Cyber and Emergent Technologies

Current and Future Ramifications

Joshua A. Sipper
Air Force Cyber College
Air University
Maxwell AFB, AL, United States
Email: joshua.sipper.1@us.af.mil

***Abstract*— We as a cyber community are now living in a cyber meta-reality (a reality about realities) where scientific and technological advances such as microscopic machines, subatomic energy manipulation, and autonomous technologies, heretofore only imagined in science fiction tales are on the verge of practical use. As the need for new, better, and more secure methods of implementing cyber increases, the unfettered desire for greater bandwidth, stronger encryption, and more rapid processing naturally follows. If the cyber community is to capitalize on new technologies, however, we need to stay acquainted with these emergent technologies and understand their ramifications. Otherwise, we stand the chance of either missing opportunities to advance or being trampled by those who do. Today scientists and technologists are buzzing about quantum entanglement, non-linear wave propagation, and Metal Organic Frameworks (MOF). The United States is in a race to the finish to make the potentialities of these amazing ideas, realities. This paper examines four very specialized technological areas and draws on these technologies to construct a cohesive narrative regarding their interoperability in order to highlight the necessity and ramifications of each area's contribution to a holistic technological scaffold. Artificial Intelligence (AI) and Machine Learning (ML) are of course, an increasingly conjoined capability with great promise, yet not fully realized. Emergent technologies related to security such as quantum encryption and multi-factor authentication are rapidly finding their place in the cyber meta-reality. Quantum computing, related to the theory of quantum entanglement and quantum encryption, will likely deliver processing and bandwidth options far beyond current possibilities. Finally, nanotechnologies such as graphene and membrane technology are already in production in some applications and will no doubt become a critical enabler of the entirety of the aforementioned technologies. Additionally, the concept of the cyber microbiome is introduced for consideration.**

Keywords- quantum, nanotechnology, meta-reality, microbiome, artificial, machine.

I. INTRODUCTION

In the cyber community, emergent technologies are a huge factor to be considered as the pace of technological development not only advances cyber capabilities, but also rapidly adds layers of complexity to the already wicked cyber puzzle. Abounding studies, experiments, and research in fields like particle physics (quanta) continuing under the auspices of Conseil Européen pour la Recherche Nucléaire (CERN), coupled with emergent nanotechnologies such as graphene and MOF, point to a near future where processing speed, bandwidth, and the full spectrum implementation of ML and AI can become realities. These possibilities are currently being expressed mostly within their own frameworks as researchers continue to nail down their mechanics, interoperability, and necessary requirements. However, these once embryonic hypotheses are now being demonstrated as realities through scientific theory development within the traditional construct of reproducible laboratory experimentation.

So, what does this mean for us in the cyber community and how can we as a community of practitioners, policy makers, and researchers benefit from these new technologies? How will these new technologies increase the power of cyber now and into the future? How will the cyber meta-reality (Figure 1) change and grow as a result of this technical dynamism? Perhaps most importantly, how will adversaries and threats to peace use the same technologies and how will we defeat them? We cannot pretend to have all of the answers, but we can begin the conversation and explore the possibilities.

Figure 1. Cyber Meta-Reality.

Of course, before we can begin to probe these questions, we must first have a basis of comprehension concerning the

ISBN: 978-1-61208-818-1

technologies that generated said questions. The theories, technologies, and capabilities are beyond doubt complex, still forming, and even dangerous. There are numerous technologies two or more decades old that are no longer emergent, but well established such as stealth, precision and machine automation, drone technology, and others. All of these have upended how warfare and other technologies are used and continue to develop. Developing technologies such as AI and ML are especially cogent contributors as they have been proven to increase efficiency and speed up decision cycles significantly [1]. The necessity and desire that accompanies human intellect drives them onward, moment by moment. Why would anyone want to understand the fundamental building blocks of matter? Because it answers important questions about the creation and inner workings of our cosmos. Because the power generated by separating these basic building blocks has led us into a resplendently wonderful and terrifyingly awful nuclear age. Because, we are curious.

