Suitability of Quantum Cryptography for National Facilities

Abdul Mirza, Makhamisa Senekane, Francesco Petruccione
Centre for Quantum Technology
University of KwaZulu-Natal
Durban, South Africa
mirzaa@ukzn.ac.za

Brett van Niekerk
School of Management, IT and Governance
University of KwaZulu-Natal
Durban, South Africa
vanniekerkb@ukzn.ac.za

***Abstract*—Quantum cryptography, or more accurately Quantum Key Distribution (QKD), provides a secure mechanism to exchange encryption keys which can detect potential eavesdroppers. However, this is a relatively new technology in terms of implementation, and there are some concerns over possible attacks. This paper describes QKD and provides an overview of the implementations in South Africa. From this, a basic vulnerability assessment is performed to determine the suitability of QKD for use in critical national facilities. While there are vulnerabilities, some of these can be easily mitigated through proper design and planning. The implementation of QKD as an additional layer to the encryption process may serve to improve the security between national key points.**

Keywords-critical infrastructure protection, quantum cryptography, quantum key distribution, vulnerability assessment

I. INTRODUCTION

In 2014 a number of security incidents illustrated that digital communication is not as secure as previously thought: in April the Heartbleed bug which resulted in vulnerabilities on the standard encryption used by many prominent websites was announced [1], and a report indicating vulnerabilities in satellites to hacking was released [2]. Consequently there is a need for additional security for sensitive transmissions over public networks.

Quantum Key Distribution (QKD), more commonly known as quantum cryptography, provides a provably secure means to key exchange between two remote parties. Furthermore, due to exploitation of the laws of physics, these type of key exchange schemes cannot be intercepted without notifying the legitimate parties. While laboratory based implementations were first introduced three decades ago, the recent past has seen the focus shift towards the practical application of this technology in existing network deployments. The American [3] and European [4] efforts lead such research. Recently, it has been reported that China is set to implement the longest quantum communication network that would see QKD being implemented for communication links of up to 2000 kilometers [5]. This underlines the fact that the prospects for QKD are very good.

Two networks have been deployed in South Africa: a permanent connection amongst a number of municipal buildings in Durban, and a temporary connection between the Moses Mabhida stadium and the Disaster Management Centre during the 2010 FIFA World Cup [6].

Whilst QKD is a relatively new technology this does not preclude it from being implemented for protecting the communications of national key points. A strong security culture does not necessarily avoid all risk; the ideal culture rather integrates incorporates creativity and an acceptance of new technologies whilst maintaining risk awareness [7].

This paper performs a vulnerability assessment based on experience with the implemented networks to assess the suitability for protecting communications between national key points. Section II provides the background to QKD, critical infrastructure protection and the vulnerability assessment framework used in the paper. Section III contains the vulnerability assessment, and Section IV discusses the suitability of QKD for national key points with regards to the vulnerability assessment. Section V concludes the paper.

II. BACKGROUND

Section A presents the background to quantum key distribution and Section B provides an overview of the implementation of QKD in South Africa. Section C describes critical infrastructure protection and Section D presents the vulnerability assessment framework used in this paper.

A. Quantum Key Distribution

The fundamental shift from conventional cryptography to quantum-based information security is the move from mathematical encapsulation to physical encoding. This methodology ensures physical protection of the key bits and active detection of a breach. Only the laws of physics, and not computational limitations, bind the security proofs of quantum cryptography. This means that in all proofs the eavesdropper is assigned the upper bound of mutual information in information theoretic terms. Such proofs make QKD secure independent of any future computational advancements [8].

S Wiesner developed the idea of quantum-based security in 1970 as a means to prevent the forgery of banknotes [9. The method incorporated a series of quantum systems into the banknotes to verify the serial numbers. The non-orthogonal bases that encoded the quantum verification code ensured that an adversary was unable to reconstruct the code with certainty. CH Bennett and G Brassard expanded the concept in 1984 as a means of symmetric key exchange [5]. Bennett and Brassard showed that QKD was an effective scheme to share symmetric keys and that it was theoretically secure [5]. This form of security analysis sets the theoretical bounds on the mutual information between Alice and Eve independent of the implementation of the protocol. The protocols are underpinned by the fundamental concepts of quantum mechanics. Since the data carriers are quantum systems, only the laws of physics bind the manipulation of the information. This ensures that the data may be secured through physical interactions. In particular the Heisenberg's Uncertainty relations denies any observer of the system to measure it without altering the state of the quantum system. This concept is further entrenched through the duality principle and the no-cloning theorem [8].

