2021

COVID-19 and Biocybersecurity's Increasing Role on Defending Forward

Xavier Palmer
Old Dominion University, xpalmer@odu.edu

Lucas N. Potter
Old Dominion University, lpott005@odu.edu

Saltuk Karahan
Old Dominion University, skarahan@odu.edu

Original Publication Citation

Palmer, X., Lucas, N. P., & Saltuk, K. (2021). COVID-19 and biocybersecurity's increasing role on defending forward. *International Journal of Cyber Warfare and Terrorism (IJCWT)*, 11(3), 15-29. https://doi.org/10.4018/IJCWT.2021070102

International Journal of Cyber Warfare and Terrorism
Volume 11 • Issue 3 • July-September 2021

COVID-19 and Biocybersecurity's Increasing Role on Defending Forward

Xavier Palmer, Old Dominion University, USA
Lucas N. Potter, Old Dominion University, USA
Saltuk Karahan, Old Dominion University, USA

ABSTRACT

The evolving nature of warfare has been changing with cybersecurity and the use of advanced biotechnology in each aspect of the society is expanding and overlapping with the cyberworld. This intersection, which has been described as "biocybersecurity" (BCS), can become a major front of the 21st-century conflicts. There are three lines of BCS which make it a critical component of overall cybersecurity: (1) cyber operations within the area of BCS have life threatening consequences to a greater extent than other cyber operations, (2) the breach in health-related personal data is a significant tool for fatal attacks, and (3) health-related misinformation campaigns as a component of BCS can cause significant damage compared to other misinformation campaigns. Based on the observation that rather than initiating the necessary cooperation COVID-19 helped exacerbate the existing conflicts, the authors suggest that BCS needs to be considered as an essential component of the cyber doctrine, within the Defending Forward framework. The findings are expected to help future cyber policy developments.

KEYWORDS

Bio-Security, Biocybersecurity, Cyberbiosecurity, Defense, Security

INTRODUCTION

The discussion of the evolution of cyber warfare requires the discussion of the consequences in terms of their impacts. One analysis of papers found that between 2010 and 2020, the notion of cyber attacks has been normalized and that in some articles, civilian losses go unmentioned, if not downplayed, despite the compared impact of tools employed (Sallinen, 2021). This indicates that the effects of cyberwarfare and cyber weapons in security studies may underestimate biological casualties when taking into account past or possible consequences of cyber conflict versus the impact on targeted facilities. Throughout the history of warfare, humans have witnessed countless modes of weaponry from rocks to nuclear warheads of which each advancement has raised the stakes and risks in engagement in direct losses, making cyberwarfare, which has been seen by the lay public in a largely computational lens, seem benign. The exception, of course, is within cases concerning ransomware and news regarding the targeting of public infrastructures such as hospitals or connected spaces (Martin et al., 2017; Spence et al., 2018). This view is not rare in consideration of modern

DOI: 10.4018/IJCWT.2021070102

cyber conflicts between rival powers as losses are primarily incurred in terms of financial loss, infrastructure functionality, corruption of data, and dismantling of logistics, and more, resulting in the reduction of direct human casualties that would be caused through use of munitions (Brenner and Clarke 2009; Evans, 2020; Metzger 2020; Moreno and Lovaas 2020; Sallinen, 2021).

In delineating the difference between cyberwar and cyber-crime, as they are sometimes used in similar instances, a core difference lies in state sponsorship or linked infrastructure of the attacks, combined with or otherwise operationally linked to armed force (Maurushat, 2013).For example, Nation A sending criminals to Nation B can be seen as hostile while not being engaged in warfare. Alternatively, for Nation A to send a battalion of soldiers would be almost unequivocally seen as warfare. The contexts of each action will differ. It is difficult to put an exact number on what number of troops or which actions elevate hostilities to war-time actions, and it is reasonable to believe that the exact number will be nebulous as the exact manpower to constitute an act of war would depend on particulars and rationale of the nations involved for such an action. As some nations engage in acts without fully declaring war, enlarging the frame for cyberwar in contexts in which nation-states utilize cyber attacks in an organized manner as a part of war-time or war-time adjacent acts is helpful for discussion and may reflect a helpful measure of defense. In the midst of conflicting literature, the authors lean towards Brenner's (2006) cyberware definition which reflects virtual conduct of military operations as they sufficiently ground the context of warfare (Brenner, 2006). Otherwise, such hostile acts, unconnected to state-actors and armed conflict, can be framed as cybercrime.

DIGITALIZATION OF BIOLOGY AND HINTS OF POSSIBLE ATTACKS

Despite this delineation, it is possible that the line between cybercrime and cyberwar may yet still find itself blurred through the overlap of the domain of biology, given biology's increasing digitalization and versatility of access. Vast research has demonstrated that health can be personalized, and aspects of it can be digitalized, allowing increasing access to human lives directly and presenting increased risk (DiEuliis et al, 2018; Berger et al, 2019). Threats to life at this intersection are quite a few for now, but may soon be found on the increase. A hint was given in September of 2020, wherein it was believed that a German patient was a fatality due to a ransomware attack. However, this later proved not to be the case, and the patient was in critical enough condition that the fatality was inevitable (Goodin, 2020; O'Neill, 2020). This, however, highlights the possibility of the case and suggests it as being a matter of when, not if, a ransomware attack can cripple hospital functions enough to cause a fatality. Considering the increase in ransomware utilized, it is relatively uncommon for lay people to think of the deaths that can occur in such cyber attacks, but this is can change (Habibzadeh et al, 2019). There is good reason to believe that bridging the digital world and biology can be further abused, and for this reason, the authors see it important discuss the emerging discipline that addressed this intersection cyberbiosecurity (Murch et al., 2018; Peccoud et al., 2018). For this paper, the authors alternatively refer to it as biocybersecurity (BCS), emphasizing the biological factors, such as physical elements like DNA or contextualized information about them in digital form, that can be used and targeted as an interlock in critical systems reliant on biometrics for authentication or processing, like hospitals. In time, cyber means can be used to select and attack demographics of populations with precision, targeting specific biological materials and qualities, from repositories in hospitals, private companies that amass citizen data, and/or personal devices. The exploitation of BCS, if performed on behalf of a nation-state, increases the potential for destruction in what could be called biocyberwarfare, that is, the exploitation of intersectional vulnerabilities in BCS as or accompanying the use of force for war-time, geopolitical gain.

