Input to the Commission on Enhancing National Cybersecurity

Information on Current and Future States of Cybersecurity in the Digital Economy
(NIST RFI on August, 10, 2016)

Pertinent topics: a) *Cybersecurity Workforce*; b) *Public Awareness and Education*

Felix Alba/President
Felix ALBA Consultants, Inc.
Draper, UT 84020

Executive Summary

President Obama said in 2009 that "America's economic prosperity in the 21st century will depend on cybersecurity". In 2012, Defense Secretary Panetta ominously coined the expression "Cyber Pearl Harbor". In April 2016, Symantec reported 1M web attacks per day, 75% unpatched websites, and 0.5B personal records stolen or lost [1]. Accordingly, in February 2016, per the *Cyber Security National Action Plan* (CNAP), the Federal Cybersecurity 2017 Budget was increased 30% ($19B) and on July 12, 2016 the White House released the first-ever Federal Cybersecurity Workforce Strategy [2] [3].

A main weakness behind Classical Cyber Security (CCS) is its relying on two unwarranted articles of faith: *Eve (the archetypal spy) has neither the knowledge nor the computer power to: a) infer the secret key from the public one in current asymmetric security cyphers, or b) cryptanalyze the current symmetric AES-256 cyphertext* [4] [5]. To aggravate the situation, it is estimated that *quantum computers* will be available by 2030 and then all current crypto-infrastructure will be utterly vulnerable [4] [6]. In fact, in August 2015, the NSA stated: …*research on quantum computing has made it clear that elliptic curve cryptography [ECC] is not the long term solution many once hoped it would be. Thus, we have been obligated to update our strategy* [7].

A new paradigm -called *Quantum Key Distribution* (QKD)- was needed: In 2013, the DHS's TTP Program announced the transition to market of a *Quantum* technology developed at Los Alamos National Laboratory (LANL) [8] [9]. Likewise, the Battelle Memorial Institute, jointly with ID Quantique (IDQ), has built a QKD network in Ohio, and plans to extend it throughout North America [6] [10]. More recently, on August 8, 2016, the National Science Foundation awarded $12M to six Universities *to develop systems that use photons in pre-determined quantum states as a way to encrypt data* [11] [12].

Cognizant of this worldwide revolution incubating for over 3 decades, interactions with Don Hayford (Battelle's Senior Research Leader till January 2016) and with Dr. Richard Hughes (former Research Director and co-inventor of LANL's technology) led us to conclude that in 5-10 years a multitude of governmental and private entities will use *quantum cryptography* for data protection though -upon inaction- without the *workforce* properly trained in this emerging and *fundamentally-different* technology.

We firmly believe that a globally-competitive *workforce* for Quantum Cyber Security (QCS) is crucial to protect our Nation and, ergo, its creation has to start immediately. Furthermore, because *Workforce* creation and *Education* must go hand-in-hand, a new paradigm in *Cyber Security* (based on *Quantum Physics*) calls for a new paradigm in *Teaching* [13] [14] -- particularly at *secondary school* and *undergraduate* levels. Also, as Malcolm & Feder state in [15] "…higher education institutions function more like a collection of discrete practices and policies, rather than being interconnected and synergistic."

Based on those premises/facts, I have united the Salt Lake Community College and the University of Utah to conceive a 10-year/3-phase plan to develop a nationally-scalable curricula/infrastructure (K-12 to Ph.D.) as well as to outreach to the human capital (trainers/trainees/employers) necessary for creating the National Workforce for Quantum/Classical Cyber Security (QCS/CCS) and enhancing the public awareness/literacy. To start our Phase I -of which I would be the Project Director- on October 6, 2016, the Salt Lake Community College will submit a Collaborative Proposal to the NSF ATE (Advanced Technological Education) Program entitled *Creating the National Workforce for Quantum Cybersecurity, Phase I: Curricula/Infrastructure for K-12/College/University Career Pathways* [14]. Upon request, we will be pleased and honored to submit to the Commission the full-text of our NSF Proposal.