Both Alice and Bob are connected to a quantum and classical channel. All authentication, post-distribution processes and encrypted communication is executed over the classical channel while the raw key distribution process is conducted over a quantum channel. After authentication, Alice begins transmission of a randomly generated stream of qubits to Bob over the quantum channel. Thereafter, the qubits undergo a post-distribution process to form a secure key. If both parties accept the security level of the key, information is encrypted via the One Time Pad scheme and sent over the classical channel. Due to the quantum nature of the particles used in the key distribution process, an eavesdropper would cause discrepancies in the key and hence be detected. The eavesdropper will have access to the ciphertext, but this will be useless as explained earlier. It should be noted that at no point is the data intended for secure communication compromised as infiltration is detected in the key distribution phase.

The key exchange in QKD through the qubits is equivalent to the asymmetric encryption in Pretty Good Privacy to securely exchange symmetric keys, with the ability to detect if an eavesdropper has attempted to access the key. The exchanged key is used to create an encrypted tunnel, similar to that of a virtual private network.

B. Implementation of QKD in South Africa

Two major projects were implemented as part of the quantum networking aspect of QKD. The QuantumCity project was developed, in partnership with the eThekwini Municipality, to showcase the feasibility of quantum cryptography in a commercial environment for extended periods of time and the development of a test-bed quantum network for future experimentation. The initiative saw the deployment of a four-node quantum-secured communication network linking strategic buildings within the eThekwini Municipality. The network is deployed in the suburbs of Westville and Pinetown. It runs through the fibre infrastructure of the eThekwini Municipality. The initiative was first installed in 2008 and has been running since then. The initiative intends to expand its coverage, converting Durban from a Smart City to the first Quantum City in Africa.

The QuantumStadium project followed from the QuantumCity initiative, the City of Durban and the CQT again partnered together to provide unprecedented communication security to Durban's 2010 FIFA World Cup operations. The CQT secured the communication link between the Venue Operations Centre at the Moses Mabhida Stadium in Durban with the off- site Join Operations Centre for the eThekwini Municipality that housed the South African Police Force, Emergency Services and National Intelligence. The secure communication link was launched by the Minister of Science and Technology and ran for the duration of the 2010 FIFA World Cup. Both the aforementioned projects encrypted all data, including telephone, internet, video, data and e-mail, through a quantum-secured link. The analysis in Section III is based on these two deployments.

C. Critical Infrastructure Protection

Critical infrastructures are those "systems and assets whose incapacity or destruction will have a debilitating impact on the national security, and the economic and social well-being of a nation" [10]. This concept has been expanded by the US Department of Homeland Security to critical infrastructure and key resources [11, 12]. Under this definition, the concept of national key points is covered. Communications between such key points can be of a sensitive and time-critical nature, and therefore require high availability, integrity and confidentiality of the communication. The remainder of the section presents an overview of risk and vulnerability assessments used for critical infrastructure, and the Minimum Essential Information Infrastructure framework.

1) Risk and Vulnerability Assessment for Critical Infrastructure

The risk assessment for infrastructures can be done using Strength-Weakness-Opportunity-Threat (SWOT) and Political, Economic, Social, Technical, Environmental, Legal (PESTEL) analyses [13]. Another assessment framework, Factor Analysis of Information Risk (FAIR) uses a series of risk matrices to rate the vulnerabilities and risks associated with an asset [14]. For the purposes of this paper the focus will be on the vulnerability, which is a function of the control strength and the threat capability [14]. The Minimum Essential Information Infrastructure (MEII) framework provides a number of considerations that can be used in vulnerability and risk analysis. These are discussed the next section.

