Emerging Technologies for Data Security in Zero Trust Environments

Patrick Davis
Maj. Sean Coffey
Dr. Lubjana Beshaj
Lt. Col. Nathaniel D. Bastian, Ph.D.

ABSTRACT

Zero Trust (ZT), simply defined, is an information security framework which monitors and protects users, assets, resources, and data on a network by positively verifying all activity and never trusting anything by default. With the push to implement ZT across the public and private sectors, this transition between cybersecurity paradigms must be accomplished in a manner that is robust and enduring. This article examines emerging technologies most likely to impart the largest impact on ZT architectures (ZTAs), so that we better anticipate the pluses and minuses that will accompany those technologies. The discussion here focuses on data security, and the potential of each technology to affect security and protection across the lifecycle of data as it is generated, collected, transmitted, utilized, and stored. Technologies appraised include differential privacy, confidential computing, homomorphic encryption, quantum technology, biological technology, blockchain, and alternative computing methods.

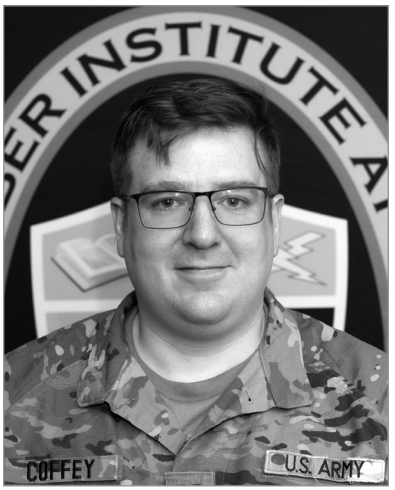
INTRODUCTION

The timing of this assessment is critical, as the Department of Defense (DoD) and the broader Federal Government have mandates to implement a baseline ZTA by 2027. Planning and implementing ZTA is further complicated by the accelerating pace of technological change in today's operating environment. Within the

Patrick Davis is a Research Scientist in the Data & Decision Sciences Division at the Army Cyber Institute within the Department of Electrical Engineering and Computer Science at the United States Military Academy (USMA) at West Point. He previously served as a Cavalry officer in the U.S. Army after graduating from USMA with honors with a degree in Electrical Engineering. He holds an MBA from The Wharton School and a Masters in Strategic Design from Parsons. His research and professional interests include data, decision sciences, applied computation, and innovation within strategic and leadership contexts of large enterprises and government.

past decade, in no small part due to the COVID-19 pandemic, both public and private organizations have embraced policies such as Bring Your Own Device (BYOD) and have moved computing workloads and data storage into commercial cloud-based services away from more costly, less capable, and less agile on-premises legacy architectures. At the same time, the volume, variety, and velocity of data has increased dramatically. The computational capacity and data availability driving the growth in Artificial Intelligence and Machine Learning (AI/ML) capabilities did not exist a few years ago, and those resources are expected to grow in scale for the foreseeable future. This creates new threat vectors and introduces new requirements for data security. Many enterprise-level security strategies struggle to keep up, especially in less data intensive industries. Given the pace of change and the nature of how technology shifts, prior approaches to data security using old technology will not hold up.

Data is critical to all network-reliant systems and operations. Adversarial actors are known to be operating domestically, internationally, and even within DoD entities, so the importance of data security cannot be overstated. DoD's 2023 Cyber Strategy details how the U.S. is continuously challenged by malicious cyber actors from the People's Republic of China, Russia, North Korea, Iran, violent extremist organizations, and transnational organizations; each pose threats to destabilize our democratic systems.[1] With the introduction of practical AI and more advanced emerging technologies for storing and processing data, we are now charged with countering these threats in an environment experiencing an explosion of change. The transition towards ZT will be a constantly moving target and the demand for a highly trained workforce will increase. Educating, recruiting, efficiently employing, and retaining talent who understand and can work with these emerging technologies is a matter of National Security.



Major Sean Coffey is a U.S. Army Cyber Warfare Officer trained in Cyberspace and Electromagnetic Activities (CEMA). Maj. Coffey currently serves as a Research Scientist and Machine Learning Engineer in the Data & Decision Sciences Division at the Army Cyber Institute within the Department of Electrical Engineering and Computer Science at the United States Military Academy (USMA) at West Point. Maj. Coffey earned an M.S. in Computer Science from the University of Minnesota and an M.S. in Data Analysis from the Georgia Institute of Technology. His research and engineering interests are in the areas of data science, artificial intelligence, machine learning, and scientific computing applied to CEMA, battlefield command and control systems, and privacy-enhancing emerging technologies.

Done well, ZTA reduces threat vectors and establishes a sustainable and adaptable framework that is forward compatible with future technologies. However, this modularity will not happen on its own. As such, this paper focuses on emerging technologies that are both critical to the future of ZT, but also require specific accommodations for a ZTA to truly actuate their potential benefits. In this paper, we provide an overview of ZT and discuss the relevant aspects of data security. Then, we introduce and discuss a series of emerging technologies that, as they mature and become more widely adopted, are postured to play a key role in advancing the Nation's ZT security posture and getting ahead of our adversaries. We conclude with a set of strategic recommendations for approaching these emerging technologies in terms of research, development, and innovation to better meet the needs of our future ZT environment.

ZERO TRUST

Since late 2018, National Institute of Standards and Technology (NIST) and National Cyber Center of Excellence researchers have worked closely with the Federal Chief Information Officer Council, federal agencies, and industry to address the challenges and opportunities for implementing ZTA across U.S. government networks. This resulted in publication of NIST Special Publication 800-207, which the DoD adopted for their definition of ZTA.[2]

ZT is the term for an "evolving set of cybersecurity paradigms that move defenses from static, network-based perimeters to focus on users, assets, and resources." At its core, ZT grants no implicit trust to assets or users based solely on their physical or network location or device ownership.[3] This shift in philosophy is a significant change in legacy perimeter-based authentication and security mechanisms. It also represents a major cultural change that stakeholders throughout DoD's ZT Ecosystem, including the

Lubjana Beshaj, Ph.D., is a Senior Research Scientist in the Data & Decision Sciences Division at the Army Cyber Institute within the Department of Electrical Engineering and Computer Science at the United States Military Academy (USMA) at West Point. She also serves on the faculty in mathematical sciences at USMA. Dr. Beshaj earned her Ph.D. in Mathematics from Oakland University. Her research interests include both cryptography and emerging technologies, specifically in algebraic curve cryptography, post quantum cryptography, homomorphic encryption, quantum stabilizer codes, blockchain technologies, and neural network cryptography.

Defense Industrial Base (DIB), will need to embrace and execute beginning with FY2023 through FY2027 and in the future.

ZT entails a collection of information security design principles intended to replace previous perimeter-based security design principles. A ZTA is a network that adheres to ZT principles to secure its systems, data, and processes. The ZT approach is built on the realization that well-defined security perimeters can no longer be relied on to protect assets and resources, as there is no single point in the security system that is robust and capable enough that it cannot be circumvented. A ZT approach assumes the network has already been compromised and that threat actors are operating and active throughout the network. As such, ZT does not automatically trust actors, systems, or services operating within a security perimeter. Instead, rigorous analysis is conducted, and strict compliance to enterprise policies are verified before, during, and after granting access to any enterprise resource. ZT focuses on protecting critical assets, particularly data, at a granular level.