For the cyber community, it comes down to power; the power to continue the creation and expansion of and capabilities within the meta-reality we call cyberspace. The same can be said concerning the nanoparticle constructs of graphene and MOFs. The ability to use these types of nano-constructs as waveguides, conductors, transistors, circuits, and many more applications can provide cool, fast processing and bandwidth operation impossible with the use of legacy electronics. Then, there is the consideration of how both quantum and physical nanotech affect the growth and application of AI and ML. What space will these potentialities grow to inhabit once they are enabled through a seemingly infinite power, processing, and dissemination stream? One might see visions of life, death, or something altogether unimaginable to us right now. But, either way the power offered through these capabilities will likely shape the future of cyber and global communications, politics, commerce, and conflict.

In the following sections, we will first discuss AI and ML and their marked effects on technology no and into the future. Emergent security will be framed in the second section, relating how various technologies are leading to increased security across the cyber meta-reality. In the third section, the amazing rise and potential of quantum computing will be presented. Finally, nanotechnology will be explored in the fourth section, giving insight into how this field affects all of the other areas and has led in concert with these areas to another type of cyber meta-reality that includes a symbiotic, technological multiverse characterized as the cyber microbiome.

II. Artificial Intelligence and Machine Learning

AI and ML are a developing construct still not fully realized within the greater cyber framework. Undoubtedly, even when the cyber meta-reality does finally capitalize on these capabilities, there will be another mountain to climb. However, we must for now consider the mountains before us in that AI and ML are certainly developing and growing in strength and power, capability and usability. With this growth comes several positive and negative ramifications. While AI increases the intelligence level of programs at an individual and collective level, it also adds layers of complexity that must be managed and mitigated (Kott, 2018). AI and ML have been demonstrated on numerous occasions as tools useful in the areas of parsing and grouping data (ML) and actual decision-making (AI). “We have a variety of learning mechanisms for both symbolic and non-symbolic AI that allow autonomous agents to improve their performance and adapt to changing environmental conditions” [2]. AI and ML have found some applicability in the field of intelligent autonomous agents such as the self-driving car experiments conducted by Google and Tesla. Agencies such as DARPA are doubling-down on these studies by going forward with the application of AI and ML on the battlefield in the form of autonomous air, land, sea, space, and cyber capabilities such as drones and in the case of cyber, code. ML and AI are similar, but distinct concepts covering multiple capabilities and constructs. Therefore, it is important to understand their subtleties.

In general, AI is divided into two varied approaches: symbolic and non-symbolic; each represents knowledge in fundamentally different ways, leading to outcomes specific to the respective approach [2]. It is important to understand these two categories in order to properly arrange AI and ML in a construct that supports co-functionality. “The systems developed as part of the DARPA Cyber Grand Challenge are primarily symbolic AI systems. These automated reasoners can identify vulnerabilities in software services, develop a patch, and deploy the patch at machine speed” [2]. The use of symbolic AI is labor intensive and includes the creation of a large matrix of interrelated information to get the AI started. However, as the AI begins to make connections and form heuristic bonds, the system can grow and adapt on its own. The same is true to a great extent for non-symbolic systems which focus instead on the patterns of learning in data for classifying objects, predicting future results, or clustering similar sets of data [2]. However, the true power of AI and ML is not their individual components, but what they can accomplish together. Such is the case in the world of intelligent autonomous agents.

Intelligent autonomous agents have been in development for some time, but are only now coming to fruition as mechanisms capable of the complex decision-making processes necessary for optimal, real-world performance. “The proliferation of intelligent agents is the emerging reality of warfare, and they will form an ever-growing fraction of total military assets. The sheer quantity of targetable friendly agents… make intelligent, autonomous cyber defense agent a necessity on the battlefield of the future” [3]. With the overlap of AI, ML, and Deep Learning (DL) capabilities across the globe, U.S. and NATO capabilities must not only keep pace with this trend, but outstrip it in order to maintain a leading edge against adversaries. This overlap is represented in Figure 2 Artificial Intelligence, Machine Learning, Deep Learning Overlap for Autonomous Agents. Another way to accomplish this goal is through human-machine partnering through cyber interfaces interleaved with AI and ML capable technologies. Human-machine teaming has become a huge topic of research and practice recently, especially as it relates to Defensive Cyberspace Operations (DCO). This teaming aspect has led to a marked need for autonomous, synthetic agents that can assist in processing, targeting, and gap-filling [2]. Through these human-cyber interactions, filtering, parsing, and decision-making can be funneled in such a way to speed up processes such as targeting and battle damage assessment, a vital feedback stream in today's joint all-domain military environments. Of course, as with all emergent capabilities, a note of caution and reflection must be considered. Questions concerning whether autonomous agents might eventually be candidates for "personhood" and held liable for accidents or purposeful destruction have arisen in light of the trend toward cyber autonomy. The European Parliament has even gone so far as to publish a report with "recommendations to the Commission on Civil Law Rules on Robotics" asking questions regarding how to categorize AI and ML enabled autonomous agents [4]. Regardless of these questions, however, the journey toward AI and ML in myriad applications is underway and there is no turning back.

