July 2025

ENTROPYA

Digital Super-Highways: Untraceable, Resilient, and Quantum Ready

ENTROPYA ENCRYPTED NETWORK (EEN)

Hidden – Post-Quantum Hardened – Zero Trust & Resilient

TABLE OF CONTENTS

Executive Summary

In an era where cyber threats are increasingly sophisticated and invasive, Entropya redefines cybersecurity by eliminating complexity and focusing on privacy, resilience, and quantum readiness. Traditional security models rely on securing perimeter access points with layers of defense and signature-based detection. This design is vulnerable to modern threat vectors such as man-in-the-middle attacks, ransomware, and zero-day exploits. Entropya's approach is fundamentally different: ***you cannot attack what you cannot find***.

Born from decades of national-level cyber operations, Entropya's patented Software-Defined Private Networking (SDPN) technology and post-quantum cryptography solutions offer a transformative security paradigm. By removing digital fingerprints, randomizing IP pathways, and eliminating self-identifying infrastructure signatures, Entropya renders systems ***untraceable*** and impervious to surveillance and exploitation.

Entropya's infrastructure-agnostic platform integrates seamlessly with existing systems, delivering ultra-low latency and uncompromised performance across all digital pathways—fiber, cloud, cellular, and space. Its solutions are built on the highest cryptographic standards, including NIST's ML-KEM 1024, ensuring resistance to current and future quantum computing threats.

Entropya's mature, operationally deployed solutions are designed for the most sensitive and critical environments. As digital threats evolve, Entropya empowers organizations to stay ahead—securely, simply, and resiliently.

Introduction

Cybersecurity is non-negotiable and expensive. Vendors offer security through proprietary complexity, with elaborate connected operating systems, dashboards, and niche integrated solutions that attempt to defend everywhere. Don't be fooled; complexity does not equal security. Emerging from decades of highly sensitive cyber tracking and exploitation activities, Entropya's technology is designed from a deep practitioner's perspective of how to find, track, and exploit the hardest-to-find people, infrastructure, and digital targets defending with advanced cybersecurity tools. Through this experience, the team designed and developed a portfolio based on the simple fact – ***you cannot attack what you cannot find*** – and then incorporated the highest level of next generation certified cryptography.

Entropya delivers uncompromising performance while implementing the cryptography gold standard. This National Institute for Standards and Technology (NIST) compliant algorithm suite resists man-in-the-middle, supercomputer, and quantum computer attacks. Entropya's products further integrate an untraceable software-defined private networking (SDPN) technology suite that is dynamically customizable. This operationally deployed environment is patented, developed, and integrated to privately broker anonymous and randomized interactions between all endpoints, infrastructure, and data, no matter the Internet connection. The punch line is that you do not have to sacrifice performance or your operational effectiveness to be secure. Entropya proves that security can be simple, meet you where you are, and work with what you have.

The reason Entropya's approach changes the game lies in the simplicity of the Internet's design and how cyber-attacks are executed. Cyber-attackers seek easy targets by exploiting the connectedness of the Internet and the self-identifying features that help technology professionals do their jobs. These

self-reporting functions share what activities and services are supported at a specific address, similar to how a business shares its hours and services at its physical address. This defines expectations for how people and systems interact. But this information can also be used by attackers to find weaknesses in your services and architecture.

These weaknesses include the doors and windows that lack protection. These doorways are called ports, and there are 131,070; the first half are Transmission Control Protocol (TCP), and the other half are User Datagram Protocol (UDP). These entry points also represent access, services, and functionality for hardware and software. Typically, layers of security tools are positioned to establish control points to manage how systems connect, interact, and gain access. Outdated software, firmware, hardware, and diverse connected technologies are usually segregated and monitored, if known and deliberately managed, but this is not always true. These factors make nearly all cyber platforms and devices vulnerable to identification and surveillance, denial of service (DDoS) attacks, zero-day exploits, and thus threat actors.[1]

Contrasting the traditional security approach, Entropya starts from a fundamentally different approach, ***camouflage and disappear.*** Decomposing the anatomy and art of a cyber-attack explains why Entropya's approach offers a new level of security previously unachievable with agile, adaptive, and non-attributable cyber platforms consisting of systems that can be deployed quickly, operate anonymously, and evolve with advancing global threats.

