ASPECTOS CARACTERIZADOS

A continuación se presentan las respuestas a las preguntas que se obtuvieron de la caracterización de los 12 aspectos más significativos debido a su alta cantidad de publicaciones y que coincidieron con dichos aspectos.

I. Establecer estándares de ciberseguridad cuántica

1.1 ¿Cómo participar en la creación de estándares y regulaciones relacionados con la ciberseguridad cuántica?

Participar en la creación de normas y reglamentos relacionados con la ciberseguridad cuántica es crucial para la adopción comercial de las tecnologías cuánticas y el desarrollo de un ecosistema cuántico europeo. Pitwon & Lee, (2021) destacan la importancia de la normalización internacional para acelerar la adopción comercial de las tecnologías cuánticas. Rodriguez, (2023) discute la necesidad de una agenda de ciberseguridad cuántica para que Europa gobierne la transición a la criptografía post-cuántica. Yesina, Ostrianska, et al., (2022) informa sobre el proceso de normalización de la criptografía poscuántica del NIST, cuyo objetivo es seleccionar uno o varios algoritmos criptográficos de clave pública que puedan proteger bien la información confidencial en un futuro próximo, incluso tras la llegada de los equipos cuánticos. Hossain Faruk et al., (2022) ofrece una revisión exhaustiva de la ciberseguridad cuántica, destacando el potencial de la computación cuántica tanto para plantear amenazas inesperadas como para ofrecer soluciones a problemas críticos de ciberseguridad. En general, los artículos sugieren que participar en la creación de normas y reglamentos relacionados con la ciberseguridad cuántica es esencial para garantizar la seguridad de las tecnologías cuánticas y su adopción con éxito en diversas industrias.

1.2 ¿Qué estándares y regulaciones existen relacionadas con la ciberseguridad cuántica?

Los documentos sugieren que hay esfuerzos por normalizar y certificar las tecnologías de ciberseguridad cuántica, pero hasta ahora no se ha ideado ningún sistema oficial de certificación específico para dispositivos cuánticos (Walenta et al., 2015). La computación cuántica plantea tanto amenazas como oportunidades para la ciberseguridad, y es necesaria una criptografía segura para protegerse de los ataques cuánticos (Hossain Faruk et al., 2022), (Taiber, 2020), (Teodoraș et al., 2023). La criptografía poscuántica y otras tecnologías cuánticas aplicables son necesarias para que el ecosistema vehículo a

todo (V2X) sea seguro desde el punto de vista cuántico (Taiber, 2020). La criptografía cuántica y la distribución cuántica de claves podrían aportar nuevas soluciones a diferentes tareas criptográficas que se sabe que son imposibles utilizando equipos normales (Teodoraș et al., 2023).

1.3 ¿Cómo identificar las mejores prácticas de ciberseguridad cuántica?

Los documentos sugieren que la computación cuántica plantea tanto amenazas como oportunidades para la ciberseguridad. Hossain Faruk et al., (2022) ofrece un panorama completo del estado actual de la computación cuántica y la ciberseguridad, destacando el potencial de la computación cuántica tanto para mejorar como para amenazar la ciberseguridad. (Ahn et al., 2021) explora específicamente las vulnerabilidades potenciales y las estrategias de defensa para las redes de recursos energéticos distribuidos (DER). (Mosca, 2018) hace hincapié en la necesidad de que las organizaciones comprendan sus riesgos específicos y planifiquen sistemas resistentes a los ataques cuánticos. (F. Xu et al., 2020) revisa el estado actual de la distribución segura de claves cuánticas, destacando los avances teóricos y prácticos en criptografía cuántica. En general, los artículos sugieren que la identificación de las mejores prácticas de ciberseguridad cuántica requerirá una comprensión profunda de las amenazas y vulnerabilidades potenciales que plantea la computación cuántica, así como el desarrollo y la aplicación de estrategias de defensa eficaces.

II. Escalada de amenazas

2.1 ¿De qué manera el aumento en las capacidades cuánticas de los atacantes contribuye a una escalada de amenazas cibernéticas que afectan la seguridad de los sistemas de TO e IC?

El aumento de las capacidades cuánticas de los atacantes contribuye a una escalada de las amenazas cibernéticas que afectan a la seguridad de los sistemas OT y las infraestructuras críticas. (Caicedo, 2017) sostiene que las capacidades cibernéticas se han vuelto críticas para todos los actores del sistema internacional, y un gran ataque cibernético podría generar un efecto masivo de disrupción, incertidumbre, pánico e inestabilidad entre individuos y organizaciones, induciendo inestabilidad global. (Yao & Almohri, 2013) propone un marco de autenticación de aplicaciones (**A2**) que reduce el riesgo de infección por potentes aplicaciones maliciosas que pueden interrumpir la ejecución adecuada de aplicaciones legítimas, robar datos privados de los usuarios y propagarse por toda la red de la organización. (Sperotto et al., 2015) destaca la importancia de medir, detectar y

mitigar las amenazas de red emergentes, y presenta técnicas de detección y mitigación de vanguardia que son efectivas contra los ataques de red y las actividades internas en las redes y redes troncales de red actuales y futuras de tamaño pequeño y empresarial. (Ponnusamy et al., 2020) revisa los ataques y contramedidas en IoT y SCF, incluidos los ataques de denegación de servicio distribuido (**DDOS**), phishing, troyanos y otros que hacen que la información de la red sea insegura. En general, los documentos sugieren que el aumento de las capacidades cuánticas de los atacantes representa una amenaza significativa para la seguridad de los sistemas OT y las infraestructuras críticas, y se necesitan medidas efectivas para detectar y mitigar las amenazas de red emergentes.

2.2 ¿Cuáles son los desafíos y requisitos para desarrollar e implementar respuestas de seguridad sofisticadas y avanzadas capaces de contrarrestar efectivamente la escalada de amenazas impulsada por las capacidades cuánticas crecientes de los atacantes?

El desarrollo de la computación cuántica plantea importantes desafíos a los sistemas criptográficos actuales y a las tecnologías emergentes (Abuarqoub, 2020;Käppler & Schneider, 2021). Los equipos cuánticos amenazan a la criptografía asimétrica, lo que hace necesario el desarrollo de la PQC para garantizar una comunicación segura (Ravi et al., 2022). La implementación de PQC se enfrenta a obstáculos como limitaciones de tiempo y una ejecución inadecuada, lo que puede llevar una década o más para su implementación completa (Käppler & Schneider, 2021). Las tecnologías cuánticas también tienen aplicaciones militares, lo que lleva al concepto de "guerra cuántica" y a la necesidad de nuevas estrategias y éticas (M. Krelina, 2021). Para abordar estos desafíos, los investigadores están explorando algoritmos resistentes a la era cuántica, QKD y otras primitivas criptográficas seguras para la era cuántica (Ravi et al., 2022). Las organizaciones deben evaluar sus riesgos específicos y planificar sistemas resistentes a la era cuántica en función de la vida útil de la seguridad de sus activos, el tiempo de migración a sistemas resistentes a la era cuántica y el cronograma para que las computadoras cuánticas rompan las medidas de seguridad actuales (Ali, 2021; Mosca, 2018).

