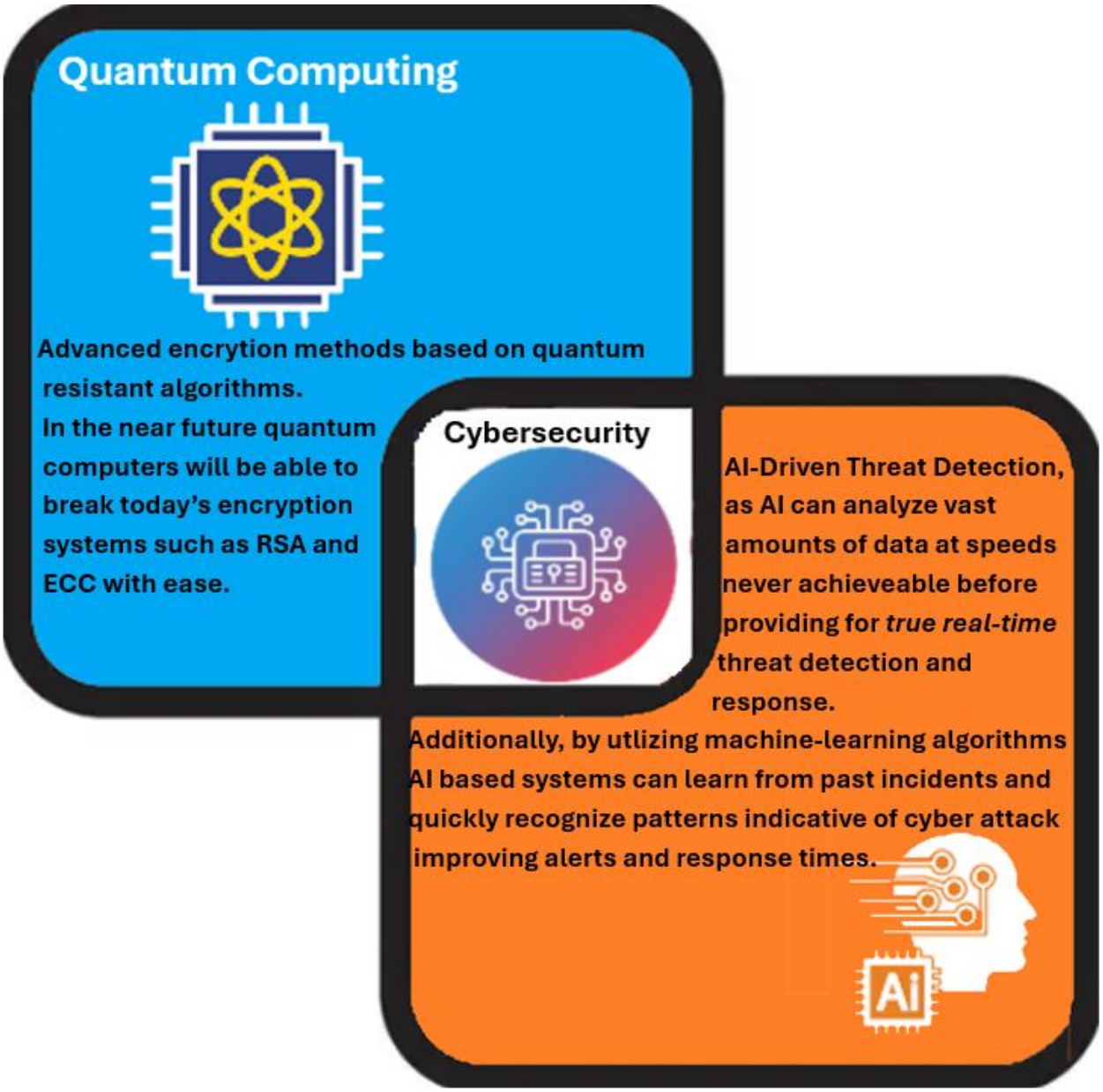


Cybersecurity

PQC and AI are set to disrupt the operation of Cybersecurity by enhancing encryption methods and improving threat detection, while also posing increased risks.