What this means for the everyday individual is that aspects of modern society that are vital for everyday living such as agriculture, healthcare, fashion, policing, and energy may become new targets for exploitation from a new angle of attack: cyber attacks with a biological interlock (Baker et al, 2019; Duncan et al, 2019; George, 2019; Mantle et al, 2019; Potter and Palmer, 2020). Anyone who

is creative enough, from the individual level to the state-level, and is endowed with the resources to leverage BCS vulnerabilities may in time beable to modify specific biological components, interface them with a computer system, and the effects of this can be magnified for actors as biocomputing and bio-based storage gain increased prominence (Katz, 2015; Goni-Moreno and Nikel 2019; Wang et al. 2019). It is worth emphasizing that state-actors are much more capable, but their level and funding are increasingly less a limiter for bio-based attacks given the increasing accessibility of biotechnology. This potential reflects that the assets susceptible to these attacks must be defended, and the necessity of the defense will only increase over time. This does not bode well for efforts of providing adequate national cyber defense, given that many countries are struggling to address current gaps in their cyber defenses.

JUSTIFICATION OF BCS AS ALTERNATIVE TO "CYBERSECURITY IN THE HEALTHCARE SECTOR"

Mild critique may exist with respect to the use of BCS versus referring to such matters as simply cybersecurity within the healthcare sector, but the authors support BCS/CBS as its own field as with many authors who have put in deep work in establishing the field (DiEulis et al., 2018; Murch et al., 2018; Peccoud et al., 2018; Richardson et al, 2019; Schabacker et al, 2019; Potter and Palmer, 2020; Turner, 2019). The authors in this paper posit three chief, but not limiting points, which are that:

- **A:** The increased inclusion of biology as interlocks or foundational units in computational and otherwise cyber processes limits the role and rationale for keeping IT centered. Example technologies within the domain are: Biometric authentication, DNA-based computation and data storage, digitalization of medical records and gesture-based entry, and Brain-Computer Interfaces, and more are on the way (DiEulis et al., 2018; Murch et al., 2018; Peccoud et al., 2018; Potter and Palmer, 2020).
- **B:** Many biological processes are no longer simply the end result of data processing and require specialized training quite distant from IT training to troubleshoot adequately. Further, many of these processes are not exclusive to healthcare. (Dieuliis et al, 2018; Potter and Palmer, 2020)
- **C:** BCS addresses a temporal matter in that biological processes are taking over aspects of digital aspects in many emerging technologies, and traditional interfaces are likely not remain -- that is, BCS better describes the direction of shifting the center of the foundation of these technologies, which are nowhere, in development, and or are in conceptualization.

Together, these points motivate the authors to move the centering of the topic from cybersecurity towards the intersection of the fields of cybersecurity, cyber-physical security, and biosecurity while emphasizing the lead or primacy that exists in biology as traditional means of conceptualizing IT become less relevant.

BCS AND DEFEND FORWARD

It is also fair to ask where the US stands with its cyber defense strategy as biology increasingly comes into consideration (Hester, 2019). Currently, the US is undergoing a shift from a defensive to an offensive stance in what is referred to as "Defending Forward" (DF), as is exemplified in the 2018 Department of Defense (DoD) Cyber Strategy, which states that the DoD "will *defend forward* to disrupt or halt malicious cyber activity at its source, including activity that falls below the level of armed conflict." The scope of this strategy has been explained by Kosseff with "three general components: (1) positioning to degrade cyber operations; (2) warning to gather information about threats and inform defenses; and (3) influencing adversaries to discourage them from deploying cyber

operations against the United States." (Kosseff, 2019). The first component "positioning" is a most critical component and the case for its legitimacy under international law is based on equivalency of an intrusive positioning to the battlefield preparation in conventional warfare (Chesney, 2018). An immediate and persistent engagement between the US and its adversaries in cyberspace remains, but grounding positions pose a difficulty. For example, once an IP address is determined to be the source of malicious activity on DoD networks, establishing a posture to be able to degrade adversarial actions is considered a legitimate activity. However, there exist many questions within the DF framework. For example, it is worth asking to what degree entities such as the DoD ought to conform malicious intent before acting in cyberspace or a bio-cyberspace as it develops. The bio-cyberspace differs from cyberspace in that it includes a direct connection to physical, biological components. Further, it is important to ask what basic security protocols should be within a Defend Forward stance in the future, which is increasingly biological. Plainly, what does DF mean to BCS? In this article, the authors aim to explore, but not definitely, possible answers to such questions in light of COVID-19 and other health-related paradigms. The authors do this through discussion of how COVID-19 fits within the paradigm of BCS, how BCS may open further difficult to predict routes of attack based on our current defensive frameworks, why biocyberwarfare may become attractive, a case for Defend Forward, how DF can be augmented through the inclusion of BCS, and projections of both BCS and DF working at the operational level. However, to note, the sheer breadth and novelty, and need for the development of the latter, a comprehensive framework of BCS and DF, restricts discussion of such an exploration. Thus, the authors aim to open discussion within the course of this work.

HOW COVID-19 FITS WITHIN THE PARADIGM OF BCS

The meaning of cybersecurity during the COVID-19 pandemic is multifaceted and is a proper question of the growing field of BCS. To reiterate from above, Murch et al. (2018) describe this new and hybridizing field as one wherein security relating to cyber-physical systems, biosecurity, and general cybersecurity meet. Peccoud et al. (2018) rightly support this by identifying how cyber-physical processes are inherent in biotechnology workflows. As COVID-19 is being addressed by biotechnological equipment, research is being protected through cybersecurity protocols to protect from sabotage and espionage, and this makes COVID-19, by extension, a matter of BCS and thus cybersecurity, as it exists within the heart of biosecurity. Many security professionals previously considered just the cyber aspect of vulnerabilities posed concerning healthcare, but they have been recently given reason to think of how biology can play a role as well (Murch et al. 2018). That is, how can people use aspects of biology to produce physical or cyber-attacks, or how can cyber security-based exploits be used to thwart biologics-based efforts such as medical relief efforts or testing. From the cybersecurity side, this can come in the form of people producing phishing campaigns under the guise of COVID-19 testing or related economic relief, people stealing vital research from labs aiming to either study COVID-19 or produce vaccines to COVID-19, or simple stalling or disruption of vaccine logistics. Another route could be through the overwhelming hospital systems, to the degree that overrides concerns of pre-existing conditions in current medical records; this would not be much different from a DDoS attack, except in physical form. An already demonstrated path with CT-Scans, but not yet adapted for COVID-19 shows that one can simply install malware which can produce false positives and negatives on machines; hypothetically, one may find an adaptation created for Covid-19, wherein electronic tests could be rigged to give false results and improperly triage infected patient (Mirsky, 2019). One more route could be through biomimicry via malware which mimics Covid-19 pathology.For example, Davis (2020) highlighted a route in which a hypothetical malware with bahvioral qualities like Covid-19 could be effective. Such malware could have at least two versions, where in an asymptomatic minority variant is benign while others wreck havoc on infected computing systems (Davis, 2020). This does not yet address the physical and biological, yet cyber route of attack which is unconventional, but these, themselves, could prove effective. A combination

of these could be used to product chaos within another nation without firing a single shot, giving emphasis to teams skillful behind the keyboard. As Xie (2020) notes, it COVID-19 gives reason to reconsider cybersecurity and the new normal which it may present. However, changes addressing just convential and marginally new avenues of attacks may fall short in BCS.

