Homefront to Battlefield: Why the U.S. Military Should Care About Biomedical Cybersecurity

Nataliya D. Brantly

ABSTRACT

Immunity to the cybersecurity risks and potential hazards presented using biomedical devices. US Military and civilian personnel use these devices on the Homefront and battlefield. As the use of biomedical devices increases with time and blurs the lines between private and professional, more attention is required of the U.S. Department of Defense (DoD) to understand the strategic importance of securing biomedical devices. This work provides a better understanding of biomedical devices and analyzes current use of biomedical devices within DoD. It also provides recommendations on actions DoD can undertake to safeguard its workforce today and in the near future. This article examines the significance of cybersecurity for biomedical devices within the context of US national security and demonstrates the important role biomedical cybersecurity plays for DoD.

Keywords: *Biomedical, cybersecurity, military, defense, DoD, policy, threat*

INTRODUCTION

The importance of cybersecurity to society and national security is growing as technology increasingly pervades all areas of our lives. This is true not only in business, travel and communications, but also in the provision of healthcare, in the sharing of medical records and the treatment of health conditions. Advances in computer science and biomedical engineering have enabled the collection of health data via a multitude of biomedical devices. Such devices offer new lifesaving solutions and enable proximate and non-proximate monitoring of a number of physiological conditions including sleep patterns, heart rate, exercise, blood glucose levels and many other measurements on a daily basis without the direct involvement of a healthcare professional.

Nataliya D. Brantly is a Doctoral Student in the Science and Technology Studies (STS) program as well as a graduate student in the Master of Public Health program at the Virginia Polytechnic Institute and State University. Her research interests are broadly in the areas of biomedical security, global health, medicine, and technology.

A number of life-sustaining and lifesaving biomedical devices are in use by the general public and U.S. Department of Defense (DoD) personnel ranging from heart monitoring devices to insulin pumps to implantable cardioverter defibrillators (ICDs). These technologies, while remarkable in their lifesaving abilities, also carry with them the potential for negative health outcomes at the hands of malicious actors. With the expanded use of biomedical devices by active duty and civilian personnel, such devices are becoming an increasing part of the DoD. As a result, the cybersecurity implications of these devices should be taken into consideration in vulnerability assessments and risk prevention programs.

As medical care becomes increasingly infused with technology unique challenges arise including: the potential loss of information, unauthorized intrusion, or manipulation of health-related data from associated biomedical devices or other manipulations, and degradations of equipment that might result in life threatening consequences. There are numerous academic and popular articles describing the multitude of medical devices.[1] Similarly, there are a number of articles examining hacks performed against biomedical devices. Those include attacks against wearable devices to disable them, obtain collected data, take advantage of the connection between the wireless device and a personal computer,[2] data breaches and theft of medical records,[3] to name just a few. In addition to potential risks to the general population, the US military is also vulnerable to novel threats in an increasingly digitally connected world. This applies not only to the growing connectivity of troops around the world but also to the wearable and medical devices used by US military personnel and their families worldwide, and also to point of care locations using medical devices to care for soldiers, their families, and veterans.

Recently, the DoD has emphasized the strategic importance of critical infrastructure cybersecurity, collaboration with international and domestic partners to promote cybersecurity,[4] the security of federal information systems and national security systems (e.g., SIPRNet and NIPRNet), supply chain cybersecurity, combating cyber espionage, or protection of intellectual property and the development of a robust cybersecurity workforce.[5] Healthcare, medical, and biomedical cybersecurity have not been explicitly articulated as items of strategic importance for the DoD. The Command Vision for U.S. Cyber Command does not mention biomedical security, nor does it list it as an area of concern. Data presented in this article aims to demonstrate the significance and relevance of biomedical cybersecurity to the DoD and present it as an essential component of the nation's overall cybersecurity strategy.

Biomedical cybersecurity differs from general cybersecurity in a number of ways. First, the benefits received from biomedical devices can be directly lifesaving or life sustaining. Often the benefits of such technology outweigh the risks. However, there is a delicate balance between providing needed biomedical technology to assist with a health issue in a timely manner versus offering timely introduction to the market of needed technology. The key is offering functionality and convenience of use while ensuring the technology is not easily vulnerable to malicious actors. Second, the data collected via cybersecurity breaches is physiological, and include personally identifiable information (PII) derived from biomedical devices. Third, the severity and consequences of potential direct cybersecurity manipulations differ. Biomedical device manipulations can result in lethal outcomes as many devices in use are essential to maintain life or provide critical information to clinicians when making healthcare decisions for a patient.

Biomedical cybersecurity is the protection of biomedical devices from unauthorized intrusion to retrieve or modify information or affect the functionality of such devices. Biomedical cyber threats affect the health, wellbeing, and safety of the US military, through the degradation of the accuracy of clinical decisions adversely affecting the operation of the devices, and impacting the timely recovery and return of military personnel to duty. Moreover, intrusions into DoD biomedical systems can also affect DoD reputation and trust, disclose physical locations on the battlefield, and cause critical mission disruptions. It is essential for US military to stay operational and at full strength on the battlefield and on the Homefront. Biomedical cybersecurity is an important component in overall cybersecurity and should be an important consideration for the DoD to keep military and civilian personnel operational. Biomedical security, awareness of potential disruptions as well as acquisition of skills in preventing and mitigating such disruptions can make the difference between mission success and mission failure.

This article is divided into four sections to address US military biomedical cybersecurity considerations. Section 1 offers a general introduction to biomedical devices. Section 2 reviews biomedical devices in use by US military now and planned use in the near future. Section 3 analyzes threats in cybersecurity of biomedical devices for US military. Section 4 concludes by discussing the importance of biomedical cybersecurity for US military and draws parallels between military biomedical security and general population biomedical security.