1. Current/Future Challenges – Classical Cyber Security (CCS) and its Vulnerabilities

In the US there are about 6,000 hospitals, tens of thousands of banks and many more financial, educational, military, industrial, and utility enterprises whose data integrity/availability are crucial for social stability, privacy, public trust, health, economy, civil liberties, and security of our Nation. The 'Internet of Things' (IoT) is at the heart of our economy with critical functions like transportation, electrical power, health, etc. More than six billion *things* will be connected in 2016 [1]. Their uninterrupted-real-time requirements make them overly vulnerable. DOE, DHS, and FBI stated Ukraine's Power Grid failure in 2015 was an "unprecedented cyberwarfare attack". *U.S. systems aren't any more protected*, the official said [16]. Per the DOE's roadmap, by 2020 the Power Grid should *survive a cyber incident while sustaining critical functions* [17]. NIST 800-160 (5/2016) clearly states this problem [18].

Online banking relies upon the HTTPS/TLS protocol to secure web traffic, with server authentication and key establishment using X.509 *certificates* and RSA *public keys*. The SWIFT network uses a Public Key Infrastructure (PKI) to sign and encrypt messages/transfers of funds [19]. The Advanced Encryption Standard (AES-256) is used worldwide to encrypt data on hard drives, email systems, and web browsers.

In sum: the Internet uses *asymmetric-key* cyphers (e.g. RSA, DH, ECC) for sharing the *secret key* needed for a *symmetric-key* protocol like the AES-256. However: These schemes are ***not*** unconditionally-secure because they rely upon two weak articles of faith: *Eve has neither the knowledge nor the computer power to: a) infer the secret key from the public one, or b) cryptanalyze the AES-256 cyphertext.*

The NSA will have in 2018 an exaflop machine (10^{18} flops /sec) to cryptanalyze AES-256 cyphertext [20]. If we can do it, our adversaries can as well... so the only way to retain our faith is to increase the *key* length and change it often. In fact, NIST declared RSA-1024 not safe five years ago and RSA-2048 will soon follow suit as RSA-3072 is already used for 'top secret' [21]. Most importantly: *Eve*'s computing resources are unknowable, and the only way to know secret data have been compromised is after the fact!

Finally, once *quantum computers* are available, increasing the key length will ***not*** work. All web traffic will be very vulnerable [19] [4] [6] [1] [10]. This is not academic: Google [22], IBM [23], Microsoft [24], Jeff Bezos [25], Intel [26], Lockheed Martin [27], and US Government [28] [12] are determined to make it a reality. Revealingly, IBM, in May 2016, launched the first quantum platform in the Cloud [29]. *And that is why NSA in 2015 announced its plan for transitioning to new quantum-resistant cryptosystems* [7].

2. Promising and Innovative Approaches already entering the Market

The solutions to CCS vulnerabilities are: a) *Quantum Key Distribution* (QKD): Each bit of the cryptographic *key* is encoded into a 'quantum object' like a single *photon*, instead of into the signal level of a laser beam (10^{16} *photons*/sec) as in classical optical networks; and b) *Post-Quantum Cryptography* (PQC), i.e. the design of new asymmetric cyphers resistant to *quantum computers* [7] [30]. PQC will be still somehow vulnerable because it will have to dynamically adjust to progress in *quantum computing* (hardware and new algorithms). With QKD, instead, secrecy is guaranteed by the Laws of Physics, ***not*** by computational complexity and human ingenuity (or lack thereof). The QKD secret *key* can be used in an *unbreakable* One-Time-Pad (OTP) encrypted message or in a robust *classical* symmetric-key cypher like the AES-256 [4].

2.1 Quantum vs. Classical Physics – QCS/CCS Unconditional Security

The quantum version of a *Bit* is the *Qubit*. A *Bit* has one *property* with two values; instead, a *Qubit* has a *continuum of attributes*, all of them *random variables* with the same two possible values. That makes all statements about a Qubit *probabilistic*. A *Bit* has only two *states;* a *Qubit* can be instead in two so-called *eigenstates* as well as in *linear combinations* of them. Unlike for a *Bit*, the *Qubit state* does not convey its *value* but the *probabilities* for its two *values*. Each *state's* component is a complex number whose squared magnitude is the *probability*. There are many ways to implement a *Qubit*, e.g. with the *polarization* of a photon or the *spin* of an electron. For High-School/2-year-degree curricula, standard *vector algebra* and *probability* prerequisites would be acceptable. For a 4-year-degree audience we could further say: s*tates*

of a *Qubit* belong to a 2-D Hilbert vector space; each *property* is related to a *linear operator* whose *eigenstates* constitute an *orthonormal basis* for the space, and its *eigenvalues* are the two possible *values*.