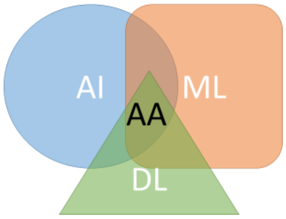

Figure 2. Artificial Intelligence, Machine Learning, Deep Learning Overlap for Autonomous Agents

Figure 2. Artificial Intelligence, Machine Learning, Deep Learning Overlap for Autonomous Agents.

III. EMERGENT SECURITY

Security issues will obviously continue to be paramount in importance as the cyber community goes forward. Protecting information from integrity attacks like man-in-the-middle and infiltrations by using existing encryption standards will only work for so long as adversaries continue to develop more advanced cracking technologies, some of which will undoubtedly include quantum computing capabilities (to be discussed in the following section). Emergent capabilities such as quantum encryption and multi-factor authentication offer the best options currently understood for defense against imminent cracking attempts.

Quantum encryption is a tool still in development that has spurred from the underlying mathematical and physics modeling and applications of particle physics and quantum theory. "A quantum procedure known as quantum cryptography or quantum key distribution can do key distribution so that the communication security cannot be compromised. The idea is based on the quantum principle that observing a quantum system will disturb the system being observed" [5]. In quantum key distribution, the disturbance of the system occurs as a result of a relationship called quantum entanglement. Quantum computers implement superposition states and quantum entanglements to perform simultaneous calculations and produce consequential calculated results. The highly efficient character of quantum entanglement and superposition are the characteristics that enable quantum computers to be exponentially faster, consistently outperforming classical computers in several areas [5]. The idea is that when two particles of matter, in this case most probably subatomic particles called fermions, become related or entangled in a relationship-dependent state, if one particle changes in state, the other one does as well; this is true no matter how far apart the particles are in physical distance which makes the application of state changes between the particles especially useful for quantum encryption and computing.

Multi-factor authentication is another area important to integrity within the cyber meta-reality. While the concept of two-factor authentication is presently in use across a wide array of devices and systems, multi-factor authentication is still a growing area. "Two-factor authentication has reduced incidences of fraud, including identity theft, in e-commerce. Consumers are no longer at high risk from thieves due to the compromise at a single point of failure in a transaction" [6]. However, as thieves and adversaries find ways to exploit weaknesses and circumvent two-factor authentication, the opportunity for deeper layering of authentication is growing. Several areas of authentication are possible according to Waters: location, possession, access, proximity, behavioral, confirmation, witnessed, and radio. By using these techniques together, multiple factors can add strength, thereby denying access to and possible manipulation of data.

IV. QUANTUM COMPUTING

Probably the most difficult expanse of emergent technology to comprehend and implement is quantum computing. This is due mostly to the profound and sometimes murky depths one must take into the areas of particle physics and applied mathematics, but also because the technologies that enable the manipulation of subatomic particles that make quantum computing possible are still developing and being modeled both mathematically and through actual laboratory experimentation. Information theory and quantum mechanics have historically been separate fields, unrelated in most research. However, it has been recognized as increasingly important and vital to bring these two scientific fields of study together in order to advance both. Only through the study of quantum information science can quantum states be understood and manipulated sufficiently and appropriately to perform information transmission and manipulation at the quantum level [7]. Five important concepts of quantum computing must be considered in order to understand how the capability is possible and why it is so powerful and applicable to the meta-reality of cyber. First, we must comprehend the basic fundamentals of a quantum system: "Quantum mechanics depicts phenomena at microscopic level such as position and momentum of an individual particle like an atom or electron, spin of an electron, detection of light photons, and the emission and absorption of light by atoms" [7]. These characteristics and the ability to manipulate the states of subatomic particles by molding these characteristics is what makes quantum computing possible. This leads to the second component of quantum computing, superposition quantum states. In quantum computing, the primary characteristic of superposition is in the computer's ability to process information. In classical computing, the computer must handle ones and zeroes separately and sequentially. However, in quantum computing, the processor handles ones and zeros at the same time, handling matter in a state that sees it as a one and a zero simultaneously [7]. This interlacing of states between subatomic particles is what forms quantum entanglement (mentioned in the previous section). This ability to relate two particles together and make changes at a distance lead to the third area of quantum computing concepts, quantum circuitry: "A quantum computer can be created from a quantum circuit with quantum gates to perform quantum computation and manipulate quantum information" [7]. This capability can only be accomplished through the relationships formed between the particles in order to make necessary changes and distribute those changes throughout the quantum system (see Figure 3 *Quantum Computing Model*). This leads to the central and fourth concept of quantum entanglement: When two particles are entangled, they actually take on each other's properties and behaviors, allowing them to not only change in close proximity, but at a distance by way of an invisible wave function that connects them [7]. This invisible interlinkage is what makes the changes in states over distances possible. This is a very sophisticated and difficult concept to grasp, only further complicated by the fifth and final concept of quantum teleportation: "Quantum teleportation is a process by which we can transfer the state of a qubit from one location to another, without transmitting it through the intervening space" [7]. It is important to understand that although information concerning the change of the state of one particle to another only transfers the change in state and not the particle itself, resulting in a pure information transfer without actually expending the energy and time it would take to transfer the particle as is currently performed in traditional electron transfer computing.

