ANSWER OF RQ4

Decrypt current encryption algorithms: Two studies mention that Critical Infrastructures (CI) face compromised cybersecurity in the quantum age due to the vulnerability of current encryption algorithms to quantum computers. These advanced machines can break traditional encryption methods, exposing sensitive data and communication. To mitigate these risks, a holistic approach encompassing quantum-resistant cryptography development, awareness campaigns, and infrastructure updates is essential to ensure the security and integrity of CPDs in CI. *Limited understanding of quantum threats*: Two studies mention that the unique and evolving nature of quantum-based attacks introduces challenges that demand specialized knowledge and expertise. This gap impedes the development of effective defenses and countermeasures against these emerging threats, leaving critical systems vulnerable to potential quantum attacks. *Adaptation of existing devices*: Two studies mention that compromised cybersecurity of CPDs in CI due to the vulnerability of current encryption algorithms to quantum attacks is further exacerbated by the challenge of retrofitting existing devices. Many of these devices lack built-in quantum-resistant security measures and retrofitting them with such measures proves complex and expensive, requiring significant updates to hardware, software, and communication protocols. *Supply chain security*: One study mention that in context of compromised cybersecurity for CPDs in the quantum age, supply chain security plays a crucial role. Ensuring the integrity and trustworthiness of components during the manufacturing and distribution of CPDs becomes increasingly important to prevent vulnerabilities from compromised or malicious components. *Quantum Resistant Authentication and Access Control*: Fourteen studies mention that the context of compromised cybersecurity for CPDs in the quantum age, the development of quantum-resistant authentication and access control mechanisms becomes essential. The advent of practical quantum computers threatens the encryption and authentication mechanisms used in CI, potentially leading to unauthorized access, data manipulation, and compromised communication between CPDs. *Transition to PQC algorithms*: Ten studies mention that in the face of the potential threat posed by quantum computing to traditional

encryption algorithms, critical infrastructures must navigate the transition to post-quantum cryptography (PQC) to safeguard the cybersecurity of CPDs. Quantum computers' ability to break existing encryption methods, such as RSA and ECC, demands the adoption of PQC algorithms that can withstand both classical and quantum attacks. However, this transition presents challenges, including compatibility concerns, limited awareness, and the need to address resource constraints, while ensuring the security and operational continuity of critical systems. *Extended lifespan and reliance on legacy technologies*: Five studies mention that cybersecurity of CI's CPDs is compromised in the quantum age due to the vulnerability of current cryptographic algorithms to quantum attacks. Quantum computers can break these algorithms, threatening data security and communication integrity. This is particularly concerning as critical infrastructures rely on legacy technologies, making the transition to quantum-resistant solutions complex and costly. The vulnerabilities introduced by quantum computing, combined with challenges in adopting PQC and addressing resource constraints, contribute to the compromised cybersecurity of these devices. *Limited awareness and preparation*: Three studies mention that compromised cybersecurity of CPDs in CI during the quantum age is due, in part, to limited awareness and preparation. The emerging threat of quantum computing is not fully understood by many organizations, leaving them vulnerable to potential breaches. This lack of awareness hinders the implementation of necessary quantum-resistant security measures, exacerbating the risks posed by quantum attacks. Additionally, the long lifespan of CI systems and their interconnected nature further contribute to the challenges of addressing this vulnerability. *Compatibility challenges*: Seven studies mention that during the quantum age, compatibility challenges contribute to compromised cybersecurity in CI. Older CPDs may struggle to integrate with new quantum-resistant encryption standards and hardware, relying on insecure protocols for compatibility. This vulnerability extends to command infrastructures, secondary channels, and even the exposure of previously protected details, posing risks to critical operations and overall cybersecurity. *Complexity and interconnectivity*: Two studies mention that complexity and interconnectivity of CI contribute to compromised cybersecurity in