Entropya enables flexible "first-mile" and "last-mile" infrastructure with dynamic and disposable systems that can be reconfigured as needed, using randomized IP addresses and resilient multi-path Internet pathways through diverse global infrastructure. This infrastructure includes any fiber, cloud, data centers, space gateways, Internet junctions, and cellular pathways into SDPN super-highways customized for purpose and function.

The shifting political struggles of today highlight a need to think differently about how we protect critical infrastructure and essential services, defend

1. Tushar Subhra Dutta, "Detecting Cyber Attack Patterns by Analyzing Threats Actors Infrastructure," *Cyber Security News* (blog), March 9, 2025, https://cybersecuritynews.com/detecting-cyber-attack-patterns/.

against emerging AI-based collection and analytics, the weaponization of dis/information, and the malign use of communication monitoring and exploitation technologies. These are real and pressing challenges and indicate a severe need for durably secure and resilient connections that enable trust and stability for business at the national, regional, and global levels. Entropya provides security for trusted business operations and transactions.

Critical Challenges

Common Attack Methods

- **Man-in-the-Middle:** A type of attack where an invader intercepts and/or alters data exchanged between two parties. "In the context of authentication, the attacker would be positioned between [user] and verifier, between registrant and [authentication service] during enrollment, or between subscriber and [Cloud Solution Provider] during authenticator binding."[2] The majority of business transactions and digital exchanges traverse global Internet infrastructure, large compute environments, data centers, as well as open space, making every touch point susceptible to monitoring, analytics, attacks, and interception.
- **Ransomware:** Commonly seeks ransom payments in exchange for decryption keys to unlock critical files and data. These attacks are usually delivered by unsuspecting employees clicking on links. The most concerning situations are companies that have business-critical systems that are connected to the network and lack sufficient protections. Once compromised, the core business activities are halted due to payment, printing, mail, customer management, and other critical business systems getting locked out.[3]
- **Penetration & Persistence:** Network penetration happens in numerous ways, but the majority start with a digital doorway to gain access. Whether through an unlocked door, a dated system, stolen credentials, a compromised computer, or some other means, the result is a threat lurking inside your network. Time and patience are key for these persistent actors exploring your network, checkpoints, connected systems, internal firewalls, routers, and authentication mechanisms. With enough time, a

2. Computer Security Resource Center Content Editor, "Man-in-the-Middle Attack (MitM) - Glossary | CSRC," accessed June 28, 2025, https://csrc.nist.gov/glossary/term/man_in_the_middle_attack.
3. "Global Cyberattacks by Type 2023," Statista, accessed June 28, 2025, https://www.statista.com/statistics/1382266/cyber-attacks-worldwide-by-type/.

proficient attacker will work through each layer of security and find the prize they are looking to extract and exploit. Whether corporate espionage, nation-state competition, emotional, political, or activist reasons, the goal is usually to gain insight into internal communications, connected critical systems, steal intellectual property, or reveal sensitive personal information, including health and financial data.[4][5][6]

Signature-Based Cybersecurity Risks

- **Vulnerable Hardware, Software, and Infrastructure Signatures:** The self-reporting digital fingerprints of infrastructure like web portals, banking and financial, healthcare, data backup and synchronization, Public Key Infrastructure (PKI), Supervisory Control and Data Acquisition (SCADA) and Industrial Control Systems (ICS) enable fingerprinting and vulnerability discovery remotely once the network penetration points are identified and exploited. Typically, the first layer of defense is a firewall. Virtual Private Network (VPN) servers paired with a firewall are also entry points that enable access to your internal network, systems, and data. All of these systems have unique and exploitable signatures.[7][8]
- **Initial Access - Firewalls & VPN Servers:** These hardware and software systems have unique signatures and can be located and targeted in many ways. Numerous examples exist to include Zero-Day exploits and remote access. Once compromised, VPN server, firewall, or firewall management operating systems provide attackers unfettered access into your internal network and explore how to get through your layers of security to your critical data and systems.[9]