DoD's ZT Strategy is shown in Figure 1. The strategy has four top-level goals that are each supported by objectives in the areas of cultural adoption, securing

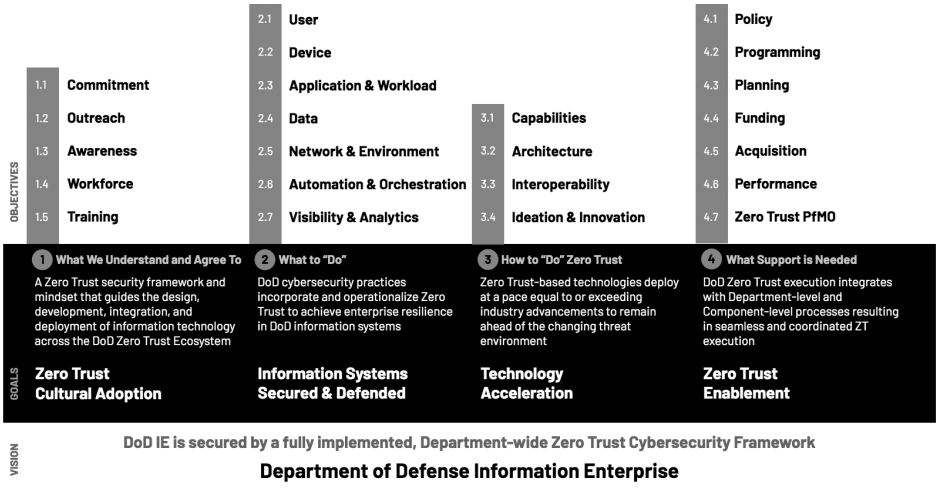


Figure 1. DoD ZT Strategy At-a-Glance

Lieutenant Colonel Nathaniel D. Bastian, Ph.D., is an Academy Professor and Cyber Warfare Officer at the United States Military Academy (USMA) at West Point. He is also concurrently serving as a Program Manager at the Defense Advanced Research Projects Agency (DARPA). At USMA, Lt. Col. Bastian serves as Division Chief, Data & Decision Sciences, Senior Research Scientist, and Chief Data Scientist at the Army Cyber Institute within the Department of Electrical Engineering and Computer Science. Lt. Col. Bastian earned a M.S. in Econometrics and Operations Research from Maastricht University and a M.Eng. in Industrial Engineering and Ph.D. in Industrial Engineering and Operations Research from Pennsylvania State University. His research interests aim to develop innovative, assured, intelligent, human-aware, data-centric, and decision-driven capabilities for cyberspace operations.

and defending information systems, technology acceleration, and execution enablement.[4] A common theme across all guidance is that data plays a central role.[5] In the following section, we will discuss key tenets of data security before turning to a discussion on emerging technologies that will increase our requirements for advancing and hardening data security within future ZT environments.

DATA SECURITY

Data is the lifeblood of the highly complex, interconnected socio-technical systems of societies, economies, and governments. It is the focal point of computation and conveys tactically and strategically valuable information about the behavior and intentions of individuals and organizations, and for that reason it is often targeted by adversarial actors. As such, the methods and practices used to secure data throughout its lifecycle are the cornerstone of any cybersecurity architecture.

The totality of benefits provided by modern computing networks can be reduced to data; the ability to store data for later, send data to others, and use data efficiently. Within network security, these states of data employment are known as “Data at Rest”, “Data in Transit”, and “Data in Use.” ZT requires us to broaden the perspective of data’s lifecycle by also considering “Data Generation” and “Data Collection” as two additional states.

ZT methods and practices enable data security by interweaving data encryption and secure network communication protocols with an encompassing data access paradigm based on two principles:[6]

1. Least privilege is the principle that any given user or automated process on a ZT network is only able to access the absolute minimum amount of data needed to perform the task at hand.

2. Assume breach is the principle where an organization never trusts any request or resource by default. Instead, all such requests need to be verified based on all available metrics. All security controls are conducted as if there was a known, yet to be located, malicious actor inside the network.

The employment of these principles across the data lifecycle – from generation to the point of collection, to storage, to data transmission, and while in use – make up the core of a ZTA. Each stage of the data lifecycle is given a brief section below which discusses some of the nuances of how the two guiding principles apply, all of which are relevant to specific emerging technologies discussed later in this paper.

Data at Rest

Data is stored at rest in databases and in file systems located on any storage system, which can be anything from dedicated servers to end user devices. Data at Rest is any data that is not currently actively in motion or in use, and as such it can be considered the default state of data.[7] The word "actively" is crucial to this definition. It is not enough to secure Data at Rest until it is about to be utilized, rather, Data at Rest needs to be secured up until the very moment when it changes to one of the other states, at which point the security procedures relevant to those states should be employed. Data at Rest can be extracted from systems and stolen when malicious actors obtain direct or indirect access to an organization's data sources or technology environments.

Critical infrastructure data is particularly vulnerable. In 2021, cybersecurity authorities in the United States, Australia, and the United Kingdom observed an increase in sophisticated, high-impact ransomware incidents against critical infrastructure organizations globally.[8] Authorities observed incidents involving ransomware against 14 of the 16 U.S. critical infrastructure sectors, including the DIB, emergency services, food and agriculture, government facilities, and IT sectors.[9] As threat actors become more technologically sophisticated, their tactics and techniques also evolve. They opportunistically identify weaknesses in personal and organizational data security, seeking to create an advantage or profit from exploiting sensitive data, including Personally Identifiable Information (PII) and Personal Health Information (PHI), trade secrets, intellectual property, and other private information stored in various formats, in different contexts, and across multiple devices and networks.

The General Data Protection Regulation (GDPR), drafted and passed by the European Union, includes provisions that relate to Data at Rest. The regulation specifies that only the minimum amount of data necessary should be stored, and in the case of personally identifiable data, it should be stored only for as long as it is needed for its intended purpose.[10] There is no federal equivalent to GDPR in the United States, although the California Consumer Privacy Act of 2018 includes privacy protections, such as the right to be forgotten, for consumers interacting with businesses that collect personal information.[11]

Data in Transit

Data in Transit, as the name implies, describes data currently in transit from one point in a network to another. While in transit, data is extremely difficult to secure, as most of the network traffic takes place across hardware and networks with different owners. Often even high-level administrators do not know the exact route network traffic will take from one point to another, even when operating in a semi-controlled environment.[12,13] This makes it particularly difficult to differentiate between malicious traffic, misrouted traffic, and normal traffic. Furthermore, these data signals are physically transmitted between devices using diverse types of transmission mediums such as twisted pair cable, coaxial cable, optical fiber, high-frequency radio waves (wireless), or lasers. Each of these mediums are uniquely vulnerable to distinct types of physical attacks, electromagnetic interference, and signal interception or tapping.

For data transmitted over the Internet, Hypertext Transfer Protocol Secure (HTTPS) is the most widely used security protocol. HTTPS is a combination of the standard HTTP protocol used for web communication and the Transport Layer Security (TLS) encryption protocol. When a user connects to a website using HTTPS, their browser initiates a TLS handshake with the web server.[14] During the TLS handshake, the server and client agree on a set of encryption and decryption algorithms to use for the session. Once the handshake is complete, all data transmitted between the server and client is encrypted using these agreed-upon algorithms, ensuring that unauthorized parties cannot intercept or tamper with the data. The security of HTTPS depends on the strength of the encryption and decryption algorithms used and the key management techniques employed. As such, it is crucial to use approved cryptography and regularly update the encryption algorithms and key management techniques to ensure that HTTPS remains secure against potential threats and attacks.

Peer-to-peer (P2P) security protocols are essential components of secure data transmission in cloud computing and on blockchains. P2P protocols enable secure data transmission between two or more devices, preventing unauthorized access and ensuring data confidentiality, integrity, and availability. TLS, for example, is widely used to secure web communications used in online banking, e-commerce, and email. Updates to TLS are managed by the Internet Engineering Task Force, and the most current version 1.3 was approved in 2018. Developers should use at least TLS version 1.2 or later. Secure Shell is another technique used to establish secure connections between devices for remote login and data transfer. Internet Protocol Security is used to secure Internet Protocol (IP) communication and is commonly used in enterprise networks, including virtual private networks.