the quantum age. These infrastructures consist of intricate, interconnected systems including SCADA networks, IoT devices, and communication protocols, making the integration of quantum-resistant security measures challenging. This complexity increases the risk of vulnerabilities and potential cyber-attacks, highlighting the necessity for proactive measures to ensure the resilience and security of critical systems. *Potential impact on critical operations*: Eight studies mention the potential impact of quantum computing on traditional encryption algorithms compromises the cybersecurity of CPDs in CI. Quantum computers can break widely used encryption methods like RSA and ECC, leaving sensitive data vulnerable to unauthorized access and manipulation. This vulnerability can lead to various security risks, including unauthorized control of critical infrastructure operations, potentially causing physical damage, economic losses, and public safety threats. The adoption of PQC is essential to address these vulnerabilities and ensure the security of critical infrastructures. Limited awareness and preparedness, along with the complexity of legacy systems, add to the challenges in securing CPDs in the quantum age. *Command Infrastructure Vulnerabilities*: One study mention that cybersecurity of CPDs in CI is compromised in the quantum age due to various command infrastructure vulnerabilities. These vulnerabilities include compatibility issues with older devices, reliance on quantum-insecure protocols for command systems, potential exposure of sensitive system details through quantum computing, and persistent vulnerabilities in secondary communication channels. These weaknesses leave critical infrastructures susceptible to cyberattacks, posing significant risks to their functionality and security. *Secondary channel vulnerabilities*: Two studies mention in the context of CI and the quantum age, secondary channel vulnerabilities refer to potential weaknesses in alternative communication channels or mechanisms beyond primary ones. These vulnerabilities could persist even after upgrading primary command channels to quantum-secure cryptography. Infrequently used systems like SCADA may remain susceptible, posing risks to the functioning and security of CPDs in CI. *Exposure of previously protected details*: One study mention that pertains to the potential revelation of confidential information about critical systems due to quantum computing. This includes system locations, operations,

vulnerabilities, and other sensitive characteristics. Adversaries can exploit this information to launch non-cryptographic attacks, leading to heightened risks for the functioning and security of CPDs within CI in the quantum age. *Improper key distribution*: Two studies mention improper key distribution in CI during the quantum age poses a cybersecurity threat due to quantum computers' potential to compromise key distribution protocols like Diffie-Hellman. This vulnerability could compromise the confidentiality and integrity of cryptographic keys used in CPDs, adding to the challenges posed by quantum computing's impact on encryption methods and security measures in critical systems. *Limited implementation of PQC*: Two studies mention while the transition to post-quantum security measures is crucial to counter quantum threats, the integration of these measures can be intricate and time-consuming. This inadequacy could leave critical systems vulnerable to quantum-based attacks, highlighting the need for comprehensive efforts to ensure the resilience of CPDs in CI. Similarly, the lack of standardized and widely adopted PQC solutions adds complexity to addressing the vulnerabilities posed by quantum computing. *Exploitation of quantum side channel attacks*: Two studies mention the susceptibility of quantum technologies, like QKD, to exploitation through side-channel attacks poses a cybersecurity risk for CI. These attacks take advantage of the physical properties of quantum hardware to extract sensitive information, potentially compromising the security of CPDs that rely on quantum technologies. This vulnerability underscores the need for comprehensive security measures to mitigate potential side-channel threats in the quantum age. *Greater connectivity and interconnection of CPS with the Internet*: One study mention increased connectivity and interconnection of CPS with the internet and other networks have exposed CI to new threats, making them susceptible to cyber-attacks exploiting vulnerabilities in open protocols. Additionally, the reliance on outdated and unsupported systems within CI, combined with the emergence of quantum computing, poses a significant cybersecurity risk. This combination of factors compromises the cybersecurity of CPDs in CI in the quantum age, necessitating comprehensive security measures to address these vulnerabilities. *Security approach by obscurity*: One study mentions the reliance on a security-by-obscurity approach, characterized by proprietary or

poorly documented technologies, within the design of SCADA systems has left CI vulnerable to cyber threats. This outdated security approach, combined with the increased connectivity of CPS to the internet and the potential threat of quantum computing, compromises the cybersecurity of CPDs in CI in the quantum age. *Time sensitive operations*: Five studies mention time-sensitive operations of CI pose a challenge to cybersecurity in the quantum age. The increased computational overhead introduced by implementing complex PQC algorithms can impact the efficiency and timeliness of operations. This additional burden on CPDs may affect their real-time responsiveness and compromise the overall functioning of critical systems.