4. "MITRE ATT&CK®," accessed June 28, 2025, https://attack.mitre.org/.
5. Irene Tham et al., "Singapore's Worst Cyber Attack: How It Unfolded," The Straits Times, July 20, 2018, https://graphics.straitstimes.com/STI/STIMEDIA/Interactives/2018/07/sg-cyber-breach/index.html.
6. "Public Report of the Committee of Inquiry into the Cyber Attack on Singapore Health Services Private Limited's Patient Database on or Around 27 June 2018" (Singapore: Ministry for Communications and Information Singapore, January 10, 2019), https://file.go.gov.sg/singhealthcoi.pdf.
7. Peter Maynard, Kieran McLaughlin, and Sakir Sezer, "Decomposition and Sequential-AND Analysis of Known Cyber-Attacks on Critical Infrastructure Control Systems," *Journal of Cybersecurity* 6, no. 1 (January 1, 2020), https://doi.org/10.1093/cybsec/tyaa020.
8. "MITRE ATT&CK®," accessed June 28, 2025, https://attack.mitre.org/.
9. Ibid.

Entropya's Approach

Entropya delivers leading-grade security by simplifying complexity. We build protected ecosystems inspired by the vulnerabilities of your most benign digital signatures. Our technology and solutions result from practitioner expertise in national-level cyber activities. We pair our untraceable super-highways with quantum-resistant cryptography to deliver novel, secure, private infrastructure safeguarding you against advanced threats. As cyber practitioners, you can't attack what you can't see!

Untraceable Networks.

Entropya's solutions allow your infrastructure to vanish into the vastness of the Internet while maintaining durable, secure, quantum-resistant connections. Using universal interfaces for seamless integration, we customize solutions to your ultra-low latency requirements and provide dynamic super-highways for all your needs.

Designed for rapid deployment, Entropya's low-to-no config solutions integrate effortlessly with legacy infrastructure. Each untraceable connection is dynamically authenticated and routed through private transport you control, with no third parties.

Leading Grade Security.

Your infrastructure leaves digital breadcrumbs that provide an insightful trail to your vulnerabilities. Entropya erases digital identity markers, obscures endpoints, and secures data at its core, further hardened with post-quantum cryptography.

Our solutions eliminate attributable Domain Name System (DNS) resolution to your infrastructure and generate randomized one-way pathways to make each location and destination untraceable. Entropya neutralizes 99.999% of attack vectors by blocking and hiding your doors and windows (i.e., stripping ports and protocols) at your public IP addresses and then deploys Zero Trust fortifications around your systems and data. Entropya future-proofs you with a fundamentally different approach reinforced by governing standards.

Key Features

01. Any Infrastructure, All Pathways

Designed as a hyper-redundant software-defined ecosystem, Entropya's transport is network agnostic, leveraging the world's fastest and largest interconnected providers. This model optimizes across hundreds of high-performance pathways, interconnections, and data centers worldwide and offers ultra-low latency. Additionally, it encompasses all digital pathways, including cellular, space, terrestrial fiber, subsea cables, Internet Service Providers, Internet junctions, and data center connectivity simultaneously and includes bare-metal, cloud, and a variety of operating systems. By using our design, you inherit leading DDoS protections. See Figure 1 for a conceptual design visualization.

02. Uncompromised Performance

Increasing security usually creates layers of complexity that induce latency and give up performance. Using the highest-performing architectures available to connect your most demanding needs, our intuitive solutions deliver leading-grade security with uncompromising performance no matter how or what you connect.

03. Leading Grade Security: HIDE. HARDEN. VERIFY.

Entropya uses digital camouflage as a design first principle and then implements the highest level of the National Institute of Standards and Technology (NIST) FIPS 203 standard, Modular-Lattice-Based Key-Encapsulation Mechanism (ML-KEM) 1024. This approach first makes your infrastructure, connections, and endpoints disappear while removing the digital fingerprints of your attackable vulnerabilities. Then, it protects with quantum-ready attack resistance and encrypted network tunnels as the second layer of defense. Entropya's privacy-first security approach simplifies your network boundaries and vulnerabilities, enabling you to focus your limited resources on specific critical defenses.