The Basics of Biomedical Devices

Advances in biomedical engineering, computer science and modern medicine enabled the development and the introduction to the market a number of medical devices that offer health monitoring, drug delivery, life maintaining and lifesaving functionality to individuals. Healthcare is being revolutionized by digital technology, mobile medical applications and by software and hardware-based products that help clinicians make decisions daily. Such biomedical engineering is defined as "the application of engineering principles, practices, and technologies to the fields of medicine and biology especially in solving problems and improving care (as in the design of medical devices and diagnostic equipment or the creation of biomaterials and pharmaceuticals)."[6] In the field of biomedical engineering scientists and engineers design hardware and software products to address problems within the fields of medicine, public health and related fields to resolve health issues and improve health outcomes.

The main authority responsible for implementing and enforcing regulations pertaining to medical devices in the US is the U.S. Food and Drug Administration's (FDA) Center for Devices and Radiological Health (CDRH).[7] The CDRH works to establish regulatory standards for the safety and efficacy of medical devices, and it places emphasis on rigorous science so that American patients are assured a reasonable degree of quality, reliability and effectiveness of healthcare.[18] The primary mission of CDRH is to protect and promote public health to "assure that patients and providers have timely and continued access to safe, effective, and high-quality medical devices and safe radiation-emitting products."[9]

The FDA groups medical devices into three classes based on risk and the ability to ensure safety and effectiveness of the device.[10] Class I devices are low-risk and include non-electronic medical devices such as bandages, tongue depressors, stethoscopes, examination gloves, handheld surgical instruments etc. Such devices are not intended to sustain life, support life or prevent disability. Class II devices have intermediate or moderate risk and include devices such as infusion pumps for intravenous medications, powered wheelchairs, and computed tomography (CT) scanners to name a few. They are intended to support or sustain human life. Class III devices are high-risk and crucial to maintain health and sustain life. Among those are artificial pacemakers, insulin pumps and deep-brain stimulators. Such devices are important in preventing impairment of human health and pose a potential risk of illness or injury if the device fails.

Biomedical devices analyzed in this paper exclude Class I devices as they are not a cybersecurity risk. Class II and Class III devices containing a central processing unit (CPU), electronic devices with wireless or wired connectivity to other devices or networks are considered in this paper. It is also important to consider other digital health products such as software for medical devices. Further discussion of biomedical devices will encompass considerations of both hardware and software.

This article groups biomedical devices into three main categories that will be further discussed in more detail and summarized in the table below. The first category is wearable devices (wearable trackers, clothing, health assist devices, infusion devices, implanted devices, ingestibles). The second category is healthcare medical devices (diagnostic devices, monitoring devices, treatment devices). The third category is software health products (health recordkeeping and sharing products, mobile apps).

1. Wearable Devices

Wearable devices (wearables) are electronic networked devices that contain sensors and microchips,[11] can collect physiological data, can be worn on the user's body and can execute a variety of actions based on user's needs and device capabilities. Wearables can be further subdivided into six groups based on function and impact. Wearable trackers (a.k.a. fitness trackers or activity trackers) are widely used in US with increasing popularity. Wearable trackers continuously track general health and wellness with outputs such as heart rate, step count, sleep patterns, exercise, and calorie consumption, as well as GPS tracking. Wearable activity trackers are the most widely used wearables within an ever-increasing segment of the US consumer market.[12]

Clothing, as biomedical technology, is gaining traction as a subset of wearable devices. This is possible through the development of novel fabrics (conductive and touch sensitive materials), "smart" accessories (e.g., buttons, belts, embroidery), and ways to integrate technology into the clothing through fabric-based sensors and electrodes.[13] Biomedical clothing has the capability to "monitor physiological, neurological, and body kinematic parameters"[14] such as Electrocardiograms (ECGs), Electromyogram (EMG), pulmonary activity, skin Ph, blood pressure, temperature, body position, comprehensive sleep patterns and impact detection. Biomedical clothing is used in gaming industry, professional sports and fitness, health, medicine,[15] and the military.[16]

Among health assist and monitoring devices are small wearable devices that help individual patients with a particular health need or issue. Among such devices are hearing aids, electronic contact lenses[17] or glasses as well as continuous glucose monitoring (CGM) systems and mobile ECG monitors. Additional health monitoring devices are wrist bands to detect elderly falls,[18] blood pressure monitors[19] and ultrasound scanners connected to smart phones.[20] Infusion devices are wearable biomedical devices designed to deliver medication to individual patients. Examples of such devices are injectable technologies to treat a number of health issues in oncology, cardiovascular and diabetes care, autoimmune disorders and infectious diseases. Insulin pumps are one of most widely used infusion devices that are customized to user's needs and provide lifesaving solutions to the patient. Implanted devices are essential for an individual's life. Examples of implanted devices include implantable cardioverter defibrillators (ICDs), heart pacemakers and ventricular assist devices (VADs). Ingestible devices include consumable pills used to monitor the gastrointestinal tract, evaluate how the patient is affected by prescribed medication and to assess medication adherence. Capsule ultrasound (CUS) device, a small ingestible disposable wireless imaging sensor based on ultrasound technology, is an example of ingestible device that provides a new method of diagnosing gastrointestinal diseases.[21] Another example is Proteus Discover, ingestible sensor that provide information about patient's health patterns and the effectiveness of medical treatment resulting in more informed healthcare.[22] Proteus Discover was first used commercially in 2012 in the UK and in 2016 in the US[23] with subsequent expansion to eight health systems in US by June 2017.[24]