Another peculiar behavior of *Qubits* is *entanglement*: their intrinsically-random values can exhibit strong *correlations* that persist regardless of their distance (*non-locality*). This is what Einstein colloquially called 'spooky action at a distance'. *Non-locality* is now an established fact and is the essence of some QKD protocols and of *quantum repeaters* under development [19] [6] [12].

This counterintuitive behavior of *Qubits* is the result of the *Heisenberg's Principle of Uncertainty*: the *standard deviations* (STDs) of any two so-called *conjugate* properties of a quantum object are inversely related: the lower is one, the higher is the other. QKD guarantees *Eve* knows neither the transmitted *bit* nor the *basis* because *Alice* quantumly randomizes them. If *Eve* uses the wrong *basis* to measure the *Qubit*, its state will be *stochastically* altered and *Alice* and *Bob* will *statistically* detect her presence:

> Unlike *classical* cryptography, *quantum* cryptography detects Eves' intrusion…
> ***before secret data are sent***!

In current commercial implementations of QKD, the qubits in the cryptographic key are encoded using four photon *polarization states*. *Alice* sends photons to *Bob* who measures them. Neither *quantum computation* nor *storage* are necessary, only *transmission* through standard optical fibers. After the raw key is transferred, *Alice* and *Bob* openly communicate through a *classical-authenticated* channel and statistically determine whether *Eve* is around or not ***before*** transmitting the actual critical data.

Finally, instead of *measuring* and *resending* to hide her presence, *Eve* could *copy* each photon's quantum state, *save* it and, after listening to *Bob* ↔ *Alice* classical communication (learning the *bases* used for each qubit), *measure* them correctly. However, even though when classically dealing with ***legions*** of photons *Eve* can ***copy*** the signal with impunity, when dealing with a ***single*** photon, the *No-Cloning Theorem* [31] assures the impossibility of copying its quantum state. In conclusion:

> QCS (properly implemented) is unconditionally-secure, ***even if the attacker has a quantum computer***

3. Quantum Cyber Security in the USA and around the World

As solid evidence that QCS has entered already the market to stay, below we present a brief non-exhaustive review of the current and future state of Quantum Cyber Security in the world.

3.1 Quantum Cyber Security around the World - Education, Research, and Manufacturers

In 2008, the European SECOQC Project demonstrated the first optical QKD network in Vienna. In 2010, a QKD network in Tokyo encrypted video data in real-time; likewise in Madrid and London. In 2009-2011, the 'SwissQuantum' Project tested ID-Quantique's QKD for 2 years in the Geneva area. In 2014, the National Physical Laboratory (UK), Toshiba, BT, and ADVA proved that quantum signals can coexist with *classical* telecom signals in an optical fiber [32]. The longest QKD network is being tested in China (2,000 km – Shanghai ↔ Beijing). Remarkably, on 8/9/2016 China successfully launched the first-ever quantum-communications satellite into orbit [33]. Quintessence Labs (Australia) has a QKD project with Lockheed Martin. NASA has a 560km QKD link to its JPL Laboratory.

The *Institute for Quantum Computing* (University of Waterloo, Canada) offers a graduate course on Applied Quantum Cryptography, a summer school on QKD, and a Quantum Cryptography course for 'young students'. The EU has a QKD Certification Project (Q-CERT). The Austrian Institute of Technology and the University of Vienna are working on entanglement-based QKD systems. The Vienna Center for Quantum Science and Technology has developed a MatLab® QKD Simulator. The University of Luxembourg has published a Web QKD simulator [34]. QCRYPTO, a European consortium for quantum-cryptography, released in 2015 a report recommending cryptographic techniques *resistant to*

quantum computers [35]. Chinese and European striking R & D and workforce-creation current and future plans are described in Section 4.

3.1.1 ID-Quantique (IDQ) Quantum Cybersecurity Technologies

IDQ is a QCS leader with government/commercial/academic customers worldwide. They deployed the world first QKD system over a commercial network [5]. IDQ technology was employed by Battelle in its QKD network within Ohio (see below), by ORNL in its Power Grid Project [36], and it is planned to be used by Acronis' data protection solutions for the Cloud [37]. ID-Quantique is one of our collaborators.