Q-Day (*researchers' phrase*) – the **quantum apocalypse** is on the horizon; it denotes the day when powerful quantum computers might use **Shor's algorithm** to break all public key

systems that depend on 'integer factorization' and other security techniques. The moment Q-day arrives will make most of today's security mechanisms obsolete.

Shor's algorithm – in 1994 Peter Shor, PhD Professor of Applied Mathematics at MIT, developed a **quantum algorithm for finding the prime factors of integers** which is exponentially faster than the best-known algorithms currently running on a classical computer. Shor's algorithm works on a **mathematical model** of a quantum computer – *it is idealized* – thankfully, present day quantum computers have not yet achieved the capabilities of Shor's idealized model. So, we have time, but the clock is ticking.

Post Quantum Computing (PQC) paves the way for quantum encryption, including Quantum Key Distribution (QKD), which uses the principles of quantum mechanics to create theoretically unbreakable encryption. This means that, while PQC can break current encryption standards, it also holds the key to a future of more secure communications.

AI vs AI we are quickly moving beyond the era of Hackers vs IT Professionals; we are now entering the era of **the AI Influencer**. Their mission is to sow enough doubt by spreading lies to 'influence public sentiment' against your company. They short sell your company stock, then before you have had the opportunity to address the lies the damage is already done – and they have plundered your value. They are not focused on penetrating your Firewall, they are after the low hanging fruit – the unprotected **public perception**. Their weapon of choice – **the Deepfake**.

Deepfake – by using the power of AI bad actors can disseminate videos that appear to be from 'you or your company' making remarks which negatively influence public perception against you. Their partner in crime is 'Time itself' – the time it takes for you to become aware – the time it takes for you to act – the time it takes for the public to realize they were duped. Time you cannot afford, time that you do not have.

AI Deepfake Detector companies claim 98% accuracy; however, social media platforms like YouTube have over 1Million videos uploaded every day, TikTok has over 34Million videos uploaded every day – suddenly 98% accuracy does not sound that safe as they may miss 20,000 videos on YouTube and 680,000 videos on TikTok – 'each day'.

Additionally, bad actors understand how these AI Deepfake Detectors companies work – so by adding noise, adjusting lighting, or applying filters they may evade detection.

Alliteration Layered Defense – unfortunately at this time there is no magic bullet for combating Deepfakes. Individuals and companies can implement these **5 Steps** to help mitigate exposure to Deepfakes:

1) **Authentication** – use techniques such as Multi-Factor Authentication (MFA) and/or Passwordless authentication (Biometrics, Hardware Security Keys)
2) **Authorization** – establish access control policies, based on 'a need-to-know basis'
3) **Automation** – use technology to perform recurring Cybersecurity tasks, such as endpoint scanning and incident response – this will help reduce human error, improve efficiency, and decrease risk.

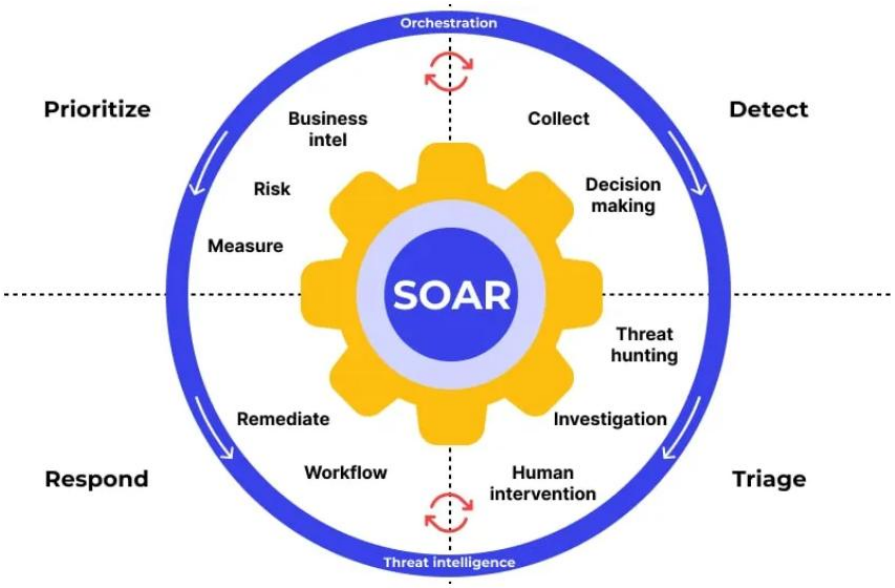
Common types of Cybersecurity Automation:

- **SIEM** – Security Information and Event Management – which focuses on collecting and analyzing event data for threat detection

SIEM Key Use Cases:

- Real-time security monitoring
- Incident investigation and forensic analysis
- Compliance reporting and log management
- User and threat monitoring

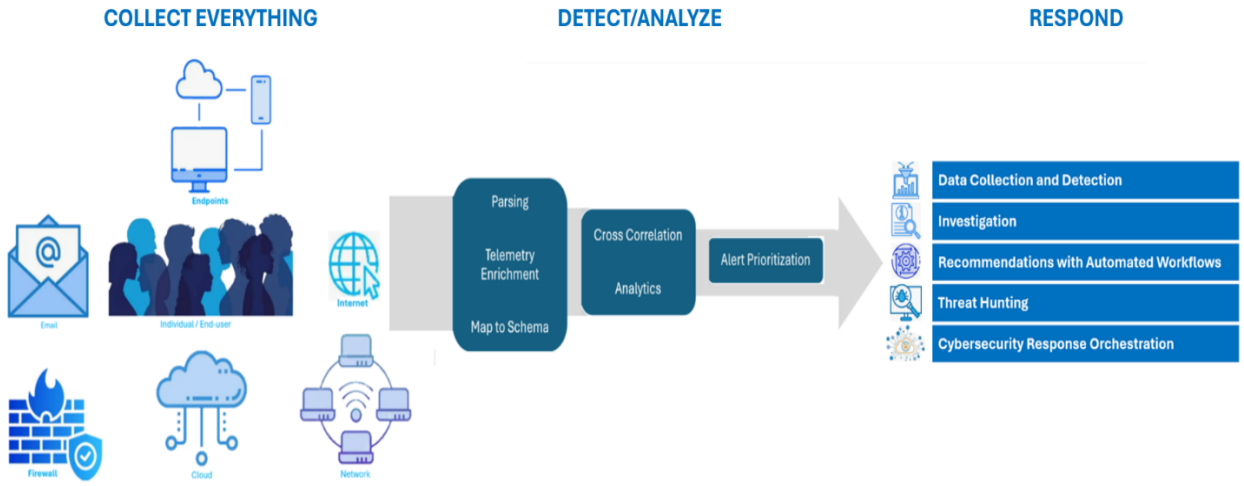
- **SOAR** – Security Orchestration Automation and Response – which focuses on automating and orchestrating incident response workflows



SOAR Key Use Cases:

- Automating responses to common alerts, like phishing and malware
- Orchestrating incident response workflows
- Improve alerts by adding threat intelligence
- Managing and tracking security incidents

- **XDR** – Extended Detection and Response – which unifies Automation and AI/ML. XDR solutions must be based on a Cloud-native architecture; however, this does not mean that XDR has to be deployed on the Cloud – XDR solutions can also be deployed on premise, or in a hybrid model



XDR Key Use Cases:

- Collect and consolidate all data from every endpoint, email, server, cloud workloads, firewall, and the internet
- Proactive threat hunting
- Correlation of data across multiple security layers
- Automating incident responses
- Utilize data aggregation and audit trails to improve regulatory compliance

4) Awareness – conduct ongoing Deepfake training so individuals know what to look for

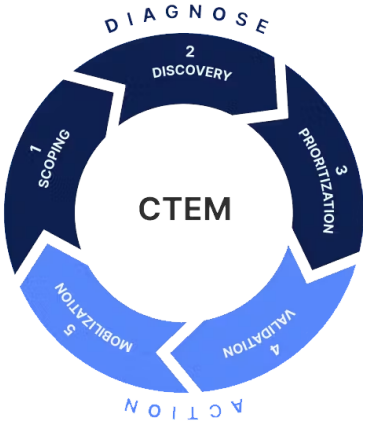
5) AI/ML – may go hand-in-hand but it is important to understand their relationship. While Machine Learning (ML) is a subset of AI and therefor relies on it to interpret, analyze, and act – AI does not solely rely on ML. In fact, AI can operate using other techniques like rule-based systems, computer vision, and natural language processing (NPL)