Applying the second principle of ZT to Data in Transit, assume breach, it is assumed that network traffic traversing network midpoints and over different mediums is compromised. From this we arrive at the requirements for Data in Transit within a ZT security model. First, data must always be end-to-end encrypted. In addition, Digital Rights Management (DRM)

policies, which are also implemented to secure Data at Rest, should map back to relevant security policies, and ensure that only the minimum relevant data is transmitted at any given time. Finally, it is necessary to log, track, and filter network traffic to enable analytical detection of any anomalous behavior.[15] Because of the sheer volume of network traffic that needs to be analyzed, organizations should deploy advanced analytical methods from AI/ML to increase the efficiency and efficacy of finding the proverbial needle in the haystack.

Data in Use

Modern digital computing largely relies on three distinct types of processing units. Central Processing Units (CPUs) are responsible for the overall performance of most computers and devices. The CPU executes instructions of programs and can perform basic arithmetical and logical operations on data inputs to generate the desired output. Sometimes CPUs include several cores, which can process data in parallel, thereby increasing capability. However, CPUs are not ideally suited to execute advanced AI/ML algorithms in a reasonable amount of time. Both Graphics Processing Units (GPUs) and Tensor Processing Units (TPUs), working in combination with CPUs, provide magnitudes more processing capability and consume less energy than CPUs alone.[16] Multi-core CPU, GPU, and TPU can be deployed on local computers or servers, or ephemerally in cloud environments.

Data being processed within machine memory can be vulnerable. Attackers with physical or logical access to equipment (e.g., printers, fax machines), network appliances (e.g., routers, firewalls), workstations (e.g., desktops, laptops, tablets), servers, mainframes, or personal devices (e.g., smartphones, smartwatches), might copy or alter information stored within the device memory while it is in use. The prevalence of personally owned devices used to process organizational data have increased due to industry trends for BYOD policies where corporate and personal data is often processed on the same smartphone or laptop. Software can be reverse engineered, data can be copied, altered, deleted, or added, sensitive information such as PII or PHI might be exposed, and critical security parameters might be compromised allowing identity theft or fraud.

Additionally, the growing need for data-driven techniques and methodologies that require copious amounts of processing hardware has led to many entities outsourcing their computing needs to third parties in the form of cloud computing. This service provides the needed computation, but significantly increases the risk of sensitive data exposure, as a customer must now rely on the cloud service provider to employ adequate security techniques with limited ability to verify it for themselves.[17] The data itself might not even be the most significant risk for exposure, as exposure of cloud computing techniques might reveal proprietary algorithms or techniques, negating any competitive advantage in that domain.

Data Generation and Collection

The security implications of data generation and collection should also be considered when exploring the impact of emerging technologies on ZT. Data cannot be stored, transmitted, or used until it exists, whether collected from humans via human-computer interfaces or generated by devices, sensors, or systems autonomously. Data takes many different forms including text, images, audio, video, location coordinates, or application use telemetry. For data to be considered valuable, it does not have to be structured or formatted in any set way. Nor do the originators or subjects of the data collection necessarily know that collection is taking place. Different forms of AI/ML, such as large pre-trained models, can generate extremely realistic synthetic data, and interpret, summarize, and find patterns in data regardless of its format.

Modern data technology increases the value of data, but also introduces new risks. Once data exists, its pervasive quasi-controlled and uninformed use is a serious threat to individuals and organizations. In fact, there exists a legal multi-billion dollar data brokerage ecosystem that consists of companies that collect and generate data that they then sell, license, and share with other companies who use it for their own purposes or to provide technical services. This often includes sensitive personal data, and studies have shown some data brokers do very little due diligence on customers they sell their data to.[18]

Historically, data collected via web-based applications introduced vulnerabilities in which threat actors could inject malicious code or scripts directly into system data storage or even directly into the memory buffer. Over time, common web development frameworks incorporated security measures such as input masking and validation to prevent these types of risks. While direct attacks can be mitigated, these measures do little to actively protect users against social engineering attacks, such as phishing, that manipulate users into disclosing sensitive information including passwords, pins, usernames. This highlights why users should be aware of their system access privileges and their responsibilities in relation to accessing, entering, and securing their organization's sensitive data.

With this foundation of data security established, we will now move on to the emerging technologies anticipated to have the largest potential impact on a ZT future.

EMERGING TECHNOLOGIES

ZT changes the data security paradigm to be more compatible with future technologies and methodologies. In the ZT Reference Architecture, the Defense Information Systems Agency and National Security Agency ZT Engineering Team view emerging technologies as technical opportunities. They state that ZT "is an evolution of technology and operational approaches which over time evolve with the threat environment it is seeking to ameliorate."[19] The following sections delve into the emerging technologies most likely to play a role in ZT as they evolve.

Privacy-Enhancing Technologies

A Privacy-Enhancing Technology (PET) is one that embodies fundamental data protection principles by minimizing personal data use, maximizing data security, and empowering individuals. PETs allow online users to protect the privacy of their PII, which is often provided to and handled by services or applications. PETs use techniques to minimize an information system's possession of personal data without losing functionality.[20]

Differential Privacy

Differential privacy is a mathematically defined series of techniques and methods intended to allow data to be utilized and shared while reducing or eliminating the risk of sensitive exposure. Differential privacy was conceived in 2006 and is now widely used in both the public and private sectors. Companies including Microsoft, Apple, Google, Uber, Facebook, Amazon, LinkedIn, and Snapchat have embedded it into their products and continue to invest in ongoing research and development.[21] Most notably, from a Public Sector standpoint, the U.S. Census Bureau executed one of the largest-scale implementations of differential privacy for the first time during the 2020 Decennial Census.[22]

From a conceptual perspective, differential privacy adds noise to datasets to reduce the likelihood that any person or entity whose information is present within a dataset could be identified. Differential privacy also protects individuals or entities from being identified as participants in a particular data collection process.[23] This second aspect is important, as it ensures that participants in the dataset cannot be identified by simply excluding everyone who did not participate.

Differential privacy is powerful tool that reduces risk inherent in collecting sensitive data, such as is required for ZT. Implementing and operating a ZTA relies on capturing and analyzing large amounts of network information including network traffic flow, user behavior statistics, and other data to identify suspicious activity and to adjudicate requests for system access. Collecting this data creates a vulnerability as it must be accessed, processed, and shared regularly by both users and systems. Employing differential privacy reduces both the risk of exposing sensitive information and the value of that information to malicious entities.

Confidential Computing

Confidential computing loosely defines a range of techniques that enhance the security and privacy of Data in Use and is a recognized way forward to implement ZT DoD-wide. While not an emerging technology, confidential computing should be applied to hardware designed and manufactured for sensitive computing use cases, and is a powerful framework within a ZTA.[24] Confidential computing seeks to reduce data vulnerability before, during, and after it is processed, and is achieved by establishing hardware-based trusted execution environments that are secured using embedded encryption keys, and embedded identity

attestation mechanisms to ensure keys are accessible solely to authorized application code. It also enhances data protection in the cloud, especially as organizations move more sensitive data and computing workloads to public cloud services.