BCS'S POSSIBILITY OF OPENING FURTHER LESS PREDICTABLE ROUTES OF ATTACK

Marushat (2013) noted unconventional cyber attacks, utilized across the world since the 1980s, from examples such as WANK to STUXNET, and that intrusions have evolved. The value in the effectiveness of unpredictable attacks, coupled with the evolving nature of attacks, lends the question of where the next wave of attacks may emerge. As Maurushat (2013) presented, security may be through obscurity or, its replacement, through absurdity. The flip side is that such an approach can also refer to exploits of vulnerabilities. The notion of absurd vulnerabilities which made the route of biology more relevant came through the work of Ney (2017), as his team demonstrated that the use of DNA in a remote attack, through which synthetic DNA could be used to deliver malware to a computer system via a sequencing utility. This attack was novel at the time in that it signaled that bio to digital attacks were possible, and other researchers have since investigated other bio-related avenues, be it hacking, such as the feasibility of hacking DNA in supply chain systems or means that might take one-day bridge research that allows for smarter means of hacking such as direct data transfer to cells or undermining bio-inspired security in the future (Bitam et al, 2016; Berezow, 2021; Gent, 2021). Additional evolutions might be seen, depending on the continued growth of biotech paired with the ingenuity of hackers, but the extent is unclear.

COVID-19 may yield a clue to one continued branch in absurd exploits. Already through it, widespread travel, trade, and relations have been disrupted, and for a good reason. COVID-19 targets multiple tissues and organs, allowing for an embedding in multiple areas of one's body and present symptoms that can last at least months as noted by Fraser (2020). Similar to an infected computer in a network, just one person carrying this biological virus is a pathway to attacking an entire community (Rothrock, 2020). Additional variants, which may hamper vaccination development and distribution efforts, also exist (Koyama et al, 2020). With reflection on how biotechnology costs have been dropping and accessibility has been increasing, it is possible that COVID-19 could be modified into fiercer threat through malicious tampering via the work of clever, malicious actors who might one day use increasingly accessible equipment to amplify its effect. This can mean tweaking of COVID-19 itself or an analogue, though commonly accessible open-sourced software combined with more easily accessible DIY biology equipment, to produce a variant that is capable of either confounding the results of testing or increasing hospitalizations. Althernatively, they could then use this pervasive virus or variants as a new interlock for attacks on the efficacy of facilities such as hospitals or policing centers or as a means of injecting malicious code. To restate and refocus, this threat could come through the work of a malicious actor who creatively uses COVID-19 as a biological interlock within an attack on a facility, building on prior work with the understanding that an infected individual or their samples may be processed and be the needed means of delivery.

The tools for the manipulation of genetic material are easily accesible, cheap, versatile, and have been available for several years (Belhaj et al, 2015; Caplan et al, 2015). Use of such tools, like Crispr, are now a matter of art in some circles, and these tools are widespread enough that the ability to stop their profileration or use is unrealistic, not that they should be, especially since citizen scientists within this domain can be instrumental in assisting in matters of biosecurity and education and have established modes of governance that are important for understanding and guiding community embrace of biotechnology (Dumitriu and Goldberg, 2019; Kuiken, 2016; Pearlman, 2017; Thomas et al, 2017). However, Gronvall and West (2020) note that the potential for malicious use of gene editing remains; and noting this, continued cooperation with all users of this class of technology

is essential. Governments will need the means to protect against emergent threats that can arise through the use of these tools, and to that end, the meaning of cybersecurity during the COVID-19 pandemic is essentially a chance to evolve, think, and dream bigger for what cybersecurity needs to be. It will also require greater degrees of cooperation between governments and citizens. Government organizations have success through their outreach to DIY Biohackers, but this success has not been universal, as noted by Wolinsky (Wolinski, 2016). If these attitudes remain incongruous worldwide, it is perhaps time for a rethink in efforts to addressing BCS frameworks. Weil and Murugesan (2020) point out that resilience is possible, and much can be learned from IT, which has and continues to facilitate many industries and activities disrupted by COVID-19. However, this may only continue as an intersectional policy focused on preparedness, effective responses, and honest critiques combined with growth are allowed unabated.

CONSIDERATIONS ON THE PREFERABILITY OF CYBER WARFARE AND THUS BIOCYBERWARFARE

It is helpful to consider the advantages that countries can gain from opting for cyberwarfare versus conventional means of warfare. Daggett (2010) noted that the cost of US military campaigns has risen over time (Daggett 2010). When accounting for the costs of troop deployment as well as the economic manpower denied through it, these costs can prove unattractive for modern nations to match. Costs rise substantially through consideration of troop quality of life and their families back home. From there, moral costs mount considerably and at a higher rate compared to a focused cyber warfare campaign. Economic losses from munitions left on battlefields and disrupted lives can further multiply costs. In contrast, a viable and protracted cyberwar campaign can easily be constrained to a much less amount. This means that destruction can be achieved with and limited to relatively cheap computers and other electronics connected to the internet, to attack from as far as an internet connection will allow an agent's devices to reach. Losses and costs can be cut considerably, and a decent cyberwarfare wing can disrupt and delay a significant military force through attacking communications and logistics, allowing for effective multi-pronged means of deterrence (Brantly 2018). For this reason, countries that are outclassed militarily by larger and more developed powers like Russia and the United States can engage in asymmetric warfare on new terrain economically by pursuing cyber warfare. This greater ease in assembling teams and carrying out attacks by countries points to a need for greater cyber defense to secure information at even the most basic levels. This can entail learning commonly safe cybersecurity practices such as improved password selection and discouraging downloading unverified apps for their smartphones. Analogously, similar levels of scrutiny may be needed at the biological level in consideration of threats within BCS, not just in labs but outside, as biologics takes increased prominence in society (Peccoud et al. 2018).

