE REPUBLIC OF CROATIA, *Biological Warfare Agents, Toxins, Vectors and Pests as Biological Terrorism Agents* 1 (2003) ("Although the use of biological agents and toxins in military conflicts has been a concern of military communities for many years, several recent events have increased the awareness regarding the potential use of these weapons by terrorists against civilian populations."); Dan Vergano, *Nazi Scientists May Have Plotted Malaria Mosquito Warfare*, NAT'L GEOGRAPHIC (Jan. 29, 2014),

during World War II the Japanese, Nazis, and Allied Forces all researched microbial biological warfare, with the Nazis researching entomological warfare vis-à-vis malaria-carrying mosquitoes.[69] Mosquitoes, like other insects, possess many qualities that make them a likely choice for weaponization. These qualities include their short life cycles, ease of production, resistance to insecticides, and ease of dissemination.[70] Of the insects capable of transmitting diseases, mosquitoes are the most infamous.[71] Mosquitoes can transmit various diseases such as Zika, West Nile, Dengue virus, Yellow Fever, and Malaria.[72]

In addition to weaponization, nefarious actors may also wreak havoc on their enemies by deploying the technology as is. As mentioned in Part I, researchers are currently using locusts to exploit their incredible sense of smell. In addition to strong sensing abilities, locusts are notoriously ferocious herbivores.[73] The threat that locusts pose to societies and governments is literally biblical.[74] Beyond scripture, locusts have been known to cause severe damage to modern societies. As recently as last year, Argentina dealt with a plague of locusts that had farmers and

---

https://news.nationalgeographic.com/news/2014/01/140130-nazi-biological-weapons-biowarfare-mosquito-malaria-history/ ("Biological warfare, the unleashing of disease-carrying living organism and natural toxins on enemies, dates to antiquity."); Stephanie Merry, *The Insect Warfare on 'The Americans' Isn't All That Outlandish*, WASH. POST (Mar. 22, 2017), https://www.washingtonpost.com/news/arts-and-entertainment/wp/2017/03/22/the-insect-warfare-on-the-americans-isnt-all-that-outlandish/?utm_term=.10499e50bf4f ("The U.S. was indeed accused of entomological warfare during the Cold War – but not by Russia.").

[69] *See* Vergano, note 68.

[70] *See* BOKAN, *supra* note 68 (listing three species of mosquitoes– Culex, Culiseta, Mansonia– as potential vectors for weaponization).

[71] *Vector-Borne Diseases: Fact Sheet*, *supra* note 64.

[72] *Mosquito-Borne Diseases*, CENTERS FOR DISEASE CONTROL AND PREVENTION (2016), https://www.cdc.gov/niosh/topics/outdoor/mosquito-borne/default.html; *see also* VECTOR-BORNE DISEASE SECTION, CAL. DEP'T OF PESTICIDE REGULATION, *Overview of Mosquito Control Practices in California* 3 (2008), http://www.cdpr.ca.gov/docs/dept/westnile/mosqover.pdf ("Some mosquitoes transmit ("vector") disease-causing viruses to humans and domestic animals when they bite.").

[73] *About Locusts*, NAT'L GEO., https://www.nationalgeographic.com/animals/invertebrates/group/locusts/ (last visited Nov. 26, 2017).

[74] *See* EXODUS 10:13–20. In the Old Testament, God sends a plague of locusts that descend upon Egypt and devour "everything growing in the fields and the fruit on the trees."

government officials scrambling in an attempt to mitigate the swarm's damages.[75] In parts of Africa, locusts have been a decade-long problem and an everyday reality.[76] As stated earlier, researchers are currently working on controlling locust's movements and behavior. Once these bomb-sniffing locusts are fully operational, an enterprising terrorist need only gain access to their navigational controls to cause agricultural destruction on a biblical scale.

Arguably, these uses of HI-MEMS may seem more apt for a Hollywood script.[77] However, one must remember that the research is primarily funded, at this point, through military agencies. Though ostensibly slated for reconnaissance and search and rescue type operations, some observers contend that the military applications of HI-MEMS technology are far more wide reaching.[78] Thus, in a world where Facebook has become the *de facto* method of political subterfuge[79] and terrorists are converting everyday items into weapons of terror,[80] one

---

[75] *See* Jonathan Gilbert, *Argentina Scrambles to Fight Biggest Plague of Locusts in 60 Years*, N.Y. TIMES (Jan. 25, 2016), https://www.nytimes.com/2016/01/26/world/americas/argentina-scrambles-to-fight-biggest-plague-of-locusts-in-60-years.html.

[76] *See Madagascar Hit by 'Severe' Plague of Locusts*, BBC NEWS (Mar. 27, 2013), http://www.bbc.com/news/world-africa-21955740 (reporting locust plagues in the 1950s and 2013); Helen Pearson, *Africa's Locust Crisis Worsens*, NATURE (Aug. 20, 2004), http://www.nature.com/news/2004/040816/full/news040816-13.html (reporting locust plague in 2004); Sheila Rule, *Drought Easing, Africa Has New Enemy: Locusts*, N.Y. TIMES (Aug. 7, 1986), http://www.nytimes.com/1986/08/07/world/drought-easing-africa-has-new-enemy-locusts.html (reporting locust plague in 1986).

[77] *See, e.g.*, Jaqueline Ronson, *'Black Mirror' Killer Bee Drones Are Coming for You IRL*, INVERSE SCI. (Oct. 25, 2016), https://www.inverse.com/article/22678-black-mirror-robot-bee-drones (discussing an episode of the TV show "Black Mirror" in which the government uses mechanical bee drones as assassins and the real life research into creating mechanical bee drones).

[78] *See, e.g.*, Dery, *supra* note 4, at 233 ("Anyone who is just a little bit creative can imagine both useful and nonproductive applications of remote-controlled animals . . . ."); Ronson, *supra* note 77 (suggesting that it is more likely that mechanical insect drones are far more likely to be used in warfare than agriculture because there are far more efficient solutions to the world's declining bee populations that do not require engineering a "robot" bee).

[79] *See, e.g.*, Mike Isaac & Diasuke Wakabayashi, *Russian Influence Reached 126 Million Through Facebook Alone*, N.Y. TIMES (Oct. 30, 2017), https://www.nytimes.com/2017/10/30/technology/facebook-google-russia.html ("Russian agents intending to sow discord among American citizens disseminated inflammatory posts that reached 126 million users on Facebook, published more than 131,000 messages on Twitter and uploaded over 1,000 videos to Google's YouTube service, according to copies of prepared remarks from the companies that were obtained by The New York Times.").