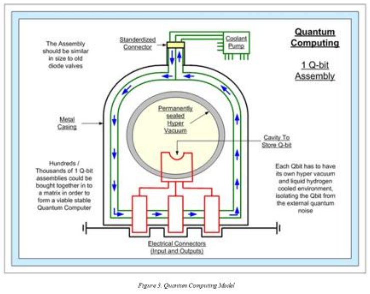
Quantum Computing
1 Q-bit Assembly
The Assembly should be similar in size to old diode valves
Standerdized Connector
Coolant Pump
Metal Casing
Permanently sealed Hyper Vacuum
Cavity To Store Q-bit
Hundreds / Thousands of 1 Q-bit assemblies could be bought together in to a matrix in order to form a viable stable Quantum Computer
Each Qbit has to have its own hyper vacuum and liquid hydrogen cooled environment, isolating the Qbit from the external quantum noise
Electrical Connectors (Input and Outputs)
Figure 3. Quantum Computing Model

Figure 3. Quantum Computing Model.

Armed with this basic understanding of quantum computing, we can now explore a few of the possibilities conceived through the use of this emergent technology. One of the most valuable capabilities available through the use of quantum computing is termed "quantum speedup". 'Quantum speedup' is simply the phenomenon that is characteristic of quantum computing speeds that allow them to perform certain calculations much faster than traditional computers [8]. This concept evolves from the fact that operations can be accomplished through the use of instantaneous and efficient data state transfer, making the speed potential of quantum computing virtually incalculable. Another area in which quantum computing has been theorized to make an enormous impact is that of collaborative scientific scaffolding to create mechanisms heretofore unheard of: "in theory it would be possible to combine advances in biotechnology, nanotechnology, and quantum computer technology to 'print' new life" [9]. While this might smack of science fiction, this kind of capability may be closer to reality than most understand, as we will see in the following section on nanotechnologies. In fact, Google recently produced a paper about its 53 qubit quantum computer *Sycamore*, titled "Quantum supremacy using a programmable superconducting processor" subsequently reported by *The Verge*, in which was printed, "Google's quantum computer was reportedly able to solve a calculation — proving the randomness of numbers produced by a random number generator — in 3 minutes and 20 seconds that would take the world's fastest traditional supercomputer, Summit, around 10,000 years. This effectively means that the calculation cannot be performed by a traditional computer, making Google the first to demonstrate quantum supremacy" [10]. Add to these advances the impending wave of 5G technologies and the wireless and electromagnetic spectrum (EMS) concerns attached to this ethereal superstructure. Quantum computing offers options for quickly transmitting data at a distance that very well may lead to a quantum 6G capability that far outstrips or possibly supports the 5G instantiation. Quantum properties can likewise support bandwidth traversal between satellites to broaden global data transmission such that hard solutions like undersea cables and hard wired national communications infrastructures could become redundant if not obsolete. Suffice it to say, quantum computing is an area of deep and broad interest in basically every area of life, especially for those of us in the cyber community.