2) Minimum Essential Information Infrastructure

The MEII framework was evolved from a U.S. cold war system ensuring communication to nuclear forces and adapted for the specific case of defending against cyber-attacks [15]. The framework is dated; however it provides a number of considerations for assessing vulnerabilities in networks and networked systems. The relevant considerations are described below:

- *Singularity and centralisation*: A choke point or single point of failure in a system which may become an attraction for attackers [15].
- *Uniqueness and homogeneity:* Homogenous systems may result in the replication of flaws or vulnerabilities throughout the entire system or network or systems, however unique systems may have undiscovered flaws, or may be difficult to replace [15].
- *Behavioural complexity*: Predictable systems enable attackers to predict the outcome or impact of their attack. Systems which are sensitive to unexpected or abnormal usage or states could be easily exploited [15].
- *Adaptability*: Systems that are not easily changed may be unable to adapt to mitigate or recover from an attack; however systems that easily malleable or 'gullible' could prove easy to exploit [15].
- *Configuration and operation*: systems that are difficult to manage or monitor may have difficulty in recovering from an attack, and incorrect configuration may make them susceptible to attacks. Systems that are operating close to their capacity could be overloaded through denial of service attacks [15].
- *Exposure*: It will be easy to reconnoitre and attack systems that are easily accessible through physical, electromagnetic and network exposure [15].
- *Dependency*: an infrastructure or system that is dependent on other infrastructure sectors may be indirectly attacked or become unreliable due to fluctuations in the supporting infrastructure [15].

These aspects still hold true. For example, [7] indicates that commonality in infrastructure and equipment and particularly desktop computers aids the transmission of malware. However, when there is a mixture of operating systems, the malware may not infect all the computers. The crash of the Blackberry messaging services illustrates the sensitivity, capacity and singularity issues in that the failure of the central servers resulted in widespread outages, and the backlog of messages created additional problems [16].

D. Vulnerability Assessment Framework

The vulnerability assessment framework was proposed in [18, 19] to be conducted for a network; the previous implementations were for a mobile network in [17] and a cloud computing network in [18]. The framework uses a modified SWOT and PESTEL analyses at a high level, where strengths are analogous to controls and weaknesses are analogous to vulnerabilities. Economic and technical aspects are the core focus, with political, economic and social factors being a secondary focus. The framework was intended for use where the potential attackers were determined to penetrate or disrupt the infrastructure, as opposed to opportunistic hackers. The output of the framework can therefore be seen as a 'worst case' scenario. To determine the vulnerability rating for each threat, a traditional vulnerability matrix is used, where the vulnerability rating is a function of the control strength and the required capability to exploit the vulnerability, as illustrated in Table I.

TABLE I. VULNERABILITY ASSESSMENT MATRIX [18]

Control Strength	**Required Threat Capability to Exploit Vulnerability**				
	Very low	***Low***	***Medium***	***High***	***Very high***
Very low	Very High	Very High	High	Med	Med
Low	Very High	High	High	Med	Low
Medium	High	High	Med	Low	Low
High	High	Med	Low	Low	Very Low
Very high	Med	Med	Low	Very Low	Very Low

Using the vulnerability matrix, vulnerability ratings for each threat category can be determined. The ratings in the matrix can be represented quantitatively as one being very low to five being very high. In order to calculate the vulnerability rating for an infrastructure or the individual quantitative vulnerability ratings for each threat category are assumed to form a vector. The infrastructure or network vulnerability rating is obtained by calculating the magnitude of the vector. This is shown in Equation 1 [17], where V_I is the infrastructure vulnerability rating, **V** is the vector of the vulnerabilities for all threats, and v_n is the *n*th vulnerability rating in the vector. The reason a vector magnitude is used is that as the number of vulnerabilities or the seriousness of a vulnerability increases, the overall vulnerability of the infrastructure can be considered to increase. Likewise, as the number of vector elements increases so does its magnitude. This method provides a single figure for the infrastructure vulnerability, and thus allows for comparing the infrastructure vulnerability rating as the vulnerability profile changes over time [17].

$$V_I = \|\mathbf{V}\| = \sqrt[2]{\sum_{n=0}^{N} v_n^2} \quad \textbf{(1)}$$

For the purposes of this paper the potential impact of a successful attack in a specific threat category will also be considered to further illustrate the severity of the vulnerability. Through the same process as described in this section, the risk can be calculated as a function of the impact and likelihood of an incident occurring.

III. VULNERABILITY AND RISK ASSESSMENT OF QKD

The vulnerability and risk assessments are presented in this section. The individual vulnerabilities for various threats are determined in Section A; Section B provides the overall vulnerability rating for the infrastructure. It is noted that the assessment was conducted on a particular implementation of a quantum network, as described in Section II B. Section III B will elaborate on the major vulnerabilities of this network and possible actions that may minimize the risk through efficient management and planning.