[80] In April 2013, two brothers detonated bombs contained in pressure cookers hidden in backpacks during the Boston Marathon killing three and injuring more than two hundred. *Boston Marathon Terror Attack Fast Facts*, CNN NEWS (Mar. 29, 2017), http://www.cnn.com/2013/06/03/us/boston-marathon-terror-attack-fast-facts/index.html. More recently, vehicles have become terrorists' weapon of choice. Sam Petulla, *Vehicles Are*

must take seriously the possibility that bad actors may look to use HI-MEMS to threaten national security.

B. *HI-MEMS Pose a Threat to Personal Privacy*

Much like their mechanical counterparts, hybrid insect drones will be capable of incorporating various technological instruments including video and sound recording capabilities, gas sensors, thermals scanners and biometric software.[81] Many Americans are aware that government agencies and local law enforcement use drones to conduct rescue and surveillance operations.[82] Much of this technology is large, operates from a distance, cannot operate indefinitely, and is expensive.[83] However, advancements in technology are giving law enforcement access to smaller, more agile surveillance drones.[84] Simultaneously, advances in technology are making HI-MEMS a more likely substitute for micro drones given their small size and ability to operate indefinitely (until the death of the insect, of course). As such, the government's use of HI-MEMS for surveillance creates the most obvious threat to personal privacy.

In his article, *Cyborg Moth's War on Terror: The Fourth Amendment Implications of the Federal Government's Emerging Surveillance Technologies*,[85] Professor George Dyer paints a picture of an alternate reality under government-run HI-MEMS surveillance. He imagines two old friends engaged in an intimate conversation in the outdoor section of a coffee shop. [86] During their discussion, person A suddenly changes topics upon realizing a moth has landed near their

---

Becoming the Weapons of Choice for Terrorist, NBC NEWS (Aug. 17, 2017), https://www.nbcnews.com/news/world/vehicles-are-becoming-weapons-choice-terrorists-n768846.

[81] *See* Matthew Feeney, *Policy Analysis: Surveillance Takes Wing: Privacy in the Age of Police Drones*, CATO INST. NO. 807 2–4 (2016), https://object.cato.org/sites/cato.org/files/pubs/pdf/pa807_1.pdf.

[82] *See id.* at 1–4.

[83] *Id.* at 4.

[84] *See id.*

[85] Dyer, *supra* note 4.

[86] *See* Dyer, *supra* note 4, at 227.

table.[87] In this alternate reality, person A may have a well-founded suspicion that the moth is actually a cyborg insect drone listening in on their conversation.[88]

Whether or not the government actually uses HI-MEMS to spy on people in public, even legitimate HI-MEMS use by police enforcement and government agencies is sure to cause distrust in some sectors of the population. For example, in 2012, reports claimed that the United States Environmental Protection Agency ("EPA") was using drones to spy on farmers.[89] Though these reports turned out to be false, the rumors caused some hysteria and probably fueled distrust in the government.[90]

In addition to government use, private use of HI-MEMS may threaten personal privacy. Much like conventional drones, private users could abuse HI-MEMS to spy on their neighbors. The reasons motivating a private user to commit such actions are numerous: curiosity, pranking, revenge, blackmail, and corporate espionage are some examples. The foundation for some of these uses may already be in place. Currently, researchers envision fitting microphones, cameras, and other sensors to HI-MEMS, making them prime targets for hackers. Additionally, an enterprising criminal or terrorist already has access to inexpensive, commercially available Do-It-Yourself ("DIY") kits and online instructions.[91] Though these kits are rudimentary, technology savvy criminals may build off of their designs.

---

[87] *See id.*
[88] *See id.*
[89] *See* Fahrenthold, *supra* note 59. However, the EPA does use conventional manned aircraft to uncover Clean Air Act and Clean Water Act violations. *Id.*
[90] *See id.*
[91] *See, e.g.*, *The RoboRoach Bundle*, BACKYARD BRAINS, https://backyardbrains.com/products/roboroach (last visited Nov. 28, 2017); Cassandra Khaw, *Make Your Own Cyborg Cockroach for Under $30*, ARSTECHNICA (Feb. 2, 2016), https://arstechnica.com/science/2016/02/make-your-own-cyborg-cockroach-for-under-30/.

C. *Cyber Security Weaknesses and Technology Issues Exacerbate Risks*

HI-MEMS, as a type of drone, will become part of the Internet-of-Things. As a result, they will be subject to the same cyber security issues as other Internet-of-Things devices.[92] Although cyber security itself is not a risk that HI-MEMS technology creates, HI-MEMS' vulnerability to cyber-attacks may exacerbate the risks they pose to national security and personal privacy. Additionally, any data they record or obtain may also be at risk. As such, this article treats cyber security as a technological risk associated with HI-MEMS technology.

Like drones, HI-MEMS technology integrates many wireless technologies, such as Global Positioning Systems ("GPS"), autonomous systems, and remote piloting technologies.[93] Recently, the Federal Trade Commission ("FTC") demonstrated the ease with which commercially available drones could be hacked.[94] Though the drones they hacked were older models retailing for less than two hundred dollars, the FTC's ability to access the drones' cameras, control navigation, and trick the drones' GPS demonstrates the type of vulnerabilities that may exist in HI-MEMS incorporating similar technologies.[95] Furthermore, private companies have been able to take over control of more expensive drones, with one company claiming to be able to hack seventy-five percent of the commercially available drones on the market.[96] To complicate things, it may not be immediately apparent to the operator that their HI-

[92] *See Introducing Drone ID*, AIRMAP Inc., https://www.airmap.com/drone-id-digicert-digital-certificate-drones/ (last visited Nov. 30, 2017).
[93] *See supra* Part I.
[94] *See* Gregory S. McNeal, *Key Questions About Securing Drones from Hackers*, FORBES (Oct 19, 2016), https://www.forbes.com/sites/gregorymcneal/2016/10/19/key-questions-about-securing-drones-from-hackers/#73aaa22233f3.
[95] *See id*.
[96] *See* Paul Szoldra, *This Company Can 'Hack' and Completely Take Over Enemy Drones for the US Military*, BUS. INSIDER (Jan. 6, 2017), http://www.businessinsider.com/department-13-mesmer-drones-2017-1.

MEMS, its onboard sensors, or data has been hacked.[97] Thus, because of these cyber security weaknesses, HI-MEMS may be prime targets for hacking.

In addition, technical malfunction, loss of positive flight control, and similar technology related issues create risks of inadvertent release or loss of HI-MEMS. One of the environmental advantages of HI-MEMS over conventional drones is that they do not cause the same environmental disturbance as larger mechanical drones when they malfunction.[98] However, because some HI-MEMS are created using genetically modified insects, technology related issues create a risk of inadvertently releasing genetically modified HI-MEMS into the environment.