AI/ML Defensive – enables proactive threat hunting and automated incident response

AI/ML Offensive – enables bad actors to create more personalized and adaptive attacks

CTEM methodology for VM

Continuous Threat Exposure Management (CTEM) is a proactive cybersecurity framework that emphasizes 'ongoing risk management' through a structed, five-step program:



1. **Scoping** – human step, typically based on analytical thought and establishing processes/procedures
2. **Discovery** – this step requires Cybersecurity tools
3. **Prioritization** – human step, typically based on analytical thought and establishing processes/procedures
4. **Validation** – this step requires Cybersecurity tools
5. **Mobilization** – this step requires Cybersecurity tools

Traditional cybersecurity Vulnerability Management (VM) revolves around a specific point-in-time, like with a Pen Test. While a Pen Test has value, since it is focused on a specific point-in-time, it leaves you vulnerable during the time between Pen Tests – *Static testing*.

Whereas, CTEM focuses on a continuous cycle of identifying, prioritizing, and validating all potential threats – *Proactive testing*.

You cannot purchase CTEM, it is not a product/tool – CTEM is an ongoing, risk-based approach to identify, prioritize, and mitigate security exposure that you must adopt.

CTEM steps broken down:

- Scoping – identify critical data and its risk to threats – where to focus security efforts
- Discovery – mapping the network across on-prem, cloud, and hybrid environments
- Prioritization – separate what is important from the noise – scoring/ranking
- Validation – making use of tools, like attack simulations, to identify vulnerabilities
- Mobilization – implementing fixes and tracking actions – continuous improvements

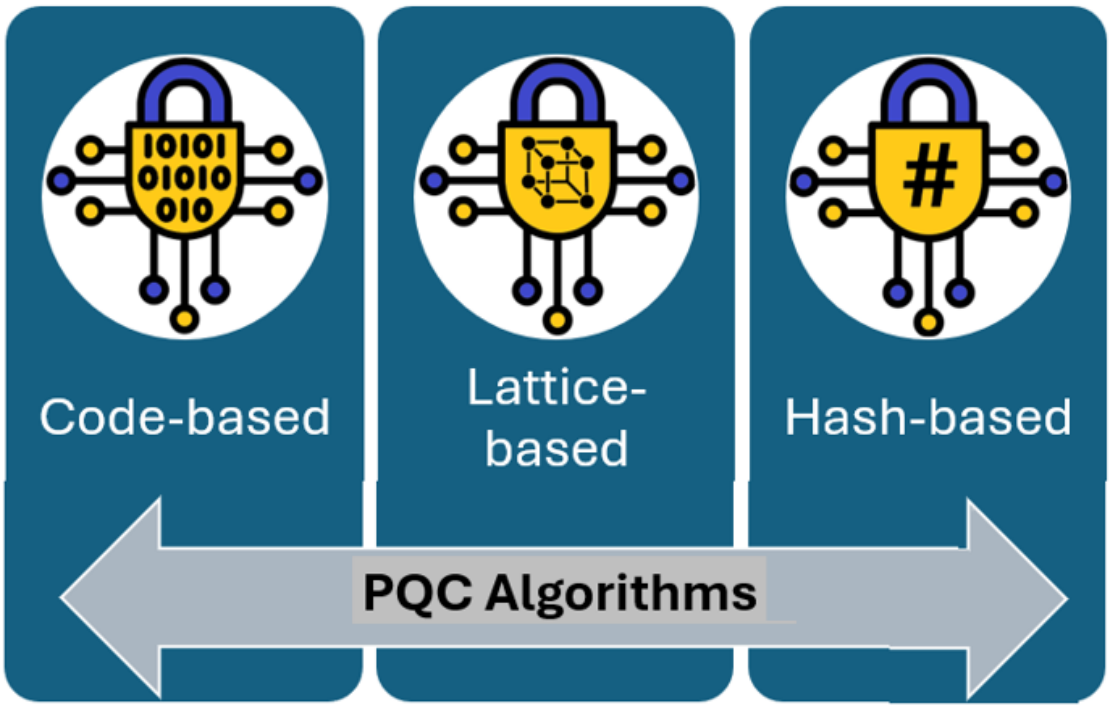
---

So as shown, the convergence of PQC and AI presents both challenges and benefits for Cybersecurity – *creating a continuous arms race*