2. Healthcare Medical Devices

Healthcare medical devices are primarily used at the point of care locations such as hospitals, clinics, urgent care facilities, group medical practices and with individual providers. Such entities collect, store and exchange significant amounts of medical data generated by diagnostic, monitoring and treatment biomedical devices. Diagnostic biomedical devices are used to conduct testing and diagnose health conditions. Examples of diagnostic devices are ophthalmoscopes, ultrasound, digital medical laboratory equipment, radiological and imaging radiological equipment (computed tomography (CT), magnetic resonance imaging (MRI), mammography, positron emission tomography (PET), radiography, fluoroscopy). Monitoring biomedical devices are used to continuously collect health data to monitor patient's vital signs. Among such devices are digital sphygmomanometers (blood pressure monitors), ECG (electrical signal evaluation in the heart) and electroencephalogram (EEG—electrical activity evaluation in the brain). Treatment biomedical devices are used for the treatment of health conditions for the support of life. Examples are drug dosing and delivery equipment such as infusion pumps, life support equipment such as cardiopulmonary bypass (CB) devices, medical ventilators, dialysis machines and neonatal incubators.

3. Software Health Products

Software health products include a large number of software products used by healthcare providers, software used on personal computers and mobile phones in the form of mobile medical applications. A variety of software products are designed to provide a health benefit for patients and provide health management solutions for healthcare providers to diagnose, treat, predict risk and treatment response.[25]

Electronic health recordkeeping systems and exchanges for health-related data are used by health care providers, hospitals, health information technology developers, patients, testing laboratories, manufacturers of medical devices (public and private entities) engaged in the evaluation of health information technology performance and other entities or individuals.[26] The severity of threats coming from such systems depend on the interoperability of biomedical devices with the systems, which security features have been implemented, and the ease of submitting, accessing and exchanging health data. Threats to health records from cybersecurity arise from a wide range of unauthorized system access types including the retrieval, modification or manipulation of health records. Consequences of such breaches range from patient inconvenience, data and monetary losses to inaccurate diagnosis and death.

Large numbers of individuals can be affected simultaneously via cybersecurity breaches at point of care entities. This can lead to significant data loses as exemplified by Community Health Systems' cyber-attack and theft of 4.5 million patient records.[27] Such entities are targeted for the volume and diversity of data collected, stored and exchanged.[28] Hackers target medical entities for the theft of records because of the high profitability of such records.[29] In 2018 IBM sponsored "The Cost of a Data Breach" study conducted independently by Ponemon Institute. This study identified $408.00 to be the average global cost per lost or stolen record for healthcare industry compared to $148.00 per stolen record of personal or sensitive information in other industries.[30] The breach of healthcare industry and biomedical cybersecurity is a lucrative business for cyber criminals.[31] After a credit card breach, one can relatively easily recover by closing the account or changing a bank.[32] On the other hand, a medical records breach offers limited options for individual remediation due to insurance restrictions and limited provider availability.[33] Threats to biomedical devices or their support systems affect not only the individual, but also the healthcare entities suffering significant financial losses.

Biomedical Devices Used or Planned for the Military

The US military uses numerous biomedical devices, both at home and on the battlefield. These include devices such as wearable trackers, biomedical clothing, health assist devices, infusion devices and implanted devices as outlined below. On the Homefront such wearable devices are used for personal fitness or health needs on a daily basis and for conducting training missions in preparation for the battlefield. Wearable biomedical devices on the battlefield are used to monitor vital signs for combat troops. The use of wearable biosensors can detect dehydration and other performance and health metrics to provide accurate assessments of these aspects of force readiness in real-time.[46] Biomedical clothing devices used by Soldiers can detect impact wounds from a bullet or shrapnel penetration, sense chemical, thermal, and physical attacks, and other battlefield hazards so that appropriate medical care or tactical awareness is provided. Such systems offer the potential for real-time non-invasive health monitoring.[47] For example, U.S. Army Research Institute of Environmental Medicine (USARIEM) conducted "field studies using wearable physiological monitors" to understand "how low core temperatures went in metabolically challenged Ranger School students, and how high they went during Marine patrolling activities in Iraq and Afghanistan."[48]

Wearable biomedical devices used by the military during training and field studies provide useful information about an individual's vital signs, health condition and stress management thus improving training outcome and reducing the time to reach desired goals. The U.S. Army uses wireless and wired monitoring systems in vehicles to monitor performance and safety in real-time, the introduction of comparable systems for Soldiers has been in research and development for over 50 years.[49] A real-time wireless physiological status monitoring system was

Table 1. Description of biomedical devices types with examples and associated risk assessment summary.

Biomedical Device Type	Examples	Risk Assessment
Wearable Devices		
Wearable Trackers	Apple Watch, Microsoft Band, Fitbit bands, CGM, Garmin VivoSport	Data theft, location disclosure, unauthorized tracking, espionage, identity theft
Biomedical Clothing	AIO smart sleeve, Owlet Smart Sock, E-Skin*[34], GT Wearable Motherboard*[35], NFC smart suit[36], Smart Pajamas*[37], Hexoskin[38], BioScarf[39]	Overheating, data theft, espionage
Health Assist and Monitoring Devices	Hearing aids, electronic contact lenses*[40] or glasses[41], CGM, ECG, Muse[42], EEG, BodyGuardian Heart[43]	Disabled device, data manipulation, modification and theft
Infusion Devices	Insulin Pump, continuous drug delivery devices	Data theft, device manipulation, overdose, hospitalization, death
Implanted Devices	Pacemakers, ICDs, VADs	Data manipulation, modification and theft,
Ingestibles	Proteus Discover, Capsule Ultrasound*[44], PillCam[45]	Data manipulation, modification and theft
Healthcare Medical Devices		
Diagnostic Devices	Ophthalmoscopes, ultrasound, digital medical laboratory equipment, radiological and imaging radiological equipment (CT, MRI, PET, DEXA scan, x-ray, nuclear medicine)	Data manipulation, modification and theft, inaccurate diagnosis, internal threats, espionage, death
Monitoring Devices	Digital sphygmomanometers, ECG, ICU equipment	Data theft, data spoofing, prolonged recovery, internal threats, espionage, prolonged recovery, death
Treatment Devices	Drug dosing systems, infusion pumps, cardiopulmonary bypass (CB) devices, medical ventilators, dialysis machine and neonatal incubators	Data manipulation, modification and theft, inaccurate diagnosis, drug overdose, internal threats, espionage, prolonged recovery, death
Software Health Products		
Software Health Products	Mobile apps, health Recordkeeping and Exchange, Health Databases, medical billing software, patient medical portals	Data manipulation, modification and theft, identity theft, clinical-billing-insurance multipoint data transfer breaches, financial loss, internal threats, outdated software/operating system, espionage, supply-chain attack method, identity theft, inaccurate diagnosis, mistreatment, death