However, cyber security flaws and technology issues are foreseeable risks. As such, researchers and developers can integrate stronger security or mitigation measures on HI-MEMS' hardware and software to minimize cyber security and technology related risks. Some of these measures could include minimum technology and software standards. For example, developers can (or can be required to) incorporate a minimum level of encryption technology in their HI-MEMS.[99] Minimum technology standards may also be able to provide less opportunity to trick the HI-MEMS GPS.[100] Additionally, specific technology can be integrated into HI-MEMS to maintain better control of them and reduce the risk of inadvertent release. For example, HI-MEMS could integrate geofencing technology, which would create an invisible fence that HI-MEMS could not cross.[101] Automatic flight termination or "return-to-base" systems could be

[97] *See* McNeal, *supra* note 95.
[98] *See* Shadbolt, *supra* note 60.
[99] *See* RODDAY, *supra* note 3, at 31.
[100] *See* Thomas Fox-Brewster, *Watch GPS Attacks that Can Kill DJI Drones of Bypass White House Ban*, FORBES (Aug. 8, 2015), https://www.forbes.com/sites/thomasbrewster/2015/08/08/qihoo-hacks-drone-gps/#2b4380322bf5 ("[GPS] weaknesses could be fixed . . . but [manufacturers] would have to do so at the GPS chip level.").
[101] Operation and Certification of Small Unmanned Aerial Systems, 81 Fed. Reg. 42063, 42135 (2016)

another way to contain the risk of inadvertent release.[102] Though these and similar technologies are not failsafe, they could reduce the cyber security risks and technological issues previously identified, which in turn may reduce national security and privacy risks.

The next section—Part III—discusses available HI-MEMS governance regimes. For simplicity, references to addressing cyber security risks in Part III include both the risks and the potential mitigation measures discussed in this section.

III. GOVERNANCE OF HI-MEMS

The previous section discussed three foreseeable risks HI-MEMS present. As with any emerging technology, there may also be unknown risks associated with HI-MEMS. Nonetheless, there are numerous beneficial applications of HI-MEMS that make cybernetic insect research worth pursuing. Thus, as we continue our research into HI-MEMS technology, we can either accept the risks or find ways to eliminate and mitigate the risks.[103]

The sections that follow will discuss some of the governance regimes applicable to HI-MEMS technology that may provide ways to mitigate and eliminate the risks previously identified. Each section will provide a brief discussion on the background, efficacy, and failings of the given governance regime. In addition, the section will discuss how the particular governance regime may provide ex ante (i.e., preventative) protections or, to a lesser extent, ex post facto (i.e., after-the-fact) remedies. This distinction is important to consider as ex ante measures potentially eliminate or ameliorate risks, whereas ex post facto measures primarily compensate or mitigate injury.

---

[102] 81 Fed. Reg. at 42136.

[103] *See* ALBERT C. LIN, PROMETHEUS REIMAGINED: TECHNOLOGY, ENVIRONMENT, AND LAW IN THE TWENTY-FIRST CENTURY 5–6 (2017).

A. *Agency Oversight*

Many Americans assume that the government is ensuring the safety of emerging technologies.[104] As such, this section will discuss agency oversight as a possible source of governance over HI-MEMS.

Specifically, this section will look at two agencies that would most likely have authority to govern HI-MEMS given their biological and mechanical nature: the Food & Drug Administration ("FDA") and the Federal Aviation Administration ("FAA"). In discussing these two agencies this section will discuss the source of each agency's potential authority over HI-MEMS, the type of governance each agency could provide, and whether either agency's expertise would be suitable for governing HI-MEMS. Finally, this section will conclude by discussing whether the specialized nature of HI-MEMS requires oversight from a new agency altogether.

1. The Food & Drug Administration

In 1986, the Coordinated Framework was established to create a governance regime between existing agencies—EPA, FDA, and USDA[105]—to regulate the different products produced through biotechnology.[106] Specifically, the Coordinated Framework sought to regulate products manufactured through genetic engineering, such as genetically modified organisms ("GMOs").[107] Under this framework, the FDA has jurisdiction over genetically engineered

[104] *Id.* at 15.
[105] United States Department of Agriculture.
[106] MODERNIZING THE REGULATORY SYSTEM FOR BIOTECHNOLOGY PRODUCTS: FINAL VERSION OF THE 2017 UPDATE TO THE COORDINATED FRAMEWORK FOR THE REGULATION OF BIOTECHNOLOGY 1 (2017) [hereafter COORDINATED FRAMEWORK UPDATE 2017].
[107] *See id.* at 2–3.

("GE") animals through its authority to regulate "New Animal Drugs" under the Federal Food, Drug, and Cosmetic Act ("FD&C").[108]

Under the FD&C, the FDA has the authority to regulate drugs.[109] "Drug" is defined as "articles (other than food) intended to affect the structure or any function of the body of man or other animals[.]"[110] A new animal drug is any drug intended for use in animals that is not generally recognized as safe.[111] As the primary purpose of the insect backpack is to affect the function of the body of the insect (i.e., by manipulating its movement), and it is intended for use in animals, HI-MEMS would seem to fall within the purview of the FDA.

As an initial point, the FDA already has authority to regulate HI-MEMS created from GE insects.[112] Assuming the FDA also has jurisdiction over non-GE HI-MEMS, it could use its authority to provide ex ante oversight before commercial release.[113] As a new animal drug, new HI-MEMS would require pre-market approval, which a developer can obtain by providing the FDA with information about the specific cyborg insect drone, including: its components and composition, the manufacturing process, evidence of its safety and effectiveness, and an environmental assessment.[114] For GE HI-MEMS, additional information specifically about its GE characteristics would be required.[115]

Even though the FDA might have statutory jurisdiction over HI-MEMS, the agency might choose not to exercise its regulatory authority over non-GE HI-MEMS. The FDA is

[108] *Id.* at 8; 21 U.S.C. §§ 301–399h.
[109] *See id.* § 321.
[110] *Id.* § 321(g)(1).
[111] REGULATION OF INTENTIONALLY ALTERED GENOMIC DNA IN ANIMALS: DRAFT GUIDANCE NO. 187 6 (2017) [hereafter DRAFT GUIDANCE NO. 187].
[112] *Id.* at 6–7.
[113] *See* COORDINATED FRAMEWORK UPDATE 2017, *supra* note 106, at 18.
[114] *See id.* at 15–22.
[115] *See id.* at 22–27.

primarily concerned with protecting public health.[116] As such, FDA has tentatively decided not to enforce its new animal drug requirements on GE animals not meant for consumption and regulated by other agencies or that are raised and used under controlled conditions.[117] Moreover, it is unclear whether the FDA would have the same motivation to regulate non-GE HI-MEMS as new animal drugs.