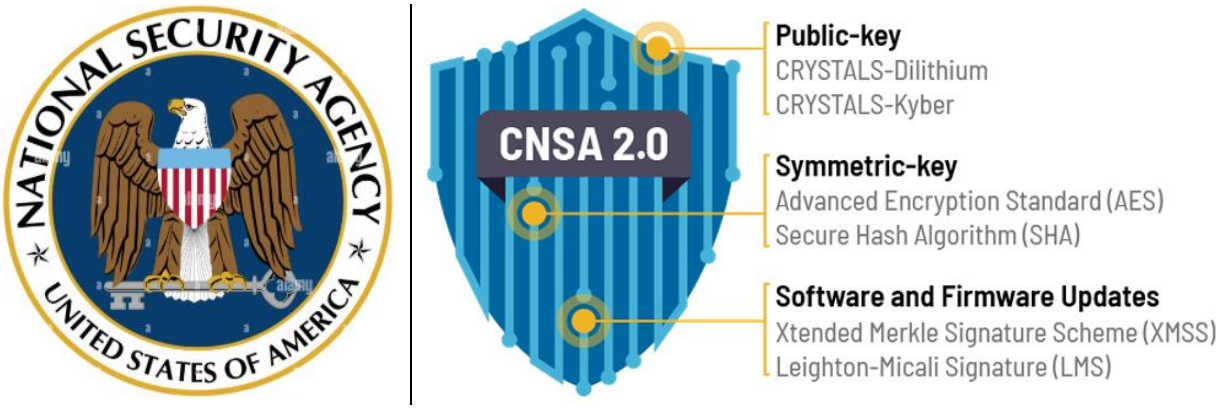
- **PQC challenges** – poses a significant threat to today's encryption standards
- **PQC benefits** – future proof Cybersecurity against quantum computing threats, seamless integration with current infrastructure, enhanced long-term data security
- **AI challenges** – bad actors are using AI to create sophisticated attacks, automate, and expose weaknesses quickly, and develop malware that 'can alter in real-time'. Making AI attacks faster, more covert, and harder to detect
- **AI benefits** – AI enables the user to identify anomalies and attack patterns using Machine Learning, automate countermeasures quickly, and allows the human cybersecurity analysts to focus their valuable time on developing strategies. AI driven Security Operations Centers can process massive amounts of data, mitigate noise, and prioritize threats

Post Quantum Computing (PQC)

PQC is basically a set of algorithms that resist quantum attacks and can run on most classical computers and networks making PQC practical to implement. Given the potential future capability of quantum computers to break traditional asymmetric cryptographic methods, the urgency to adopt these new PQC algorithms is highlighted by the risk of **Steal Now – Decrypt Later** (**SNDL**) attacks, where adversaries store encrypted data to decrypt later using quantum technology when more readily available.



Code-based	Lattice-based	Hash-based
Security is based on decoding unknown error-correcting linear codes.	Security is based on three Lattice problems: SVP – Shortest Vector Problem CVP – Closest Vector Problem LWE – Learning With Errors	Security is based on one-way functions that map bit strings of an arbitrary length to short, fixed-length strings called hash values.
Requires larger keys compared to Lattice-based and Hash-based.	Requires smaller keys compared to Code-based and Hash-based.	Either Stateful (smaller key size) or Stateless (larger key size): Stateful tracks one-time keys to ensure they are not reused. Stateless uses complex algorithms instead of one-time keys.
The most mature method	Better than Code-based for applications with limited bandwidth and/or storage.	
Used for encryption and signatures.	Used for encryption and signatures.	Primarily used for signatures.
Examples: Classical McEliece, BIKE, and HQC	Examples: ML-KEM (Kyber) and ML-DSA (Dilithium)	Examples: LMS and XMSS are Stateful where SPHINCS+ is Stateless



In 2022, the NSA released the **CNSA 2.0 Standards** establishing requirements and timelines for adopting PQC algorithms which apply to all National Security Systems and related assets. Meeting the CNSA 2.0 requirements and timelines is critical for any company who wants to do business with the US Government.

