Bibliografía

Aliro, The Quantum Networking Company. (s.f.*). Navigating security threats posed by Q-Day.* https://www.aliroquantum.com/navigating-security-threats-posed-by-q-day

Asenjo, R. (25 de agosto de 2025). *Qué es HUMINT, la inteligencia de fuentes humanas.* LISA News. https://www.lisanews.org/inteligencia/que-es-humint-la-inteligencia-de-fuentes-humanas/

BlackRock Inc. (19 de septiembre de 2025). *Geopolitical risk dashboard*. https://www.blackrock.com/corporate/insights/blackrock-investment-institute/interactive-charts/geopolitical-risk-dashboard#risk-summary

Braunstein, A. (19 de diciembre de 2024). *Q-Day and the impact of breaking RSA2048*. IONQ. https://ionq.com/blog/q-day-and-the-impact-of-breaking-rsa2048

Brodersen, J. (1 de junio de 2025). *"Q-Day": cuál es el riesgo que corren las computadoras y por qué hay una rama "post cuántica" de la ciberseguridad*. Clarín. https://www.clarin.com/tecnologia/q-day-riesgo-corren-computadoras-rama-post-cuantica-ciberseguridad_0_RFHJtpkeEw.html

Brooks, C. (31 de agosto de 2025). *The coming inflection point for quantum technology*. Forbes. https://www.forbes.com/sites/chuckbrooks/2025/08/29/the-coming-inflection-point-for-quantum-technology/

Castilla, J. C. (17 de septiembre de 2025). *La OTAN entre Washington y La Haya: crisis de identidad y discurso.* Centro Superior de Estudios de la Defensa Nacional (CESEDEN). Ministerio de Defensa. https://www.defensa.gob.es/ceseden/-/ieee/la_otan_entre_washington_y_la_haya_2025_dieeea57

Fortune, D., Roetteler, M. & Aiello, M. (19 de diciembre de 2024). *Predicting Q-Day and the impact of breaking RSA2048*. Secureworks. https://www.secureworks.com/blog/predicting-q-day-and-impact-of-breaking-rsa2048

Goel, A. (23 de agosto de 2025). *The finance industry's urgent role in preparing for the quantum threat*. Encryption Consulting. https://www.encryptionconsulting.com/finance-industry-role-in-preparing-for-the-quantum-threat/

Ibrahim, S. (14 de enero de 2025). *What's the environmental cost of Switzerland's new supercomputer?* SWI Swissinfo.ch https://www.swissinfo.ch/eng/swiss-ai/whats-the-environmental-cost-of-switzerlands-new-supercomputer/88720218#:~:text=The%20environmental%20impact%20of%20supercomputing,to%20water%20loss%20through%20evaporation.

Ivezic, M. (1 de marzo de 2025). *Quantum geopolitics: the global race for quantum computing*. PostQuantum. https://postquantum.com/quantum-computing/quantum-geopolitics/

Ivezic, M. (23 de junio de 2025). *What will really happen once Q-Day arrives – when our current cryptography is broken?* [Entrada en Linkedin]. https://www.linkedin.com/pulse/what-really-happen-once-q-day-arrives-when-our-current-marin-ivezic-zn1bc/

LISA Institute. (30 de agosto de 2024). *Análisis estratégico: qué es, métodos y cómo aplicarlo en tu empresa*. LISA News. https://www.lisanews.org/estrategia/analisis-estrategico-que-es-metodos-y-como-aplicarlo-en-tu-empresa/

MetaCompliance. (29 de septiembre de 2025*). 5 damaging consequences of data breach: protect your assets*. https://www.metacompliance.com/blog/data-breaches/5-damaging-consequences-of-a-data-breach

NIST Computer Security Resource Center. (13 de agosto de 2024). *Post-quantum cryptography*. Departamento de Comercio. https://csrc.nist.gov/projects/post-quantum-cryptography

Organización del Tratado del Atlántico Norte. (16 de enero de 2024). *Summary of NATO's quantum technologies strategy*. https://www.nato.int/cps/en/natohq/official_texts_221777.htm

Organización del Tratado del Atlántico Norte. (19 de agosto de 2025). *Science for peace and security*. https://www.nato.int/cps/en/natohq/topics_85373.htm

Palo Alto Networks. (23 de junio de 2025). *The quantum computing threat*. https://docs.paloaltonetworks.com/network-security/quantum-security/administration/quantum-security-concepts/the-quantum-computing-threat