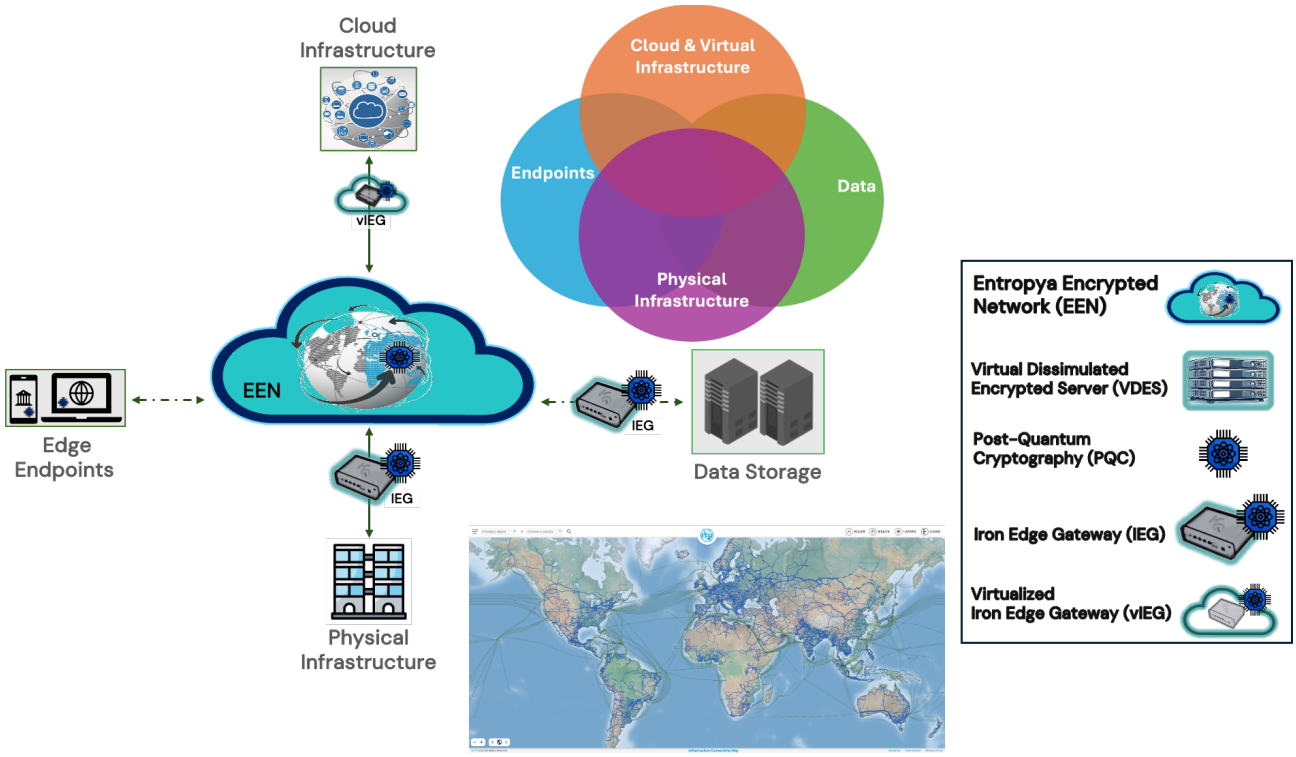

Figure 1. Entropya Encrypted Network, Any Infrastructure, and All Pathways.

Next Generation Cryptography

ENTROPYA MAKES YOU QUANTUM READY

Current asymmetric cryptographic algorithms are based on complex mathematical problems, often factoring large numbers. Today's most powerful supercomputers are believed to take hundreds to thousands of years to crack these keys, depending on their complexity. Research conducted over 20 years ago by Peter Shor at MIT demonstrated that a large-scale quantum computer could theoretically solve the same decryption problem in days or hours.[10] Yes, quantum computers are emergent today, but that's not the only concern. Widely implemented key exchanges are susceptible to man-in-the-middle and other more traditional attack methods that can compromise or steal stored credentials. No quantum computer is required in either of the cases above.