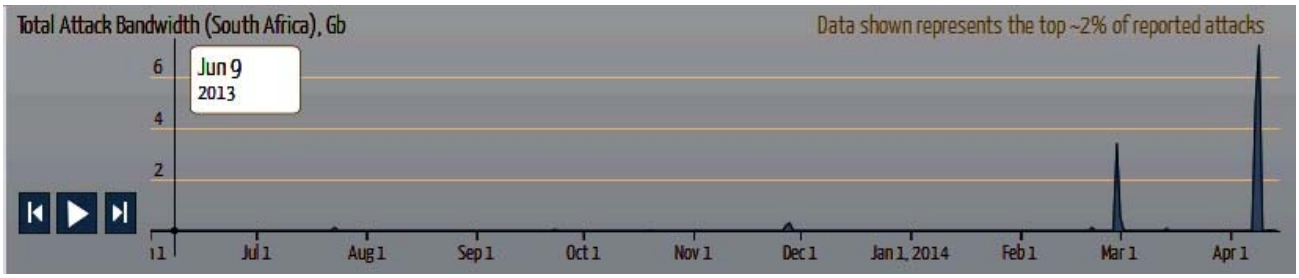

Figure 1. DDoS attacks against South Africa [19]

A. Individual Vulnerabilities toThreats and the Associated Risk

The assessment of individual vulnerability and risk elements are presented in this section based on experience with the implemented QKD networks. The current implementation in Durban is a star topology. This has an obvious central point which may be easy for an attacker to overcome by focusing on the central site; the required capability is therefore rated as low. As little can be done to correct this other than changing the topology, the control strength is weak, resulting in high vulnerability. The likelihood and impact are rated as medium as central points tend to be the focus of attacks on networks, and the result could noticeably degrade performance; this results in a risk rating of medium. However, through design considerations, these central points of failure can be reduced by employing a more resilient topology; this will be discussed in more detail later.

As with many IT technologies, QKD is dependent on electricity. The detectors draw most current for cooling. But as the technology advances, the detectors would require less power, such a technology would make it possible to have detectors with a very high detection efficiency at room temperature; eliminating the need for cooling. Also, since QKD is dependent on power, very little skill is required to disrupt power supply as physical damage to a substation will have this affect. The implemented controls are very weak; at best the UPS has a few minutes of backup power. This results in a very high vulnerability. However, the impact specific to QKD is low, as all IT equipment will experience the same conditions. In South Africa, the likelihood of power outages is high, resulting in an overall medium risk rating. Additional measures, such as improved UPS backup and Green IT technologies may assist in reducing the vulnerability and risk; these will be discussed later.

The dependence on other networks is limited to the actual transferring of information; should the network or service provider fail, no information could be transferred regardless of the presence of QKD. The threat capability is rated as medium, as this would require the skills to significantly impact the network performance of a large service provider; the control strength is rated as high as the contract with the service provider should specify allowable downtime and repair time. This results in a low vulnerability rating. The impact and likelihood are low, resulting in a low risk, particularly as this impact is not specific to QKD. To further illustrate this Figure 1 provides a screenshot of the DDoS attack data against South Africa. As is evident, there are very few attacks and the impact has not been severe enough for it to be noticeable by the popular news media.

As with many information technologies, QKD components require cooling to dissipate the heat generated from the equipment. Overheating of the components may reduce performance. The breach of Target's network appeared to be due to an external heating, ventilation and air conditioning (HVAC) contractor [20]; this indicates that HVAC systems connected to the network could potentially be targeted, and ultimately affect the QKD infrastructure. Therefore this is an indirect attack vector which does not necessarily require great capability to achieve. However, the control strength should be relatively high as the HVAC is protected by perimeter security. This results in a medium vulnerability. There are many scenarios where the cooling may need to be shut off, including maintenance, in addition to the potential for attacks, however the impact is not significant other than degrading performance, and is therefore rated as medium. The risk is therefore calculated to be high.