RAND. (s.f.). *Developing a quantum technology observatory for policy and society*. https://www.rand.org/randeurope/research/projects/2025/developing-quantum-technology-observatory-for-policy-and-society.html

Sadurni, J.M. (17 de junio de 2024). *Alan Turing, el arma secreta de los aliados*. National Geographic. https://historia.nationalgeographic.com.es/a/alan-turing-arma-secreta-aliados_16352

Singh, S. (25 de junio de 2025). *New Google research shows RSA 2048 could be broken sooner than expected*. Encryption Consulting. https://www.encryptionconsulting.com/new-google-research-shows-rsa-2048-could-be-broken-sooner-than-expected/

Schneider, J. (s.f.). *Cryptography use cases: From secure communication to data security*. IBM. https://www.ibm.com/think/topics/cryptography-use-cases

World Economic Forum (19 de enero de 2022). *Quantum computing governance principles*. https://www.weforum.org/publications/quantum-computing-governance-principles/

Zhong, H.-S., Wang, H., Deng, Y.-H., Chen, M.-C., Peng, L.-C., Luo, Y.-H., Qin, J., Wu, D., Ding, X., Hu, Y., Hu, P., Yang, X.-Y., Zhang, W.-J., Li, H., Li, Y., Jiang, X., Gan, L., Yang, G., You, L.… (2020). *Quantum computational advantage using photons. Science*, 370(6523), 1460–1463. https://doi.org/10.1126/science.abe8770

ANÁLISIS PROSPECTIVO DEL DÍA-Q. ¿CISNE NEGRO SILENCIOSO O CISNE GRIS INEVITABLE?

Victor Pérez Fernández

victor.perezfernandez@hotmail.com

1. Introducción

El mundo se encuentra en un período turbulento. Guerras a las puertas de Europa, tensiones diplomáticas en ascenso, ciberataques respaldados por gobiernos y una carrera tecnológica entre Oriente y Occidente que evoca la Guerra Fría.

En este contexto, millones de transacciones, comunicaciones y decisiones críticas dependen de algoritmos criptográficos como RSA y ECC. Pero basta un avance silencioso en un laboratorio cuántico para colapsar todo ese sistema de confianza.

Ese punto de inflexión es el día-Q: el momento en el que un actor logra romper la criptografía asimétrica mediante algoritmos cuánticos. No se trata solo de un reto tecnológico, sino de un acontecimiento con capacidad para alterar la seguridad, la economía y la política internacional.

Desde ese momento, cualquier comunicación cifrada clásicamente será vulnerable, cualquier dato podrá ser expuesto y cualquier transacción podría ser explotada. Esto afectaría directamente a sistemas críticos, como las comunicaciones gubernamentales o al sistema financiero.

2. Cuerpo del análisis

Para detallar el impacto global del día-Q comenzaremos aplicando un análisis PESTEL de la situación general:

- **Político**: El primer actor estatal en conseguirlo obtendría una ventaja estratégica comparable a la carrera nuclear del siglo XX o al descifrado de Enigma en la Segunda Guerra Mundial.
- **Económico**: La pérdida de confianza en la criptografía pondría en riesgo la estabilidad de los mercados, generando pérdidas millonarias.

- **Social**: La exposición masiva de datos personales sensibles y comunicaciones privadas minaría la confianza ciudadana en el sistema, pudiendo erosionar la legitimidad democrática y alimentar movimientos de desinformación.
- **Tecnológico**: Esta ruptura obligaría la aceleración de la adopción de la criptografía poscuántica (PQC), generando una nueva carrera tecnológica global.
- **Ambiental**: El despliegue de superordenadores cuánticos implica alto consumo energético y de refrigeración, problemático en un contexto de crisis climática.
- **Legal**: La ausencia de marcos regulatorios internacionales crearía un vacío jurídico aumentando el riesgo de proliferación tecnológica sin control.

La incógnita es si el día-Q se manifestará como cisne negro silencioso, explotado en secreto por el primer actor en lograrlo, o como un cisne gris inevitable, cuyo impacto conocemos, pero para el que no estamos preparados. Dos preguntas dominan: ¿Quién? y ¿Cuándo?

Sobre el cuándo, la mayoría de estimaciones sitúan el día-Q en la década de 2030, aunque estudios más recientes lo adelantan. Incluso China ya demostró en 2020 un avance significativo al reducir cálculos de millones de años a minutos. La adopción de PQC es urgente.