Symmetric encryption algorithms used to protect data at rest, such as Advanced Encryption Standard (AES),[11] were expected to remain secure in a quantum world provided that complete entropy keys are used. However, this is no longer true. For example, large quantum computers running Grover's algorithm, which uses quantum concepts to search databases rapidly, could result in a quadratic improvement of brute-force attacks on symmetric encryption algorithms like AES and RSA.[12]

One response to this evolution involves implementing post-quantum computing-resistant algorithms, which use mathematical structures such as Module-Lattice-Based algorithms impervious to quantum attacks. The National Institute of Standards and Technology (NIST) down-selected, refined, and

10. Peter W. Shor, "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer," *SIAM Journal on Computing* 26, no. 5 (October 1997): 1484–1509, https://doi.org/10.1137/S0097539795293172.
11. Morris J. Dworkin et al., "Advanced Encryption Standard (AES)" (National Institute of Standards and Technology (NIST), Morris J. Dworkin, Elaine Barker, James R. Nechvatal, James Foti, Lawrence E. Bassham, E. Roback, James F. Dray Jr., November 26, 2001), https://www.nist.gov/publications/advanced-encryption-standard-aes.
12. Lov K. Grover, "A Fast Quantum Mechanical Algorithm for Database Search" (arXiv, November 19, 1996), https://doi.org/10.48550/arXiv.quant-ph/9605043.

published the standards for Post-Quantum Cryptography (PQC) in August 2024.[13] This journey took NIST and world-renowned cryptographers nearly a decade to accomplish with the cipher suite Module-Lattice-Based Key Encapsulation Mechanism (ML-KEM) standard. ML-KEM protects against man-in-the-middle attacks, data harvesting and analytics, and ensures you are ready for both today's most advanced attacks and external facing zero-day attacks as well as emergent quantum computer-based attacks and decryption.[14] Protection is here today to secure all transmitted and currently stored encrypted data against scalable supercomputers and quantum computers.

Entropya's Quantum Agents use the gold standard of this quantum-ready cryptography as defined by NIST in Federal Information Processing Standards (FIPS) Publication 203 for ML-KEM and Digital Signature Construction. ML-KEM is indistinguishable under chosen-cyphertext attack (IND-CCA2) secure key encapsulation mechanism (KEM) whose security uses the hardness of solving the learning-with-errors (LWE) problem over module lattices. The CCA-secure ML-KEM is built on top of a chosen-plaintext attack (CPA) secure cryptosystem based on the hardness of Module-LWE.[15] ML-KEM cipher suite has the same security as AES-256 but with no digital signature or key management vulnerabilities.

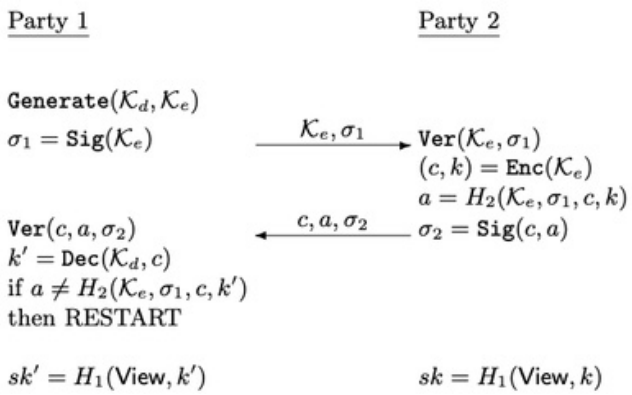

Figure 3. A Generic AKE construction from "The Whole is Less than the Sum of its Parts: Constructing More Efficient Lattice-Based AKEs."[16]

13. National Institute of Standards and Technology, "Module-Lattice-Based Key-Encapsulation Mechanism Standard" (U.S. Department of Commerce, August 13, 2024), https://doi.org/10.6028/NIST.FIPS.203.
14. Deloitte, "Harvest Now, Decrypt Later Attacks Pose a Security Concern as Organizations Consider Implications of Quantum Computing," accessed June 28, 2025, https://www.prnewswire.com/news-releases/harvest-now-decrypt-later-attacks-pose-a-security-concern-as-organizations-consider-implications-of-quantum-computing-301628445.html.
15. National Institute of Standards and Technology, "Module-Lattice-Based Key-Encapsulation Mechanism Standard" (U.S. Department of Commerce, August 13, 2024), https://doi.org/10.6028/NIST.FIPS.203.
16. Rafael del Pino, Vadim Lyubashevsky, and David Pointcheval, "The Whole Is Less Than the Sum of Its Parts: Constructing