In addition to the cost and capability associated with cyber warfare, the scope of active measures has also expanded with the increasing prominence of the biological component of cybersecurity. In addition to the traditional active measures, health-related information, propaganda on nations' responses to the pandemic have become part of Russian active measures. Information about biologics, true and false, have been used to affect the public mood and create potential openings among the public to exploit, leading to a potential need for nations to examine how this may be weaponized and disarmed. Stone (2019) reported the use of Novichok nerve agent known as A-234 against former Russian spy Sergei Skripal and his daughter Yulia Sergei Skripal, indicating that chemical and biological weapons are still seen as means of adversarial acts for some nations (Stone, 2019). While using biological and chemical agents for adversarial acts, Russia has also conducted misinformation campaigns, as reflected in a report by the BBC on how Russian state media fabricates news about a supposed death lab in Georgia (Goddard, 2018). The false accusations were investigated by the BBC, and their investigation revealed that activities in a US-funded lab in Georgia to cure Hepatitis-C were presented as biological warfare experiments; Russian media and officials made false claims

about the laboratory's activities and presented the funding from the DoD as evidence of biological warfare experiments (Goddard, 2018). While the story was disproved, its use by the Russian media serves as an instrument to consider the use of biological warfare, perhaps also related propaganda, as an acceptable component of warfare. This phenomenon is expanded to other labs in Ex-Soviet countries such as Kazakhstan, Georgia, Armenia, and more, which were part of a former anti-plague system (Stronski, 2020). Stronski (2020) notes that these now-retrofitted labs, owed in part to the Nunn-Lugar program, used for tracking outbreaks and plague prevention, were accused of harboring and boosting bioweapons research, which damaged their reputation (Stronski, 2020). Considering that the possibility of actors obscuring their tracks exists within BCS, as in cybersecurity, it would not be an exaggeration to expect countries to use cyber methods to trigger biological consequences, with difficulty in attribution. There exists an uncounted possibility of scenarios where such methods may be deployed, although their trace may not appear for years. In the case of international terrorism, malicious actors have more targets that can be pursued, and it is wise that a nation works to get as much of a running start as possible in defense and forensics.

COVID-19 has proved to be a case where the expectations for complete cooperation against a global pandemic failed, and waves of disinformation in the biological area were not curbed despite the necessity to fight against a global pandemic. Disinformation and misinformation campaigns already had a significant impact on public policy. (Landon-Murray. et al., 2019). There is little reason to believe that these campaigns would have lost steam due to COVID-19 and are seen as valuable enough to continue amid the pandemic. In July 2020, Associated Press reported from US officials that such disinformation campaigns were used by Russia either to spread false news or to amplify certain accusations from China to create confusion and advance certain narratives (Tucker, 2020). This problem is not just limited to the East, as Nie (2020) reports; the spread of misinformation is a wider phenomenon indicating an imperative for improved cooperation, communication, and trust in helping to contain emergent threats within the misinformation sown (Nie, 2020).

THE CASE FOR "DEFEND FORWARD" INTERNATIONALLY AND DOMESTICALLY

The shift in the approach of several western nations from a defensive to an offensive approach in cybersecurity brings even more significance to the importance of BCS. (Smeets et al., 2018). France and Germany recently adopted an offensive approach in cybersecurity (Laudrain, 2019; Schulze and Herpig, 2018; Kavanagh, 2019). Traditionally, the European approach had always emphasized privacy, tried to avoid government intervention, and was not inclined to offensive cyber operations (Tatar et al., 2014). However, increasing activities of international actors, especially the "Paris Call for Trust and Security in Cyberspace" by the end of 2018, which emerged as an initiative to establish international norms for the internet, triggered new initiatives. (France Diplomatie:: Ministry for Europe and Foreign Affairs, 2019). This was followed by a new doctrine by France, who initiated the Paris Call. In 2019, France published its "Doctrine for Offensive Cyber Operations," and cyber activities were integrated into conventional military operations (Laudrain, 2019). Similarly, Germany's preparations for a new cyber defense strategy with components of offensive operations and changes to the German Basic Law were reported in the media (Prager, 2019).

This trend is also seen in the US Department of Defense (DoD) through the DoD Cyber Strategy (Mattis, 2018; Volz, 2019). This shift is reflected in the removals of restrictions in the Obama-era Presidential Policy Directive 20 (PPD-20) and the publication of the recent DoD Cyber Strategy (Geller & Schwartz, 2018). The concepts of "persistent engagement" and "defend forward" acknowledge that there already is an ongoing war in cyberspace, and the DoD, which oversees securing the nation from foreign adversaries, has the task of defending the nation in war; this task demands the use of cyber capabilities in adversarial networks, within the authority granted to the US military by Title 10 (Kosseff, 2019). This trend can also be observed in the revision of the Joint Publication 3-12 in 2018.

It is noted that 3-12 does not include the biological dimension and poorly talks about the cognitive dimension. However, with the fact that possible attacks that include both dimensions have been demonstrated to be possible, at least in lab environments, as shown through the work of Ney, Puzis, and others, it is reasonable to update the document. (Ney, 2017; Puzis, 2020). Although the former version of Joint Publication (JP) 3-12 was published in 2013, it has a very similar outline with JP 3-12 (2018), which expands further in the definition of cyberspace, and delineates core activities in cyberspace. The definition of Offensive Cyberspace Operations (OCO) in the 2018 document refers to "in and through "foreign" cyberspace" while the 2013 document mentions just "in and through cyberspace." This was also reflected in the fact that the US Cyber Command was elevated to a unified combatant command in May 2018, which meant that the commander of the Cyber Command would have the authority to act in the cyber domain similar to the actions other combatant command commanders can take in war zones. While this approach is still problematic when considering US IP addresses, within the scope of "foreign cyberspace," taking the direct consequential effects of BCS into account improves the justification of "defend forward" as a necessary strategy with bio-cyber technological convergence as threats in this intersection can permeate US localized devices, locations, and bodies connected to US IP addresses. (George 2019).