Although somewhat new to market capability, it is fully fielded and available from several private sector vendors.[25] Many consider confidential computing as an overarching term that defines all Data in Use protection techniques, to include homomorphic encryption.[26] However, the original term, coined by Intel in 2015, referred to a hardware level encryption technique, in which modern CPUs establish physically and/or logically secure enclaves during computation run-time. This secure enclave is logically removed from other operations within the CPU, and, for specific implementations by companies like Intel and Advanced Micro Devices (AMD), it also is physically separated from the rest of the CPU, although still on the same chip.[27]

Confidential computing has some key drawbacks, such as the absence of any mechanism to confirm data security throughout the entire process without continuously monitoring all incoming, outgoing, and internal data operations, which would be highly unfeasible, especially when relying on third party cloud computing resources. This drawback is flagged here, because vulnerabilities have been identified in confidential computing enclaves in the past.[28]

Software Guard Extension (SGX) is Intel's first iteration of a CPU with a secure hardware enclave. In 2017, researchers found a serious potential vulnerability in its implementation when they were able to extract RSA keys from within the enclave, and the enclave itself actually hid the presence of the malware, increasing the severity of the issue.[29] This led to Intel deprecating support for SGX for a number of years, until its competitor, AMD, partnered with Amazon to launch a competing confidential computing cloud service, which motivated Intel to bring the product line back.

The second major drawback of confidential computing is that implementations are hardware specific and rely on how the CPU is physically constructed.[30] When Intel abruptly suspended its SGX series CPUs, highly significant research to develop platform specific SGX implementations was ongoing.[31] These and other drawbacks notwithstanding, confidential computing remains a largely reliable and viable framework. The cloud based confidential computing services market is expected to multiply fourfold over the next five years, so it is highly likely all known drawbacks will be mitigated as the underlying technology and systems evolve.[32]

Homomorphic Encryption

Homomorphic encryption schemes allow computations on encrypted data without needing the secret decryption key. Fully homomorphic encryption maintains the privacy of search engine queries and enables the searching and editing of data and information that stays encrypted.[33] In AI/ML, fully homomorphic encryption maintains the security of not only

model input prompts and outputs, but also details of the model itself and the contents of its potentially sensitive training data.

Homomorphic encryption was first envisioned by Rivest, Adleman, and Dertouzos in 1978, well before a system with the required processing power could be built, and decades before Craig Gentry found the first practical implementation of a fully homomorphic system in 2009.[34] He did this using a lattice-based encryption scheme and a process called squashing and bootstrapping. Modern quantum resistant encryption schemes rely on the ring learning with errors problem which also uses highly-dimensional lattices.[35]

Fully homomorphic encryption allows a company or individual to have its data encrypted while other known parties run computations on that data without being able to decrypt it.[36] Traditionally the other party would need a private key to decrypt the data, modify it, encrypt it, and then send it back. This poses a security concern, especially when it comes to sensitive data, because if the outsourced company is subject to a cyber-attack, the attacker will gain access to all the unencrypted sensitive data. However, if homomorphic encryption is used, even if the attacker gains access to the data, it is encrypted through the entire process, yielding no clues as to what the actual data is or how it is being used. Therefore, homomorphic encryption could make a significant impact in the world of cryptography and data security.

Blockchain Technology

Blockchain technology was introduced in 2008 with the invention of Bitcoin by Satoshi Nakamoto.[37] Blockchain has seen significant evolution in recent years since its introduction. Bitcoin's market capitalization, the largest among all cryptocurrencies, currently exceeds $1 trillion and it continues to be the global standard bearer for digital currency. The second largest blockchain by market capitalization, Ethereum, is worth over $400 billion.[38] Ethereum has established itself as a versatile platform for various applications beyond its native cryptocurrency, ETH. Ethereum's blockchain facilitates smart contracts, decentralized applications, and decentralized autonomous organizations, showcasing its multifaceted utility. Today, there are over 200 blockchains, each with their own functional utility, with total market values over $1 million.[39] The proliferation of non-fungible tokens and other digital assets further highlights blockchain's expanding influence and utility.

Recent legislative efforts in Congress to begin regulating digital assets underscore the growing recognition and integration of blockchain technologies into mainstream financial and technological ecosystems.[40] This rapid evolution and increasing regulatory attention underscore blockchain's trajectory towards widespread adoption and its potential to revolutionize various industries.

A blockchain is an ever-growing, secure, shared, record-keeping system in which each user of the data holds a copy of the records, which can only be updated if all parties involved in a transaction agree to update. It is a P2P distributed ledger that is cryptographically

secure, append-only, immutable, and updateable only via consensus or agreement among peers. Blockchain can be thought of as a layer of a distributed P2P network running on top of the internet.[41]

Blockchain uses cryptographic techniques and operates over a decentralized network of nodes, where each node maintains a copy of the entire blockchain. Blockchain is considered to be a novel approach to distributed computing and data storage. In the context of computing, blockchain technology enables the management and storage of data across multiple systems, ensuring data integrity, transparency, and security. Blockchains are known as distributed networks because the data and control over the network are not centralized but are instead shared among participants. Each participant (node) in a blockchain network typically maintains its own copy of the entire ledger, and updates to the ledger are achieved through a consensus mechanism among these nodes. The consensus protocols in blockchain networks are crucial as they ensure all nodes in the network agree on the validity of transactions. The most common consensus protocols used in blockchain networks are Proof-of-Work (PoW) and Proof-of-Stake.

Data stored on blockchains must be verified by nodes on the network before entering the chain. Once a certain number of nodes agree on what data can be added, each by solving and sharing results of the same computationally complex consensus algorithm (in the case of PoW), the block containing the data is added to the chain. Data stored on blockchains are immutable and transactions are fully traceable. In contrast to traditional data networks, the robust cross-validation of blocks entering a blockchain network provides extra levels of security that cannot be found elsewhere. The computational power and associated costs required for each node to execute the consensus algorithm serves as an economic disincentive for attackers who might otherwise try to execute or confirm a nefarious transaction by tricking the requisite number of nodes (usually many) into forming a consensus at the same time for the same invalid blocks. Attacks like this are prohibitively expensive due to the intentional design of the network and are not guaranteed to succeed, even if attempted at great cost.

Quantum Technology

Quantum technology is an emerging field of physics and engineering that encompasses technologies that rely on the properties of quantum mechanics.[42] For the purposes of this analysis, we will address the three primary applications of quantum computing, quantum communications, and quantum sensing.

Quantum Computing

Quantum computing leverages quantum mechanical principles of entanglement and superposition to create quantum computers. A quantum bit, or qubit, can exist in an infinite number of states simultaneously and can also resolve to an identifiable binary state. Unlike the extremely reliable bits that underpin conventional computing, qubits are highly prone to

error and only operate in specific physical environments. Power-expensive error correction mechanisms are needed. Qubits tend to be prone to several types of environmental interference, so they can only be transmitted over limited distances and require special sensors to measure their state. Despite the challenges, there is rapid progress happening in quantum computing, in no small part a result of DoD-originated funding and research.[43]

Because qubits can be built with a variety of technologies, including superconducting circuitry, trapped ions, and photons, there are several variations of quantum computing currently being developed and researched.[44] Circuit-based, the most conventional or mainstream type, is the focus of investment by many major technology companies. Circuit-based quantum computers can be based on transmons (the focus of Google's and IBM's efforts) or based on trapped ions (employed by IonQ). Topological quantum computing employs exotic quasiparticles called anyons that are naturally resistant to errors and perturbations.[45] This fault-tolerant approach is being developed by Microsoft but is still in the early stages of physical realization of even one qubit. Another type of quantum computing known as measurement-based, or one-way, quantum computing exists, but is still in its conceptual stage.

Quantum annealing is a non-general approach to quantum computing that applies specifically to solving combinatorial optimization problems, where the goal is to find the optimal combination or arrangement of elements from a large set. The energy usage of the system corresponds to the objective function of the optimization problem, and the annealing process efficiently finds the lowest energy configuration that is also the optimal solution. This combined hardware- and software-based approach is being developed by D-Wave, who make instances of their computing solution available in the cloud. This shows tremendous promise, particularly for efficiently solving previously intractable optimization problems encountered in AI/ML use cases.[46] As quantum computers advance, their capabilities will further accelerate analytical progress and supercharge use cases across all industries.