**Biomedical devices in development*

used to monitor thermal work-strain during Marine Corps training at Camp Geiger, NC, which identified trainees could be challenged more to reach a higher fitness level.[50] Such systems are able to provide individual data so that training can be tailored more effectively to reach higher output. In 2018 the Pentagon restricted the use of wearable trackers and apps that rely on geolocation for deployed service members at sensitive locations.[51] However, such devices and apps are still used by US military members and civilian employees on military installation and other locations not designated as operational areas.[52]

Biosensor development and use by US military is used to "provide combat casualty care and is targeted towards Soldiers and support personnel on battlefields."[53] The US military is investing resources into biomedical research. For example, the U.S. Air Force Office of Scientific Research is supporting research in "smart" pajamas, biomedical clothing that can monitor sleep patterns, heartrate, movement, pressure changes and posture.[54] Researchers and military personnel realize the importance of sleep in productivity, stress management, disease prevention, mental agility and improvement of decision-making skills through better sleep habits.[[55] Additionally a large number of military members suffer from hearing loss, tinnitus and other hearing disabilities therefore hearing aids or prosthetic devices are widely used.[56]

US military personnel also use to wearable devices for personal medical needs. There are a number of medical conditions that can disqualify an individual from joining the military;[57] however, if health conditions were diagnosed during the military service an individual might be allowed to continue serving. For example, Diabetes Mellitus of any type is listed as a disqualifying condition, but an active duty military member diagnosed with Type 1 Diabetes Mellitus (T1DM) is more likely to continue service with reliance on biomedical devices and telemedicine for remote locations.[58] A Soldier with T1DM has the same health needs, the same access to biomedical devices and the same vulnerabilities associated with such devices as non-military patients.

Medical devices to diagnose, monitor and treat individuals are available via multiple healthcare providers. Generally, biomedical devices whether on the Homefront or on the battlefield suffer from same cybersecurity vulnerabilities. However, some remote locations might have less availability for such devices thus reducing the associated cybersecurity threat. The DoD has worked to bridge the gap and provide needed medical care to soldiers in remote locations. Teleradiology is an example of such an effort. The US military has pioneered the implementation of teleradiology to provide access to needed services in remote locations around the world.[59] Teleradiology has enabled cost and travel time reductions, increased safety, and saved resources for the US military.[60]

Software health products, health recordkeeping and sharing systems remain vulnerable regardless of the location of soldiers since such records are in an electronic format and often stored in the cloud. Software health products also have multiple points of vulnerability as medical records and patient's PII are transferred between doctor's offices, billing services, insurance companies for reimbursement, etc.

Threats in Cybersecurity of Biomedical Devices for the Military

Biomedical device cybersecurity failures on the Homefront or battlefield can lead to serious consequences, not only for individual Soldier's health and wellbeing, but also for the overall mission success. Such threats can be grouped into three risk categories based on severity of consequences: low, moderate, and high. It is also important to highlight that the threat levels of biomedical device cybersecurity differ depending whether it is used on the Homefront or the battlefield.

This article defines low-risk threats as those with little effect on human life and mission success. Among low-risk threats on the Homefront are wearable activity trackers, from activity bands to "smart" watches. The nature of the information collected by such devices is not likely to cause injury or to affect mission. However, threats that would generally be considered low risk on the Homefront, such as the use of fitness wearables and potential loss of information collected by such technology, can have a different effect when considered in terms of battlefield effects. As most wearables today have integrated GPS capabilities, a threat of location disclosure for US forces can lead to mission failure and potentially to loss of life.

In 2017, Strava's disclosure of the heat map data visualization of its user's activities and the early 2018 uncovering of military personnel activity tracking are examples of such an operational security breach.[61] Strava is a fitness app and a self-described "social network for athletes," such as runners and cyclists, to track, analyze and share a number of workout metrics. Strava's heat map disclosed the locations of remote military bases, individual's exercise routines on base and "the identities of soldiers based there."[62] Additionally, data collected by the Polar app, another application used for exercise tracking, revealed service members' names, home addresses, deployment history locations, "soldiers' movements in hotspots like the Crimea, Baghdad, and Guantanamo" to name a few.[63] The Pentagon's subsequent restriction of wearable trackers and apps that rely on geolocation for deployed service members at sensitive locations, does not apply to US military members and civilian employees on military installations and other locations not designated as operational areas.[64]

In Ukraine, Russian information warfare units utilized the devices of individual soldiers to engage in location tracking, propaganda and disinformation, and for direct and indirect fires targeting.[65] The battlefield use of devices such as Strava, Polar, or others is no longer abstract, the tracking of military members in the field has been achieved with deadly effect.[66] All indications are that barriers to infiltrating, manipulating, tracking or otherwise harnessing personal devices used for biomedical or similar uses are rapidly disappearing as adversary nations are developing the skills to utilize our own devices against us.[67]

Moderate risk threats might have a significant effect on an individual's wellbeing and can have an effect on the mission. Hospital diagnostic equipment or software assisting clinicians with a diagnosis can cause inaccurate treatment or diagnosis, causing prolonged treatment, worsening of a health condition, mistreatment, prescription of incorrect medications, overdose and/or potentially a loss of life.