Entropya implements the highest level of this cryptography standard throughout its portfolio and is operationally deployed today. Entropya's Quantum Agents are Authenticated Key Exchanges (AKE) comprised of ML-KEM 1024 with an ephemeral signature.[17] These mature Technology Readiness Level Nine (TRL-9) solutions are ready for your most challenging conditions and pressing security problems.

More Efficient Lattice-Based AKEs," in *Security and Cryptography for Networks*, ed. Vassilis Zikas and Roberto De Prisco (Cham: Springer International Publishing, 2016), 273–91, https://doi.org/10.1007/978-3-319-44618-9_15.
17. Ibid.

Conclusion

The digital landscape continues to rapidly evolve. Most cybersecurity solutions add layers of complexity creating fissures in modern architectures. The traditional security approach is insufficient. Entropya thinks differently starting with a foundationally different viewpoint. Simplify complexity and save on costly infrastructure upgrades while increasing overall security by making it all disappear first.

Entropya's approach centers on a dynamic, secure, and untraceable transport infrastructure that provides highest grade security surrounding and encapsulating the findable entry points for access to your network boundary. Our solutions are built on Zero Trust principles and dynamically adapt to stay ahead of attackers. By combining Software-Defined Private Networking (SDPN) with cutting-edge and durable Post-Quantum Cryptography (PQC), we safeguard both data at rest and in motion against the most advanced threats. Entropya provides standards driven unparalleled protection, independently tested and operationally deployed. Whether it's preventing surveillance, avoiding data breaches, protecting critical communications, or untraceably synchronizing data, we provide the tools and infrastructure you need.

As the scope of digital targets continues to expand, now is the time to rethink traditional security to become durable and quantum ready while safeguarding what matters most for decades to come. Entropya provides ***Uncompromising Performance and Leading Grade Security for Everything you have***. Embrace elegant simplicity and contact Entropya today.

REFERENCES

Bos, Joppe, Léo Ducas, Eike Kiltz, Tancrède Lepoint, Vadim Lyubashevsky, John M. Schanck, Peter Schwabe, Gregor Seiler, and Damien Stehlé. 2017. "CRYSTALS -- Kyber: A CCA-Secure Module-Lattice-Based KEM." Cryptology ePrint Archive. https://eprint.iacr.org/2017/634.

Computer Security Resource Center Content Editor. n.d. "Man-in-the-Middle Attack (MitM) - Glossary | CSRC." Accessed June 28, 2025. https://csrc.nist.gov/glossary/term/man_in_the_middle_attack.

"Cyber Threats and Advisories | Cybersecurity and Infrastructure Security Agency CISA." n.d. Accessed June 28, 2025. https://www.cisa.gov/topics/cyber-threats-and-advisories.

Deloitte. n.d. "Harvest Now, Decrypt Later Attacks Pose a Security Concern as Organizations Consider Implications of Quantum Computing." Accessed June 28, 2025. https://www.prnewswire.com/news-releases/harvest-now-decrypt-later-attacks-pose-a-security-concern-as-organizations-consider-implications-of-quantum-computing-301628445.html.

Dutta, Tushar Subhra. 2025. "Detecting Cyber Attack Patterns by Analyzing Threats Actors Infrastructure." *Cyber Security News* (blog). March 9, 2025. https://cybersecuritynews.com/detecting-cyber-attack-patterns/.

"Global Cyberattacks by Type 2023." n.d. Statista. Accessed June 28, 2025. https://www.statista.com/statistics/1382266/cyber-attacks-worldwide-by-type/.

"Global Trends 2040." 2021. Washington, DC: United States of America, Office of the Director of National Intelligence. https://www.dni.gov/index.php/gt2040-home/gt2040-media-and-downloads.

Grover, Lov K. 1996. "A Fast Quantum Mechanical Algorithm for Database Search." arXiv. https://doi.org/10.48550/arXiv.quant-ph/9605043.

