www.pipelinepub.com
Volume 21, Issue 1

Not for distribution or reproduction.

Shifting the Balance: Rethinking Cybersecurity in the Age of AI and Quantum Computing

By: Mark Pohto - CTO, Dispersive Holdings Inc.

The quickly accelerating pace of technological advancement brings both unparalleled opportunities and unprecedented threats. Emerging technologies like generative AI and quantum computing have the potential to revolutionize industries, but they also present grave challenges for cybersecurity. In this digital landscape, where threats evolve faster than many defenses can keep up, traditional passive approaches are no longer enough. Organizations must adopt a proactive, multi-layered defense strategy to address new threats head-on, leveraging cutting-edge innovations like Automated Moving Target Defense (AMTD) and Active Cyber Defense (ACD).

In this article we will explore how the ever-changing landscape of cyber threats requires a comprehensive rethinking of cybersecurity strategies, the crucial role of innovation, and how businesses can better prepare for the future by embracing next-generation technologies and fostering deeper collaboration across the security community.

The Expanding Threat Landscape

Today's cyber adversaries are not just script-kiddies or lone hackers donning hoodies; they are sophisticated, well-funded organizations with significant resources. Nation-state actors, organized crime syndicates, and hacktivists leverage an array of digital tools to exploit vulnerabilities across systems. Nation state actors are well-funded, and their agencies work night and day, 365 days a year against their designated targets. What’s most concerning is that attackers now have and share access to advanced technologies like AI and machine learning, enabling them to scale their efforts and adapt to defensive controls in near real time. The time is quickly approaching when cryptographic algorithms, foundational to much of our security, may be defeated by quantum computing

© Pipeline Publishing, L.L.C. All Rights Reserved.

capabilities. The countdown to this moment demands immediate action from cybersecurity professionals.

Passive security models that focus on detection are no longer sufficient. If we want to stay ahead of threat actors, we need to focus on preemptive actions — anticipating, detecting, and neutralizing threats before they materialize. We need an approach as sophisticated and nimble as our adversaries.

The Rising Sophistication of Attacks

The breadth of attack vectors has grown dramatically. Today's adversaries exploit everything from operational technology (OT) to IoT devices, supply chain vulnerabilities, and human behavior. As the attack surface expands, so does the range of consequences, from business disruption to financial loss, reputational damage, and even threats to human life. Gartner predicts that by 2025, cyber attackers will have weaponized OT environments to successfully harm or kill humans. This stark projection highlights the evolving nature of cyber threats and underscores the need for more advanced defensive measures.

Moreover, malevolent actors are increasingly capable of using AI for automation and efficiency, deploying AI-driven phishing campaigns, creating deepfakes, and even conducting AI-powered reconnaissance on potential targets. These developments can render traditional controls and detections ineffective. To counter such sophisticated tactics, security professionals must elevate their game by incorporating cutting-edge solutions like AMTD and ACD.

Advanced Defensive Technologies: AMTD and ACD

AMTD is an innovative approach that continually shifts the attack surface, making it harder for attackers to conduct effective and undetected reconnaissance, or plan and launch a successful attack. This strategy prevents adversaries from getting a beachhead in the network by regularly changing configurations, parameters, protocols, or resources within the system. Deception is an important part of AMTD. Deception lures the attacker into actions that expose them and their methods. Think of it as a moving target that's incredibly difficult to hit surrounded by benign targets that expose the attacker and inform the defenders. With AMTD, the focus is no longer on simply detecting and responding to a breach but on preventing attackers from gaining any meaningful access in the first place.

Active Cyber Defense (ACD) goes a step further by integrating offensive tactics into defensive frameworks. Instead of passively defending against attacks, ACD allows organizations to engage with adversaries proactively. This approach might include intelligence gathering, conducting counter-reconnaissance, or deploying deceptive systems designed to trap and mislead attackers. By creating a dynamic and hostile environment for attackers, ACD tilts the balance of power towards the defender. These technologies represent a fundamental shift in cybersecurity, with less passive, static defense mechanisms to agile, adaptive strategies capable of defeating attackers at their points of entry.

Not for distribution or reproduction

© Pipeline Publishing, L.L.C. All Rights Reserved.