The threat of hacking a biomedical device that individuals rely on for diagnosis and treatment is particularly worrisome. And this is just not a possibility; it is a reality today. Edited medical records or malware enabled modified radiological images with removal or addition of cancerous nodules can lead to misdiagnosis and mistreatment for patients that need critical and timely care.[68] The removal of cancerous growth from X-ray images in patients with cancer led to 94% rate of misdiagnosis of such patients as being healthy.[69] The 2018 reports of malware infected computers that support biomedical devices such as MRIs and X-Rays machines demonstrated the reality of such threat.[70]

High risk threats are those that will lead to loss of life and/or complete mission failure. Devices that support or sustain life have the highest chance of causing lethal effects if compromised. Among these are implanted devices such as insulin pumps that, if compromised, can administer lethal dose of insulin. The above-mentioned risks apply to both Homefront and the battlefield. The risks of such threats on the battlefield can have larger consequences. Even if a single individual is affected during a critical mission, the consequences of such threat can lead to the whole team to be affected. Every individual on the team plays a role; hence, having even a single service member out can lead to insufficiency of resources for the mission, lack of critical skill or lack of leadership.

Researchers demonstrated unauthorized access to an implantable cardiac defibrillator and were able to retrieve name, date of birth and diagnosis, switch off saved settings, thereby leaving the device unresponsive to emergencies, remotely causing it to emit a shock.[71] Modern implantable pacemakers are also equipped with wireless connectivity and transmit data to and from the device.[72] In 2007, the cardiologist for Vice President Dick Cheney disabled the wireless functionality of the Vice President's pacemaker because of the cybersecurity risks posed by the device.[73] In 2012, researcher at Black Hat security conference demonstrated how a deadly 830-volt shock can be delivered by a pacemaker through hacking vulnerabilities in the device using a laptop computer from distance of 50-feet away from a potential victim.[74] Insulin pumps have similarly been found to have cybersecurity risks, and studies show how easy it is to gain unauthorized access to the device to disable it, cause delivery of modified amount of insulin or empty the content of the pump into the patient to deliver a lethal dose of the medication.[75]

The increased connectivity of multiple devices poses additional challenges. Synchronization of biomedical devices with smartphones, computers and other non-biomedical technology by design is becoming a use-driven demand from industry and consumers. A Wireless Body Area Network (WBAN) is a "sensor network that enables various medical sensors located inside or outside the human body to communicate seamlessly with one another, and integrate automatically with existing devices, such as smartphones".[76] There are challenges in securing WBAN not only because of the connectivity among multiple devices, but also because the individual is often on the move along with the network.

The DoD should also start thinking beyond visible wearable devices. The FDA has started regulating precision medical devices such as next generation sequencing (NGS) technology that can now examine genomic variances of a large number of individuals at the same time to determine if an individual has certain health conditions or is at a risk of a disease.[77] The DoD should take note of such technology and how it can affect US military. In particular, the potential of NGS technology to quickly detect health conditions and target individuals should be of great concern.

CONCLUSION

The DoD is investing significant resources both in financial and intellectual capital to improve soldier survivability on the battlefield to ensure mission success. Using biomedical technology and the development of lighter, more efficient toolkits, the DoD is preparing warfighters for technologically advanced conflicts. To outsmart the other side, the US military must be aware of and capable at battling cyber espionage, cybercrime, and other cyber threats. Biomedical technologies are becoming increasingly essential tools in modern conflict. Consequently, the cybersecurity threats to such technologies cannot be ignored. It is important to prepare US military personnel for the biomedical cybersecurity threats of today as well as proactively analyze and address critical threats that will arise in the future. The DoD should consider biomedical security from the micro to the macro scale, from the vantage point of an individual, team, DoD, and the nation.

It is important to conduct education, training, active learning and regular reviews of potential cyberthreats to develop awareness on an individual level. Individual awareness of cybersecurity vulnerabilities to biomedical devices and associated systems begins the process of identifying potential risks and threats affecting individual health situations. It is vital to prepare and educate individuals to be conscious of biomedical cyber threats affecting them at the Homefront or the battlefield. One individual's actions can significantly affect a mission, the safety of a team and the security of the nation. The DoD would benefit from adopting the Patient Centric Cybersecurity Framework as a tool to empower the workforce and foster trust, effective communication, and more accurate data flows to enhance decision-making processes.[78]

Every US military unit and team should take stock of biomedical devices in use on and off duty to ensure awareness, be proactive in assessing potential threats, and determine how to avoid or correct issues. The DoD should elevate the security of biomedical devices in use by the military to a level of strategic importance. This does not only apply to combat biomedical devices, but also to biomedical devices for personal use. The DoD should effectively regulate such devices via policy to ensure the fidelity of medical devices, and should raise awareness via workforce education, research, internal reviews as well as cooperation and teamwork against cyber-criminal networks exploiting biomedical devices. These efforts should span multiple levels with the intent of fostering best practices and creating synergies better able to detect and combat malicious behaviors. Biomedical devices used by the general population are also used by military personnel. The device ecosystems are deeply intertwined and vulnerabilities within biomedical devices within either the military or the civilian sectors of biomedical devices, are unlikely to stay segregated from one another. The result is that both are exposed to increased levels of risk.

Finally, US military and the Department of Veterans Affairs acquisitions within the broader landscape of the US healthcare market are large and expanding. While the arbitrary implementation of wide-ranging regulation should be avoided, the DoD's directed and conscientious effort to provide better implementation of cybersecurity for biomedical devices will be a significant factor in future conflicts. Moreover, DoD innovations in biomedical cybersecurity will assure better outcomes for the nation as a whole.