CNSA 2.0 requirements and timelines:

- Software/firmware signing : PQC as the default/preferred algorithm by 2025
- Web browsers/servers: PQC as the default/preferred algorithm by 2025
- Cloud services: PQC as the default/preferred algorithm by 2025
- Traditional networking equipment: PQC as the default/preferred algorithm by 2026
- Operating systems: PQC as the default/preferred algorithm by 2027
- CNSA 2.0 compliance will be **mandatory by 2030** for all National Security Systems

NIST's Post-Quantum Cryptography (PQC) algorithms standards

On August 13, 2024, NIST released three algorithms designed to remain secure even against large-scale, fault-tolerant quantum computers:

- **FIPS 203:** Module-Lattice-Based Key-Encapsulation Mechanism standard (ML-KEM) is a cryptographic protocol designed for secure key exchange over public networks and is derived from the **CRYSTALS-KYBER** methodology. ML-KEM operates by leveraging the Module Learning with Errors (MLWE) problem, a computationally hard problem in lattice-based cryptography. This ensures its robustness against both classical and quantum attacks

  ML-KEM enables **two parties to establish a shared secret key securely**, which can be used with symmetric cryptographic algorithms for encryption and authentication

CRYSTALS (Cryptographic Suite for Algebraic Lattices**) KYBER** methodology represents a significant step for ensuring digital security in the era of PQC

- ML-KEM defines three security parameter sets:
  - ML-KEM-512: which offers the lowest security strength, but highest performance
  - ML-KEM-768: which offers a balance of security and performance
  - ML-KEM-1025: offers the highest security strength, but with reduced performance

- **FIPS 204:** Module-Lattice-Based Digital Signature standard (ML-DSA) describes module-lattice-based digital signature algorithm (ML-DSA) and can both generate and verify digital signatures, providing **authentication of the signer**, **integrity of the transaction**, and **non-repudiation by the signer** – based on CRYSTALS-Dilithium

- **FIPS 205:** Stateless Hash-Based Digital Signature standard (SHL-DSA) describes state-less hash-based digital signature algorithm (SLH-DSA) – based on SPINCS+

Cryptographic scheme called ML-KEM

- FIPS 203 CRYSTALS-KYBER

Refers to a set of algorithms and protocols used to secure data

Digital Signature schemes called ML-DSA and SHL-DSA

- FIPS 204 CRYSTALS-Dilithium
- FIPS 205 SPHINCS+

Uses a pair of keys (public and private) to authenticate the sender of a digital message

- **FIPS 206:** (*not yet released*) FFT NTRU-Based Digital Signature standard (FN-DSA) utilizes NTRU lattices
  - **FFT** – Fast Fourier Transform is used to speed up polynomial multiplication, it is executed over the ring of polynomials, where the hardware is designed for the FFT and then implementing the FFT in software
  - **NTRU** – Number-Theoretic Testable Unit algorithm is an open-source public-key cryptosystem that uses lattice-based cryptography to encrypt and decrypt data. It consists of two algorithms: **NTRUEncrypt**, which is used for encryption, and **NTRUSign**, which is used for digital signatures. It is based on the shortest vector problem in a lattice

Artificial Intelligence (AI)

The myth is that AI/ML are the 'silver bullet' that will finally solve all Cybersecurity issues. However, this simply is not reality – AI/ML does not replace human judgement, nor policy development, AI/ML do not understand Cybersecurity – they merely follow instructions.

One of the cornerstones for controlling AI/ML is that *'governments can mitigate its risks by enacting strong policies, backed by stern penalties'*. **Really?** Not only are we confronted by individual rogue hackers who refuse to follow the law, but we are also dealing with hostile bad actor nation-states. Sorry, as the saying goes '*once the genie is out of the bottle'*...

The reality is that we can enjoy the benefits of AI/ML , but at the same time we must deal with its consequences.

Because of the amount of data AI/ML can manage, at speeds close to real-time, we will require – technology, tools, and automation to assist us. One such technology is **RDMA**.