III. Integración de tecnologías cuánticas

3.1 ¿Cuáles son los desafíos y complejidades involucrados en la incorporación de tecnologías cuánticas, como la computación y la comunicación cuántica, en las infraestructuras existentes?

La incorporación de tecnologías cuánticas a las infraestructuras existentes presenta tanto retos como oportunidades. (I. Khan, 2018a) analiza el uso de la QKD para proporcionar una arquitectura de comunicación segura a largo plazo, mientras que (Hughes et al., 2013) describe las comunicaciones cuánticas centradas en la red (**NQC**) como una instanciación escalable de la criptografía cuántica que se puede aplicar como una actualización de seguridad a las instalaciones de fibra óptica existentes. (Karol & Życzkowski, 2015) proponen el uso de interferómetros de fotón único para proteger las instalaciones de infraestructura, en particular las líneas de transmisión, y (Majumder et al., 2023) presenta un enfoque cuántico para implementar la partición de la red como medio para analizar el riesgo en IC. En general, los documentos sugieren que, si bien las tecnologías cuánticas ofrecen soluciones prometedoras para proteger la infraestructura crítica, todavía hay desafíos que deben abordarse en términos de implementación e integración con los sistemas existentes.

3.2 ¿Qué riesgos potenciales y problemas de seguridad pueden surgir si la integración de tecnologías cuánticas en infraestructuras existentes no se realiza de manera adecuada y cuidadosa?

La integración de tecnologías cuánticas en las infraestructuras existentes sin el cuidado y la atención adecuada podría dar lugar a riesgos potenciales y problemas de seguridad. (Mistry et al., 2021) destacan la importancia de la criptografía cuántica para mejorar la transmisión segura a través de Internet cuántico, mientras que (Carle et al., 2012) enfatizan la necesidad de sistemas de alerta temprana para detectar ataques distribuidos y coordinados a IC. (Hamza et al., 2020) analizan las vulnerabilidades de los dispositivos IoT y la necesidad de soluciones de seguridad sólidas para prevenir los ciberataques. (Schwalb & L, 2007) proponen el uso de un mercado de "derivados explotados" para predecir y prevenir ciber-ataques, pero solo después de cambios en el entorno regulatorio actual. En general, los documentos sugieren que la integración de las tecnologías cuánticas en las infraestructuras existentes requiere una cuidadosa consideración de los aspectos de seguridad y privacidad para prevenir riesgos potenciales.

IV. Cambios tecnológicos continuos

4.1 ¿Cuál es la importancia de que las IC se adapten continuamente a nuevas tecnologías, incluidas las cuánticas, para garantizar un nivel de seguridad óptimo?

Los documentos sugieren que la adaptación continua de las IC a las nuevas tecnologías, incluidas las tecnologías cuánticas, es crucial para garantizar un nivel óptimo de seguridad. (Pătraşcu, 2021) sostiene que las tecnologías emergentes, como el Internet de las cosas, son necesarias para optimizar la protección y defensa de las infraestructuras críticas. (Antoliš et al., 2015) destaca las vulnerabilidades que las nuevas tecnologías aportan a la seguridad de las infraestructuras críticas, haciendo hincapié en la necesidad de la seguridad de las TIC como componente de la seguridad de las IC. (Commission et al., 2017) habla de la importancia de la ciberseguridad en la protección de las infraestructuras críticas frente a los ciberataques, que cada vez se perciben más como un problema creciente y real. (Eng Vasile Florin POPESCU, 2019) enfatiza que la ciber-protección se ha vuelto crucial en todos los sectores de actividad, y la ausencia de medidas para proteger las infraestructuras críticas amenaza con causar un gran daño al funcionamiento de la empresa. En general, los documentos sugieren que la adaptación continua de las infraestructuras críticas a las nuevas tecnologías, incluidas las tecnologías cuánticas, es esencial para garantizar un nivel óptimo de seguridad.

4.2 ¿Cuáles son los principales desafíos y necesidades que enfrentan las IC para mantenerse al día con los avances rápidos y constantes en la tecnología cuántica?

Los documentos sugieren que las IC se enfrentan a importantes desafíos para mantenerse al día con los rápidos y constantes avances en la tecnología cuántica. (I. Khan, 2018b) y (Goy et al., 2021) discuten la necesidad de redes de comunicación seguras y el desarrollo de infraestructura de QKD para proteger la IC de los ataques de computadoras cuánticas. (Alcaraz & Zeadally, 2015) destaca las vulnerabilidades y amenazas a las que se enfrentan las IC modernas, incluidos los sistemas de control industrial, y describe las medidas de protección. (Ståhl, 2013) analiza los retos de los sistemas de monitorización de IC, incluida la necesidad de resiliencia y el desarrollo de herramientas y escenarios de formación para los operadores. En general, los documentos sugieren que las IC deben adaptarse al cambiante panorama tecnológico e implementar medidas para protegerse contra las amenazas cuánticas.

V. Gestión de recursos

5.1 ¿Cuál es el impacto financiero y de recursos que implica la implementación de medidas de seguridad cuántica en organizaciones y entidades?

Los documentos sugieren que la implementación de medidas de seguridad cuántica en organizaciones y entidades puede tener impactos financieros y de recursos. (Campbell, Sr., 2020) analiza la necesidad de un marco de gestión de riesgos de contabilidad distribuida empresarial ciber-resistente para gestionar los riesgos de seguridad en las transacciones distribuidas empresariales. (Воропай et al., 2022) proponen mecanismos para la prestación de servicios de seguridad basados en algoritmos post-cuánticos para garantizar la estabilidad de los canales de comunicación y elementos de la estructura de los sistemas de supervisión, control y adquisición de datos (**SCADA**). (Mistry et al., 2021) describen la criptografía cuántica como una solución para la comunicación segura de datos a través de Internet cuántico, que se puede implementar en redes de inteligencia, comunicación satelital e IC. (Sturgeon, 2012) analiza el potencial de la computación cuántica para hacer que los datos y las redes sean menos seguros, lo que lleva a un aumento del espionaje, los ataques a instituciones financieras e IC, y la necesidad de que los estados aprendan a disuadir a los actores no estatales de utilizar ilícitamente esta tecnología. En general, los documentos sugieren que la implementación de medidas de seguridad cuántica puede ser costosa y requerir recursos significativos, pero puede ser necesaria para garantizar la seguridad de las organizaciones y entidades frente a las amenazas emergentes.

5.2 ¿Cómo contribuye la falta de fondos y de recursos adecuados a debilitar la ciberseguridad y la protección frente a ciber-amenazas emergentes?

La falta de financiación y recursos adecuados es uno de los principales factores que contribuyen al debilitamiento de la ciberseguridad y la protección contra las ciber-amenazas emergentes. (Streich, 2023) argumenta que el mosaico actual de regulaciones federales de ciberseguridad en los EE. UU. no maximiza la defensa del país contra las ciber-amenazas, y sugiere expandir la autoridad de reglamentación y aplicación de la Agencia de Seguridad de Infraestructura y Ciberseguridad para monitorear y mitigar las amenazas cibernéticas en diversos sectores. (Olofinbiyi, 2022) encuentra que el nivel de conciencia sobre la ciberseguridad entre la población sudafricana es muy bajo, mientras que las legislaciones implementadas han hecho poco para aliviar las tendencias y proteger a la población en general de la ciberguerra. (Shane, 2012) argumenta que EE.UU. carece de un marco de leyes y regulaciones que incentive adecuadamente a las partes con mayor capacidad para mejorar la ciberseguridad a hacerlo, y sugiere un amplio debate nacional dirigido a definir el bien público con respecto a la ciberseguridad. (Flowers et al., 2013)

presenta una revisión exhaustiva de las leyes y regulaciones actuales de los Estados Unidos que se están utilizando para disuadir las actividades de ciberdelincuencia y apoyar la ciberseguridad, y describe los esfuerzos legislativos que se están llevando a cabo en otros países.