V. NANOTECHNOLOGY

With microcomputers shrinking to smaller and smaller sizes yet offering faster processing, larger storage, wider bandwidth, and greater power, Moore's law is quickly approaching a breaking point. With this reality encroaching on manufacturers and consumers alike, numerous organizations are leveraging new scientific breakthroughs in nanotechnology to deliver the promise of continued lower cost and precipitous technological progress. Of course, the area that is seen to most probabilistically deliver is nanotechnology. Through the discovery and manipulation of such products as graphene and MOFs, materials capable of making the leap downward in size to a level capable of accommodating the attributes necessary for non-linear waveform manipulation, microscopic circuitry, and subatomic particle transmissions necessary for quantum computing are not only possible, but available for experimentation and eventual use. These advances also have direct applicability to advances in AI and ML as the processing, bandwidth, and other system requirements necessary to allow for the rapid acquisition, sorting, filtering, and decision making processes to continue AI and ML potentialities are vital to progression. Similarly, as quantum computing and AI/ML continue to grow, so too will quantum encryption capabilities.

As with quantum computing, it is important to understand some of the mathematical and particle physics concepts undergirding the inner workings of nanotechnology. A great deal of workability is wrapped up in the graphene honeycomb structure (see Figure 4 Graphene Honeycomb Lattice) capable of providing waveform packet containment and direction for subatomic particle manipulation that makes quantum computing viable. “There has been intense interest within the fundamental and applied physics communities in [honeycomb] structures… Graphene, a single atomic layer of carbon atoms, is a two-dimensional structure with carbon atoms located at the sites of honeycomb structures” [11]. To further explain this concept, one must grasp a sometimes comical anecdotal example based on the “nonlinear Schrödinger (NLS) equation” [12]. The story goes that Austrian physicist Erwin Schrödinger’s concept of superposition (matter occupying two states simultaneously) can be described through the example of a cat in an enclosure such as a box and with it a device that has a 50% chance of killing the cat. The idea is that until we open the box, we can’t state with any degree of certainty whether the cat is alive or dead. So, the cat basically occupies two states (alive and dead) simultaneously. This is a very elementary description of the concept, but it serves as a basic principle of the same issue attached to the ability of a subatomic particle to occupy two states simultaneously which makes quantum entanglement, quantum states, etc. possible. This has been demonstrated in laboratory experiments and through mathematical models such as the ones posited by Fefferman and Weinstein, Ablowitz and Zhu, and Hirokawa and Kosaka. The third team states in their research, “We gave concrete formulae explicitly showing the one-to-one correspondence between every self adjoint extension of the minimal Schrödinger operator and the boundary condition of the wave functions of the Schrôdinger particle. We proved that the boundary conditions are classified into two types: one is characterized by the wave function’s perfect reflection at the boundaries and the other by the wave function’s imperfect reflection with penetration from one island to another island” [13]. To put this in simpler terms, the outcome was a graphene waveform packet conductor capable of transmitting state data between two subatomic particles whose states had become entangled, thus allowing them to share state data at a distance within a system. This capability is a fundamental part of what creates the conditions necessary for quantum computing.

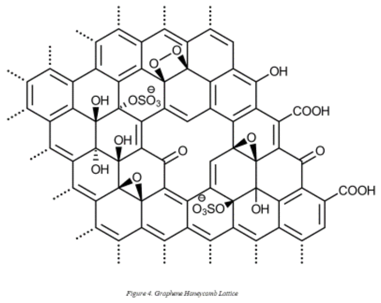

Figure 4. Graphene Honeycomb Lattice.

A separate technology also useful for data transmission is MOFs. “Thin films of inorganic porous crystals, zeolites and MOFs, have been developed for use as sensors, electronic materials, micro-reactors, and separation membranes. In particular, zeolite membranes have been attracting intense research interest as separation materials in the past decades. MOFs have also been studied in the field of membrane research in recent years” [14]. The ability to use these types of materials as sensors, reactors, and other electronic materials highlights their potential in systems architecture, especially in the area of power transfer, have wide applicability in the field of computing. While this technology has been used for decades in other areas, new applications for energy storage such as batteries and high-volume capacitors shows promise in the areas of cyber-enabled electronic drones as well as micro-drone clusters, not to mention portable computing devices.