BCS AND LEGITIMACY OF "DEFEND FORWARD"

This legitimacy of the DF paradigm is more valid for the attacks threatening BCS due to a more direct biological emphasis and a threat to life compared to common cyber-attacks which focus rather on finances, privacy, or non-medical infrastructure; this reality puts cases of BCS at the margins closest to armed conflict within the territory of "short of armed conflict" (Karabacak and Tatar, 2014). While every cyber attack has its unique consequences, the attacks within the scope of BCS are categorically closer to life-threatening consequences as in an armed conflict. This certainly does not negate the attribution problem within cybersecurity. Despite the support of countries that favor defend forward, attribution is still a problem in cyberspace (Tatar, Gokce, and Gheorghe, 2017). It is difficult to figure out whether the source of the attack is determined accurately, and this casts doubts on legitimacy in any offensive action. While the attribution problem has a limiting effect on overall cyber defense and any offensive cyber operations, it also supports the case for "defend forward" when BCS is considered a critical component of overall security. Positioning in line with DF is more justifiable in the context of BCS due to the greater need for attribution as biological elements can be more precisely targeted and include a greater dimension for tracking, especially where the biological interlock is defined. Regional sources of pandemics can more or less be triangulated. This context can generate outcomes different from the negative public opinion in the post 9/11 world wherein the US forces were positioned in the Middle East and became engaged in wars with the rationale that uncertainty legitimized preemptive strikes (Amoore and De Goede, 2008). While this notion can and has been criticized in terms of long-term consequences, it has a stronger relevance in a BCS setting (Amoore and De Goede, 2008). Biocyber attacks, like those of nuclear attacks, could create problems that remain and accumulate in our bodies and environments (Bromet et al., 2011; Shaul and Lower, 2015). Unlike the negative effects related to public perceptions due to the "preemptive strikes" in the war on terror, positioning in cyberspace is not very clear and would not necessarily constitute a source of negative public opinion. However, public opinion of current administrations could turn negative upon failure to meet biological cyber threats regarding their effects if unaddressed. Reflecting on the support for the military and anti-terror initiatives, an administration would do well to have a plan of action to engage in such threats.

An important question is what form this engagement would take. Realistically, this means improved funding towards STEM education, greater expertise sharing between labs focusing on specialized areas of biology, promotion of initiatives that study the growing synergy between biology and computing, updating best practices for the regulation of biological products, promotion of

community bio spaces and allowing security forces to pursue agents who aim to use the intersection for terror (George 2019; Murch et al. 2018; Potter & Palmer 2020). In all areas, this means growing proactivity to keep up with the explosive growth of biocybertechnology, as well as educating society, to allow for superior flexibility in navigating such threats. A policy that fails to do this runs the risk of rapid obsolescence, waste, and expanding liabilities for the nation's future.This concern has only increased due to the cyberattacks on the healthcare systems during COVID-19. Prior to the pandemic, Kruse et al. (2017) noted numerous modern healthcare threats already in existence that may grow. A bipartisan letter from several US senators to the heads of the Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA), National Security Agency, and US Cyber Command was urging CISA and Cyber Command to "Evaluate further necessary action to defend forward to detect and deter attempts to intrude, exploit, and interfere with the healthcare, public health, and research sectors"(US Senate, 2020).

BCS AND DEFEND FORWARD AT THE OPERATIONAL LEVEL

In addition to the impact of BCS in strategic defense posture, it has immense potential to influence future warfare through expanding the number of available and potential targets, with the potential for off-target effects for both user and target. This entails a need to find ways to contain threats before they start. In terms of biocyberwarfare, ISTAR (intelligence, surveillance, target acquisition, and reconnaissance) activities become further complicated as more routes to attack enter into the discussion. The US Joint Publication 3-12 "Joint Intelligence Preparation of the Operational Environment" describes the information environment as "the aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information" and repeatedly indicates that cyberspace is included in the information environment (Joint Publication 3-12 Cyberspace Operations, 2019). In a persistent engagement world, the investigation of malicious actors trying to penetrate biotechnological assets and taking deterrent, preventive, or disruptive measures in their systems becomes a natural component of operational planning. This allows us to revisit our earlier question regarding DF from the context of BCS. In "positioning to degrade biocyber operations," this can mean gathering the general means to contain and dismantle operations by malicious actors through ongoing research and preparation. The second means, which is to "gather information about threats and inform defenses," takes the form of surgically gathering adequate expertise to dynamically develop risk assessments and methods of containment for specific threats. Lastly, the step of "influencing adversaries to discourage them from deploying cyber operations against the United States" can be through stiff penalties for low-level actors, leading up to sanctions and preemptive action against state-level actors. The main difference in extending DF involves applying a deeper degree of consideration for how biology can play a part in cyber operations and applying more expertise towards it.

CONCLUDING THOUGHTS TOWARD A FUTURE AND MORE COMPREHENSIVE WORK

This paper serves to discuss the topic of BCS and the implications of COVID-19 on BCS within the context of DF. It first discusses the prominence of the emerging field of BCS and provides a foundation for future argument as to why it needs to be considered as a critical component of cyber warfare. There are three lines of BCS that make it a critical component of overall cyber defense within the context of defending forward: (1) Cyber operations within the area of BCS have life-threatening consequences to a greater extent than other cyber operations, (2) The breach in health-related personal data is a significant tool for fatal attacks, and finally (3) Health-related misinformation campaigns as a component of BCS can cause significant damage compared to other misinformation campaigns. The notion is further supported by the observation that the fight against COVID-19 did not initiate

the necessary cooperation, but on the contrary, exacerbated the existing conflicts. As the effects of the pandemic threatened lives, the existing fear has been used for misinformation campaigns.

Following the discussion on the increasing importance of BCS and how this role has gained prominence, the paper suggests that BCS needs to be considered as an essential component of the cybersecurity doctrine within the Defending Forward framework. While key factors in the emergence of BCS include the pace of improvements in biotechnology, the nature of attacks related to BCS, potential attacks that may emerge, and the criticality of attribution in such attacks that could benefit from a national security-based approach to BCS, the cases related to COVID-19 proved that BCS serves as an amplifying factor for conflict in cyberspace and its spill to other domains of warfare. The authors suggest that the experiences regarding the lack of cooperation in the COVID-19 environment have served as a means to increase awareness about BCS and strengthened the arguments for the defense forward approach within cybersecurity. The authors additionally suggest that BCS needs to be considered as a critical component of national cybersecurity strategies and the incidents during COVID-19 further exposed this necessity. The authors specifically encourage further research in the inclusion of BCS concerning the assessment of national security.

Given the breadth of such a combined framework, the authors believe that such can be assisted by an updated mapping of BCS research and cases of real-world exploits at the intersection that is BCS. Combined with the latest Joint Publication, a more meaningful foundation for inclusion can be established. It is the authors' opinion that the endeavor towards a comprehensive BCS-DF framework is in the best interests of national security for each nation.