VI. Resiliencia y continuidad operativa

6.1 ¿Qué planes de contingencia y recuperación existen que tengan en cuenta ataques cuánticos y su impacto en la operación?

Las ponencias aportan ideas sobre planes de contingencia y recuperación que tienen en cuenta los ataques cuánticos y su impacto en la operación. (Mosca, 2018) subraya la importancia de que las organizaciones comprendan sus riesgos específicos y planifiquen la resistencia de sus sistemas a los ataques cuánticos. (Ali, 2021) repasa los conceptos cuánticos predominantes y analiza su impacto previsto en diversos aspectos de las tecnologías modernas de comunicación y seguridad de la información. También presenta algunos conceptos importantes en forma de preguntas y analiza las tendencias recientes adaptadas en los diseños criptográficos para frustrar los ataques cuánticos. (Zobel & Khansa, 2012) propone un enfoque general para caracterizar la resistencia de las ciber-infraestructuras frente a múltiples ciberataques maliciosos, que considera tanto el momento como la cantidad de pérdidas asociadas a cada ataque individual. (Rieffel et al., 2015) informa sobre un estudio de caso en la programación de un recocido cuántico temprano para atacar problemas de optimización relacionados con la planificación operativa, proporcionando conocimientos útiles para la programación y el diseño de futuros recocidos cuánticos.

6.2 ¿Cómo garantizar la resiliencia de SCF y la continuidad de las operaciones críticas?

Los artículos sugieren que garantizar la resistencia de los SCF y la continuidad de las operaciones críticas requiere un enfoque global que incluya mecanismos de restauración basados en la redundancia, tolerancia a fallos, medidas de seguridad y metodologías de diseño y desarrollo robustas. (Woo et al., 2008) proponen una metodología de diseño y desarrollo que unifica la ingeniería formal de software con leyes de control de realimentación y monitorización de recursos. (Alcaraz, 2018) presenta un enfoque de resiliencia dinámica asistida por la nube que utiliza mecanismos de restauración basados en redundancia para proteger un subconjunto de dispositivos de control ciber-físico. (Mihalache et al., 2019) revisan el estado del arte de los métodos para mejorar la

resiliencia de los sistemas ciber-físicos, incluyendo redundancia, tolerancia a fallos y medidas de seguridad. (Abdi et al., 2018) proponen un enfoque de diseño basado en el reinicio que garantiza la seguridad de las plantas físicas incluso cuando el sistema se ve comprometido. En general, los artículos sugieren que para garantizar la resistencia de los sistemas ciber-físicos y la continuidad de las operaciones críticas se requiere un enfoque de varios niveles que incluya mecanismos de restauración basados en la redundancia, tolerancia a fallos, medidas de seguridad y metodologías sólidas de diseño y desarrollo.

VII. Colaboración interdisciplinaria

7.1 ¿Cómo fomentar la colaboración entre expertos en ciberseguridad, computación cuántica y TO?

La colaboración entre expertos en ciberseguridad, computación cuántica y tecnología operativa es importante para mejorar la ciberseguridad. (Hui et al., 2010) analizan las dificultades de la colaboración entre analistas de ciberseguridad y proponen un marco de colaboración para facilitar la colaboración entre analistas. (Albataineh & Nijim, 2021) proponen un modelo educativo de ciberseguridad que incluye la computación cuántica para mejorar los conocimientos, la formación y las habilidades de los expertos en ciberseguridad. (Ramirez & Choucri, 2016) sostiene que la cooperación interdisciplinar es necesaria para abordar el problema polifacético de la ciberseguridad y propone directrices para estandarizar la terminología de la ciberseguridad con el fin de facilitar la colaboración. (Rajamaki, 2018) presenta un ejemplo de colaboración entre la industria y la universidad en materia de educación en ciberseguridad IoT y concluye que las competencias futuras en relación con los SPI son multidisciplinares y requieren un cambio hacia el pensamiento de resiliencia. En general, los artículos sugieren que la colaboración entre expertos en diferentes campos es necesaria para mejorar la ciberseguridad y que la cooperación interdisciplinaria y la educación son clave para lograr este objetivo.

7.2 ¿Cómo abordar los desafíos desde una perspectiva interdisciplinaria para proponer soluciones integrales?

Los documentos sugieren que la colaboración interdisciplinar es necesaria para abordar problemas y retos complejos. (Bililign, 2013) sostiene que la educación y la investigación interdisciplinarias son esenciales para el desarrollo humano sostenible y que las universidades deben reducir las barreras a la participación del profesorado en el trabajo interdisciplinario. (Witteman & Stahl, 2013) proponen cuatro métodos para facilitar la

colaboración interdisciplinar en la atención sanitaria: inmersiones profundas, un marco interdisciplinar, ejercicios de improvisación y esbozos rápidos. (Holley, 2009) analiza los retos y las oportunidades de las iniciativas interdisciplinares en la enseñanza superior, haciendo hincapié en la necesidad de diálogo e interacción entre diversas ideas, personas y conjuntos de conocimientos. (Kneller & Fayans, 2019) esbozan un enfoque interdisciplinar no tradicional para resolver tareas, que implica la sistematización de objetos, sus tipos de tareas relacionadas y métodos de solución. En general, los artículos sugieren que la colaboración interdisciplinar es necesaria para abordar problemas complejos, y que las universidades e instituciones deben crear entornos que faciliten el trabajo interdisciplinar.

VIII. Actualizar infraestructuras heredadas

8.1 ¿Cómo actualizar las infraestructuras ciber-físicas para aplicar medidas de seguridad cuántica?

Los artículos sugieren colectivamente que es necesario incorporar medidas de seguridad poscuántica a las infraestructuras ciber-físicas para protegerse de las amenazas a largo plazo que plantea la computación cuántica. (Paul et al., 2022) propone dos soluciones para integrar primitivas post-cuánticas en el protocolo industrial OPC UA, mientras que (Malina et al., 2023) revisa las recomendaciones de seguridad actuales y presenta una evaluación práctica de algoritmos de criptografía poscuántica seleccionados recientemente. (Ahn et al., 2021) exploran posibles estrategias de defensa para recursos energéticos distribuidos utilizando distribución de claves cuánticas y criptografía poscuántica. Por último, (Aguado et al., 2018) proponen un diseño de nodo para proporcionar seguridad mejorada mediante distribución de clave cuántica en servicios de extremo a extremo y analiza los requisitos del plano de control para la prestación de servicios en redes de transporte. En general, los artículos sugieren que la incorporación de medidas de seguridad poscuántica a las infraestructuras ciber-físicas requiere una cuidadosa consideración de los requisitos de rendimiento y comunicación, así como de las posibles vulnerabilidades de seguridad que plantea la computación cuántica.