More specifically as it relates to nanotechnology and nanomaterials is the question of their application to security within cyber systems. “Nanotechnology is expected to be a key enabling technology (KET) to sustain the development of future smart sensing systems and/or Cyber-Physical Systems (CPS) that will jointly integrate sensing, computation, communication and energy management functions” [15]. The applications vary widely with security applications at every layer of cyberspace. However, the most marked areas for advancement are probably authentication and cryptography systems. Currently, nano-optics are in development and have proven to be useful for the most sophisticated security authentication techniques. However, with the advancement of nano-enabled multi-parameter sensors, authentication may in the future include sophisticated access keys based on individualized multi-parameter techniques, including biological signals, which would be difficult to reproduce [15]. The complexity involved in producing authentication systems such as these rests heavily on nano capabilities as do those involved in cryptography. However, the encryption techniques and methods stem from a different angle. Since quantum computers are based on the fundamental information component of the qubit, they actually process information at the atomic level. As quantum technology and computing advance, so will the complexity of encryption, pattern recognition, and other security capabilities, making current cryptographic systems obsolete, if not in drastic need of reengineering [15].

Perhaps one of the most exciting and far reaching nano-enabled capabilities within the cyber meta-reality will be AI and ML. The United States, the National Strategic Computing Initiative (NSCI) made persistent demands on supercomputers to achieve incredible new levels of performance and power efficiency, insisting on the integration of new, more powerful exaflop supercomputers. Exaflop supercomputers will be about 30 times more powerful than today's fastest machines, and their graphics processing units will be able to handle up to ten times more operations per unit of energy compared to existing computers [15]. With processing capabilities like this, AI and ML computation, sorting, filtering, decision-making, and heuristics can be increased dramatically, allowing systems to learn and grow at an exponential rate.

The overall impact of nanotechnologies on the cyber meta-reality leads to amazing possibilities that are already breaching cyberspace and the physical domains as well. With such growth and impact, the introduction of the concept of a cyber microbiome may be of some interest and is worth additional thought and research beyond the scope of this paper. As the Earth and indeed human beings share their chemical/biological physicality with a host of enabling flora and fauna (Earth) and bacteria, fungi, protozoa, and even viruses (humans), the cyber meta-reality is growing into a type of non-physical, yet tangible sphere where stripping away or adding to it could have far-reaching ramifications yet understood. The human microbiome (Figure 5) has most recently been estimated to outnumber human cells by several orders of magnitude [16]. A cyber microbiome (Figure 6.) has already begun to take shape, characterized by viruses, archived data, dark Web outgrowths, and other symbiotic code and applications that will ostensibly grow rapidly as AI and ML begin to create additional code and data in the future. While the cyber microbiome may not be, in some cases, considered a direct part of the created domain we experience, it certainly must not be stripped away, eradicating the good along with the bad. The cyber microbiome is similar to its planetary and human corollaries in that it contains various undetectable components that serve to support its function in difficult to discern ways. For instance, the "dark web" as referenced in Figure 6 is much like the unseen portion of the iceberg under the surface. This indicates another way in which the cyber microbiome is so similar to its antecedents; the cyber microbiome is likely larger than visible cyberspace by many orders of magnitude. These basic understandings about the cyber microbiome serve as area of interest and concern and are worthy of further consideration.

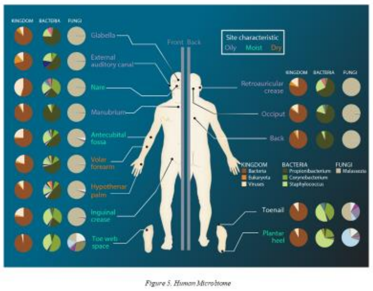

Figure 5. Human Microbiome.

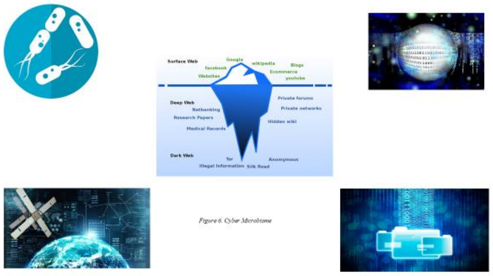

Figure 6. Cyber Microbiome.