REFERENCES

Amoore, L., & De Goede, M. (2008). Transactions after 9/11: The Banal Face of the Preemptive Strike. *Transactions of the Institute of British Geographers*, *33*(2), 173–185. doi:10.1111/j.1475-5661.2008.00291.x

Baker, J., Strychalski, E., Rogers, K., & Lee, K. (2019). Cyberbiosecurity for Biopharmaceutical Products. *Frontiers in Bioengineering and Biotechnology*, 7. PMID:31214582

Belhaj, K., Chaparro-Garcia, A., Kamoun, S., Patron, N. J., & Nekrasov, V. (2015). Editing plant genomes with CRISPR/Cas9. *Current Opinion in Biotechnology*, *32*, 76–84. doi:10.1016/j.copbio.2014.11.007 PMID:25437637

Berezow, A. (2021, January 14). *Hacking DNA Sequences: Biosecurity Meets Cybersecurity*. Retrieved from https://www.acsh.org/news/2021/01/14/hacking-dna-sequences-biosecurity-meets-cybersecurity-15273

Berger, K., & Schneck, P. (2019). National and Transnational Security Implications of Asymmetric Access to and Use of Biological Data. *Frontiers in Bioengineering and Biotechnology*, *7*, 7. doi:10.3389/fbioe.2019.00021 PMID:30859099

Bitam, S., Zeadally, S., & Mellouk, A. (2016). Bio-inspired cybersecurity for wireless sensor networks. *IEEE Communications Magazine*, *54*(6), 68–74. doi:10.1109/MCOM.2016.7497769

Blumenthal. (2020). Retrieved from https://www.blumenthal.senate.gov/imo/media/doc/2020.04.20%20-%20CISA%20and%20CC%20-%20Coronavirus%20Cybersecurity%20-%20FINAL.pdf

Brantly, A. (2018). The cyber deterrence problem. *2018 10th International Conference on Cyber Conflict (CyCon).*

Brenner, S. (2006). Cybercrime, cyberterrorism and cyberwarfare. *Revue internationale de droit pénal*, *3*(3-4), 453-471. 10.3917/ridp.773.0453

Brenner, S. W., & Clarke, L. L. (2009). Civilians in cyberwarfare: Casualties. *SMU Sci. & Tech. L. Rev.*, *13*, 249.

Bromet, E. J., Havenaar, J. M., & Guey, L. T. (2011). A 25 year retrospective review of the psychological consequences of the Chernobyl accident. *Clinical Oncology*, *23*(4), 297–305. doi:10.1016/j.clon.2011.01.501 PMID:21330117

Brown, K. (2020, June 25). *One Biohacker's Improbable Bid to Make a DIY Covid-19 Vaccine*. https://www.bloomberg.com/news/articles/2020-06-25/one-biohacker-s-improbable-bid-to-make-a-diy-covid-19-vaccine

Caplan, A. L., Parent, B., Shen, M., & Plunkett, C. (2015). No time to waste—the ethical challenges created by CRISPR: CRISPR/Cas, being an efficient, simple, and cheap technology to edit the genome of any organism, raises many ethical and regulatory issues beyond the use to manipulate human germ line cells. *EMBO Reports*, *16*(11), 1421–1426. doi:10.15252/embr.201541337 PMID:26450575

Chesney, R. (2018, September 25). *The 2018 DOD Cyber Strategy: Understanding' Defense Forward' in light of the NDA*. https://www.lawfareblog.com/2018-dod-cyber-strategy-understanding-defense-forward-light-ndaa-and-ppd-20-changes

Daggett, S. (2010, June). *Costs of major US wars*. Library of Congress.

Davis, N. (2020, June 1). *What COVID-19 teaches us about cybersecurity – and how to prepare for the inevitable global cyberattack*. https://www.weforum.org/agenda/2020/06/covid-19-pandemic-teaches-us-about-cybersecurity-cyberattack-cyber-pandemic-risk-virus

Dieuliis, D., Lutes, C. D., & Giordano, J. (2018). Biodata Risks and Synthetic Biology: A Critical Juncture. *Journal of Bioterrorism & Biodefense*, *9*(1). Advance online publication. doi:10.4172/2157-2526.1000159

Dumitriu, A., & Goldberg, S. (2019). Make Do and Mend: Exploring gene regulation and CRISPR through a FEAT (Future Emerging Art and Technology) residency with the MRG-Grammar Project. *Leonardo*, *52*(1), 66–67. doi:10.1162/leon_a_01466

Duncan, S., Reinhard, R., Williams, R., Ramsey, F., Thomason, W., Lee, K., Dudek, N., Mostaghimi, S., Colbert, E., & Murch, R. (2019). Cyberbiosecurity: A New Perspective on Protecting US Food and Agricultural System. *Frontiers in Bioengineering and Biotechnology*, *7*, 7. doi:10.3389/fbioe.2019.00063 PMID:30984752

Evans, C. V. (2020). Future Warfare: Weaponizing Critical Infrastructure. *Future*, *5*, 15–2020.

Fraser, E. (2020). *Long term respiratory complications of COVID-19*. Academic Press.

French Diplomatie Ministry for Europe and Foreign Affairs. (2019). *Cybersecurity: Paris Call of 12 November 2018 for Trust and Security in Cyberspace*. Available at: https://www.diplomatie.gouv.fr/en/french-foreign-policy/digital-diplomacy/france-and-cyber-security/article/cybersecurity-paris-call-of-12-november-2018-for-trust-and-security

Geller, E., & Schwartz, J. (2018, August 16). *Trump scraps Obama rules on cyberattacks, giving military freer hand*. Retrieved November 21, 2019, from https://www.politico.com/story/2018/08/16/trump-cybersecurity-cyberattack-hacking-military-742095

Gent, E. (2021, January 13). *New research could enable direct data transfer from computers to living cells.* Retrieved from https://singularityhub.com/2021/01/11/new-research-could-enable-direct-data-transfer-from-computers-to-living-cells/

George, A. M. (2019). The National Security Implications of Cyberbiosecurity. *Frontiers in Bioengineering and Biotechnology*, *7*, 51. Advance online publication. doi:10.3389/fbioe.2019.00051 PMID:30968020

Goddard, M. (Ed.). (2018, November 12). *Russian disinformation and the Georgian 'lab of death'.* Retrieved September 25, 2020, from https://www.bbc.com/news/av/world-46157507/russian-disinformation-and-the-georgian-lab-of-death

Goni-Moreno, A., & Nikel, P. I. (2019). High-performance biocomputing in synthetic biology–integrated transcriptional and metabolic circuits. *Frontiers in Bioengineering and Biotechnology*, *7*, 40. doi:10.3389/fbioe.2019.00040 PMID:30915329