Quantum Communications

Communications channels secured by quantum technology differ from classical information exchange in that the two parties know when a third party has attacked. This is because measuring an unknown quantum state changes it. If a third party eavesdrops on an exchange by trying to measure the key, this creates detectable anomalies in the quantum state. In the 1970s, well before his time, Stephen Wiesner introduced the concept of quantum conjugate coding—based on a method of transmitting multiple messages such that reading one destroys the others.[47] In 1984, his theory was used as a base for Bennet and Brassard to propose a method for secure communication called BB84. The BB84 scheme is at the basis of quantum key distribution (QKD) methods which are based on the idea of one-time pad (OTP). OTPs are in theory the strongest possible algorithmic cipher: if the key is used properly, they cannot be broken, even in theory.[48]

Post Quantum Cryptography

If large-scale quantum computers are ever built, they will be able to break many of the public-key cryptosystems currently in use. This would seriously compromise the confidentiality and integrity of digital communications on the Internet and elsewhere. The goal of post-quantum cryptography (also called quantum-resistant cryptography) is to develop cryptographic systems that are secure against both quantum and classical computers and with existing communications protocols and networks.

Since 2016, NIST publicly acknowledged that when large-scale quantum computers are realized, they will be able to break many of the public-key cryptosystems currently used in digital communications and for encrypting data. To counter this future vulnerability, NIST initiated a process to solicit, evaluate, and standardize quantum-resistant public-key cryptographic algorithms.[49] Following a November 2017 deadline for submission, NIST has continued to lead a public-facing process to narrow down the scope of possible candidates, and there are currently three algorithms still under consideration: CRYSTALS-Dilithium, CRYSTALS-KYBER, and SPHINCS+. The intent of NIST's effort is to specify one or more unclassified, publicly disclosed digital signatures, public-key encryption, and key-establishment algorithms and make them available for use around the world.[50]

Quantum Sensing

Quantum sensors and measurement devices provide accuracy, stability, and new capabilities that offer advantages for commercial, government, and scientific applications. Examples such as atomic clocks for GPS navigation and nuclear spin control for magnetic resonance imaging are already widely used, with transformative impacts for society. Further advances in quantum information science and technology will enable a new generation of similarly transformative sensors that will increase the volume, variety, and value of data that can be generated. While quantum sensors can potentially enhance decision-making in a military context, adversarial use of the same technologies against us has serious security implications. Researching how to work with, secure, and trust data generated by quantum sensors will help drive innovation and serve as a competitive advantage against adversaries.

Biological Technology

Biological technology, or biotechnology, is expected to have a major impact across various sectors, including health, energy, and national security. Data is crucial for advancing biotechnology innovations, and ZT is an appropriate security framework for protecting sensitive health information and proprietary research data within the field. In "Bold Goals for U.S. Biotechnology and Biomanufacturing: Harnessing Research and Development to Further Societal Goals," The White House Office of Science and Technology Policy highlights the pivotal role of data and the importance of data standards in the future of biotechnology:

> Global bioeconomy strategies recognize that a sustainable, safe, and secure bioeconomy is built upon standards and the availability of high-quality data. Data, particularly from genomics and multiomics, underpins advances in biotechnology, for example, by enabling the rapid design of systems to produce needed medicines, food, and materials. Standards, particularly international data standards, can help accelerate research and development (R&D) and commercialization of new, safe, and effective medicines and therapeutics; contribute to food product safety, quality, and consistency; promote international trade; and instill confidence among consumers for products in all sectors of the economy. For industry, standards can promote research and manufacturing innovation, streamline regulatory review, and enable international alignment, interoperability, and coordination. As biotechnology converges with automation, connected devices, and AI, a robust data infrastructure can also accelerate R&D and commercialization of emerging technology.[27]

DNA Computing

By 2025, it is estimated that the entire data universe will be 175 zettabytes.[53] Storage systems that now hold the world's data in the form of 0's and 1's will not be able to keep up, so finding ways to store and compute biological forms of data have become increasingly relevant problems. One approach is DNA-based data storage.

DNA is genetic material in all organic organisms and is composed of two polynucleotide chains that coil around each other in a double helix formation. Each polynucleotide is composed of smaller units consisting of one of four nitrogen containing nucleobases: cytosine (C), guanine (G), adenine (A), or thymine (T).[54] Researchers are harnessing these pattern-based strands to store data. By allowing each nucleobase to represent a two-element binary value (00=A, 01=T, 10=C, 11=G), DNA can be made to represent a table for use in bitwise arithmetic operations. Encoding DNA to represent data occurs through DNA synthesizing.[55] This recent research opens the cyber world up to the possibility of harnessing DNA as a medium for larger-scale computations and data storage. DNA can be sequenced and accurately copied and is quite stable. A single gram of DNA can store a single Zettabyte (one billion terabytes).

DNA also can be very useful to encrypt and decrypt data. Nucleotides, representing binary values, allow theoretical algorithms to be derived for encrypting and decrypting data. DNA cryptography is a proposed technique of encryption and decryption in which data can be hidden within a DNA sequence. This technique is very promising due to the powerful potential of DNA computing and data storage. Hiding data within DNA alone is insufficient to keep it secret, but applying known and new ciphers to data already sequenced into DNA shows great promise.[56]

DoD has a vested interest in and actively contributes towards research and development to understand, harness, and manage the implications of advances in each of these emerging technologies on society, in warfare and for diplomacy. Data, and the security of data in these

new human-technological contexts, will continue to be an important topic of discussion, debate, investment, and innovation as the opportunities and vulnerabilities of our future technological environment become more clear. Now that we have covered the preliminaries of ZT, data security, and emerging technologies, we consider their future implications.

ANALYSIS AND DISCUSSION

In the evolving landscape of ZT, quantum technology, biotechnology, blockchain, and PETs (e.g. differential privacy, confidential computing, and homomorphic encryption), present both opportunities and challenges for data security. DoD's ZT Strategy emphasizes seven key data capabilities necessary for implementing ZT: data catalog risk alignment, DoD enterprise data governance, data labeling and tagging, data monitoring and sensing, data encryption and rights management, data loss prevention, and data access control.[57] These capabilities must be examined for all new data-driven applications of technology both through the lens of data security and across the entire data lifecycle, which encompasses Data Generation, Data Collection, Data at Rest, Data in Transit, and Data in Use.

Data security implications vary significantly across different applications of technology. In ZT environments, enforcing the principle of least privilege ensures that users, devices, and systems access only the necessary data for their specific purposes. When assuming breach, every interaction involving data must be authenticated and never trusted by default. This is particularly challenging when designing secure applications in tactical environments where devices and communications are subject to denial, disconnection, intermittency, or limited bandwidth (DDIL).[58] Devices and systems that comprise the Battlefield Internet of Things, although highly capable in some cases, are often resource constrained and can only execute their main functionality, making them less capable of defending themselves against attacks. Advances in quantum computing, applied in the AI/ML development process, can reduce the size and complexity of security models, enabling them to run in resource constrained devices in DDIL environments.

In tactical environments, Electronic Warfare (EW) weapons can disrupt data generation and collection by jamming sensors and communication devices, leading to corrupted or incomplete data. For Data at Rest, electromagnetic pulses or directed energy weapons could physically damage storage infrastructure, highlighting the need for physical security and redundancy. Data in Transit is particularly vulnerable to EW, where interception and jamming can delay or compromise the transmission of sensitive information. Quantum-safe encryption and secure communication protocols, including QKD as it progresses towards operational readiness, will be vital in safeguarding Data in Transit. While emerging technologies offer potentially promising solutions, they also introduce new layers of complexity which could be infeasible given operational constraints. Regardless, in designing secure devices and applications, particularly in sensitive and tactical environments, trade-offs are inevitable,

and the focus must remain on robust data access control and continuous authentication to ensure data security.