8.2 ¿Qué sistemas de monitorización existen que puedan detectar actividades inusuales o ataques cuánticos en tiempo real?

Los artículos aportan ideas para evaluar la compatibilidad de las tecnologías cuánticas con los sistemas heredados y diseñar estrategias de transición. (Pérez-Castillo et al., 2021) propone un enfoque de modernización del software para reestructurar los sistemas

clásicos a fin de que funcionen en conjunción con los sistemas cuánticos, permitiendo la reutilización de los conocimientos incorporados en los sistemas heredados. (Linke et al., 2017) comparan dos arquitecturas de computación cuántica y sugiere que las aplicaciones y el hardware de los equipos cuánticos deberían co-diseñarse. (Serrano et al., 2023) revisa los principales componentes y plataformas de software cuántico y propone un conjunto de requisitos de calidad para su desarrollo y evaluación de la calidad. (A. A. Khan et al., 2022) realizan una revisión sistemática de la literatura sobre la arquitectura de software para sistemas de computación cuántica y sugieren que los procesos y notaciones existentes pueden adaptarse para derivar las actividades de arquitectura y desarrollar lenguajes de modelado para el software cuántico. En general, los artículos sugieren que es necesario un enfoque sistemático para evaluar la compatibilidad de las tecnologías cuánticas con los sistemas heredados y diseñar estrategias de transición, y que el co-diseño de las aplicaciones cuánticas con el hardware y el desarrollo de técnicas y herramientas de ingeniería de software cuántico son pasos cruciales para lograr una tecnología de computación cuántica útil.

IX. Gestionar claves cuánticas

9.1 ¿Qué protocolos se deben establecer para la generación, distribución y administración de llaves cuánticas?

Los artículos presentan distintos protocolos de QKD y analizan sus requisitos de aplicación y sus problemas de seguridad. (Singh et al., 2014) presenta un estudio comparativo de varios protocolos QKD, entre ellos BB84, SARG04 y E91. (G. Xu et al., 2015) proponen un novedoso protocolo QKD multi-partito que realiza la generación, distribución y copia de seguridad de claves en un único proceso, y que puede generalizarse a escenarios multi-gestor y multiusuario. (Kalra & Poonia, 2017) analiza el funcionamiento del protocolo B92 y propone un nuevo protocolo basado en él. (Bruß & Lütkenhaus, 2000) revisa los principales protocolos QKD y aborda la cuestión de la seguridad desde una perspectiva tanto teórica como práctica. En general, los artículos ofrecen distintos enfoques de los protocolos QKD y destacan la importancia de la seguridad en su aplicación.

9.2 ¿Cómo implementar QKD para garantizar la distribución segura de claves en SCF?

Los artículos sugieren que garantizar la integridad y autenticidad de las claves cuánticas para evitar ataques requiere una combinación de pruebas teóricas de seguridad y una

aplicación práctica que se ajuste a los modelos teóricos. (Goorden et al., 2014) proponen la autenticación cuántica segura (**QSA**) de una clave clásica de dispersión múltiple que es cuánticamente segura frente a la emulación digital. (Nitin Jain Birgit Stiller & Leuchs, 2016) analizan varios ataques a sistemas prácticos de QKD y sus mecanismos de prevención. (Dixon et al., 2017) informa sobre un sistema QKD diseñado para proporcionar seguridad tanto en la implementación teórica como física, que se instaló en un enlace de 45 km de una red metropolitana de telecomunicaciones durante un periodo de 2,5 meses y demostró seguridad frente a varios ciberataques. (Cerf et al., 2002) consideran dos esquemas criptográficos cuánticos que se basan en la codificación de la clave en qudits y deriva la información obtenida por un potencial espía que aplica un ataque individual basado en la clonación, junto con un límite superior en la tasa de error que garantiza la seguridad incondicional contra ataques coherentes.

X. Implementar QKD

10.1 ¿Cómo implementar QKD para garantizar la distribución segura de claves en SCF?

Los estudios muestran colectivamente que la QKD puede utilizarse para asegurar la distribución segura de claves en SCF. (Luo et al., 2023) proponen un esquema de consenso para establecer relaciones de confianza y transmitir claves en una perspectiva global de red QKD, que puede acomodar hasta la expresión: MIN(C-1,⌊(N-1)/3⌋), que se refiere a la determinación del número máximo de nodos no confiables en un sistema o red, dado un conjunto de condiciones. (Cao et al., 2017) discuten la integración de QKD con redes ópticas definidas por software (SDON) para asegurar la arquitectura SDON mediante la introducción de un novedoso esquema de clave por demanda (KoD). (Tomita, 2019) aborda el proceso de certificación de seguridad en la implementación de sistemas QKD, lo cual es indispensable para la implementación social de estos. (Mink et al., 2010) proponen cómo se podría integrar QKD en protocolos de seguridad comunes como IPsec y TLS, y sugiere una capa de soporte que proporciona un conjunto de servicios QKD comunes entre este protocolo y las aplicaciones de seguridad.

10.2 ¿Cómo diseñar e integrar QKD en la infraestructura de TO?

Los documentos sugieren colectivamente que QKD puede integrarse en las redes ópticas existentes, pero existen limitaciones y desafíos para su realización práctica. (Gatto et al., 2022) y (Lancho et al., 2010) analizan la necesidad de un canal físico dedicado para transportar las señales cuánticas débiles sin perturbaciones, pero también enfatizan la

importancia de integrar QKD con tecnologías de red convencionales. (Martelli et al., 2021) presentan una evaluación de una implementación de costo reducido del protocolo BB84 para QKD, mientras que (Zavitsanos et al., 2022) muestran un esquema práctico de multiplexación cuántica/clásica para la integración de QKD en un segmento de transporte óptico móvil de x-haul. En general, los artículos sugieren que QKD se puede integrar en redes ópticas utilizando varios enfoques, pero se necesita más investigación para abordar las limitaciones y desafíos de la implementación práctica.

XI. Desarrollar algoritmos cuánticos resistentes

11.1 ¿Cuáles son los algoritmos criptográficos resistentes a ataques cuánticos que existen?

Los estudios muestran colectivamente que existen algoritmos criptográficos que son resistentes a los ataques cuánticos. AES-256 es un ejemplo de tal algoritmo que puede resistir ataques cuánticos, como demostró (Kumar Rao et al., 2017). (Perlner & Cooper, 2009) proporciona una revisión de algoritmos criptográficos de clave pública que se cree que son resistentes a ataques basados en computación cuántica. (Fernandez-Carames & Fraga-Lamas, 2020) proponen la necesidad de criptografía blockchain post-cuántica y proporciona una revisión de criptosistemas post-cuánticos que se pueden aplicar a blockchains. (Mao et al., 2014) proponen un nuevo protocolo de intercambio de claves y un esquema de cifrado que es resistente a ataques cuánticos, basado en estructuras algebraicas no conmutativas. En general, los documentos sugieren que existen algoritmos criptográficos que pueden resistir ataques cuánticos y que los investigadores y desarrolladores deberían considerar estos algoritmos al diseñar sistemas seguros.