VI. Conclusion

The world we encounter every day has an undercurrent of possibilities. There are new discoveries just below the skin of our reality and moving through and across what can be seen as the *cyber meta-reality*. With the rise of this cyber world of interconnections and technological upheaval, new capabilities are beginning to shape and expand the horizons of cyber and humans alike. AI and ML are reaching into areas and affecting systems in amazing and sometimes concerning ways. Quantum computing brings with it new capabilities including quantum encryption, enormous storage, unparalleled processing speeds, and seemingly infinite bandwidth. Nanotechnology and nanomaterials are critical enablers of all of these systems, providing the physical constructs to make them possible and practicable. Finally, with the almost organic, but silicone-based *cyber meta-reality* comes the emergence of a *cyber microbiome*; a symbiotic, construct yet unmapped that may lead to further understandings of the *cyber meta-reality* as well as our own physical one.

References

[1] M. Guillot, "Emerging Technology: Creator of Worlds" *Strategic Studies Quarterly*, Emerging Technology Special Edition (FALL 2016), Vol. 10, No. 3, pp. 3-8, 2016.

[2] F. Maymí and S. Lathrop, 2018. "AI in Cyberspace: Beyond the Hype," *The Cyber Defense Review* (FALL 2018), Vol. 3, No. 3, pp. 71-82, 2018.

[3] A. Kott. Intelligent Autonomous Agents are Key to Cyber Defense of the Future Army Networks, *The Cyber Defense Review* (FALL 2018), Vol. 3, No. 3, pp. 57-70, 2018.

[4] L. Janssens, *A Prospect Of The Future: How Autonomous Systems May Qualify as Legal Persons*, Amsterdam University Press, 2018.

[5] Y. Wang, “Quantum Computation and Quantum Information,” *Statistical Science* (August 2012), Vol. 27, No. 3, pp. 373-394, 2012.

[6] T. Waters, 2017. “Multifactor Authentication – A New Chain of Custody Option for Military Logistics,” *The Cyber Defense Review* (FALL 2017), Vol. 2, No. 3, pp. 139-148, 2017.

[7] Y. Wang, “Quantum Computation and Quantum Information,” *Statistical Science* (August 2012), Vol. 27, No. 3, pp. 373-394, 2012.

[8] M. Cuffaro, “How-Possibly Explanations in (Quantum) Computer Science,” *Philosophy of Science* (December 2015), Vol. 82, No. 5, pp. 737-748, 2015.

[9] M. Guillot, "Emerging Technology: Creator of Worlds” *Strategic Studies Quarterly*, Emerging Technology Special Edition (FALL 2016), Vol. 10, No. 3, pp. 3-8, 2016.

[10] J. Porter, “Google may have just ushered in an era of ‘quantum supremacy,” *The Verge*, accessed 8 October 2019 from https://www.theverge.com/2019/9/23/20879485/google-quantum-supremacy-qubits-nasa, 2019.

[11] C. Fefferman and M. Weinstein. “Honeycomb Lattice Potentials and Dirac Points,” *Journal of the American Mathematical Society* (OCTOBER 2012), Vol. 25, No. 4, pp.1169-1220, 2012.

[12] M. Ablowitz and Y. Zhu, “Nonlinear Waves in Shallow Honeycomb Lattices,” *SIAM Journal on Applied Mathematics*, Vol. 72, No. 1, pp. 240-260, 2012.

[13] M. Hirokawa and T. Kosaka, “One-Dimensional Tunnel-Junction Formula for The Schrödinger Particle,” *SIAM Journal on Applied Mathematics*, Vol. 73, No. 6, pp. 2247-2261, 2013.

[14] M. Sakai, M. Seshimo, and M. Matsukata. 2018. *Membrane Technology: How, Where, and Why*, Amsterdam University Press.

[15] A. Ionescu, “Nanotechnology and Global Security,” *Connections* (Spring 2016), Vol. 15, No. 2, pp. 31-47, 2016.

[16] N. Fierer et al., “From Animalcules to an Ecosystem: Application of Ecological Concepts to the Human Microbiome,” *Annual Review of Ecology, Evolution, and Systematics*, Vol. 43, pp. 137-155, 2012.

The views expressed are those of the author and do not necessarily reflect the official policy or position of the Air Force, the Department of Defense, or the U.S. Government.

DoD School Policy. DoD gives its personnel in its school environments the widest latitude to express their views. To ensure a climate of academic freedom and to encourage intellectual expression, students and faculty members of an academy, college, university, or DoD school are not required to submit papers or material that are prepared in response to academic requirements and not intended for release outside the academic institution. Information proposed for public release or made available in libraries or databases or on web sites to which the public has access shall be submitted for review.