NOTES

1. Jamin Casselman, Nicholas Onopa, and Lara Khansa, “Wearable healthcare: Lessons from the past and a peek into the future,” *Telematics and Informatics,* 34, no. 7 (2017): 1011-1023, https://doi.org/10.1016/j.tele.2017.04.011.
2. Matteo Langone, Roberto Setola, Javier Lopez, “Cybersecurity of Wearable Devices: An Experimental Analysis and a Vulnerability Assessment Method,” *IEEE 41st Annual Computer Software and Applications Conference (COMPSAC)* (2017): 304-309, doi: 10.1109/COMPSAC.2017.96.
3. “The Cost of a Data Breach,” *Briefings on HIPAA*, Health Services Administration: USA, 16, no.11 (2016): 4-7.
4. “Cybersecurity Reference and Resource Guide,” U.S. Department of Defense (2019), updated February 2020, https://dodcio.defense.gov/Portals/0/Documents/Cyber/2019%20Cybersecurity%20Resource%20and%20Reference%20Guide_DoD-CIO_Final_2020FEB07.pdf.
5. “National Cyber Strategy of the United States of America,” National Cyber Strategy, The White House, Washington, D.C. (2018), https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.
6. “Definition of biomedical engineering”, *Merriam-Webster Dictionary*, accessed February 25, 2021, https://www.merriam-webster.com/dictionary/biomedical%20engineering.
7. “Digital Health Innovation Action Plan,” U.S. Food and Drug Administration (2017), accessed February 25, 2021, https://www.fda.gov/media/106331/download.
8. “CDRH Mission, Vision and Shared Values,” U.S. Food Drug Administration (2017), accessed February 25, 2021, https://www.fda.gov/AboutFDA/CentersOffices/OfficeofMedicalProductsandTobacco/CDRH/ucm300639.htm
9. “2018-2020 Strategic Priorities, Center for Devices and Radiological Health,” U.S. Food and Drug Administration (2018), accessed February 25, 2021, https://www.fda.gov/downloads/AboutFDA/CentersOffices/OfficeofMedicalProductsandTobacco/CDRH/CDRHVisionandMission/UCM592693.pdf.
10. “Code of Federal Regulations – Title 21 – Food and Drugs”, USCODE-2010 – Title 2 – Chapter 9 – subchapter V – Part A – Section 360c, Classification of Devices Intended for Human Use (2018), accessed February 25, 2021, https://www.govinfo.gov/content/pkg/USCODE-2010-title21/pdf/USCODE-2010-title21-chap9-subchapV-partA-sec360c.pdf.
11. Adam Thierer, “The Internet of Things and Wearable Technology: Addressing Privacy and Security Concerns without Derailing Innovation,” *Richmond Journal of Law & Technology,* 21, no.2 (2015), http://dx.doi.org/10.2139/ssrn.2494382.
12. Sara Shahrimi, “Wearing Your Data on Your Sleeve: Wearables, the FTC, and the Privacy Implications of This New Technology,” *Texas Review of Entertainment Sports Law,* 18, no.1 (2017): 1-25.
13. Gilsoo Cho, Seungsin Lee, and Jayoung Cho, “Review and Reappraisal of Smart Clothing,” in S*mart Clothing: Technology and Applications*, ed. Gilsoo Cho, (CRC Press, 2009).
14. Ibid.
15. Andreas Lymberis and Silas Olsson, “Intelligent Biomedical Clothing for Personal Health and Disease Management: State of the Art and Future Vision,” *Telemedicine Journal and e-Health*, 9, no. 4 (2004), http://doi.org/10.1089/153056203772744716.
16. C.A. Winterhalter et al., "Development of electronic textiles to support networks, communications, and medical applications in future U.S. Military protective clothing systems," *IEEE Transactions on Information Technology in Biomedicine,* 9, no. 3 (2005): 402-406, doi: 10.1109/TITB.2005.854508.
17. Jihun Park et al., “Soft, smart contact lenses with integrations of wireless circuits, glucose sensors, and display,” *AAAS, Science Advances*, 4, no. 1 (2018) doi: 10.1126/sciadv.aap9841.
18. T. Elakkiya, "Wearable safety wristband device for elderly health monitoring with fall detect and heart attack alarm," IEEE 2017 Third International Conference on Science Technology Engineering & Management (2017): 1018-1022, doi: 10.1109/ICONSTEM.2017.8261318.
19. Jim Li and Yukiya Sawanoi, "The History and Innovation of Home Blood Pressure Monitors," 2017 IEEE History of Electrotechnolgy Conference (2017): 82-86, doi: 10.1109/HISTELCON.2017.8535736.
20. Hatice Koydemir and Aydogan Ozcan, “Smartphones Democratize Advanced Biomedical Instruments and Foster Innovation”, *Clinical Pharmacology & Therapeutics Development,* 104, no. 1 (2018), https://doi.org/10.1002/cpt.1081.
21. Junyi Wang et al., “Capsule Ultrasound Device: Characterization and Testing Results,” IEEE International Ultrasonics Symposium (2017): 1-4, doi: 10.1109/ULTSYM.2017.8092071.
22. “Proteus digital health” (2020), accessed May 21, 2020, https://www.proteus.com/discover/.