11.2 ¿Qué mecanismos de cifrado y autenticación pueden soportar la capacidad de cálculo cuántico?

Los documentos sugieren que la criptografía cuántica puede proporcionar una seguridad mejorada para los mecanismos de cifrado y autenticación. (Kumar et al., 2019) proponen un protocolo mejorado de distribución de claves cuánticas para autenticación de seguridad. (Kanamori et al., 2009) y (Kanamori, Seong-Moo Yoo, et al., 2005) proponen protocolos de autenticación que utilizan estados de superposición cuántica en lugar de partículas cuánticas entrelazadas. (Fehr & Salvail, 2017) proponen un esquema de cifrado teóricamente seguro para mensajes clásicos con textos cifrados cuánticos que ofrece detección de ataques de escucha y reutilización de la clave. Estos documentos sugieren colectivamente que la criptografía cuántica puede proporcionar una seguridad

mejorada para los mecanismos de cifrado y autenticación, y que los estados de superposición cuántica pueden ser utilizados para la autenticación.

XII. Identificar amenazas cuánticas

12.1 ¿Cómo reconocer nuevas amenazas cuánticas contra los algoritmos criptográficos actuales de los SCF?

Los estudios muestran colectivamente que el surgimiento de la computación cuántica representa una amenaza significativa para los algoritmos criptográficos actuales utilizados en SCF. (Ali, 2021) y (Käppler & Schneider, 2021) discuten la necesidad de la PQC para desarrollar sistemas criptográficos que sean resistentes a los ataques cuánticos. (Raheman, 2022) propone un enfoque de cifrado agnóstico llamado cómputo de cero vulnerabilidades (ZVC) que potencialmente puede hacer que las computadoras sean resistentes a la computación cuántica. (Yesina, Potii, et al., 2022) enfatiza la importancia de un soporte científico y metodológico estandarizado para la evaluación de riesgos en el período post-cuántico. Los documentos resaltan la urgencia de comprender los ataques cuánticos y sus implicaciones criptográficas para diseñar sistemas criptográficos resistentes a la computación cuántica.

12.2 ¿Cómo las amenazas pueden afectar los SCF en infraestructuras de TO?

Los documentos sugieren que los SCF en la infraestructura de tecnología operativa son vulnerables a varias amenazas de seguridad que pueden causar daño físico. (Taylor & Sharif, 2017) y (Zhang et al., 2013) identifican amenazas de seguridad para los SCF, incluidos los ataques a sensores y actuadores, la fuga de datos y estándares de seguridad inadecuados. (Huang et al., 2018) propone un método de evaluación de riesgos para cuantificar el impacto de los ciberataques en el sistema físico de los SCF, lo que puede ayudar a llevar a cabo medidas adecuadas de mitigación de ataques. (Karim & Phoha, 2014) destaca las posibles consecuencias de violaciones de seguridad en los SCF, que pueden afectar a un gran grupo de población, una agencia gubernamental importante o una entidad empresarial influyente. En general, los documentos sugieren que las amenazas a los SCF en la infraestructura de TO son una preocupación seria y requieren medidas de seguridad adecuadas para prevenir daños físicos.

Referencias

Abdi, F., Chen, C.-Y., Hasan, M., Liu, S., Mohan, S., & Caccamo, M. (2018). Guaranteed Physical Security with Restart-Based Design for Cyber-Physical Systems. 2018 ACM/IEEE 9th International Conference on Cyber-Physical Systems (ICCPS), 10–21. https://doi.org/10.1109/ICCPS.2018.00010

Abuarqoub, A. (2020). Security Challenges Posed by Quantum Computing on Emerging Technologies. The 4th International Conference on Future Networks and Distributed Systems (ICFNDS), 1–1. https://doi.org/10.1145/3440749.3442651

Aguado, A., Lopez, V., Martinez-Mateo, J., Peev, M., Lopez, D., & Martin, V. (2018). Virtual Network Function Deployment and Service Automation to Provide End-to-End Quantum Encryption. Journal of Optical Communications and Networking, 10(4), 421. https://doi.org/10.1364/JOCN.10.000421

Ahn, J., Chung, J., Kim, T., Ahn, B., & Choi, J. (2021). An Overview of Quantum Security for Distributed Energy Resources. 2021 IEEE 12th International Symposium on Power Electronics for Distributed Generation Systems (PEDG), 1–7. https://doi.org/10.1109/PEDG51384.2021.9494203

Albataineh, H., & Nijim, M. (2021). Enhancing the Cybersecurity Education Curricula Through Quantum Computation. In H. R. and D. L. and H. M.-S. and T. F. G. Daimi Kevin and Arabnia (Ed.), Advances in Security, Networks, and Internet of Things (pp. 223–231). Springer International Publishing. https://doi.org/10.1007/978-3-030-71017-0_16

Alcaraz, C. (2018). Cloud-Assisted Dynamic Resilience for Cyber-Physical Control Systems. IEEE Wireless Communications, 25(1), 76–82. https://doi.org/10.1109/MWC.2018.1700231

Alcaraz, C., & Zeadally, S. (2015). Critical infrastructure protection: Requirements and challenges for the 21st century. International Journal of Critical Infrastructure Protection, 8, 53–66. https://doi.org/10.1016/j.ijcip.2014.12.002

Ali, A. (2021). A Pragmatic Analysis of Pre- and Post-Quantum Cyber Security Scenarios. 2021 International Bhurban Conference on Applied Sciences and Technologies (IBCAST), 686–692. https://doi.org/10.1109/IBCAST51254.2021.9393278

Antoliš, K., Mišević, P., & Miličević, A. (2015). VULNERABILITIES OF NEW TECHNOLOGIES AND THE PROTECTION OF CNI. https://hrcak.srce.hr/file/206704

Bililign, S. (2013). The Need for Interdisciplinary Research and Education for Sustainable Human Development to Deal with Global Challenges. In International Journal of African Development (Vol. 1, Issue 1). http://scholarworks.wmich.edu/ijad

Bruß, D., & Lütkenhaus, N. (2000). Quantum Key Distribution: from Principles to Practicalities. Applicable Algebra in Engineering, Communication and Computing, 10(4), 383–399. https://doi.org/10.1007/s002000050137

Воропай, О. В., Погасій, С. С., Король, О. Г., & Мілевський, С. В. (2022). Development of security mechanisms for scada systems in the postquantium period. Системи Обробки Інформації, 2 (169), 25–34. https://doi.org/10.30748/soi.2022.169.03

Caicedo, D. S. (2017). Global critical infrastructure: Attacking the vulnerability of global cyber networks to create societal collapse. https://api.semanticscholar.org/CorpusID:55418315

Campbell, Sr., R. E. (2020). The Need for Cyber Resilient Enterprise Distributed Ledger Risk Management Framework. The Journal of The British Blockchain Association, 3(1), 1–9. https://doi.org/10.31585/jbba-3-1-(5)2020

Cao, Y., Zhao, Y., Colman-Meixner, C., Yu, X., & Zhang, J. (2017). Key on demand (KoD) for software-defined optical networks secured by quantum key distribution (QKD). Optics Express, 25(22), 26453. https://doi.org/10.1364/OE.25.026453