According to the FDA, the agency chooses to regulate an article based on an evaluation of risk factors including anything about the article that poses a human, animal or environmental risk.[118] As described in Part II, the threats cyborg insect drones pose to humans, animals, and the environment are not related to health or safety,[119] unless the insect hosts are genetically modified. Rather, threats posed by HI-MEMS are a result of nefarious exploitation of their dual-use characteristics. As such, non-GE HI-MEMS drones generally pose no greater threat than their purely biological counterparts as a result of inadvertent release.[120] As for GE HI-MEMS, such as DragonflEye, they would probably already be subject to FDA oversight as GE insects (assuming they are not classified as pesticides).[121]

Finally, it is not clear the FDA is a suitable agency to govern HI-MEMS overall. First, the kind of threats that the FDA is concerned about are not the threats that HI-MEMS inherently present, unless they have been genetically modified. Second, the ex ante regulation that the FDA could provide (i.e., premarket approval), may not be enough to minimize the risks described in

[116] *What We Do*, FDA (Apr. 4, 2017), https://www.fda.gov/AboutFDA/WhatWeDo/ ("The Food and Drug Administration is responsible for protecting the public health by ensuring the safety, efficacy, and security of human and veterinary drugs, biological products, and medical devices; and by ensuring the safety of our nation's food supply, cosmetics, and products that emit radiation.").
[117] DRAFT GUIDANCE NO. 187, *supra* note 111, at 8.
[118] *Id.* at 9.
[119] Though a risk to national security could include a risk to humans, animals, and environment, this risk is not caused by the inadvertent release of non-GE HI-MEMS.
[120] Of course, release of some non-GE insects such as locusts would arguably pose risks to the environment. However, these risks are present in these insect regardless of whether they are HI-MEMS.
[121] GE insects classified as pesticides are subject to EPA oversight. *See id.* at 7 n.9.

Part II without requiring, for example, specific cyber security standards. However, the FDA is generally not known for its expertise in national security, personal privacy, or cyber security. Thus, the FDA would likely not be an appropriate agency to govern HI-MEMS technology.

2. The Federal Aviation Administration

As discussed in Part I, hybrid insect drones can be controlled, at least part of the time, like conventional drones. For this reason, many of the threats posed by HI-MEMS are the same threats posed by the conventional aerial drones that the FAA already regulates. Given the similarity between HI-MEMS and conventional drones, the FAA might be the appropriate agency to govern HI-MEMS.

In 2012, the Congress directed the FAA to integrate civil Unmanned Aircraft Systems ("UAS") into the nation's airspace.[122] The definition for UAS covers unmanned aircraft and the associated elements necessary for remote piloting.[123] 49 U.S.C. section 40102 defines "aircraft" as "any contrivance invented, used or designed to navigate, or fly in, the air."[124] FAA recently used this language to regulate small Unmanned Aircraft Systems ("small UAS" or "small drones").[125]

The new small UAS regulations apply to drones weighing less than fifty-five pounds that operate for non-hobby and non-recreational purposes,[126] such as, crop monitoring, research and development, educational uses, rescue operations, and wildlife nesting area evaluations.[127] Many of these uses are similar to the civilian applications that researchers envision for HI-MEMS.[128] Moreover, as the insects currently being researched are well under the fifty-five pound maximum

[122] FAA Modernization and Reform Act of 2012, P.L. 112-95, § 331, 126 Stat. 72 (2012).
[123] *See id.*
[124] *See also* 14 C.F.R. § 1.1 (defining "Aircraft" as "a device that is used or intended to be used for flight in the air.")
[125] Operation and Certification of Small Unmanned Aerial Systems, 81 FR 42063 (2016).
[126] 81 Fed. Reg. 42063 at 42066.
[127] *Id.*
[128] *See* Part I.

and are technically unmanned, these proposed civilian applications of HI-MEMS would fall under the purview of the small UAS regulations. However, as discussed below, the current small UAS regulations would not do much to offer ex ante protection from the risks associated with HI-MEMS.

The small UAS regulations set forth various requirements including pilot licensing requirements. However, despite these requirements, the small UAS regulations would largely defeat the purposes of using the HI-MEMS for their intended applications. First, the regulations include "operational limitations" that limit the application of commercial civilian drones.[129] These operational limitations require daylight only operations, a visual line-of-sight, and a close enough proximity for the remote pilot to see the UAS. Additionally, a pilot may only operate one small UAS at a time and may not operate over persons or under covered structures.

The requirement to operate within the line of sight of the pilot and the prohibition on operation under covered structures would severely impact HI-MEMS use in civilian search and rescue missions, mapping closed environments, and countless other potential applications for which they are designed. Additionally, the one-pilot-per-UAS limitation would make using HI-MEMS impracticable because some intended uses (e.g., mapping and search and rescue) require an autonomously controlled swarm.[130] Although the small UAS regulations include a "waiver mechanism" to account for "quickly changing technology,"[131] the preceding discussion illustrates the difficulty in applying the general small UAS regulations to HI-MEMS. Moreover, the small UAS regulations do not address the risks associated with the implementation of HI–MEMS identified in Part II.

---

[129] 81 Fed. Reg. at 42066.
[130] *See, e.g.*, Ackerman, *supra* note 48 ("For a disaster scenario, we could release hundreds of flying and crawling cyborg insects . . . .").
[131] 81 Fed. Reg. at 42066.

Specifically, the FAA did not include in the small UAS regulations an "airworthiness certification" requirement as it does with other aircraft.[132] An airworthiness certification could require HI-MEMS to integrate technologies that the FAA "finds necessary for safety in air commerce and national security."[133] This discretion could be used to minimize the cyber security risks, and in turn, the national security risks by requiring integration of some of the protective technologies discussed in Part II.C. However, the FAA reasoned that commercially available drones did not pose a threat to national security because the regulations require daylight and line-of-sight operations, which would cue the operator to hacking.[134] However, as stated in Part II.C., an operator may not always be aware that a drone has been compromised. This may be particularly true with regard to HI-MEMS because they are small and meant to be remotely or autonomously piloted in large numbers.