Goodin, D. (2020, September 18). *A Patient Dies After a Ransomware Attack Hits a Hospital*. https://www.wired.com/story/a-patient-dies-after-a-ransomware-attack-hits-a-hospital/

Habibzadeh, H., Nussbaum, B. H., Anjomshoa, F., Kantarci, B., & Soyata, T. (2019). A survey on cybersecurity, data privacy, and policy issues in cyber-physical system deployments in smart cities. *Sustainable Cities and Society*, *50*, 101660. doi:10.1016/j.scs.2019.101660

Hester, R. J. (2020). Bioveillance: A Techno-security Infrastructure to Preempt the Dangers of Informationalised Biology. *Science as Culture*, *29*(1), 153–176. doi:10.1080/09505431.2019.1705270

Joint Publication 3-12 Cyberspace Operations. (2019). Available at: https://info.publicintelligence.net/JCS-CyberspaceOperations.pdf

Karabacak, B., & Tatar, Ü. (2014). Strategies to Counter Cyberattacks: Cyberthreats and Critical Infrastructure Protection. *Critical Infrastructure Protection*, *116*, 63.

Katz, E. (2015). Biocomputing— Tools, aims, perspectives. *Current Opinion in Biotechnology*, *34*, 202–208. doi:10.1016/j.copbio.2015.02.011 PMID:25765672

Kavanagh, R. (2019). *France Develops Cyber Policy For Defence & Offence*. Retrieved from https://www.southeusummit.com/europe/france/france-develops-cyber-policy-for-defence-offence/

Kosseff, J. (2019). The Contours of 'Defend Forward' Under International Law. In *2019 11th International Conference on Cyber Conflict (CyCon)* (Vol. 900, pp. 1-13). IEEE.

Koyama, T., Weeraratne, D., Snowdon, J. L., & Parida, L. (2020). Emergence of drift variants that may affect COVID-19 vaccine development and antibody treatment. *Pathogens (Basel, Switzerland)*, *9*(5), 324.

Kruse, C. S., Frederick, B., Jacobson, T., & Monticone, D. K. (2017). Cybersecurity in healthcare: A systematic review of modern threats and trends. *Technology and Health Care*, *25*(1), 1–10.

Kuiken, T. (2016). Governance: Learn from DIY biologists. *NATNews*, *531*(7593), 167.

Landon-Murray, M., Mujkic, E., & Nussbaum, B. (2019). Disinformation in contemporary US foreign policy: Impacts and ethics in an era of fake news, social media, and artificial intelligence. *Public Integrity*, *21*(5), 512–522.

Laudrain, A. (2019). *France's New Offensive Cyber Doctrine*. Lawfare. Available at: https://www.lawfareblog.com/frances-new-offensive-cyber-doctrine

Lewis, D. (2019). Rare bird's detection highlights promise of 'environmental DNA.'. *Nature*, *575*(7783), 423–424. doi:10.1038/d41586-019-03522-3

Mantle, J. L., Rammohan, J., Romantseva, E. F., Welch, J. T., Kauffman, L. R., McCarthy, J., & Lee, K. H. et al. (2019). Cyberbiosecurity for biopharmaceutical products. *Frontiers in Bioengineering and Biotechnology*, *7*, 116.

Martin, G., Martin, P., Hankin, C., Darzi, A., & Kinross, J. (2017). Cybersecurity and healthcare: How safe are we? *BMJ (Clinical Research Ed.)*, 358.

Mattis, J. (2018). *Summary of the 2018 national defense strategy of the United States of America*. Department of Defense Washington United States.

Maurushat, A. (2013). From cybercrime to cyberwar: Security through obscurity or security through absurdity? *Canadian Foreign Policy*, *19*(2), 119–122.

Metzger, R. S. (2020). Cyber safety in the era of cyber warfare. *Scitech Lawyer*, *16*(3), 30–34.

Mirsky, Y., Mahler, T., Shelef, I., & Elovici, Y. (2019). CT-GAN: malicious tampering of 3D medical imagery using deep learning. In *Proceedings of the 28th USENIX Conference on Security Symposium (SEC'19)*. USENIX Association.

Moreno, A., & Lovaas, P. (n.d.). *Cyber-Security Vulnerabilities: Domestic Lessons from Attacks on Foreign Critical Infrastructure*. Academic Press.

Murch, R., So, W., Buchholz, W., Raman, S., & Peccoud, J. (2018). Cyberbiosecurity: An Emerging New Discipline to Help Safeguard the Bioeconomy. *Frontiers in Bioengineering and Biotechnology*, 6.

Ney, P., Koscher, K., Organick, L., Ceze, L., & Kohno, T. (2017). *Proceedings of the 26th Usenix Security Symposium*. Vancouver, BC: USENIX Association.

Nie, J. B. (2020). In the Shadow of Biological Warfare: Conspiracy Theories on the Origins of COVID-19 and Enhancing Global Governance of Biosafety as a Matter of Urgency. *Journal of Bioethical Inquiry*, 1–8.

O'Neill, P. (2020, November 12). *Ransomware did not kill a German hospital patient*. Retrieved from https://www.technologyreview.com/2020/11/12/1012015/ransomware-did-not-kill-a-german-hospital-patient/

Pauwels, E. (2020, June 18). *3 challenges to tackling cyberbiosecurity threats after COVID-19*. https://www.weforum.org/agenda/2020/06/prevent-cyber-bio-security-threats-covid19-governance/

Pearlman, A. (2017). Biohackers are using CRISPR on their DNA and we can't stop it. *New Scientist*, 15.

Peccoud, J., Gallegos, J. E., Murch, R., Buchholz, W. G., & Raman, S. (2018). Cyberbiosecurity: From Naive Trust to Risk Awareness. *Trends in Biotechnology*, *36*(1), 4–7. doi:10.1016/j.tibtech.2017.10.012

Potter, L., & Palmer, X. (2020, April 18). *Human Factors in Biocybersecurity Wargames*. https://arxiv.org/abs/2005.02135

Prager, A. (2019). *Germany's cyber defence strategy discussed behind closed doors*. https://www.euractiv.com/section/cybersecurity/news/germanys-cyber-defence-strategy-discussed-behind-closed-doors/

Richardson, L., Connell, N., Lewis, S., Pauwels, E., & Murch, R. (2019). Cyberbiosecurity: A Call for Cooperation in a New Threat Landscape. *Frontiers in Bioengineering and Biotechnology*, 7.