Carle, G., Debar, H., Dressler, F., & König, H. (2012). Network Attack Detection and Defense Early Warning Systems - Challenges and Perspectives (Dagstuhl Seminar 12061). Dagstuhl Reports, 2(2), 1–20. https://doi.org/10.4230/DagRep.2.2.1

Cerf, N. J., Bourennane, M., Karlsson, A., & Gisin, N. (2002). Security of Quantum Key Distribution Using d-Level Systems. Phys. Rev. Lett., 88(12), 127902. https://doi.org/10.1103/PhysRevLett.88.127902

Commission, E., Centre, J. R., Kopustinskas, V., Eid, M., Žutautaitė, I., & Simola, K. (2017). Critical infrastructures – Enhancing preparedness & resilience for the security of citizens and services supply continuity – Proceedings of the 52nd ESReDA seminar hosted by the Lithuanian Energy Institute & Vytautas Magnus University (V. Kopustinskas, M. Eid, I. Žutautaitė, & K. Simola, Eds.). Publications Office. https://doi.org/doi/10.2760/07157

Dixon, A. R., Dynes, J. F., Lucamarini, M., Fröhlich, B., Sharpe, A. W., Plews, A., Tam, W., Yuan, Z. L., Tanizawa, Y., Sato, H., Kawamura, S., Fujiwara, M., Sasaki, M., & Shields, A. J. (2017). Quantum key distribution with hacking countermeasures and long term field trial. Scientific Reports, 7(1), 1978. https://doi.org/10.1038/s41598-017-01884-0

Eng Vasile Florin POPESCU, L. (2019). THE CYBER SECURITY OF CRITICAL INFRASTRUCTURES IN AN INCREASINGLY CONNECTED WORLD. http://en.wikipedia.org/

Fehr, S., & Salvail, L. (2017). Quantum Authentication and Encryption with Key Recycling (pp. 311–338). https://doi.org/10.1007/978-3-319-56617-7_11

Fernandez-Carames, T. M., & Fraga-Lamas, P. (2020). Towards Post-Quantum Blockchain: A Review on Blockchain Cryptography Resistant to Quantum Computing Attacks. IEEE Access, 8, 21091–21116. https://doi.org/10.1109/ACCESS.2020.2968985

Flowers, A., Zeadally, S., & Murray, A. (2013). Cybersecurity and US Legislative Efforts to address Cybercrime. Journal of Homeland Security and Emergency Management, 10(1). https://doi.org/10.1515/jhsem-2012-0007

Gatto, A., Ferrari, M., Brunero, M., Gagliano, A., Tarable, A., Bodanapu, D., Giorgetti, A., Andriolli, N., Paganelli, R., Strambini, L., Martelli, P., & Martinelli, M. (2022). Integration of QKD Technologies in Advanced Optical Networks. 2022 IEEE 15th Workshop on Low Temperature Electronics (WOLTE), 1–4. https://doi.org/10.1109/WOLTE55422.2022.9882652

Goorden, S. A., Horstmann, M., Mosk, A. P., Škorić, B., & Pinkse, P. W. H. (2014). Quantum-secure authentication of a physical unclonable key. Optica, 1(6), 421–424. https://doi.org/10.1364/OPTICA.1.000421

Goy, M., Berlich, R., Kržič, A., Rieländer, D., Kopf, T., Sharma, S., & Steinlechner, F. O. (2021). High performance optical free-space links for quantum communications. In Z. Sodnik, B. Cugny, & N. Karafolas (Eds.), International Conference on Space Optics — ICSO 2020 (p. 18). SPIE. https://doi.org/10.1117/12.2599163

Hamza, A., Gharakheili, H. H., & Sivaraman, V. (2020). IoT Network Security: Requirements, Threats, and Countermeasures. http://arxiv.org/abs/2008.09339

Holley, K. A. (2009). Special Issue: Understanding Interdisciplinary Challenges and Opportunities in Higher Education. Ashe Higher Education Report, 35, 1–131. https://api.semanticscholar.org/CorpusID:146511487

Hossain Faruk, M. J., Tahora, S., Tasnim, M., Shahriar, H., & Sakib, N. (2022). A Review of Quantum Cybersecurity: Threats, Risks and Opportunities. 2022 1st International Conference on AI in Cybersecurity (ICAIC), 1–8. https://doi.org/10.1109/ICAIC53980.2022.9896970

Huang, K., Zhou, C., Tian, Y. C., Yang, S., & Qin, Y. (2018). Assessing the physical impact of cyberattacks on industrial cyber-physical systems. IEEE Transactions on Industrial Electronics, 65(10), 8153–8162. https://doi.org/10.1109/TIE.2018.2798605

Hughes, R. J., Nordholt, J. E., McCabe, K. P., Newell, R. T., Peterson, C. G., & Somma, R. D. (2013). Network-Centric Quantum Communications. Frontiers in Optics 2013, FW2C.1. https://doi.org/10.1364/FIO.2013.FW2C.1

Hui, P., Bruce, J., Fink, G., Gregory, M., Best, D., McGrath, L., & Endert, A. (2010). Towards efficient collaboration in cyber security. 2010 International Symposium on Collaborative Technologies and Systems, 489–498. https://doi.org/10.1109/CTS.2010.5478473

Kalra, M., & Poonia, R. C. (2017). Design a new protocol for quantum key distribution. Journal of Information and Optimization Sciences, 38(6), 1047–1054. https://doi.org/10.1080/02522667.2017.1374723

Kanamori, Y., Seong-Moo Yoo, Gregory, D. A., & Sheldon, F. T. (2005). On quantum authentication protocols. GLOBECOM '05. IEEE Global Telecommunications Conference, 2005., 3, 5 pp. https://doi.org/10.1109/GLOCOM.2005.1577930

Kanamori, Y., Yoo, S.-M., Gregory, D. A., & Sheldon, F. T. (2009). Authentication Protocol Using Quantum Superposition States. International Journal of Network Security, 9(2), 101–108. http://ijns.jalaxy.com.tw/contents/ijns-v9-n2/ijns-2009-v9-n2-p101-108.pdf

Käppler, S. A., & Schneider, B. (2021). Post-Quantum Cryptography: An Introductory Overview and Implementation Challenges of Quantum-Resistant Algorithms. 61–49. https://doi.org/10.29007/2tpw

Karim, M. E., & Phoha, V. V. (2014). Cyber-physical systems security. In Applied Cyber-Physical Systems (Vol. 9781461473367, pp. 75–83). Springer New York. https://doi.org/10.1007/978-1-4614-7336-7_7

Karol, M., & Życzkowski, M. (2015). Quantum technology in critical infrastructure protection. Safety and Security Engineering VI, 1, 109–119. https://doi.org/10.2495/SAFE150101

Khan, A. A., Ahmad, A., Waseem, M., Liang, P., Fahmideh, M., Mikkonen, T., & Abrahamsson, P. (2022). Software Architecture for Quantum Computing Systems - Asystematic Review. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.4040490

Khan, I. (2018a). Quantum Communication in Space – Challenges and Opportunities. Imaging and Applied Optics 2018 (3D, AO, AIO, COSI, DH, IS, LACSEA, LS&C, MATH, PcAOP), AM5A.2. https://doi.org/10.1364/AIO.2018.AM5A.2