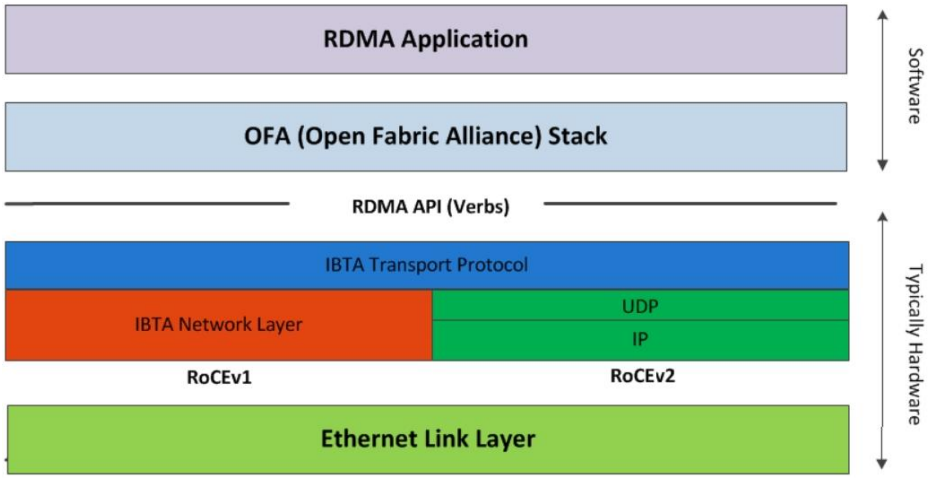
RDMA (Remote Direct Memory Access) technology allows networks to exchange data directly without involvement from the Operating System (OS), network stack, and Central Processing Unit (CPU). Since the CPU is bypassed, RDMA enables the faster processing times required by AI workloads

RoCEv2 (RDMA over Converged Ethernet-version 2) is a transformative technology for AI by offering:

- Ultra-low Latency – minimizes software stack processing time
- High Throughput – maximizes bandwidth utilization
- Zero-Copy Operations – data is transferred directly to the Graphics Processing Unit (GPU) memory, bypassing CPU involvement, and the need for system memory copies
- Layer 2/Layer 3 Transport – offers deployment flexibility by operating either at Layer 2 or Layer 3, thus traversing IP subnets, avoiding the limitations of the Layer 2 domain
- Broad industry wide Adoption – a standards-based technology with wide support from Network Interface Card (NIC) vendors, Switch manufacturers, and AI Framework developers – RoCEv2 offers a foundational element for building high-performance GPU fabrics capable of handling vast amounts of data exchanges

Converged Ethernet – combines multiple types of networks, such as Local Area Networks (LANs) and Storage Area Networks (SANs) into an integrated infrastructure

- RoCEv1 which operates at the Ethernet link layer, v1 is best suited where all nodes reside on a confined data center – v1 is not routable
- RoCEv1.5 uncommon/experimental – uses the IP protocol to differentiate traffic
- RoCEv2 which uses the UDP/IP stack, v2 is more flexible than v1, supporting nodes across dispersed data centers – v2 is routable



RoCEv1 compared with RoCEv2

NIST is at the forefront of establishing AI standards related to data formats, testing methodologies, transfer protocols, cybersecurity, and privacy that promote innovation while addressing associated risks, thereby enhancing the overall trust in AI technologies.

- **SP 800-53:** Control Overlays for Securing AI Systems
  NIST is developing overlays with AI-specific concerns like *model integrity*, *data provenance*, *adversarial robustness*, and *transparency*. (NIST is planning to release the first overlay in FY2026) The aim of these overlays is to promote consistency and interoperability across different AI systems and organizations. NIST is building these overlays upon existing frameworks such as the AI RMF 1.0

- **AI RMF 1.0:** AI Risk Management Framework – is a comprehensive guide to help organizations manage the risks associated with AI. As part the AI RMF Roadmap, NIST has made it a priority to align with related applicable international standards, guidelines, and practices – e.g.:
  - **ISO/IEC 5338:2023** Information technology – AI system life cycle processes, it is not intended to replace existing software lifecycle processes, just extend them to include AI-specific considerations
  - **ISO/IEC 22989:2022** Information technology – AI common vocabulary to facilitate consistent communications among nations and stakeholders