Quantum Computing: An Imminent Challenge

Quantum computing delivers extraordinary processing power, but it also threatens to help defeat the cryptographic algorithms that secure today's data. With quantum computing comes the risk that attackers will decrypt previously secure communications and data. A recent study suggests that commonly used encryption methods, such as RSA and ECC, could be rendered obsolete in a post-quantum world. The window for preparing defenses is rapidly closing; businesses must prepare now.

Preparing for quantum-enabled attacks means adopting quantum-resistant encryption methods, exploring novel algorithms, and integrating them into both public and private infrastructures. The U.S. National Institute of Standards and Technology (NIST) has been leading the charge, developing quantum-resistant cryptography standards. Businesses that delay transitioning to quantum-safe protocols run the risk of being caught unprepared when these threats materialize.

Not for distribution or reproduction

Architect for Now

While preparing for the future is essential, organizations must architect for the present with existing solutions. Employing a defense-in-depth strategy, integrating multiple layers of security across hardware, software, and processes, creates an environment where no single point of failure exists. This approach leverages current cryptographic methods and commercial solutions that are proven to deter or mitigate today's threats. Domestic and foreign entities can immediately implement these measures without waiting for emerging technologies like homomorphic encryption or delayed guidance from agencies like CISA, NIST, or NSA. By combining today's best practices with multiple overlapping defenses, especially moving target defenses, organizations can drastically improve their security posture and reduce the impact of potential cyberattacks right now.

The Human Element: Cybersecurity's Weakest Link

As technology advances, it's easy to forget that people remain one of the most vulnerable components of any cybersecurity system. Insider threats, whether through malicious intent or negligence, can undo even the most sophisticated defenses. As attackers refine their tactics, such as using AI to craft convincing phishing attacks, employees are increasingly falling victim to these schemes. The 2022 Verizon Data Breach Investigations Report revealed that 82 percent of breaches involved some form of human element, whether through social engineering, misuse, or human error.

Addressing this weakness requires ongoing training, regular security drills, and a culture that prioritizes cybersecurity at every level. Implementing multi-factor authentication, role-based and two-person access controls, and stringent auditing processes can help mitigate human risk. But perhaps most importantly, employees must be trained to recognize sophisticated threats in real-time.

Securing the Entire Ecosystem

As we build defenses, we must think holistically, encompassing every part of the digital ecosystem, from hardware and software to people and processes. The interconnected nature of supply chains, third-party vendors, and cloud services means that a vulnerability in one part of the ecosystem can

© Pipeline Publishing, L.L.C. All Rights Reserved.

compromise the entire system. The infamous SolarWinds attack of 2020 demonstrated how easily supply chains can be exploited, highlighting the need for comprehensive security controls that span physical and logical security.

Ensuring that all code is signed and validated, limiting the scope of vendor access, and conducting regular audits of supply chains are essential steps in safeguarding this ecosystem. Moreover, proactive engagement with industry partners and government initiatives can help identify and mitigate vulnerabilities before they are exploited.

Fostering Collaboration in the Cybersecurity Community

In the fight against cyber threats, no organization is an island. Cybersecurity professionals must foster collaboration across industries, sharing threat intelligence, best practices, and emerging solutions. Government agencies, academic institutions, and private enterprises can all benefit from working together, especially when it comes to developing standards, creating frameworks, and advancing research in next-generation defense technologies.

At Dispersive, we believe in the power of collective defense. By working closely with our partners and participating in global cybersecurity initiatives, we aim to create a more secure digital ecosystem for all.

Conclusion: Shifting the Balance of Power

The cybersecurity landscape is more complex and challenging than ever before. As attackers become increasingly sophisticated, leveraging AI and quantum technologies, defenders must rise to the occasion by adopting proactive, multi-layered strategies like AMTD and ACD. By embracing continuous innovation, securing the entire digital ecosystem, and fostering greater collaboration, businesses can tilt the balance of power away from attackers and toward defenders.

As the future unfolds, the organizations that will thrive are those that embrace the challenges ahead and take proactive steps to defend against an evolving array of threats. In this digital arms race, innovation, vigilance, and collaboration are our most potent weapons. Together, we can build a more secure future.

Not for distribution or reproduction.

© Pipeline Publishing, L.L.C. All Rights Reserved.