DEFENSE INTELLIGENCE AGENCY

WASHINGTON, D.C. 20340-5100

FOIA-00118-2022
U-22-3587/IMO-2 (FOIA) July 18, 2022

John Greenewald
27305 W. Live Oak Rd. Suite #1203
Castaic, CA 91384

Dear Mr. Greenewald,

This responds to your Freedom of Information Act (FOIA) request, dated March 23, 2022 that you submitted to the Defense Intelligence Agency (DIA) requesting a copy of records (which includes videos/photos), electronic or otherwise, of the following document: Worldwide: Biohacking: A Potential Covert Communication Method, published 28 September 2009. I apologize for the delay in responding to your request as DIA continues its efforts to eliminate the large backlog of pending requests.

A search of DIA's systems of records located one document (3 pages) responsive to your request.

During the review, while considering the foreseeable harm standard, I have determined that some portions of the document (3 pages) must be withheld in part from disclosure pursuant to the FOIA. The withheld portions are exempt from release pursuant to Exemptions 1, 3, and 6 of the FOIA, 5 U.S.C. § 552 (b)(1), (b)(3), and (b)(6). Exemption 1 applies to information properly classified under the criteria of Executive Order 13526. Exemption 3 applies to information specifically exempted by a statute establishing particular criteria for withholding. The applicable statute is 10 U.S.C. § 424. Statute 10 U.S.C. § 424 protects the identity of DIA employees, the organizational structure of the agency, and any function of DIA. Exemption 6 applies to information which if released would constitute an unwarranted invasion of the personal privacy of other individuals. DIA has not withheld any reasonably segregable non-exempt portions of the records.

If you have additional questions/concerns you may:

Contact the FOIA Public Liaison	Email: FOIA1@dodiis.mil Phone: 301-394-6253
File an administrative appeal (must be submitted within 90 days of the date on the letter) please contact us via one of the following and use FOIA-00118-2022 when referencing your case)	Email: FOIA1@dodiis.mil Mail: Defense Intelligence Agency ATTN: IMO-2C (FOIA) 7400 Pentagon Washington, DC 20301-7400

For mediation services, you may contact the Office of Government Information Services (OGIS) at the National Archives and Records Administration to inquire	Email: ogis@nara.gov Phone: 202-741-5770 Toll-Free 1-877-684-6448 Facsimile: 202-741-5769 Mail: Office of Government Information Services National Archives and Records Administration 8601 Adelphi Road-OGIS College Park, MD 20740-6001

Sincerely,

(for)
Cheryl Cross-Davison
Chief, Records and Open Government

Enclosure

WORLDWIDE

(U) Biohacking: A Potential Covert Communication Method

~~(C//REL)~~ Biohacking—experimentation on DNA and other aspects of genetics by "hobbyists"—is increasing as pertinent technology and data become more accessible and as online support groups facilitate sharing of information and knowledge. Over the next 5 years as biohacking capabilities spread, the techniques and tactics needed to employ DNA-based steganography (concealing of messages within messages) are likely to spread as well. Although we have no evidence to suggest adversaries currently are experimenting with this technology, DIA assesses with high confidence that as biohackers develop the knowledge to exploit this technique, state or nonstate actors will endeavor to use DNA-based steganography to circumvent existing intelligence collection capabilities.

~~(C//REL)~~ Biohacking is gaining in popularity as the availability of technology and the low cost of laboratory equipment move bioscience out of the formal laboratory and into the garage or basement. We judge that over the next 5 years, more individuals will acquire the knowledge to exploit techniques such as DNA-based steganography, and adversarial groups would realize the potential and recruit persons with the necessary ability. Many biohackers are hobbyists working in nonscientific fields, who use the Internet to obtain step-by-step instructions for genetic transformation experiments, as well as access to "do it yourself biohacking" online communities for support and information sharing.

UNCLASSIFIED

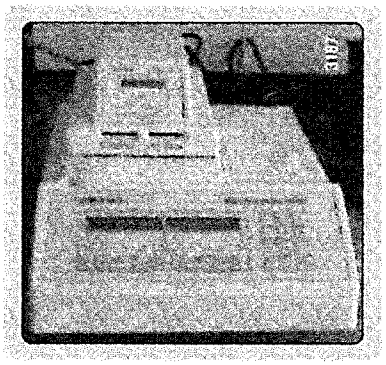

Image: www.Molecularstation.com

(U) **PCR Machine.** This machine, suitable for expanding DNA-encrypted microdots, sold on eBay for $59.