Security considerations should be proactively integrated into the earliest phases of innovation and engineering for any application or system that touches data throughout its lifecycle. This is consistent with "Secure by Design" guidance published by the Cybersecurity Infrastructure Security Agency and global partners, which empowers designers and engineers to consider security throughout the design process.[59] Neglecting security and privacy in incipient phases will inevitably result in an ineffective reactionary security posture. At the scale and speed that modern networks operate, and as adversaries become more sophisticated, this is untenable. Therefore, it is essential for designers, engineers, and security professionals to have a shared understanding of how PETs, for instance, may apply to a data security problem as well as their unique implementation considerations.

While technologically advanced adversaries can disrupt data generation and collection, and also generate, collect, and use data for their own intelligence purposes, it is often much easier to target Data at Rest and Data in Transit in more vulnerable legacy systems. Identifying and addressing these vulnerabilities is crucial, especially as adversaries find new ways to attack us and degrade our capabilities. Frameworks such as MITRE's ATT&CK and ATLAS are invaluable for understanding the threat. The ATT&CK knowledge base compiles adversary tactics and techniques from real-world observations and aids in developing threat models and methodologies across various sectors.[60] Similarly, MITRE ATLAS describes adversary tactics and techniques in AI systems based on observed attacks and realistic demonstrations by AI red teams.[61] These frameworks show how adversaries target and exploit data, and should be leveraged in the early phases of design to define an application's data security requirements; they exemplify the benefits of collaboration across industry, academia, and government, and provide a common taxonomy for threat intelligence further enabling the testing and development of improved network and system defenses.

Advances in quantum computing will revolutionize critical analytical capabilities needed for bolstering defenses and achieving ZT. Quantum machines already have the ability to solve formerly unsolvable, highly-dimensional optimization problems by processing vast amounts of data at incredible speeds and exploring extremely large solution spaces near instantaneously. Furthermore, there are known data- and model-related challenges in classical AI/ML approaches that quantum compute solutions can potentially overcome which warrant further investigation and research. As DoD increases reliance on AI/ML for security monitoring, network intrusion detection, and other ZT related use cases, quantum compute is poised to further enhance data capabilities, increase efficiency and accuracy of these systems, save time, and enable deployment further to the edge by requiring fewer compute resources.

Quantum computing can also be used to create extraordinarily realistic datasets for training AI/ML models, particularly in cases where training datasets are insufficient or not available. Data labeling and tagging is now a mission critical capability. For many cybersecurity use cases, biotechnology initiatives in particular will rely on increasingly sensitive and large scale biological data (e.g., DNA and human genes) that necessitates precise labeling and tagging. AI/ML-enhanced automation can help improve accuracy and consistency of training datasets. PETs can also be leveraged when the labeling and tagging process involves sensitive data that could be either inadvertently exposed or purposefully exploited or manipulated by adversaries intending to attack or steal information about the underlying models, their intended capabilities, or the data used to train them.

Quantum sensing capabilities will enable the generation of precise and accurate data for sensing and measuring objects and phenomenon currently invisible to us and our systems. Examples of applications include more accurate and reliable geolocation, improved medical diagnostic imaging, safer navigation of autonomous vehicles, better guidance systems, and detection, imaging, and mapping of underground environments.[62] Quantum sensing will also significantly accelerate our ability to integrate data from several disparate sources and sensors for near real time monitoring and analysis, even in noisy environments. These are particularly valuable data generating use cases for DoD, but quantum sensing is still a capability that few people know about and has yet to reach widespread adoption.[63] Although quantum sensing has fewer immediate implications on data security and ZT, the intellectual property associated with ongoing research is highly sensitive and needs to be protected in accordance with ZT principles.

For systems that require many users and devices to generate, collect, store, transmit, or use sensitive data, blockchain technology will play an increasingly key role in enterprise data governance. Blockchains provide, by design, secure and transparent methods for tracking data lineage and automating compliance with governance and security policies. Its decentralized and immutable ledger guarantees that all actions and modifications to data are logged and auditable. Custom private blockchain platforms can track access to data for labeling and tagging, monitoring and sensing, and data loss prevention in a ZT environment. In addition, the rules necessary for data catalog risk alignment, rights management, and access control can be programmatically defined, managed, and automatically executed on a blockchain platform.

As emerging technologies reshape the landscape of data processing and storage, the need for robust privacy-enhancing technologies will remain critical. Homomorphic encryption allows computations directly on encrypted data, which can be used to enhance DRM and for data loss prevention without compromising privacy. It can also be used in data labeling and tagging use cases where details of the models and data used to train them need to remain secret but could

become exposed (or derived) during their usage. Engineering challenges in implementing, assuring, and verifying fully homomorphic encryption schemes necessitate advanced methods for their design and testing before they can be broadly adopted within ZTAs.

Confidential computing secures data processing at the hardware level. It therefore plays an important role in securing environments where AI/ML is used for sensitive computation and strict policies need to be enforced for Data in Use. As cloud adoption grows and global competition for semiconductors intensifies, supply chain gaps and vulnerabilities in chip design and fabrication pose serious risks. Advanced verification methods are required to ensure that sophisticated chips are free from security flaws and function as intended, as such risks may only surface during future use. Furthermore, novel confidential computing techniques will be necessary to secure the unique hardware used in quantum and biotechnological computing use cases.

Differential privacy protects individual privacy of subjects included in data sets used for model training, analysis, statistics, or informational reporting products. This will become increasingly vital as progress in quantum technology and biotechnology heighten the sensitivity and implications of Data in Use, especially in contexts which require transparency. This is the case for securely sharing data for decision-making, R&D, or innovation, as well as meeting regulatory or compliance requirements. Standards for evaluating effectiveness and providing assurance for differential privacy and other PET implementations will be necessary as ZTAs become more mature and widespread.

ZT fundamentally strengthens data security by ensuring that trusted user and device access to sensitive data is closely monitored to identify and prevent malicious exploitation. Together, the technologies discussed not only align with, but also enhance DoD's ZT posture, creating a robust, resilient, and secure data environment that can withstand evolving cybersecurity threats introduced by new technologies and persistent adversaries.

CONCLUSION

Given the immense potential of emerging technologies and their transformative applications, ZT stands as the ideal framework to guide data security practices and decision-making. Interplay among these emerging technologies and PETs underscores a complex yet promising future for ZT environments. Quantum technology enhances data generation, computation, processing, and security; biotechnology introduces new forms of data computation, storage, and relies on sensitive data that requires rigorous protection; and blockchain provides a decentralized, tamper-evident framework for data integrity and secure transactions. At the same time, PETs ensure that data produced and consumed by modern data systems remains secure and private throughout its lifecycle.

Addressing ZT security challenges at the interface between humans and machines will require innovation that capitalizes on the capabilities of today's emerging technologies. Innovation ecosystems are already emerging to support quantum technology, biotechnology, and blockchain. These communities can contribute towards addressing society-wide challenges and opportunities related to data security and privacy, but doing so will require a common vision, coordination, collaboration, and research. Prioritized and synchronized R&D is important in strategic areas such as workforce education, innovation and engineering, partnership building, and scientific research. Sustainable innovation requires careful balance between risk and reward, managing resource constraints, and making cost-benefit trade-off decisions in an extremely complex environment. The technologies described are poised to revolutionize and optimize how we do all these things in the future.

ZT is a large and complex engineering and cultural undertaking. No data technology is out of scope, whether on the bleeding edge or embedded in legacy systems. DoD's mission to accelerate decision advantage and sustained focus on data security must drive these efforts in support of broader national security objectives. DoD is uniquely suited to address complex multi-faceted problems such as ZT, where real world consequences raise the stakes above profit-oriented objectives. DoD must continue leading and expanding efforts to partner with industry, allies, and academia to drive innovation based on science and evidence-based decision-making.