Krause, Joern. 2024. "Non-Terrestrial Networks (NTN)." 3GPP.Org. May 14, 2024. https://www.3gpp.org/technologies/ntn-overview.

Li, Yuchong, and Qinghui Liu. 2021. "A Comprehensive Review Study of Cyber-Attacks and Cyber Security; Emerging Trends and Recent Developments." *Energy Reports* 7 (November):8176–86. https://doi.org/10.1016/j.egyr.2021.08.126.

"Major Cyber Attacks 2025: A Comprehensive Analysis of the Year's Most Devastating Data Breaches and Ransomware Incidents." 2025. Breached Company. May 28, 2025. https://breached.company/major-cyber-attacks-2025-a-comprehensive-analysis-of-the-years-most-devastating-data-breaches-and-ransomware-incidents/.

Maynard, Peter, Kieran McLaughlin, and Sakir Sezer. 2020. "Decomposition and Sequential-AND Analysis of Known Cyber-Attacks on Critical Infrastructure Control Systems." *Journal of Cybersecurity* 6 (1). https://doi.org/10.1093/cybsec/tyaa020.

"MITRE ATT&CK®." n.d. Accessed June 28, 2025. https://attack.mitre.org/.

Mohr, Clare, Shawn Cozzolino, An David, and Will Burns. 2025. "Cybersecurity Report 2025: AI Threats, Email Server Security, and Advanced Threat Actors | Deloitte US." Deloitte & Touche LLP. https://www.deloitte.com/us/en/services/consulting/articles/cybersecurity-report-2025.html.

"Nation-State Cyber Actors | Cybersecurity and Infrastructure Security Agency CISA." n.d. Accessed June 28, 2025. https://www.cisa.gov/topics/cyber-threats-and-advisories/nation-state-cyber-actors.

"NIC Releases Global Trends - Paradox of Progress." n.d. Accessed June 28, 2025. https://www.dni.gov/index.php/features/1685-nic-releases-global-trends-paradox-of-progress.

Pino, Rafael del, Vadim Lyubashevsky, and David Pointcheval. 2016. "The Whole Is Less Than the Sum of Its Parts: Constructing More Efficient Lattice-Based AKEs." In *Security and Cryptography for Networks*, edited by Vassilis Zikas and Roberto De Prisco, 273–91. Cham: Springer International Publishing. https://doi.org/10.1007/978-3-319-44618-9_15.

"Public Report of the Committee of Inquiry into the Cyber Attack on Singapore Health Services Private Limited's Patient Database on or Around 27 June 2018." 2019. Singapore: Ministry for Communications and Information Singapore. https://file.go.gov.sg/singhealthcoi.pdf.

Schwabe, Peter. n.d. "Kyber Cryptographic Suite for Algebraic Lattices (CRYSTALS)." Text. Accessed June 28, 2025. https://pq-crystals.org/kyber/.

Shor, Peter W. 1997. "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer." *SIAM Journal on Computing* 26 (5): 1484–1509. https://doi.org/10.1137/S0097539795293172.

Technology, National Institute of Standards and. 2024. "Module-Lattice-Based Key-Encapsulation Mechanism Standard." Federal Information Processing Standard (FIPS) 203. U.S. Department of Commerce. https://doi.org/10.6028/NIST.FIPS.203.

Technology (NIST), National Institute of Standards and, Morris J. Dworkin, Elaine Barker, James R. Nechvatal, James Foti, Lawrence E. Bassham, E. Roback, and James F. Dray Jr. 2001. "Advanced Encryption Standard (AES)." National Institute of Standards and Technology (NIST), Morris J. Dworkin, Elaine Barker, James R. Nechvatal, James Foti, Lawrence E. Bassham, E. Roback, James F. Dray Jr. https://www.nist.gov/publications/advanced-encryption-standard-aes.

Tham, Irene, Rachel Au-Yong, Tin May Linn, and Rodolfo Pazos. 2018. "Singapore's Worst Cyber Attack: How It Unfolded." The Straits Times. July 20, 2018. https://graphics.straitstimes.com/STI/STIMEDIA/Interactives/2018/07/sg-cyber-breach/index.html.