> (U) Publicly accessible databases, including the National Institutes of Health-affiliated National Center for Biotechnology Information Genome Database, have sufficient genetic data available for skilled private individuals to experiment with altering DNA. In addition, biohackers have access to several commercially available steganography tools they can use or modify to encrypt and decrypt DNA-based communications.

(U) Source Summary Statement

~~(C//REL)~~ DIA bases this assessment on analysis of reputable open sources, such as the National Institutes of Health and the Massachusetts Institute of Technology, which provide direct access to the scientific data necessary for an adversary to develop DNA-based encrypted communications (b)(1):Sec. 1.4(c)

REVERSE BLANK

Derived from: (b)(3):10 USC 424
Declassify on: 9 September 2024

> (U) New or used scientific equipment is readily available for purchase on the Internet. According to a report in the January edition of *New Scientist*, eBay sold a polymerase chain reaction (PCR) machine, which is useful for expanding DNA-encrypted microdots, for $59. In addition, biohackers can purchase new and used equipment suitable for home laboratories from several specialty websites.

> (U) According to a blog posted on the *Discover Magazine* website, a computer programmer in San Francisco uses online resources to guide her experiments in genetically modifying bacteria. Another biohacker started a "Do It Yourself Biology" group instead of pursuing a PhD in biology because he wanted "to help people do biology as a hobby."

(U) What Is Biohacking?

(U) Biohacking is experimentation with DNA and other aspects of genetics by hobbyists. A biohacker is similar to a computer hacker, who creates and modifies computer software or hardware as a hobby, but should not be confused with a bioterrorist, whose intent is the release of viruses, bacteria, or other germs to cause illness or death in people, animals, or plants. Using available resources, including a laptop computer, published gene sequence information, and mail-order synthetic DNA, almost anyone has the potential to be a biohacker by constructing genes or entire genomes from scratch. However, the reagents required for some genomic applications may not be easy or inexpensive to obtain. Biohacking has multiple benign and threatening applications, ranging from amateur designing of seeds to collaborative research on medications to production of novel biological warfare agents.

~~(C//REL)~~ One potential application of biohacking, DNA-based steganography, is the concealment of communications. DNA-based steganography would conceal a DNA-encoded secret message on a microdot that could be hidden in a document, powder, liquid sample, or photograph. Not only is use of this technique difficult to identify, but one needs to know the exact DNA primer sequences used to encrypt the message in order to decrypt it (about 10^{24} primer sequence codes are possible).

> (U) Polestar Limited Technology Transfer Group (TTG), a Bermuda-based agent company, provides China with access to DNA-based technologies that Beijing could modify to conceal communications. A TTG website posting notes that Polestar President Wendell Smith completed a conference call with Canada, China, and California to discuss a transfer deal involving use of DNA codes from DNA Lock TM technologies. DNA Lock TM is an anticounterfeiting DNA-coded watermark authentication molecule concealed within a vast genomic DNA.

> (U) In India, the Central Scientific Instruments Organization has developed DNA-based encryption software that can encrypt and hide information, such as photographs and maps, in an undetectable DNA sequence, according to a September 2004 unclassified article in India's *The Tribune.*

11

(~~C//REL~~) Over the next 5 years, use of biohacking can pose a serious challenge to U.S. intelligence collection capabilities. The undetermined number of individuals with little scientific expertise having easy access to the technology to create nearly undetectable communications elevates the risk.

(~~C//REL~~) Enforcing strict security and accountability to protect equipment and ingredients, including restricting access to research laboratories and to various online product websites, would limit the spread of biohacking and its associated potential threats. However, stricter enforcement also would result in suppression of socially useful outcomes of biohacking. Secure passwords for university and government databases would enable tracking of individuals who are illegally or nefariously accessing, downloading, and using genomic information. DE

(b)(3):10 USC 424;(b)(6)