Even though these emerging technologies will be cross-cutting and broadly impactful, each use case is unique. Both the magic and the devil are in the details. This requires careful prioritization and resource allocation towards current R&D efforts and for the future maintenance, sustainability, and protection of systems and infrastructure that we are increasingly dependent upon. This reinforces the absolute necessity of nurturing and expanding a diversified pipeline of educated, experienced, and motivated talent who can work with these emerging technologies and help shape the future. Failing to plan for and anticipate our future needs poses a serious risk to our technological society.

DISCLAIMER

The views expressed here are of the authors alone. They do not reflect the policy or position of the U.S. Military Academy, U.S. Army, U.S. Department of Defense, or U.S. Government.

NOTES

1. U.S. Department of Defense, *Summary of the 2023 Cyber Strategy of The Department of Defense*, (September 12, 2023). https://media.defense.gov/2023/Sep/12/2003299076/-1/-1/1/2023_DOD_Cyber_Strategy_Summary.pdf, 1-2.
2. National Institute of Standards and Technology, "Implementing Zero Trust Architecture," NIST National Cybersecurity Center of Excellence, accessed May 20, 2008, https://www.nccoe.nist.gov/projects/implementing-zero-trust-architecture.
3. Scott Rose, Oliver Borchert, Stu Mitchell, and Sean Connelly, "NIST Special Publication 800-207: Zero Trust Architecture," (August 2020). *Computer Security*, https://doi.org/10.6028/NIST.SP.800-207, ii.
4. U.S. Department of Defense (DoD) Chief Information Office (CIO), Zero Trust Portfolio Management Office, *DoD Zero Trust Strategy* (October 21, 2022). https://dodcio.defense.gov/Portals/0/Documents/Library/DoD-ZTStrategy.pdf, vi.
5. Defense Information Systems Agency DISA) and National Security Agency (NSA), *Department of Defense Zero Trust Reference Architecture version 2.0*, (July 2022). https://dodcio.defense.gov/Portals/0/Documents/ Library/(U)ZT_RA_v2.0(U)_Sep22.pdf, 21-23.
6. Barclay Osborn, Justin McWilliams, Betsy Beyer, and Max Saltonstall, "BeyondCorp: Design to Deployment at Google," (Spring 2016). *Usenix, The Advanced Computing Systems Association Journal*, volume 41, no. 1, https://storage.googleapis.com/gweb-research2023-media/pubtools/pdf/44860.pdf, 28-32.
7. Iftekhar Ahmed, Tahmin Nahar, Shahina Sultana Urmi, and Kazi Abu Taher, "Protection of Sensitive Data in Zero Trust Model," (March 2020). *ICCA 2020: Proceedings of the International Conference on Computing Advancements*, https://doi.org/10.1145/3377049.3377114, 1-5.
8. U.S. Department of Justice, U.S. Cybersecurity and Infrastructure Agency, U.S. National Security Agency, Australian Cyber Security Centre, and U.K. National Cyber Security Centre, "Joint Cybersecurity Advisory: 2021 Trends Show Increased Globalized Threat," (February 9, 2022) https://www.cisa.gov/sites/default/files/publications/AA22-040A_2021_Trends_Show_Increased_Globalized_Threat_of_Ransomware_508.pdf
9. U.S. Department of Justice et al., "Joint Cybersecurity Advisory: 2021 Trends Show Increased Globalized Threat."
10. European Parliament and Council of the European Union, "General Data Protection Regulation- Regulation (EU) 2016/679," (April 27, 2016). *Official Journal of the European Union*, L 119: 1-86. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679.
11. State of California Department of Justice, "The California Consumer Privacy Act (CCPA) of 2018," (last modified April 2024), https://cppa.ca.gov/regulations/pdf/cppa_act.pdf.
12. Pascal Poupart, Zhitang Chen, Priyank Jaini, Fred Fung, Hengky Susanto, Yanhui Geng, Li Chen, Kai Chen and Hao Jin, "Online Flow Size Prediction for Improved Network Routing," (November 8, 2016). IEEE 24th International Conference on Network Protocols (ICNP) Workshop on Machine Learning in Computer Networks, https://doi.org/10.1109/ICNP.2016.7785324, 1-6.
13. William Su, Sung-Ju Lee and Mario Gerla, "Mobility Prediction and Routing in Adhoc Wireless Networks," (January 18, 2001). *International Journal of Network Management* volume 11, no. 1, https://doi.org/10.1002/nem.386, 3-30.
14. Su, Lee, and Gerla, "Mobility Prediction and Routing in Adhoc Wireless Networks," 4.
15. DISA and NSA, "Zero Trust Reference Architecture," 19.
16. Goran Nikolic, Bojan R. Dimitrijevic, Tatjana R. Nikolic, and Mile K. Stojcev, "A Survey of Three Types of Processing Units: CPU, GPU and TPU," (June 16, 2022). *57th International Scientific Conference on Information, Communication and Energy Systems and Technologies (ICEST)*, https://doi.org/10.1109/ICEST55168.2022.9828625, 1-6
17. Osborn, McWilliams, Beyer, and Saltonstall, "BeyondCorp," 28-34.
18. Justin Sherman et al., "Data Brokers and the Sale of Data on U.S. Military Personnel: Risks to Privacy, Safety, and National Security," (November 2023). Sanford School of Public Policy, Duke University, https://techpolicy.sanford.duke.edu/wp-content/uploads/sites/4/2023/11/Sherman-et-al-2023-Data-Brokers-and-the-Sale-of-Data-on-US-Military-Personnel.pdf.
19. DISA and NSA, "Zero Trust Reference Architecture," 63.
20. The Dutch Data Protection Authority PISA Consortium, "PET" in *Handbook of Privacy and Privacy-Enhancing Technologies: The case of Intelligent Software Agents*, (November 2003). The Hague: College Bescherming Persoonsgegevens, ed. G.W. Blarkom, J.J. Borking, and J.G.E. Olk, https://doi.org/10.13140/2.1.4888.7688, 33-53.