NOTES

23. Jonah Comstock, “California hospital becomes first in US to prescribe ingestible sensors from Proteus,” *MobiHealthNews*, (2016), accessed May 21, 2020, https://www.mobihealthnews.com/content/california-hospital-becomes-first-us-prescribe-ingestible-sensors-proteus.
24. “Tiny Ingestible Sensor Aids Rush Doctors, Patients,” Rush University Medical Center (2017), accessed February 25, 2021, https://www.rush.edu/news/tiny-ingestible-sensor-aids-rush-doctors-patients.
25. “Final Document: Software as a Medical Device (SaMD): Clinical Evaluation,” International Medical Device Regulators Forum *(IMDRF)*, Software as a Medical Device Working Group (2017), http://www.imdrf.org/docs/imdrf/final/technical/imdrf-tech-170921-samd-n41-clinical-evaluation_1.pdf.
26. “21st Century Cures Act,” PUBLIC LAW 114-255, 114th Congress (2016), https://www.congress.gov/114/plaws/publ255/PLAW-114publ255.pdf.
27. Dan Munro, “Cyber Attack Nets 4.5 Million Records from Large Hospital System,” Forbes (2014), accessed May 21, 2020, https://www.forbes.com/sites/danmunro/2014/08/18/cyber-attack-nets-4-5-million-records-from-large-hospital-system/#69647ff77f07.
28. Daniel Nigrin, “When ‘Hacktivists’ Target Your Hospital,” *New England Journal of Medicine*, 371, no. 5 (2014): 393-395, doi: 10.1056/NEJMp1407326.
29. “2018 Cost of Data Breach Study: Impact of Business Continuity Management,” Ponemon Institute (2018), accessed February 25, 2021, https://www.ibm.com/downloads/cas/AEJYBPWA.
30. Ibid.
31. Ibid.
32. Ibid.
33. “The Cost of a Data Breach,” Briefings on HIPAA, Health Services Administration: USA, 16, no. 11 (2016): 4-7.
34. Takao Someya, “Bionic Skin for a Cyborg You,” *IEEE Spectrum* (2013), accessed February 25, 2021, https://spectrum.ieee.org/biomedical/bionics/bionic-skin-for-a-cyborg-you.
35. “Georgia Tech Wearable Motherboard™: The Intelligent Garment for the 21st Century,” Georgia Tech, accessed May 21, 2020, http://www.smartshirt.gatech.edu.
36. “CES 2016: NFC-Enabled Wearables, IoT Home Systems, And Sunburn Sensors,”, NFC Forum (2016), https://nfc-forum.org/ces-2016-nfc-enabled-wearables-iot-home-systems-and-sunburn-sensors/.
37. “Smart sleepwear: Introducing 'phyjama,' a physiological-sensing pajama,” *Science Daily,* source: University of Massachusetts at Amherst (2019), accessed February 25, 2021, https://www.sciencedaily.com/releases/2019/09/190912162528.htm.
38. “HEXOSKIN Health Sensors and AI,” *HEXOSKIN* Smart Garments Specifications, accessed May 21, 2020, https://www.hexoskin.com.
39. “The 1st scarf with air pollution, allergy, cold & flu protection built right in!” *BioScarf,* accessed May 21, 2020, https://www.bioscarf.com.
40. “Electronic Contact Lenses for Better Vision,” *Med Gadget* (2008), accessed May 21, 2020, https://www.medgadget.com/2008/01/electronic_contact_lenses.html.
41. “Top 5 Electronic Glasses for the Blind and Visually Impaired,” IrisVision, accessed May 21, 2020, https://irisvision.com/electronic-glasses-for-the-blind-and-visually-impaired/.
42. “EEG-Powered Sleep: Tracking & Meditation,” *Muse,* accessed May 21, 2020, https://choosemuse.com.
43. “Listen to the Beat,” *BodyGuardian Heart*, accessed May 21, 2020, https://www.preventicesolutions.com/patients/body-guardian-heart.
44. Benjamin Cox et al., “Ultrasound capsule endoscopy: sounding out the future,” *Annals of Translational Medicine*, 5. no. 9 (2017), https://doi.org/10.21037/atm.2017.04.21.
45. “PILLCAM™ SB 3 SYSTEM,” Medtronic, accessed May 21, 2020, https://www.medtronic.com/covidien/en-us/products/capsule-endoscopy/pillcam-sb-3-system.html.
46. “Wearable sensors could leverage biotechnology to monitor personal, environmental data,” CCDC Army Research Laboratory Public Affairs (2019), accessed May 21, 2020, https://www.army.mil/article/221184.
47. Gilsoo Cho, Seungsin Lee, and Jayoung Cho, “Review and Reappraisal of Smart Clothing,” in *Smart Clothing: Technology and Applications,* ed. Gilsoo Cho (Boca Raton, FL: CRC Press, 2009).