- **ISO/IEC 24028:2020** Information technology – AI guidelines to ensure trustworthiness and robustness among distributed AI systems
- **ISO/IEC 20546:2019** Information technology – Big Data common vocabulary to facilitate consistent communications among nations and stakeholders
- **ISO/IEC 38507:2022** Information technology – Governance of IT – provides a framework for governance AI within organizations

U.S. Leadership in AI: A Plan for Federal Engagement in Developing Technical Standards and Related Tools Aug 9, 2019
(link to NIST eBOOK)
https://www.nist.gov/system/files/documents/2019/08/10/ai_standards_fedengagement_plan_9aug2019.pdf

Data Repositories (e.g.: for algorithm training) are essential for evaluating AI models. Some publicly available AI datasets: (NOTE: above eBOOK, pg. 32, provides a larger list)

- **MNIST:** dataset of handwritten digits has a training set of 60,000 examples, and a test set of 10,000 examples. It is a subset of a larger set available from NIST http://www.pymvpa.org/datadb/mnist.html
- **DATA.GOV:** maintains a catalog of over 350,000 open-sourced government datasets in topics such as agriculture, climate, consumer, ecosystems, education, energy, finance, health, local government, manufacturing, maritime, ocean, public safety and science https://data.gov

Generative AI – uses existing data to generate original outputs (create new content), whereas traditional AI analyzes existing data to automate tasks

Predictive AI – uses existing data to forecast outcomes (makes educated guesses)

OUR SOLUTION

VIAVI (formerly Spirent) CyberFlood platform is a powerful, easy-to-use test solution that generates realistic application traffic to test the performance, scalability, and security of your app-aware network devices and solutions. It makes it easy too:

- Test and enforce application traffic policies across on-perm, cloud, and hybrid environments
- Benchmark performance and network capacity by simulating from thousands to hundreds of thousands of real users over a network
- Executes many of the testing and validation steps within a **CTEM framework**, e.g.
  - **Validation** – CyberFlood directly supports the 'validation' stage of CTEM by providing tools to test and validate network security effectiveness, performance, and the impact of threats
  - **Discovery** – CyberFlood ability to emulate realistic traffic and attacks can be used to discover vulnerabilities and incorrect setups within a network
  - **Mobilization** – CyberFlood provides objective and repeatable test results, thus help to mobilize resources to make informed decisions about security performance
- Security and Performance Testing for **SASE** and **Zero Trust Architecture (ZTA)**
- **PQC cipher suites** are fully integrated into extensive HTTP protocols and TestCloud Applications ensuring validation under realistic, traffic conditions
- Validate network security efficacy, including **NIST FIPS 203** (ML-KEM) and **204** (ML-DSA) *NOTE: ***FIPS 205*** *(SHL-DSA) is on the roadmap, under development*
- **Hybrid KEM** testing (hybrid X25519MLKEM768) effectively validating robust fallback strategies, and pinpointing interoperability challenges
- Vendor neutral, leverage **MITRE ATT&CK** and **NetSecOPEN** methodologies
- Supports the newly ratified **IETF RFC9411** methodologies for next gen security
- Supports **RDMA/RoCEv2** and real-world **AI workloads**

CyberFlood

Want to learn more and schedule a Demo…

Claude Sweeton, Director of Test & Measurement Solutions
claude.sweeton@dualos.com
630.881.2288 Cell
linkedin.com/in/claudesweeton

- +45yrs in the Test & Measurement industry
- US Navy Veteran 1978-86

Dualos, LLC (Native American, SBA-Certified WOSB, Small Disadvantaged Business)
Founded in 2008
1520 Steele Ave
Sumner, WA 98390

Dualos applies our expertise and products, along with industry-leading partner solutions, to serve the Aerospace and Defense industry. We provide tailored solutions designed to address the complex testing challenges our customers encounter.

253.750.5125

www.dualos.com

CITATIONS

- NIST Computer Security Resource Center – FIPS 203, 204, 205
  https://csrc.nist.gov/News/2024/postquantum-cryptography-fips-approved
- NSA Central Security Service – CNSA 2.0
  https://media.defense.gov/2025/May/30/2003728741/-1/-1/0/CSA_CNSA_2.0_ALGORITHMS.PDF
- ISO Organization
  https://www.iso.org/home.html
- IEC Organization
  https://www.prd.iec.ch/homepage