Finally, the small UAS regulations are currently inadequate to address the threats presented by HI-MEMS in one more respect: personal privacy. The small UAS regulations fail to address privacy concerns raised by drones in general.[135] Instead, "[t]he FAA strongly encourages all UAS pilots to check local and state laws before gathering information through remote sensing technology or photography."[136] These laws, discussed in section D., largely provide ex post facto remedies, whereas FAA may be capable of providing ex ante protection. Of course, this is

---

[132] *Id.* at 42070.
[133] *See* 49 U.S.C. 44701(a)(5).
[134] 81 Fed. Reg. at 42181.
[135] *See Press Release–DOT and FAA Finalize Rules for Small Unmanned Aircraft Systems*, FAA (June 21, 2016), https://www.faa.gov/news/press_releases/news_story.cfm?newsId=20515 ("Although the new rule does not specifically deal with privacy issues in the use of drones, and the FAA does not regulate how UAS gather data on people or property, the FAA is acting to address privacy considerations in this area.").
[136] *See Press Release–DOT and FAA Finalize Rules for Small Unmanned Aircraft Systems*, FAA (June 21, 2016), https://www.faa.gov/news/press_releases/news_story.cfm?newsId=20515. As a result of the FAA's failure to add privacy protections, the Electronic Privacy Information Center has twice sued the FAA for failing to establish drone privacy rules. EPIC v. FAA: *Challenging the FAA's Failure to Establish Drone Privacy Rules*, EPIC.ORG, https://epic.org/privacy/litigation/apa/faa/drones/ (last visited Nov. 5, 2017).

assuming that a given jurisdiction has laws governing drones. In its defense, it is unclear whether the FAA has the expertise to design ex ante regulations protecting personal privacy.

As written, the small UAS regulations appear to frustrate the purpose behind creating HI-MEMS, while providing little protection against the threats they pose to national security and personal privacy. Perhaps, this hesitance to regulate is to be expected of an agency tasked with developing expertise in an unfamiliar, rapidly evolving field. Or perhaps, the FAA's lack of foresight is an indication that it is not a suitable agency to regulate HI-MEMS. For instance, even though the FAA might have authority over HI-MEMS with flight capabilities, the FAA could not regulate purely terrestrial HI-MEMS (e.g., cockroaches and flightless beetles). Thus, given the early stages of HI-MEMS technology, Congress should consider creating a new agency with particular expertise in HI-MEMS and similar technologies.

3. A New Technology-Based Agency

Agencies' expertise and efficiency in a specific regulatory field can make them dependable sources of regulation and oversight.[137] As the previous subsections have pointed out, it is arguable whether existing agencies such as the FDA or FAA are the proper agencies to oversee the emergence of HI-MEMS. Specifically, hybrid insect drones implicate issues of national security, personal privacy, and cyber security that do not completely align with the FDA or FAA's respective goals or expertise. Rather than force either of these agencies to develop such nuanced expertise in HI-MEMS technology,[138] perhaps HI-MEMS technology and similar technologies require the creation of a new agency.

Professor Ryan Calo argues that the expansion of robotics throughout various sectors of society require the creation of a new agency (i.e., the "Federal Robotics Commission" or "FRC")

[137] *See* Ryan Calo, *Robotics and the Lessons of Cyberlaw*, 103 CALIF. L. REV. 513, 557 (2015).
[138] *See id.* (arguing that, at some point, it is inefficient to task existing agencies to develop expertise in the "complexities" of robotics).

dedicated to dealing with the complexities of robotics.[139] As he notes, currently a multitude of agencies are dealing with robotics in slightly different applications: the FAA regulates drones; the National Highway Traffic and Safety Administration regulates driverless cars; and the FDA regulates medical robots.[140] Instead of a fractured product-based regulatory structure,[141] the FRC could provide an agency with technology-based expertise able to provide guidance and set standards for other agencies, industry, and courts.[142]

If such an agency did exist, its (likely broad) legislative mandate could provide authority to regulate HI-MEMS because of the technology's robotic nature.[143] Further, the FRC's expertise in robotics would make it the most appropriate agency to regulate HI-MEMS technology. For instance, HI-MEMS technology integrates many of the same technologies that make drones, driverless cars, and medical robots possible: autonomous and remote navigational systems, GPS, precision electronics and software, wireless capabilities, and a variety of sensors (to name a few). Similarly, the national security, personal privacy, and cyber security risks that persist in HI-MEMS technology are also prevalent in the above-mentioned technologies.[144] Unlike the FAA, the FRC could exercise its authority over all HI-MEMS regardless of their ability to fly. As such, the FRC could provide the type of ex ante governance that could mitigate or prevent many of the risks associated with HI-MEMS technology discussed in Part II.[145]

---

[139] *Id.* at 556.
[140] *Id.*
[141] *see Id.* at 555.
[142] *See id.* at 556–58.
[143] As discussed in Part I, researchers plan to make this technology, at least partially, autonomous, i.e., controlled by some form of Artificial Intelligence.
[144] *See, e.g.*, Self Drive Act, H.R. 3388 115th Congress (2017-2018) (requiring manufacturers to create a "cybersecurity plan" and "privacy plan" for sale of automated vehicles); *DJI Drones To Gain Privacy Mode After US Army Ban*, BBC NEWS (Aug. 15, 2017), http://www.bbc.com/news/technology-40935860 (noting that the Army prohibited its troops from using DJI produced drones because of cyber-security concerns)[hereafter *Army Bans DJI Drone*].
[145] To be sure, there are plenty of other technology-based agencies or commissions that Congress could create to govern HI-MEMS and like technologies. For example, Congress could create an agency with authority over

As attractive as creating a new agency sounds, this would require Congressional action. Moreover, it would take the new agency time to build its expertise, create guidance documents, propose rules, and so on. This may have the undesired effect of stifling some technologies in the short term. Thus, though a new agency might be the best long-term solution, interested stakeholders need to also look to short-term ex ante and ex post facto governance.

B. *Indirect Government Influence*

In addition to command and control regulations, some agencies have other ways of providing ex ante control of HI-MEMS research. For instance, agencies may apply conditions to HI-MEMS funding. Currently, many of the HI-MEMS projects are funded by DARPA through military agencies, such as the Office of Naval Research.[146] Currently, DARPA funding comes with many conditions. For example, there are conditions requiring compliance with federal laws such as the Clean Air Act and the Clean Water Act.[147] There are also conditions requiring "whistleblower protections" and "historic preservation."[148] DARPA even has research specific conditions related to research involving recombinant DNA molecules.[149]

Following this practice, DARPA could attach conditions to HI-MEMS funding that could mitigate the threats mentioned in Part II. For example, DARPA could require designated minimum standards for technology and cyber security to reduce the risk of hacking HI-MEMS and their onboard sensors. DARPA could also require integration of certain technologies such as

---

cybernetic research or biorobotics. The creation of such an agency may be inevitable as technology and the human body become more integrated. *See, e.g.*, Kevin Warwick, *The Future of Artificial intelligence and Cybernetics*, MIT TECHNOLOGY REV. (Nov. 10, 2016), https://www.technologyreview.com/s/602830/the-future-of-artificial-intelligence-and-cybernetics/.