Khan, I. (2018b). Quantum Communication in Space – Challenges and Opportunities. Imaging and Applied Optics 2018 (3D, AO, AIO, COSI, DH, IS, LACSEA, LS&C, MATH, PcAOP), AM5A.2. https://doi.org/10.1364/AIO.2018.AM5A.2

Kneller, V. Yu., & Fayans, A. M. (2019). Solving interdisciplinary tasks: the challenge and the ways to surmount it. Journal of Physics: Conference Series, 1379(1), 012011. https://doi.org/10.1088/1742-6596/1379/1/012011

Kumar, A., Dadheech, P., Singh, V., Raja, L., & Poonia, R. C. (2019). An enhanced quantum key distribution protocol for security authentication. Journal of Discrete Mathematical Sciences and Cryptography, 22(4), 499–507. https://doi.org/10.1080/09720529.2019.1637154

Kumar Rao, S., Mahto, D., Kumar Yadav, D., & Ali Khan, D. (2017). The AES-256 Cryptosystem Resists Quantum Attacks. International Journal of Advanced Research in Computer Science, 8(3), 404–408. https://doi.org/https://doi.org/10.26483/ijarcs.v8i3.3025

Lancho, D., Martinez, J., Elkouss, D., Soto, M., & Martin, V. (2010). QKD in Standard Optical Telecommunications Networks. In S. and V. P. Sergienko Alexander and Pascazio (Ed.), Quantum Communication and Quantum Networking (pp. 142–149). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-11731-2_18

Linke, N. M., Maslov, D., Roetteler, M., Debnath, S., Figgatt, C., Landsman, K. A., Wright, K., & Monroe, C. (2017). Experimental comparison of two quantum computing architectures. Proceedings of the National Academy of Sciences, 114(13), 3305–3310. https://doi.org/10.1073/pnas.1618020114

Luo, Y., Li, Q., & Mao, H.-K. (2023). How to Achieve End-to-end Key Distribution for QKD Networks in the Presence of Untrusted Nodes. https://doi.org/https://doi.org/10.48550/arXiv.2302.07688

M. Krelina. (2021). Quantum Warfare: Definitions, Overview and Challenges.

Majumder, S. R., Giani, A., Shen, W., Neculaes, B., Zhu, D., & Johri, S. (2023). Quantum computation: Efficient network partitioning for large scale critical infrastructures. http://arxiv.org/abs/2302.02074

Malina, L., Dobias, P., Hajny, J., & Choo, K.-K. R. (2023). On Deploying Quantum-Resistant Cybersecurity in Intelligent Infrastructures. Proceedings of the 18th International Conference on Availability, Reliability and Security, 1–10. https://doi.org/10.1145/3600160.3605038

Mao, S., Zhang, H., Wu, W., Liu, J., Li, S., & Wang, H. (2014). A resistant quantum key exchange protocol and its corresponding encryption scheme. China Communications, 11(9), 124–134. https://doi.org/10.1109/CC.2014.6969777

Martelli, P., Gatto, A., Brunero, M., Bodanapu, D., Rapisarda, M., Comi, P. M., & Martinelli, M. (2021). Integration of QKD in WDM networks. 2021 International Conference on Optical Network Design and Modeling (ONDM), 1–3. https://doi.org/10.23919/ONDM51796.2021.9492394

Mihalache, S. F., Pricop, E., & Fattahi, J. (2019). Resilience Enhancement of Cyber-Physical Systems: A Review. In S. and B. N. Mahdavi Tabatabaei Naser and Najafi Ravadanegh (Ed.), Power Systems Resilience: Modeling, Analysis and Practice (pp. 269–287). Springer International Publishing. https://doi.org/10.1007/978-3-319-94442-5_11

Mink, A., Frankel, S., & Perlner, R. (2010). Quantum Key Distribution (QKD) and Commodity Security Protocols: Introduction and Integration. http://arxiv.org/abs/1004.0605

Mistry, N. R., Dholakiya, A. Y., Prajapati, J. P., Mistry, N. R., Dholakiya, A. Y., & Prajapati, J. P. (2021). Security and Privacy Aspects Using Quantum Internet. In https://services.igi-global.com/resolvedoi/resolve.aspx?doi=10.4018/978-1-7998-6677-0.ch004 (pp. 62–81). IGI Global. https://doi.org/10.4018/978-1-7998-6677-0.ch004

Mosca, M. (2018). Cybersecurity in an Era with Quantum Computers: Will We Be Ready? IEEE Security & Privacy, 16(5), 38–41. https://doi.org/10.1109/MSP.2018.3761723

Nitin Jain Birgit Stiller, I. K. D. E. C. M., & Leuchs, G. (2016). Attacks on practical quantum key distribution systems (and how to prevent them). Contemporary Physics, 57(3), 366–387. https://doi.org/10.1080/00107514.2016.1148333

Olofinbiyi, S. A. (2022). A reassessment of public awareness and legislative framework on cybersecurity in South Africa. ScienceRise: Juridical Science, 2(20), 34–42. https://doi.org/10.15587/2523-4153.2022.259764

Pătraşcu, P. (2021). Emerging Technologies and National Security: The Impact of IoT in Critical Infrastructures Protection and Defence Sector. Land Forces Academy Review, 26(4), 423–429. https://doi.org/10.2478/raft-2021-0055

Paul, S., Scheible, P., & Wiemer, F. (2022). Towards post-quantum security for cyber-physical systems: Integrating PQC into industrial M2M communication1. Journal of Computer Security, 30(4), 623–653. https://doi.org/10.3233/JCS-210037

Pérez-Castillo, R., Serrano, M. A., & Piattini, M. (2021). Software modernization to embrace quantum technology. Advances in Engineering Software, 151, 102933. https://doi.org/10.1016/j.advengsoft.2020.102933

Perlner, R. A., & Cooper, D. A. (2009). Quantum resistant public key cryptography. Proceedings of the 8th Symposium on Identity and Trust on the Internet, 85–93. https://doi.org/10.1145/1527017.1527028

Pitwon, R. C. A., & Lee, B. H. L. (2021). Harmonising international standards to promote commercial adoption of quantum technologies. In K. Bongs, M. J. Padgett, A. Fedrizzi, & A. Politi (Eds.), Quantum Technology: Driving Commercialisation of an Enabling Science II (Vol. 11881, p. 16). SPIE. https://doi.org/10.1117/12.2602888

Ponnusamy, V., Regunathan, N. D., Kumar, P., Annur, R., & Rafique, K. (2020). A Review of Attacks and Countermeasures in Internet of Things and Cyber Physical Systems. In https://services.igi-global.com/resolvedoi/resolve.aspx?doi=10.4018/978-1-7998-2803-7.ch001 (pp. 1–24). IGI Global. https://doi.org/10.4018/978-1-7998-2803-7.ch001

Raheman, F. (2022). The Future of Cybersecurity in the Age of Quantum Computers. Future Internet, 14(11), 335. https://doi.org/10.3390/fi14110335

Rajamaki, J. (2018). Industry-university collaboration on IoT cyber security education: Academic course: "Resilience of Internet of Things and cyber-physical systems." 2018 IEEE Global Engineering Education Conference (EDUCON), 1969–1977. https://doi.org/10.1109/EDUCON.2018.8363477