Eavesdropping on the quantum network is very unlikely because its (QKD's) security is guaranteed by Heisenberg's uncertainty principle [21], which makes it impossible for an eavesdropper to measure with certainty an unknown quantum state. Thus, the threat capability is then rated as low. It is also the case with the threat due to injection attacks. Its threat is rated low because no-cloning theorem [22] and a decoy-state QKD protocol [23] would make it impossible for an eavesdropper to successfully inject the attacks on the communication link. The threat of electromagnetic interference is rated medium because QKD uses optical communication, which can be susceptible to electromagnetic interference. Finally, since, as already mentioned, the QKD technology is dependent on electricity, the risk posed by this is rated medium.

As QKD is an emerging technology, there is a degree of dependency on the experts who have developed and implemented such networks. However, the required access to the experts can be strongly controlled through contracts. The vulnerability is therefore calculated as low. However, as the experts are not abundant, there may be some delays in receiving aid from them with some impact; both can be rated as medium, resulting in a medium risk. A summary of the individual ratings in this discussion are presented in Table II.

TABLE II. VULNERABILITY AND RISK RATINGS

Threat	Required threat capability	Control strength	Vulnerability	Likelihood	Impact	Risk
Eavesdropping	High	Stong	Low (2)	Very low	Low	Very low (1)
Cable break	Medium	Weak	High (4)	Very low	High	Low (2)
Injection attack on cables	Medium	Strong	Low (2)	Very low	High	Low (2)
Capacity	Very Low	Medium	High (4)	High	High	High (4)
Central points of failure	Low	Weak	High (4)	Medium	Medium	Medium (3)
Physical damage to components	Very low	Strong	High (4)	Low	High	Medium (3)
Electromagnetic interference	Medium	Medium	Medium (3)	Very low	High	Low (2)
Electricity dependancy	Low	Very weak	Very High (5)	High	Low	Medium (3)
Cooling dependency	Low	Strong	Medium (3)	High	Medium	High (4)
Other network dependencies	Medium	Strong	Low (2)	Very low	Very low	Very low (1)
Component availability	Low	Weak	High (4)	Low	Low	Low (2)
Expertise dependency	Medium	Strong	Low (2)	Medium	Medium	Medium (3)

B. Infrastructure Vulnerability and Risk Rating

From the individual ratings provided above and summarized in Table II, the overall vulnerability and risk for the system can be calculate using the vector magnitude.

The infrastructure vulnerability rating is calculated to be 11.79, and the infrastructure risk rating is calculated to be 9.27. The maximum possible rating (where all vulnerabilities are rated as ‘very high’) is 17.32; if all the ratings were ‘high’ then the overall rating would be 13.86 and if all were medium the overall rating would be 10.39. Therefore the vulnerability can be considered medium to high, and the risk as approaching medium.

Through proper management and planning, such as keeping sufficient spares and having proper contracts with experienced persons and additional service providers, a high level of availability can be assured. This will therefore reduce the vulnerability and risk of the QKD network. By designing the network with a more resilient topography (e.g. ring or mesh), the vulnerability to central points of failure is reduced to low, and by forward planning and keeping more spares in stock, the vulnerability to lack of components can be rated as medium. By utilizing additional UPS backup, generators, and Green IT technologies, such as solar and wind turbines, the IT infrastructure may be supported for a longer period. This will improve the control strength to weak, resulting in a high vulnerability.

From these alterations, the overall vulnerability is then reduced to 10.54. Similarly, the change in the central point of failure can be rated as low for risk, reducing the overall risk to 9. The implications of these ratings with regards to the suitability for strategic national facilities are discussed in the following section.

IV. SUITABILITY OF QKD

As many of the components are rack-mounted, they are co-located with traditional IT infrastructure, and will therefore be protected by the same physical means. For more critical applications, more spares can be kept on hand to replace failing or damaged equipment. The repair of such equipment, however, will incur a longer lead time due to the limited expertise in South Africa.

The network topography may also provide redundancy: a star topography, as implemented, is susceptible to issues regarding a central point of failure. Using a ring of partial mesh topographies will increase the resilience of the network, but will also be more expensive.

Further measures, such as redundancy of cables, specialized shielding, additional physical security, and improved UPS backup, and fail-safes for QKD infrastructures outages (for example, ensuring standard key-exchange protocols resume), will help reduce the vulnerability and risk of deploying such a technology.

Much research has been conducted around the development of an intelligent Key Management Network layer [M]. The intention of such a network layer is to route and manage the various stacks of keys produced by the QKD nodes. This layer is positioned between the network and data link layers.