NOTES

48. Reed Hoyt, Karl Friedl, “The future of wearable tech,” U.S. Army (2016), accessed May 21, 2020, https://www.army.mil/article/161761/the_future_of_wearable_tech.
49. Ibid.
50. Ibid.
51. Tara Copp, “Fitbits and fitness-tracking devices banned for deployed troops,” *Military Times* (2018), accessed May 21, 2020, https://www.militarytimes.com/news/your-military/2018/08/06/devices-and-apps-that-rely-on-geolocation-restricted-for-deployed-troops/.
52. “Use of Geolocation-Capable Devices, Applications, and Services,” Deputy Secretary of Defense, Memorandum (2018), accessed May 21, 2020, https://partner-mco-archive.s3.amazonaws.com/client_files/1533573228.pdf.
53. Rainee Simons, “Body-Sensor Networks for Space and Military Applications,” in A*ntennas and Propagation for Body-Centric Wireless Communications*, 2nd ed. Peter Hall, Yang Hao (New York: Artech House, Inc., 2012), 271-290.
54. “‘Smart’ pajamas could monitor and help improve sleep,” American Chemical Society (2019), accessed May 21, 2020, https://www.acs.org/content/acs/en/pressroom/newsreleases/2019/april/smart-pajamas-could-monitor-and-help-improve-sleep-video.html.
55. Ibid.
56. Larry Humes, Lois Joellenbeck, and Jane Durch, eds., *Noise and Military Service: Implications for Hearing Loss and Tinnitus*, Institute of Medicine (Washington, D.C.: The National Academies Press, 2006), https://doi.org/10.17226/11443.
57. “Join the Military: Eligibility Requirements. Medical Conditions That Can Keep You From Joining the Military,” *Military.com*, accessed May 21, 2020, https://www.military.com/join-armed-forces/disqualifiers-medical-conditions.html.
58. Sammy Choi and Jon Cucura, “US Army Soldiers With Type 1 Diabetes Mellitus,” *Journal of Diabetes Science and Technology*, 12, no. 4 (2018), 854-858, https://doi.org/10.1177/1932296818767700.
59. E.R. Ranschaert and Barneveld Binkhuysen, “Teleradiology: Evolution and Concepts,” *European Journal of Radiology*, 78 no. 2 (Elsevier Ireland Ltd, 2011), 205-209, doi:10.1016/j.ejrad.2010.08.027.
60. M.R. Brumage, S. Chinn, and K. Cho, “Teleradiology in a Military Training Area,” *Journal of Telemedicine and Telecare*, 7, no. 6 (2001), 348-52, doi:10.1258/1357633011936994.
61. Katelyn Newman, "Fitness App Strava Reveals Military Security Oversight," *USNews.com* (2018,) accessed May 5, 2019, Gale General OneFile, https://link.gale.com/apps/doc/A525573438/ITOF?u=viva_vpi&sid=ITOF&xid=ca0fc22a.
62. "How Strava's Heat Map Uncovers Military Bases," *NYTimes.com Video Collection*, World History in Context (2018), accessed May 5, 2019, https://link.gale.com/apps/doc/CT526718358/WHIC?u=viva_vpi&sid=WHIC&xid=0cbc492f.
63. "After Strava, fitness app Polar exposes location history of soldiers and spies," *Media Nama* (2018), Computer Database, accessed May 5, 2019, https://link.gale.com/apps/doc/A545911140/CDB?u=viva_vpi&sid=CDB&xid=71107de7.
64. Tara Copp, “Fitbits and fitness-tracking devices banned for deployed troops,” *Military Times* (2018), accessed May 21, 2020, https://www.militarytimes.com/news/your-military/2018/08/06/devices-and-apps-that-rely-on-geolocation-restricted-for-deployed-troops/.
65. Aaron F. Brantly, Nerea Cal, and Devlin Winkelstein, “Defending the Borderland: Ukrainian Military Experiences with IO, Cyber, and EW,” T*he Cyber Defense Review* (2017), https://cyberdefensereview.army.mil/Portals/6/Documents/UA%20Report%20Final%20AB.pdf.
66. Jeff Roberts, “How Russia Used a Poisoned App to Spy on Ukraine’s Military,” *Fortune* (2016), accessed February 25, 2021, https://fortune.com/2016/12/22/russia-ukraine-app/.
67. Aaron F. Brantly and Liam Collins, “A Bear of a Problem: Russian Special Forces Perfecting Their Cyber Capabilities,” *Army Magazine*, 68, no. 12 (2018).
68. Kim Zetter, “Hospital viruses: Fake cancerous nodes in CT scans, created by malware, trick radiologists,” *The Washington Post* (April 3, 2019), accessed May 21, 2020, https://www.washingtonpost.com/technology/2019/04/03/hospital-viruses-fake-cancerous-nodes-ct-scans-created-by-malware-trick-radiologists/?noredirect=on&utm_term=.5e1b44764063.
69. Michael Kan, “Scary Hacking Threat: Editing X-Ray Images to Add or Remove Cancer,” *PCmag* (2019), accessed May 21, 2020, https://www.pcmag.com/news/367598/scary-hacking-threat-editing-x-ray-images-to-add-or-remove.
70. Ibid.

NOTES

71. Neal Leavitt, “Researchers Fight to Keep Implanted Medical Devices Safe from Hackers,” *Computer*, 43, no. 8 (Washington, D.C.: IEEE Computer Society Press, 2010), 11-14, doi: https://doi.org/10.1109/MC.2010.237.

72. Aaron F. Brantly, “The Violence of Hacking: State Violence and Cyberspace,” *The Cyber Defense Review* (2017), 73-92, doi:10.2307/26267402.

73. Daniel Clery, “Could your pacemaker be hackable?” *Science*, 347, no. 6221, (AAAS, 2015): 499, https://science.sciencemag.org/content/sci/347/6221/499.full.pdf.

74. Mandeep Khera, “Think Like a Hacker,” Journal of Diabetes Science and Technology, 11, no. 2, (2016): 207-212, doi:10.1177/1932296816677576.

75. David Klonoff, “Cybersecurity for Connected Diabetes Devices,” *Journal of Diabetes Science and Technology*, 9, no. 5 (2015): 1143-1147, https://doi.org/10.1177/1932296815583334.

76. Jamin Casselman, Nicholas Onopa, and Lara Khansa, “Wearable healthcare: Lessons from the past and a peek into the future,” *Telematics and Informatics*, 34, no. 7 (2017): 1011-1023, https://doi.org/10.1016/j.tele.2017.04.011.

77. “FDA Advances Precision Medicine Initiative by Issuing Draft Guidances on Next Generation Sequencing-Based Tests,” U.S. Food and Drug Administration, (2016), accessed February 25, 2021, https://www.fda.gov/NewsEvents/Newsroom/PressAnnouncements/ucm509814.htm.

78. Aaron F. Brantly and Nataliya D. Brantly, “Patient-centric cybersecurity,” *Journal of Cyber Policy*, 5, no.3 (2020): 372-391, https://doi.org/10.1080/23738871.2020.1856902.