[146] *See supra* Part I. For ease, reference to DARPA in this section incorporates, by reference, applicable Department of Defense (DOD) funding.

[147] *See, e.g.*, DOD, R&D GENERAL TERMS AND CONDITIONS 97 (2015).

[148] *Id.* at 101-02.

[149] DOD, DARPA AGENCY SPECIFIC TERMS AND CONDITIONS: EXHIBIT A 4 (2016).

geofencing[150] to limit where they can fly and prevent inadvertent release. Further, DARPA could refuse to fund research on insects that pose the most dual-use threat (e.g., vectors) and ethically problematic animals (e.g., mammals). In the future, DARPA could simply refuse to do business with companies that do not include these same minimum standards in their HI-MEMS.[151]

Alternatively, agencies with particular interest in HI-MEMS technology—such as those charged with protecting national security or personal privacy—may be able to take on a more active role in communicating directly with researchers and developers. Any agency so inclined could take a cue from the Federal Bureau of Investigation ("FBI"). Since 2009, the FBI has been reaching out and communicating with the DIY synthetic biology ("biohacker") community.[152] Ostensibly, the FBI's involvement and presence in the "amateur biology scene" is a way to educate both sides and is mutually beneficial.[153] In practice, it is an opportunity for the FBI to stay current with the capabilities of DIY biohackers. It is also perhaps the most direct and efficient way for the FBI to determine what, if any, threats DIY biohackers pose.[154] The FBI's consistent presence in the DIY biohacker community also provides parties with information to provide a contact in the bureau. The Federal Trade Commission and National Telecommunications and Information Administration have engaged in similar industry and community engagement activities.[155]

Much like the DIY synthetic biology scene, HI-MEMS technology has the potential to spur its own DIY community. As described in Part I, the basic technology and science needed

[150] Geofencing is a technology that can be used to keep drones within or out of designated areas. *See* Kaveh Wadell, *The Invisible Fence that Keeps Drones Away from the President*, ATLANTIC (Mar. 2, 2017), https://www.theatlantic.com/technology/archive/2017/03/drones-invisible-fence-president/518361/.
[151] *See, e.g.*, *Army Bans DJI Drone*, *supra* note 144.
[152] Howard Wolinsky, *The FBI and Biohackers: An Unusual Relationship*, EMBO REPORTS (Apr. 22, 2016), https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5278613/.
[153] *Id.*
[154] *See id.* ("The [FBI's] Biological Countermeasures Unit's mission is to prevent misuse or illicit acquisition of materials, technology, and expertise in the life sciences by would-be terrorists.").
[155] *See infra* Part III.D.

create a functional, albeit rudimentary, cyborg insect is quite simple. Though HI-MEMS technology is still in the relatively early research and development stages, commercial DIY kits and instructions are already widely available and inexpensive.[156] As these DIY kits are primarily geared toward students and other interested DIYers,[157] bourgeoning HI-MEMS communities may already be underway. Thus, this may be a good time for agencies concerned with national security, such as the FBI, to start fostering communication with potential HI-MEMS DIYers and get ahead of the technology.

C. *The Fourth Amendment*

As much as government agencies can provide ex ante control (or to, a limited extent, ex post facto remedies), government agencies (including law enforcement) may also be guilty of abusing HI-MEMS technology. As already discussed, government surveillance may pose the most obvious threat to personal privacy.[158] However, to a limited extent, Fourth Amendment jurisprudence on unreasonable searches and seizures may provide ex ante and ex post facto protections from unwarranted government intrusion using HI-MEMS—at least within one's home.[159]

The Fourth Amendment offers the strongest protection from government surveillance to people in their homes.[160] For example, in *Florida v. Jardines*,[161] the Court held that officers

---

[156] *See supra* note 91.
[157] *See Ethical Issues Regarding the Use of Invertebrates in Education*, BACKYARD BRAINS, http://wiki.backyardbrains.com/Ethical_Issues_Regarding_Using_Invertebrates_in_Education [herafter *Invertebrates in Education*] (last visited Nov. 28, 2017).
[158] *See supra* Part II.
[159] *Cf.* Feeney, *supra* note 81, at 4–8.
[159] *Id.*
[160] *See* U.S. CONST. AMENDMENT IV ("The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated . . . ."); *see also* Florida v. Jardines, 133 S. Ct. 1409 (2013) (holding that officers could not use a drug-sniffing down in the curtilage of the home to detect drugs inside the home without a warrant); Kyllo v. United States, 533 U.S. 27 (2001) (holding that officers could not use a thermal-imaging device aimed at a private home to obtain information that could not be obtained without entering

could not bring a drug-sniffing dog onto the curtilage of a home, without a warrant, in order to alert the officer to drugs in the home. Similarly, in *Kyllo v. United States*,[162] the Court held that the officers could not use thermal-imaging technology to detect heat signatures emanating from a home, even though the officers never entered onto the property. However, outside of the home, a person has limited Fourth Amendment protection.

Under the current jurisprudence, a person's Fourth Amendment protection depends on the Court's two-prong "expectation of privacy" test.[163] Under this standard, a person must have (1) "exhibited an actual (subjective) expectation of privacy" that (2) "society is prepared to recognize as reasonable."[164] Using this two-prong test, the Court has found that the government does not need a warrant to conduct visual, outdoor surveillance of a person's property from an aircraft.[165] This is true even when the government has conducted unwarranted surveillance using high-tech cameras.[166] However, the Court has drawn a line when the government's surveillance causes a trespass to property.[167]

As the preceding discussion shows, the Fourth Amendment jurisprudence on searches and seizures may do little to placate those who fear living under constant government surveillance, especially since a person has a limited expectation of privacy in public.[168] First, the current Fourth Amendment jurisprudence generally does not require the government to seek a warrant

---

the home without a search warrant); *see also* Dyer, *supra* note 4, at 240 (discussing the indoor versus outdoor distinction in the Supreme Court's Fourth Amendment jurisprudence).

[161] 133 S. Ct. 1409 (2013).

[162] 533 U.S. 27 (2001).