Whilst QKD is a new technology this does not preclude it from being implemented for protecting the communications of national key points. A strong security culture does not necessarily avoid all risk; the ideal culture rather integrates incorporates creativity and an acceptance of new technologies whilst maintaining risk awareness [7].

The shift in security from mathematical assumptions to the laws of physics is the fundamental benefit provided by quantum key distribution. While the implementation available today increases the required capability of an adversary, the

theoretical concepts are future-proof and technology independent. Furthermore, QKD is theory independent as well. This means that no matter what future technology of theoretical developments occur, the process, and all that has been secured through it, will remain secure.

The QKD process ensures that there is no compromise to the classified information since the key is the only exchanged information prior to a security check. If the key is found to lack a minimum level of secrecy the QKD process is aborted and restarted. Only upon a successful key exchange is the sensitive information exchanged. Quantum hacking is a recent phenomenon that requires highly specialized skills. This allows the adversaries to exploit technological limitations in the systems to determine the state of the qubit. These, however, are technological and if managed correctly, can minimize any such exposure. However, QKD only protects the communication channel. It does not protect the endpoints, therefore it is still possible to breach sensitive information through other networks, such as the HVAC network or due in improperly configured security components on the network.

The QKD solution is infrastructure intensive. The need for dedicated lines and low speeds are the foremost bottlenecks in this regard. This will improve as the technology matures. The vulnerabilities discussed above can be mitigated through proper design and planning, therefore there is a low risk in using QKD from a technical vulnerability perspective.

V. Future Work in QKD

The spatial limitation of QKD is intrinsic to the quantum data carrier. In order to circumvent this limitation larger quantum networks are designed with trusted nodes. A point-to-point configuration is implemented between each node and the key is exchanged via a hop-by-hop procedure across the nodes. The nodes may further sketch a backbone for a secure network with a dedicated key management layer. Of particular interest is the growing research into satellite-based QKD systems in order to develop a Quantum Global Area Network. The system uses LEO satellites as secure nodes. Various feasibility assessments have been demonstrated for such a implementation [24, 25]. The networks use both ground-satellite and inter-satellite QKD links to span across the Earth. While the feasibility of such a network has returned with positive results, there are various technical aspects of the implementation that require adaptation before this solution may be realized.

Another cryptographic scheme that might be worth exploring for suitability to national facilities is quantum secret sharing (QSS). QSS is a quantum version of secret sharing schemes, which were introduced by Blakley [26] and Shamir [27] in the 1970's. Secret sharing is a method by which one party splits the message into different parts and distributes the shares among different parties in such a way that only authorized subsets of the party can reconstruct the original message. The quantum version of secret sharing combines the quantum key distribution with the secret sharing to ensure that the presence of an eavesdropper is revealed [28].

VI. Conclusion

Quantum key distribution is an emerging technology which distributes encryption keys and provides an in-built mechanism for detecting if the key has been compromised. The paper described deployments of QKD in South Africa, and provided a vulnerability and risk assessment of these deployments. Based on these assessments and the following discussion, it is evident that QKD is suitable for providing additional communication security to national facilities. There are some aspects of concern, however proper planning and management can easily overcome a number of these. Another disadvantage is the possible cost implications, however the benefits of improving the confidentiality of communications for sensitive facilities is paramount.

Acknowledgment

This work is based upon the research supported by the South African Research Chair Initiative of the Department of Science and Technology and the National Research Foundation.

References

[1] Ashford, W. EFF calls for rapid mitigation of Heartbleed Internet bug, Computer Weekly, 9 April 2014. Retrieved 9 April 2014 from http://www.computerweekly.com/news/2240217841/EFF-calls-for-rapid-mitigation-of-Heartbleed-internet-bug

[2] Higgins, K.J. Satellite communications wide open to hackers, Dark Reading, 17 April 2014. Retrieved 22 April 2014 from http://www.darkreading.com/vulnerabilities---threats/satellite-communications-wide-open-to-hackers/d/d-id/1204539

[3] Elliott, C., et al., *Current status of the DARPA quantum network* in *Quantum Information and Computation III*, E. Donkor, A. Pirich, and H. Brandt, Editors. 2005, SPIE. p. 138-149.

[4] Peev, M., et al., *The SECOQC quantum key distribution network in Vienna.* New Journal of Physics, 2009. **11(7),** 075001

[5] Qiu, J., Quantum communications leap out of the lab. Nature, 2014. **508**. p. 441-442.