Rothrock, R. (2020, June 17). *COVID-19 Cybersecurity: Parallels and Lessons from a Pandemic*. https://www.nti.org/analysis/atomic-pulse/covid-19-cybersecurity-parallels-and-lessons-pandemic/

Sallinen, M. (2021). *Weaponized malware, physical damage, zero casualties–what informal norms are emerging in targeted state sponsored cyber-attacks? The dynamics beyond causation: an interpretivist-constructivist analysis of the US media discourse regarding offensive cyber operations and cyber weapons between 2010 and 2020*. Academic Press.

Schabacker, D., Levy, L., Evans, N., Fowler, J., & Dickey, E. (2019). Assessing Cyberbiosecurity Vulnerabilities and Infrastructure Resilience. *Frontiers in Bioengineering and Biotechnology*, 7.

Schmale, D., Ault, A., Saad, W., Scott, D., & Westrick, J. (2019). Perspectives on Harmful Algal Blooms (HABs) and the Cyberbiosecurity of Freshwater Systems. *Frontiers in Bioengineering and Biotechnology*, 7.

Schulze, M., & Herpig, S. (2018). Germany Develops Offensive Cyber Capabilities Without a Coherent Strategy of What to Do With Them. *Council on Foreign Relations.* Retrieved from: https://www.cfr.org/blog/germany-develops-offensive-cyber-capabilities-without-coherent-strategy-whatdo-them

Shaul, T. R., & Lower, B. H. (2015). *3.4 The Lingering Effects of the Chernobyl Disaster*. Environmental ScienceBites.

Simpson, M. L. (2001). *Whole-Cell Biocomputing*. Trends in Biotechnology. https://www.sciencedirect.com/science/article/abs/pii/S0167779901016912

Simpson, M. L., Sayler, G. S., Fleming, J. T., & Applegate, B. (2001). Whole-cell biocomputing. *Trends in Biotechnology*, *19*(8), 317–323. doi:10.1016/s0167-7799(01)01691-2

Smeets, M., & Lin, H. S. (2018). Offensive cyber capabilities: To what ends? In *2018 10th International Conference on Cyber Conflict (CyCon)* (pp. 55-72). IEEE.

Stone, R. (2018). *UK Attack Puts Nerve Agent in the Spotlight*. Science. Available at: https://science.sciencemag.org/content/359/6382/1314

Stronski, P. (2020, June 25). *Ex-Soviet Bioweapons Labs Are Fighting COVID-19. Moscow Doesn't Like It*. https://foreignpolicy.com/2020/06/25/soviet-bioweapons-labs-georgia-armenia-kazakhstan-coronavirus-russia-disinformation/

Tatar, Ü., Çalik, O., Çelik, M., & Karabacak, B. (2014). A Comparative Analysis of the National Cyber Security Strategies of Leading Nations. In International Conference on Cyber Warfare and Security (p. 211). Academic Conferences International Limited.

(2017). Strategic cyber defense: a multidisciplinary perspective. InTatar, U., Gheorghe, A. V., & Gökçe, Y. K. (Eds.), *Sub-Series D, Information and Communication Security*. IOS Press.

Spence, N., Niharika Bhardwaj, M. B. B. S., & Paul, D. P. III. (2018). Ransomware in Healthcare Facilities: A Harbinger of the Future? *Perspectives in Health Information Management*, 1–22.

Thomas, M. L., Gunawardene, N., Horton, K., Williams, A., O'Connor, S., McKirdy, S., & van der Merwe, J. (2017). Many eyes on the ground: Citizen science is an effective early detection tool for biosecurity. *Biological Invasions*, *19*(9), 2751–2765.

Tucker, E. (2020). *US officials: Russia behind spread of virus disinformation*. https://apnews.com/3acb089e6a333e051dbc4a465cb68ee1

Turner, G. (2019). The Growing Need for Cyberbiosecurity. *Proceedings of the 2019 InSITE Conference*.

Volz, D. (2019). *Trump, Seeking to Relax Rules on US Cyberattacks, Reverses Obama Directive*. Available at: https://www.wsj.com/articles/trump-seeking-to-relax-rules-on-u-s-cyberattacks-reverses-obama-directive-1534378721

Wang, Y., Noor-A-Rahim, M., Gunawan, E., Guan, Y. L., & Poh, C. L. (2019). Construction of bio-constrained code for DNA data storage. *IEEE Communications Letters*, *23*(6), 963–966.

Weil, T., & Murugesan, S. (2020). IT Risk and Resilience—Cybersecurity Response to COVID-19. *IT Professional*, *22*(3), 4–10. doi:10.1109/mitp.2020.2988330

West, R. M., & Gronvall, G. K. (2020). CRISPR Cautions: Biosecurity Implications of Gene Editing. *Perspectives in Biology and Medicine*, *63*(1), 73–92.

Wolinsky, H. (2016). The FBI and biohackers: an unusual relationship: the FBI has had some success reaching out to the DIY biology community in the USA, but European biohackers remain skeptical of the intentions of US law enforcement. *EMBO Reports*, *17*(6), 793–796.

Xie, K. (2020, June 18). *We must rethink cybersecurity in the COVID-19 era. Here's how*. https://www.weforum.org/agenda/2020/06/we-must-rethink-and-repurpose-cybersecurity-for-the-covid-19-era

Xavier-Lewis Palmer is a Biomedical Engineering Ph.D. Student, developing expertise in regenerative medicine and policy, overall. The focus of his doctoral research is on the importance of the micro-environment in breast cancer. His past and ongoing additional work remains interdisciplinary, including, but not limited to MEMS, microfluidics, machine learning, and other aspects of tissue engineering.

Lucas Potter is a Biomedical Engineering PhD Student and member of the SAMPE (Systems Analysis of Metabolic Physiology) Lab at Old Dominion University. His doctoral research is focused on cellular metabolism. Past research endeavors include human factors research (including human factors analysis of performance in virtual reality), modeling of physiology, and materials engineering.

Saltuk Karahan is Program Coordinator at the School of Cybersecurity at Old Dominion University. He is also a lecturer in the Department of Political Science and Geography. Before joining Old Dominion University, Karahan worked in various leadership roles within NATO. Karahan's long military career was focused on national security strategy, transformation in national and international organizations and technological capability development. He earned his Ph.D. in International Studies from Old Dominion University, Norfolk, VA with a concentration on Conflict and Cooperation and his Master's in Modeling and Simulation from Naval Postgraduate School, Monterey, CA with a concentration on Human-Computer Interaction.