[163] *See* Katz v. United States, 389 U.S. 347, 360-64 (1967) (Harlan, J., concurring). Though this was a concurring opinion, Justice Harlan's two prong test became the Court's reasonable expectation of privacy standard. *See* Dyer, *supra* note 4, at 236 ("In later decisions, the Court adopted Harlan's 'reasonable expectation of privacy' definition . . . .").

[164] *Katz*, 389 U.S. at 361 (Harlan, J., concurring).

[165] *See* Feeney, *supra* note 81, at 5 (citing California v. Ciraolo, 476 U.S. 207 (1986)).

[166] *See id*. at 6 (citing Dow Chemical Co. v. United States, 476 U.S. 227 (1986)).

[167] *See id.* at 7 (citing United States v. Jones (2012)).

[168] *See* Dyer, *supra* note 4, at 247-48 ("The cumulative impact from the Court's [Fourth Amendment] precedent seems clear - to genuinely ensure privacy from government prying, one should 'retreat into his own home.'"); Feeney, *supra* note 81, at 6–8.

prior to conducting surveillance in public places. Because the government may not use HI-MEMS to spy on people in their homes, this may create—as Professor Dyer describes—a national bunker mentality.[169] Moreover, though the Fourth Amendment would preclude the admission of evidence obtained through the government's unconstitutional surveillance (i.e., search), it would not necessarily prevent government from conducting questionably legal surveillance using HI-MEMS.[170] As such, the Fourth Amendment primarily functions as an ex post facto remedy for decidedly unconstitutional government surveillance. Further, the Fourth Amendment's effectiveness against unreasonable searches is limited to government searches. Thus, it does not apply to the average drone hobbyist or other private users.[171]

Due to the existence of academic literature dealing with Fourth Amendment jurisprudence as it relates to surveillance drones[172] and HI-MEMS (in particular),[173] this article does not elaborate further on the Fourth Amendment's potential for governing government and private surveillance vis-à-vis HI-MEMS. However, two more observations about the Fourth Amendment as it relates to HI-MEMS are worth mentioning. First, even though the Fourth Amendment jurisprudence might evolve to offer more protection from "unreasonable" government searches in public, it would not protect the privacy of individuals and businesses from private actors. Second, the Fourth Amendment would not address any of the national security or cyber security issues associated with HI-MEMS technology. Thus, though the Fourth

[169] *See* Dyer, *supra* note 4, at 244.
[170] Because HI-MEMS have the capacity to act on their own when not controlled, there may be situations in which law enforcement passively gathers data that it later attempts to admit into evidence. This may give rise to many Fourth Amendment issues of first impression for the Court.
[171] Stephen Carter, *Commentary: A Battlefield of Drones and Privacy in Your Backyard*, CHI. TRIB. (Aug. 3, 2015), http://www.chicagotribune.com/news/opinion/commentary/ct-drones-privacy-laws-20150803-story.html.
[172] For a thorough discussion about the Fourth Amendment implications of government drone surveillance, see generally Feeney, *supra* note 81.
[173] For a thorough discussion about the Fourth Amendment implications of government HI-MEMS surveillance, see generally Dyer, *supra* note 4.

Amendment may eventually be a solution to part of the puzzle, it alone would not be enough to combat the threats to national security and personal privacy posed by HI-MEMS.

D. *State Laws*

Perhaps one way to protect against the threat to personal privacy is by using state laws to offer ex ante protections and ex post facto remedies. Several states have laws that protect against surveillance by government actors. Some of these laws are specific to drone technology. For example, Virginia law requires law enforcement and regulatory agencies to obtain a warrant prior to drone surveillance.[174] In creating the warrant requirement, the Virginia law fills the gap left by the current Fourth Amendment jurisprudence on outdoor, government drone surveillance. Further, the law strikes a balance between protecting personal privacy, while allowing unwarranted drone use in emergency situations (e.g. during Amber alerts). At least eleven other states have similar laws.[175]

In contrast, some state laws may be generally applicable to surveillance technology. In many respects, these types of state laws may protect or provide a remedy for private citizens from intrusive use of HI-MEMS and similar technologies by private actors. For example, California Penal Code Section 632 makes it a crime to use an electronic recording device to eavesdrop or record confidential communications. Violation of Section 632 is punishable by a fine of up to $ 2,500 or up to one year in jail or state prison for a first offense and up to $10,000 dollars for a subsequent offense.[176] California even provides injured persons a civil remedy of $5,000 per violation against the perpetrator and allows for triple damages.[177]

---

[174] *Warrant Requirement for Drone Usage Now Law; ACLU of Virginia Celebrate Key Victory*, ACLU (May 1, 2015), https://www.aclu.org/news/warrant-requirement-drone-usage-now-law-aclu-virginia-celebrates-key-victory.
[175] *Id.*
[176] CAL. PENAL CODE § 632(a).
[177] *Id.* § 637.2(a)–(b).

On its face, general privacy protections such as California penal code section 632 would seem to provide ex post facto remedies for illicit HI-MEMS use.[178] The penalties may even be enough to deter uses of more obvious technology such as drones or hidden cameras. However, HI-MEMS pose a particular threat to privacy because of their agility, small size, and inconspicuous shape. As a result, some actors may find the potential rewards outweigh the relatively low penalties given the low probability of detection. Thus, states with laws generally protecting privacy may need to reconsider whether their laws have a sufficient deterrent effect with regard to emerging technologies such as HI-MEMS.

E. *Self-Regulation*

Although not discussed in depth in this article, perhaps the biggest threat facing the development and widespread use of HI-MEMS technology is negative public perception. As HI-MEMS technology develops, it may be that many of the threats identified in Part II never materialize. However, perceived threats or societal distrust of the technological may be enough to hamper the development and beneficial implementation of this technology. For this reason, it may be best for researchers and potential manufacturers, consumers, investors, industry partners, and other stakeholders to initiate public participation or undertake voluntary actions to foster interest and familiarity with HI-MEMS.[179] In addition to quelling public concern or misinformation,[180] such voluntary actions may convince regulators and politicians to take a "wait-and-see" approach instead of initiating precautionary regulations and defensive laws.

[178] Based on its preamble, the California Legislature seems to have enacted this code in anticipation of threats posed by technological advancements such as those underpinning HI-MEMS. *See Id.* § 630.
[179] *See* LIN, *supra* note 103, at 19–22 (discussing the utility of public participation in technology and risk assessment).
[180] *See id.* at 21 (arguing that laypersons may offer a breadth of knowledge notwithstanding incorrect assumptions about science and technology).