Ramirez, R., & Choucri, N. (2016). Improving Interdisciplinary Communication With Standardized Cyber Security Terminology: A Literature Review. IEEE Access, 4, 2216–2243. https://doi.org/10.1109/ACCESS.2016.2544381

Ravi, P., Chattopadhyay, A., & Bhasin, S. (2022). Security and Quantum Computing: An Overview. 2022 IEEE 23rd Latin American Test Symposium (LATS), 1–6. https://doi.org/10.1109/LATS57337.2022.9936966

Rieffel, E. G., Venturelli, D., O'Gorman, B., Do, M. B., Prystay, E. M., & Smelyanskiy, V. N. (2015). A case study in programming a quantum annealer for hard operational planning problems. Quantum Information Processing, 14(1), 1–36. https://doi.org/10.1007/s11128-014-0892-x

Rodriguez, A. (2023). A quantum cybersecurity agenda for Europe Governing the transition to post-quantum cryptography. https://api.semanticscholar.org/CorpusID:260055338

Schwalb, M., & L, Y. J. (2007). EXPLOIT DERIVATIVES & NATIONAL SECURITY. http://www.gao.gov/new.items/d05231

Serrano, M. A., Cruz-Lemus, J. A., Perez-Castillo, R., & Piattini, M. (2023). Quantum Software Components and Platforms: Overview and Quality Assessment. ACM Computing Surveys, 55(8), 1–31. https://doi.org/10.1145/3548679

Shane, P. M. (2012). Texas Law Review See Also Response Cybersecurity: Toward a Meaningful Policy Framework. https://doi.org/https://doi.org/10.31228/osf.io/b8hms

Singh, H., Gupta, D. L., & Singh, A. K. (2014). Quantum Key Distribution Protocols: A Review. IOSR Journal of Computer Engineering, 16(2), 01–09. https://doi.org/10.9790/0661-162110109

Sperotto, A., Hofstede, R., Dainotti, A., Schmitt, C., & Rodosek, G. D. (2015). Special issue on measure, detect and mitigate–challenges and trends in network security. International Journal of Network Management, 25(5), 261–262. https://doi.org/10.1002/nem.1905

Ståhl, B. (2013). Monitoring Infrastructure Affordances [Blekinge Tekniska Högskola, Sektionen för datavetenskap och kommunikation, Karlskrona : Blekinge Institute of Technology]. http://urn.kb.se/resolve?urn=urn:nbn:se:bth-00544

Streich, G. (2023). (Re-)Configuring Federal Cybersecurity Regulation: From Critical Infrastructures to the Whole-of-the-Nation. Indiana Law Review, 55(4), 733–766. https://doi.org/10.18060/27133

Sturgeon, J. G. (2012). Taking a Quantum Leap in Cyber-Deterrence. https://api.semanticscholar.org/CorpusID:114567315

Taiber, J. (2020). Unsettled Topics Concerning the Impact of Quantum Technologies on Automotive Cybersecurity. https://doi.org/10.4271/EPR2020026

Taylor, J. M., & Sharif, H. R. (2017). Security challenges and methods for protecting critical infrastructure cyber-physical systems. 2017 International Conference on Selected Topics in Mobile and Wireless Networking (MoWNeT), 1–6. https://doi.org/10.1109/MoWNet.2017.8045959

Teodoraș, D.-A., Popovici, E.-C., Suciu, G., & Sachian, M.-A. (2023). Quantum technology's role in cybersecurity. In M. Vladescu, I. Cristea, & R. D. Tamas (Eds.), Advanced Topics in Optoelectronics, Microelectronics, and Nanotechnologies XI (Vol. 12493, p. 99). SPIE. https://doi.org/10.1117/12.2643300

Tomita, A. (2019). Implementation Security Certification of Decoy-BB84 Quantum Key Distribution Systems. Advanced Quantum Technologies, 2(5–6), 1900005. https://doi.org/10.1002/qute.201900005

Walenta, N., Soucarros, M., Stucki, D., Caselunghe, D., Domergue, M., Hagerman, M., Hart, R., Hayford, D., Houlmann, R., Legré, M., McCandlish, T., Page, J.-B., Tourville, M., & Wolterman, R. (2015). Practical aspects of security certification for commercial quantum technologies. In D. A. Huckridge, R. Ebert, M. T. Gruneisen, M. Dusek, & J. G. Rarity (Eds.), Electro-Optical and Infrared Systems:

Technology and Applications XII; and Quantum Information Science and Technology (Vol. 9648, p. 96480U). SPIE. https://doi.org/10.1117/12.2193776

Witteman, H. O., & Stahl, J. E. (2013). Facilitating interdisciplinary collaboration to tackle complex problems in health care: report from an exploratory workshop. Health Systems, 2(3), 162–170. https://doi.org/10.1057/hs.2013.3

Woo, H., Yi, J., Browne, J. C., Mok, A. K., Atkins, E., & Xie, F. (2008). Design and Development Methodology for Resilient Cyber-Physical Systems. 2008 The 28th International Conference on Distributed Computing Systems Workshops, 525–528. https://doi.org/10.1109/ICDCS.Workshops.2008.62

Xu, F., Ma, X., Zhang, Q., Lo, H.-K., & Pan, J.-W. (2020). Secure quantum key distribution with realistic devices. Reviews of Modern Physics, 92(2), 025002. https://doi.org/10.1103/RevModPhys.92.025002

Xu, G., Chen, X.-B., Dou, Z., Yang, Y.-X., & Li, Z. (2015). A novel protocol for multiparty quantum key management. Quantum Information Processing, 14(8), 2959–2980. https://doi.org/10.1007/s11128-015-1021-1

Yao, D. D., & Almohri, H. M. J. (2013). High assurance models for secure systems. https://api.semanticscholar.org/CorpusID:110786313

Yesina, M. V., Ostrianska, Ye. V., & Gorbenko, I. D. (2022). Status report on the third round of the NIST post-quantum cryptography standardization process. Radiotekhnika, 3(210), 75–86. https://doi.org/10.30837/rt.2022.3.210.05

Yesina, M. V., Potii, O. V., Gorbenko, Yu. I., & Ponomar, V. A. (2022). Risk estimation methodology in the post-quantum period. Radiotekhnika, 209, 7–15. https://doi.org/10.30837/rt.2022.2.209.01

Zavitsanos, D., Ntanos, A., Toumasis, P., Raptakis, A., Kouloumentas, C., Stathopoulos, T., Setaki, F., Theodoropoulou, E., Lyberopoulos, G., Giannoulis, G., & Avramopoulos, H. (2022). Coexistence Studies for DV-QKD Integration in Deployed RAN Infrastructure. 2022 International Workshop on Fiber Optics in Access Networks (FOAN), 6–9. https://doi.org/10.1109/FOAN56774.2022.9939691

Zhang, L., Wang, Q., & Tian, B. (2013). Security threats and measures for the cyber-physical systems. Journal of China Universities of Posts and Telecommunications, 20(SUPPL. 1), 25–29. https://doi.org/10.1016/S1005-8885(13)60254-X

Zobel, C. W., & Khansa, L. (2012). Quantifying Cyberinfrastructure Resilience against Multi-Event Attacks. Decision Sciences, 43(4), 687–710. https://doi.org/10.1111/j.1540-5915.2012.00364.x