Sin embargo, el foco de este análisis lo centraremos en el "¿Quién?". El actor que rompa la seguridad determinará la naturaleza del escenario geopolítico. Para eso, aplicamos una matriz de escenarios utilizando actor y visibilidad como variables clave. Debido al impacto que tiene en la seguridad nacional la pertenencia a la OTAN, este será el criterio para identificar los diferentes actores.

Actor / Visibilidad	Secreto	Público
Estado no OTAN	**Riesgo crítico**: explotación encubierta, asimetría informativa, difícil detección, secretos de estado y estrategias militares expuestas.	**Riesgo alto**: carrera armamentística abierta, pánico en mercados y crisis de confianza en occidente.

Actor / Visibilidad	Secreto	Público
Estado OTAN	**Riesgo medio**: tensiones internas por compartir o no, espionaje con ventaja controlada.	**Riesgo bajo**: anuncio refuerza disuasión y liderazgo, acelera PQC.
Centro independiente	**Riesgo bajo**: probable apropiación estatal y uso limitado.	**Riesgo alto**: sensación de inseguridad general y shock sistémico.

Sobre esta matriz, analizaremos en detalle un escenario de cada actor. Consideraremos el que tenga el riesgo más alto de cada par.

2.1 Escenario 1: Estado no OTAN en Secreto

Dinámicas inmediatas: Un actor externo alcanza en secreto la capacidad y explota datos interceptados, accediendo a archivos diplomáticos, inteligencia militar y transacciones financieras.

Impacto geoestratégico: Genera la mayor asimetría informativa: el adversario altera negociaciones y operaciones sin que occidente lo perciba.

Aspectos irreparables: Exposición de redes HUMINT, desclasificación de acuerdos secretos y pérdida de confianza en infraestructuras financieras globales.

Indicadores de detección: Movimientos políticos o militares inexplicablemente precisos, filtraciones selectivas de información sensible o patrones anómalos en mercados financieros.

2.2 Escenario 2: Estado OTAN en Secreto

Dinámicas inmediatas

Un estado aliado logra la ventaja cuántica en secreto. Usa la capacidad para espionaje externo, manteniendo silencio incluso frente a socios.

Impacto geoestratégico: El riesgo no viene de adversarios, sino de la erosión de cohesión en la Alianza. La asimetría interna genera desconfianza y dependencia estratégica.

Aspectos irreparables: Fractura de confianza transatlántica, pérdida de autonomía estratégica del bloque contrapuesto (USA vs. Europa) y dificultad para un marco normativo común.

Indicadores de detección: Cambios súbitos en política exterior de un aliado, reticencia en proyectos conjuntos de ciberseguridad y ventajas desproporcionadas en negociaciones militares.

2.3 Escenario 3: Centro independiente y Público

Dinámicas inmediatas: Un centro de investigación anuncia públicamente la ruptura de RSA/ECC. La noticia se difunde en revistas científicas y en redes sociales.

Impacto geoestratégico: Provoca un shock sistémico: mercados en caída, servicios suspendidos, gobiernos en emergencia digital. El conocimiento se democratiza y dispara la carrera global hacia PQC. Tecnología accesible para todos. Grupos terroristas pueden hacerse con esta tecnología para realizar ciberataques.

Aspectos irreparables: Pérdida de confianza en certificados digitales y exposición retroactiva de datos históricos.

Indicadores de detección: Publicaciones académicas o filtraciones en repositorios abiertos.

3. Conclusiones y perspectiva de futuro

El día-Q será un punto de inflexión histórico: un hito capaz de transformar la seguridad militar, económica y política. Los escenarios muestran que la gravedad no depende solo de quién alcance la capacidad sino de cómo gestione su carácter secreto o público.

La conclusión principal es la necesidad de anticipación: debemos acelerar la transición hacia PQC en infraestructuras críticas, fomentar una cooperación reforzada en el seno de OTAN, y definir marcos internacionales de transparencia cuántica. Nuestras acciones

decidirán si el orden internacional del futuro se construye sobre confianza compartida o sobre asimetrías informativas que alimenten el conflicto.

El día-Q no es solo un reto tecnológico; es la prueba definitiva de resiliencia para la gobernanza internacional. La diferencia entre un cisne gris inevitable y un cisne negro silencioso dependerá de nuestra capacidad para anticipar la situación y adaptarnos a tiempo.