In some respects, companies such as Backyard Brains that manufacture cyborg insect DIY kits are already undertaking some of these actions. Backyard Brains has been engaging educators and younger generations through their DIY kits and high school workshops.[181] Through these actions, they may be getting ahead of some of the bad press by pre-emptively addressing ethical issues and promoting the educational value of the technology to a captive audience. [182] However, in some circumstances, direct public engagement may be counterproductive. For instance, community engagement may require stakeholders to address controversial questions regarding the ethics, morality, and ulterior motives behind HI-MEMS research.[183] Still, HI-MEMS technology might provide the kind of sci-fi allure and mystique that lends itself well to public education and other passive forms of public participation.

In addition to public engagement and education, stakeholders can voluntarily implement standards and codes of conduct to win the public's (and regulators') trust. To begin with, current and potential stakeholders can develop voluntary best practices. An example of what this process would look like comes from the National Telecommunications & Information Administration (NTIA). In 2015, President Barack Obama established a "multi-stakeholder engagement process to develop and communicate best practices for privacy, accountability, and transparency issues" regarding commercial and private drone use.[184] Though the document itself is nonbinding, it does include a section of supporters that includes Amazon, Intel, and various drone organizations. In this case, the creation of this document was initiated at the direction of

[181] *See Invertebrates in Education*, *supra* note 157.
[182] *See id.*
[183] *See, e.g.*, *id* (discussing the ethical issues regarding the manipulation of living insects).
[184] NAT'L TEL. & INFO. ADMIN., VOLUNTARY BEST PRACTICES FOR UAS PRIVACY, TRANSPARENCY, AND ACCOUNTABILITY 1 (2016), https://www.ntia.doc.gov/files/ntia/publications/uas_privacy_best_practices_6-21-16.pdf.

President Barack Obama and effectuated through NTIA.[185] However, there is no reason why industry stakeholders could not initiate a similar process. A HI-MEMS best practice guide could cover any number of topics, including: research best practices, ethical considerations, minimum technological standards, privacy concerns, and prohibitions on vector and non-insect research.

Though a similar HI-MEMS best practice document may not be binding, it would still show the public, regulators, and politicians that researchers and industry partners are aware of the potential issues implicated by HI-MEMS and are taking proactive steps to address them. Moreover, creating voluntary best practices might be a way for stakeholders to meaningfully involve the public.[186] However, the efficacy of this type of voluntary self-regulation depends, in part, on stakeholders' fidelity to the goals and standards contained in the document.

IV. SUGGESTIONS & RECOMMENDATIONS

In Part III, several governance regimes and their potential for providing ex ante and ex post facto governance were discussed. From this discussion, it seems that no single governance regime would be sufficient to govern the risks associated with HI-MEMS technology. Therefore, this part provides some suggestions and recommendations for governing HI-MEMS.

As an initial point, it seems that ex ante governance would be the most effective way to mitigate the national security, personal privacy, and cyber security risks associated with HI-MEMS. As shown, agencies, such as the FDA and FAA, may have great influence on whether a product makes it to market.[187] This makes agency oversight the preferred method for providing ex ante protections. However, as shown in Part III.A, neither of these agencies is quite suitable to govern HI-MEMS because they lack the expertise or ability to comprehensively govern the risks

[185] *See id.* at 1.
[186] *See* Memorandum for the Heads of Executive Departments and Agencies, From John P. Holdren, Director, Office of Sci. and Tech. Pol'y 2 (Mar. 11, 2011).
[187] *See supra* Part III.A.

associated with HI-MEMS. Further, though these agencies might regulate certain HI-MEMS or specific aspects of the technology, they would not necessarily be able to govern similar technology such as flightless drones. Assuming jurisdiction over HI-MEMS by either agency would create further inefficiency in an already fractured product-based regulatory regime. Thus, Congress should create a technology-based agency, uniquely situated to handle HI-MEMS and similar technologies. One possibility for such an agency is the Federal Robotics Commission suggested by Professor Calo.[188]

An agency, such as the FRC, could require HI-MEMS and similar technology to include minimum cyber security or technology standards making them harder to hack. This could minimize national security and privacy threats by making it harder for unintended parties to remotely pilot the cyborg insect drone or access its sensors. An agency could also require developers to give all relevant information about the HI-MEMS to the agency and ensure that it will not cause harm to national security, personal privacy, humans, or the environment. If an agency is not satisfied that the HI-MEMS will pose no threat to these interests, the agency could prevent the HI-MEMS market release. Further, the agency could require commercial users to notify the agency whenever the HI-MEMS are deployed. Though not discussed in this article, this could make it easier to allocate fault should injury to people or property occur.

As identified in Part III.A.3, the downside to establishing a new agency is the time required to get the agency up and running. As such, creating a new agency at this point might provide a long-term solution but leave a gap in the short-term. Therefore, stakeholders and government actors should take proactive steps to provide ex ante protections.

[188] *See supra* Part III.A.3.

First, stakeholders should take this opportunity to self-regulate by creating and adhering to voluntary best practices and standards. This could serve the dual purpose of influencing a nascent agency's regulatory stance and providing an opportunity to meaningfully engage the public. Government actors could facilitate this process by conditioning research funds on adherence to voluntary best practices or other minimum standards. Government actors could also proactively begin communications with stakeholders. Finally, state government could provide ex ante privacy protections from unwarranted surveillance by law enforcement through state laws. State governments could also enact laws that provide ex post facto remedies for violations of personal privacy by private actors.

Though these regimes cannot completely dispense with the risks associated with HI-MEMS, they may be able to discourage nefarious actors and mitigate potential damage.

CONCLUSION

Though cyborg insects may be the product of science fiction,[189] the practical application and beneficial uses of HI-MEMS may potentially alter the way we view, interact, and manipulate the living environment around us. From mapping otherwise undiscoverable terrain to monitoring some of the world's most precious environments, cyborg insect drones may soon be integrated into our everyday lives. However, some actors may also exploit HI-MEMs dual-use attributes to threaten our national security and personal privacy. Fortunately, there is still time while the technology is in its R&D phase to discuss ways in which governance regimes can mitigate the risks.[190]

[189] ANTHES, *supra* note 7, at 148–49.

[190] In addition to the concerns discussed in this article, stakeholders should also consider the ethical and policy questions that HI-MEMS technology represents. These questions may affect the way we utilize, expand, and limit the use of this technology.

In attempting to predict how best to govern the evolution of HI-MEMS technology, stakeholders should consider the extent to which the chosen governance regimes address the identifiable risks. They should also consider whether the chosen governance regimes provide ex ante control or ex post facto remedies and whether the governance regimes provide both short-term and long-term solutions. Finally, stakeholders should be proactive in finding solutions to perceived threats rather than waiting for threats to materialize.