[6] Mirza, A. and F. Petruccione, *Realizing long-term quantum cryptography.* JOSA B, 2010. **27(6):** p. A185-A188.

[7] Amoroso, E.G. Cyber attacks: protecting national infrastructure. Student edition. Waltham, MA: Butterworth-Heinemann, 2013.

[8] Renner, R., *Security of quantum key distribution.* International Journal of Quantum Information, 2008. **6(01):** p. 1-127.

[9] Wiesner, S. Conjugate coding. ACM SIGACT News, 15(1), p. 78-88, 1983.

[10] Dunn, M., and Wigert, I. International CIIP Handbook 2004. Zurich: Swiss Federal Institute of Technology, 2004.

[11] Department of Homeland Security. Critical Infrastructure and Key Resources, 5 April, 2010. Retrieved 25 May 2010, from: http://www.dhs.gov/files/programs/gc_1189168948944.shtm

[12] Department of Homeland Security. A Guide to Critical Infrastructure and Key Resources Protection at the State, Regional, Local, Tribal, and Territorial Level, September 2008. Retrieved 6 March 2014 from http://www.dhs.gov/xlibrary/assets/nipp_srtltt_guide.pdf

[13] Habegger, B (ed.) International Handbook on Risk Analysis and Management. Zurich: Swiss Federal Institute of Technology, 2008.

[14] Jones, J. A. An Introduction to Factor Analysis of Information Risk (FAIR), Risk Management Insight, 2005. Retrieved 25 November 2010 from: http://www.riskmanagementinsight.com/media/documents/FAIR_Introduction.pdf.

[15] Anderson, R. H., Feldman, P. M., Gerwehr, S., Houghton, B., Mesic, R., Pinder, J., et al. Securing the US Defense Information Infrastructure: A Proposed Approach., Santa Monica: RAND Institute, 1999.

[16] Press Association. 'BlackBerry users vent frustrations on third day of service disruption,' The Guardian, 12 October 2011. Retrieved 13 October 2011 from: http://www.guardian.co.uk/technology/2011/oct/12/blackberry-service-disruption-third-day

[17] van Niekerk, B., Vulnerability Assessment of Modern ICT Infrastructure From an Information Warfare Perspective, PhD Thesis, Westville, South Africa: University of KwaZulu-Natal, 2012.

[18] van Niekerk, B., and Maharaj, M. 'Infrastructure Vulnerability Analysis from an Information Warfare Perspective,' South Africa Computer Lecturer's Association Conference (SACLA 2011), Ballito, 6-8 July, 2011, pp. 76-85.

[19] Arbour Networks and Google. Digital attack map, 2014. Retrieved 14 April 2014 from http://www.digitalattackmap.com/#anim=1&color=0&country=ZA&time=15864&view=map

[20] Krebs, B. Target hackers broke in via HVAC company, KrebsOnSecurity, 5 February 2014. Retrieved 12 February 2014 from http://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/

[21] Busch, P., et al., Heisenberg's unvertainty principle. Physics Report, 2007. **452** (6). P. 155-176.

[22] WK Wooters and WK Zurek, Quantum no-cloning theorem. Nature, 299:802, 1992.

[23] Lo, H-K., et al., Decoy state quantum key distribution. Physical Review Letters A, 2005. 94, 230504

[24] P. Villoresi, T. Jennewein, F. Tamburini, M. Aspelmeyer, C. Bonato, R. Ursin, C. Pernechele, V. Luceri, G. Bianco, A. Zeilinger, and C. Barbieri. Experimental verification of the feasibility of a quantum channel between space and earth. New J. Phys., 10(033038), 2008.

[25] Bonato, C., Tomaello, A., Da Deppo, V., Naletto, G., & Villoresi, P. (2009). Feasibility of satellite quantum key distribution. New Journal of Physics, 11(4), 045017.

[26] Blakley, G. Safeguarding cryptographic keys. Proceedings of 1979 AFIPS National Computer Conference, 48, AFIPS, P. 313-317, 1979.

[27] Shamir, A. How to share a secret. Communications of ACM, 22, p. 612-613, 1979.

[28] Cleve, R., and Gottesman, D. How to share a quantum secret. Physical Review Letters, 83, p. 648, 1999.