3.2 Quantum Cyber Security in the USA - Education, Research, and Manufacturers

The Federal Government plays a crucial role in the incubation and adoption of emerging technologies for cybersecurity. Conspicuous examples include the 'Transition to Practice' (TTP) programs of the DHS Advanced Research Projects Agency (HSARPA) and of the NSF SaTC. The first QKD network was the 'DARPA Network' linking Harvard University, Boston University, and BBN Technologies in 2004 [38]. LANL and NIST have worked on QKD for over 15 years. The Oak Ridge National Lab (ORNL), with IDQ and GE, had a project called 'Practical Quantum Security for Grid Automation' [36]. The University of Arizona (UA) has a DOD R&D project on QKD with the Universities of Illinois, Duke, and Boston. Pace University (NY) has a project on QKD. Caltech and TU Delft offer an online course on QKD [39]. In FY 2017, IARPA and DOE plan to support new programs in Quantum Information Science (QIS) [12].

There are four main domestic QCS/CCS vendors: Qubitekk, which focuses on Power Grid Security [40]; MagiQ with QCS/CCS integration [41]; Acronis with data protection for the Cloud [37], and Whitewood Encryption Systems (licensee of LANL's technology) marketing an *Entropy Engine* [9].

3.2.1 NIST on Cyber Security (Standards, Education, and Research) – NICE Resources

NIST's role in Cybersecurity is vital. The Advanced Data Encryption Standard (AES) is now the preferred crypto for IEEE 802.11 (wireless networks), and mandatory in the Transport Layer Security (TLS) protocol [42]. In 2013, NIST established the National Cybersecurity Center of Excellence (NCCoE) to adopt standards-based solutions to the diversity of configurations across the Government, which creates significant vulnerabilities [43].

NIST also focuses on metrology for quantum communications, quantum computation, and quantum measurements [12]. In a QKD survey [44], 93% agreed that standards, quality assurance, and metrology are crucial for QKD commercial success. NIST has developed a QKD test bed for OTP video signals [45] and is working on QKD networks, *quantum repeaters*, and the *Quantum Randomness Beacon* [46]. In April 2015, NIST hosted the 'Workshop on Cybersecurity in a Quantum World' [47]. After NSA's announcement of its plan to transition to *quantum-resistant* algorithms in August 2015 [7], on April 28, 2016, NIST released its first *Report on Post-Quantum Cryptography* (NISTIR 8105) [48].

NICE is a partnership between government, academia, and the private sector focusing on cybersecurity education, training, and workforce development. Under its Strategic Plan, NICE developed the National Cybersecurity Workforce Framework to provide a common taxonomy/lexicon to categorize workers [49]. In tune with NICE's value of *Drive Change – seek creative and innovative solutions that might disrupt or defy the status quo* [49], we look forward to collaborating within NICEWG on the inclusion of QCS/CCS in the NSA/DHS/NICE *Cybersecurity Core Curriculum* to be developed under the White House's Cyber Security National Action Plan (CNAP) [2].

3.2.2 Los Alamos National Laboratory (LANL)

LANL has worked on QKD for 17 years. In 2013, DHS-HSARPA identified LANL's technology as "a next-generation encryption system that leverages the quantum properties of light, as an innovative solution to better protect the nation's critical cyber infrastructure". Patents were granted to R. Hughes et al, and licensed to Whitewood Encryption Systems [8].

3.2.3 The Battelle Memorial Institute

In 2013 Battelle deployed the first QKD commercial network between Columbus and Dublin. ID-Quantique servers protect its technical, IP, financial, and customer data using QKD/AES encryption. Battelle plans to connect Ohio to Washington DC and build a North-America Network [6] [10].

4. Workforce Demand for Cyber Security Technologies (QCS/CCS)

In 2015, 29% of North America traffic was encrypted, and the number is steadily growing. At the same time, over 80% of enterprises currently lack the right skills and human resources to protect their IT assets; "little wonder why cybercrime is so rampant" [50]. According to the US Department of Labor's Occupational Outlook for *Computer and Information Technology*, employment will grow 12% from 2014 to 2024, faster than for all occupations [51]. This is due to *cloud computing*, *big data*, *IoT*, and *mobile computing* -- and these projections do not include the *emerging quantum technologies* for cyber security.