NOTES

21. Raina Gandhi, "Technology Factsheet: Differential Privacy," (Fall 2020). Belfer Center for Science and International Affairs, Kennedy School, Harvard University, https://www.belfercenter.org/publication/technology-factsheet-differential-privacy.
22. Michael B. Hawes, "Implementing Differential Privacy: Seven Lessons From the 2020 United States Census," (September 2020). *Harvard Data Science Review* vol. 2, no. 2, https://doi.org/10.1162/99608f92.353c6f99, 2-3.
23. Daniel L. Oberski and Frauke Kreuter, "Differential Privacy and Social Science: An Urgent Puzzle," (January 2020). *Harvard Data Science Review* vol. 2, no. 1, https://doi.org/10.1162/99608f92.63a22079, 4-6.
24. DISA and NSA, "Zero Trust Reference Architecture," 70-71.
25. Rick Merritt, "What is Confidential Computing?," (March 1, 2023). NVIDIA, https://blogs.nvidia.com/blog/2023/03/01/what-is-confidential-computing/.
26. Sergei Arnautov, Bohdan Trach, Franz Gregor, Thomas Knauth, Andre Martin, Christian Priebe, Joshua Lind, Divya Muthukumaran, Dan O'Keeffe, Mark L. Stillwell, David Goltzsche, David Eyers, Rüdiger Kapitza, Peter Pietzuch, and Christof Fetzer, "SCONE: secure Linux containers with Intel SGX," (November 2, 2016). P*roceedings of the 12th USENIX conference on Operating Systems Design and Implementation*, Savannah, GA: The Advanced Computing Systems Association, https://www.usenix.org/system/files/conference/osdi16/osdi16-arnautov.pdf, 689-690.
27. Do Le Quoc, Franz Gregor, Jatinder Singh, and Christof Fetzer, "SGX-PySpark: Secure Distributed Data Analytics," (May 2019). *WWW '19: The World Wide Web Conference*, San Francisco, CA: Association for Computing Machinery, https://doi.org/10.1145/3308558.3314129, 3564-3565.
28. Richard Chirgwin, "Boffins Show Intel's SGX Can Leak Crypto Keys," *The Register,* March 7, 2017, accessed November 1, 2023, https://www.theregister.com/2017/03/07/eggheads_slip_a_note_under_intels_door_sgx_ can_leak_crypto_keys/.
29. Chirgwin, "Boffins Show Intel's SGX Can Leak Crypto Keys".
30. Arnautov et al., "SCONE: secure Linux containers with Intel SGX," 689-690.
31. Arnautov et al., "SCONE: secure Linux containers with Intel SGX," 702.
32. Merritt, "What is Confidential Computing?".
33. Craig Gentry, "A Fully Homomorphic Encryption Scheme," (September 2009). *A Dissertation Submitted to the Department of Computer Science and the Committee of Graduate Studies of Stanford University*, https://crypto.stanford.edu/craig/craig-thesis.pdf.
34. Chiara Marcolla, Victor Sucasas, Marc Manzano, Riccardo Bassoli, Frank H.P. Fitzek, and Najwa Aaraj, "Survey on Fully Homomorphic Encryption, Theory, and Applications," (October 2022). *Proceedings of the IEEE* vol. 110, no. 10, https://doi.org/10.1109/JPROC.2022.3205665, 1572-1609.
35. Marcolla et al., "Survey on Fully Homomorphic Encryption, Theory, and Applications," 1576–1584.
36. Marcolla et al., "Survey on Fully Homomorphic Encryption, Theory, and Applications," 1572.
37. Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," (October 31, 2008) Accessed May 28, 2024, https://bitcoin.org/bitcoin.pdf.
38. CoinDesk, "CoinDesk Digital Assets Data and Research, Cryptocurrency Index," Accessed June 18, 2024, https://www.coindesk.com/indices
39. CoinDesk, "CoinDesk Digital Assets Data and Research, Cryptocurrency Index"
40. Alexandra Andhov, "The U.S. Financial Innovation and Technology Act: Initial Overview," (May 29, 2024). *Forbes*, Accessed May 30, 2024, https://www.forbes.com/sites/digital-assets/2024/05/29/the-us-financial-innovation-and-technology-act-initial-overview/.
41. Imran Bashir, *Mastering Blockchain*, 3rd. Edition, (August 31, 2020) Birmingham, U.K.: Packt Publishing.
42. "Quantum Technology," *Wikipedia*, accessed May 6, 2024. https://en.wikipedia.org/wiki/quantum_technology.
43. Sydney J. Feedberg Jr., "Off to the Races: DARPA, Harvard Breakthrough Brings Quantum Computing Years Closer," (December 7, 2023). *Breaking Defense*, https://breakingdefense.com/2023/12/off-to-the-races-darpa-harvard-breakthrough-brings-quantum-computing-years-closer/.
44. Michael Brooks, "What's Next for Quantum Computing," (January 6, 2023). *MIT Technology Review*, accessed December 15, 2023, https://www.technologyreview.com/2023/01/06/1066317/whats-next-for-quantum-computing/.

NOTES

45. Ville Lahtinen and Jiannis K. Pachos, "A Short Introduction to Topological Quantum Computation," (September 9, 2017). *SciPost Physics* vol. 3 no. 021, 1-44, https://doi.org/10.21468/SciPostPhys.3.3.021.
46. Patrick Davis, Sean Coffey, Lubjana Beshaj, and Nathaniel Bastian, "Quantum Machine Learning for Feature Selection in Internet of Things Network Intrusion Detection," (June 7, 2024). *Proceedings of Quantum Information Science, Sensing, and Computation XVI*, volume 13028, 1-15, https://doi.org/10.1117/12.3013539.
47. Stephen Wiesner, "Conjugate Coding," (January 1, 1983). ACM SIGACT News, vol,. 15, no. 1, Association for Computing Machinery, https://dl.acm.org/doi/10.1145/1008908.1008920, 78-88.
48. Steven M. Bellovin, "Frank Miller: Inventor of the One-Time Pad," (July 1, 2011). *Cryptologia* vol. 35 no. 3, https://doi: 10.1080/01611194.2011.583711, 203-222.
49. National Institute of Standards and Technology (NIST), "Post Quantum Cryptography Overview," (last modified May 28, 2024). *NIST Computer Security Resource Center*, accessed May 28, 2024, https://csrc.nist.gov/projects/post-quantum-cryptography.
50. NIST, "Post-Quantum Cryptography Standardization," (last modified May 28, 2024). *NIST Computer Security Resource Center*, accessed May 28, 2024. https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization.
51. Office of the President of the United States, *Bringing Quantum Sensors to Fruition*. (March 2022). Report, National Science and Technology Council, Subcommittee on Quantum Information Science, https://www.quantum.gov/wp-content/uploads/2022/03/BringingQuantumSensorstoFruition.pdf.
52. Office of the President of the United States, *Bold Goals for U.S. Biotechnology and Biomanufacturing: Harnessing Research and Development to Further Societal Goals*," (March 2023). Report, The White House Office of Science and Technology Policy, https://www.whitehouse.gov/wp-content/uploads/2023/03/Bold-Goals-for-U.S.-Biotechnology-and-Biomanufacturing-Harnessing-Research-and-Development-To-Further-Societal-Goals-FINAL.pdf, 32
53. Sang Yup Lee, "DNA Data Storage Is Closer Than You Think," (July 1, 2019). *Scientific American*, accessed May 28, 2024, https://www.scientificamerican.com/article/dna-data-storage-is-closer-than-you-think/.
54. Rachael Rettner, "What is DNA?," (March 17, 2023). *Live Science*, accessed November 1, 2023, https://www.livescience.com/37247-dna.html.
55. Federico Tavella, Alberto Giaretta, Triona Marie Dooley-Cullinane, Mauro Conti, Lee Coffey, and Sasitharan Balasubramaniam, "DNA Molecular Storage System: Transferring Digitally Encoded Information through Bacterial Nanonetworks," (September 2021). *IEEE Transactions on Emerging Topics in Computing* vol. 9 no. 3, https://doi.org/10.1109/TETC.2019.2932685, 1566-1580.
56. Samuel Crislip, "Operationalize DNA Technology for U.S. Defense," (April 1, 2023). *AMS Special Session on Cybersecurity and Cryptography, American Mathematical Society*, American Mathematical Society, https://meetings.ams.org/math/spring2023e/meetingapp.cgi/Paper/24268 .
57. DOD CIO Zero Trust Portfolio Management Office, "DoD Zero Trust Strategy," 22.
58. Tom Gaines and Alex Suh, "Reimagining Contested Communications," (August 23, 2023). *The Modern War Institute at West Point*, https://mwi.westpoint.edu/reimagining-contested-communications/.
59. U.S. Cybersecurity & Infrastructure Security Agency, et al., "Secure by Design. Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Secure by Design Software," (October 2023). https://www.cisa.gov/resources-tools/resources/secure-by-design.
60. The MITRE Corporation, "MITRE ATT&CK v15.1," (last modified April 23, 2024), accessed June 17, 2024, https://attack.mitre.org/.
61. The MITRE Corporation, "MITRE Adversarial Threat Landscape for Artificial-Intelligence Systems (ATLAS)," accessed June 17, 2024, https://atlas.mitre.org/.
62. BAE Systems, "What is Quantum Sensing?," accessed June 17, 2024, https://www.baesystems.com/en-us/definition/what-is-quantum-sensing.
63. BAE Systems, "What is Quantum Sensing?"