The US Government hired over 3,000 CCS workers in the first half of 2016 and expects to hire 3,500 more by Dec 2016, stating that supply is "simply not sufficient' to meet demand [3]. At the May 2016 NICEWG meeting we learnt that 1.5M more CCS jobs will be needed by 2020; only 25% of applicants were qualified; the biggest skill gap was lack of business understanding; and only 10% of the workforce comprises women [52]. Likewise, the unemployment rate for ages 16-24 is 35.5%; 20% of Latinos and 30% of Blacks with ages 18-24 are unemployed; and 41% of students in low-performing districts finish high school with no access to STEM education/career guidance. *It is thus clear that, even for CCS, there is plenty of education and outreach to employers and potential employees to be undertaken.*

QCS merges Quantum Physics with Information/Communications Technology (ICT). In 2013, ICT accounted for 41% of the $323B US private R & D -- 2.5 times bigger than Pharmaceuticals [53]. Internet traffic has exploded and new technologies affecting consumer and job markets emerge daily, e.g. photon detectors are widely used in medical devices, LIDAR, communications, automotive, cell phones, etc. [28]. Ergo, cybersecurity challenges are gigantic and unpredictable: "2016 will be a year of massive ramp-up in the arms race around quantum encryption" [54].

A few examples: a) The UK invested £270M in *quantum technologies* for 2014-2019, and committed £204M for ***workforce*** training in 2016 [55]; b) The European Commission announced in April 2016 a €1B project in *quantum technologies* [56] [57]; c) Researchers at the Niels Bohr Institute have received millions to produce 'photon-gun' chips, essential for a future cost-effective and secure *quantum internet* [58]; d) In 8/29/2016, the Australian Government invested over $25M to "initiate the Quantum Era" [59]; e) On 7/7/2016, Google announced that its Chrome browser will use a *post-quantum* key-exchange algorithm on top of the *classical* ECC [30]; and f) On 8/8/2016, NSF awarded $12M to six Universities for the *photonic* implementation of Quantum Cyber Security [11]. However, to put things in the proper perspective, U.S. Federal Quantum Research funding is a mere $200 million annually, while China allegedly invested $101 **b**illion in 2015 on basic research in *Quantum Technologies* [33].

It is thus evident that -after over 3 decades of incubation- QCS/CCS technology is reaching maturity and its commercial reality is inevitable. However, the cited QKD survey [44] stated that the real bottleneck will be ***installation*** & ***maintenance***. In fact, about ***60%*** of Swiss IDQ's employees are ***technicians,*** and Chinese QuantumCTek employs around ***300 technicians***. Likewise, a NSTC Report dated July 2016 identified ***education and workforce training needs*** as one of the "impediments to progress" in Quantum Information Science [12]. Clearly thus, the ***properly-trained*** *workforce* is paramount -- reinforcing the need for a long-term comprehensive educational vision whose immediate implementation is imperative.

5. A Proposed 10-year 3-phase Project to Create the Workforce and Educate the Public

Cognizant of this worldwide revolution gestating for over 3 decades, interactions with Don Hayford (Battelle's Senior Research Leader till January 2016) and with Dr. Richard Hughes (former Research Director and co-inventor of LANL's technology) led us to conclude that in 5-10 years a multitude of governmental and private entities will use *quantum cryptography* for data protection though -upon inaction- without the *workforce* properly trained in this emerging and *fundamentally-different* technology.

Most millennials do not receive in high-school any insights on how to pursue a cyber career [60]. The Community College Research Center (CCRC) provides revealing statistics [61]. Paraphrasing Malcolm & Feder: … *completion for STEM aspirants is under 50%, with the lowest rates for Blacks/Hispanics/Native Americans… It is clear 2 & 4-year institutions do not deliver a high-quality education experience… Improving STEM education for all requires a systemic approach that includes evidence-based decisions, learning communities, faculty networks, and* ***partnerships*** *across the education system* [15].

We firmly believe that a globally-competitive *workforce* for Quantum Cyber Security is crucial to protect our Nation and, ergo, its creation has to start immediately. Furthermore, a new paradigm in *Cyber Security* (based on *Quantum Physics*) calls for a new paradigm in *Teaching* [13] [14] -- particularly at *secondary school* and *undergraduate* levels. In addition, Malcolm & Feder also stated that "…higher education institutions function more like a collection of discrete practices and policies, rather than being interconnected and synergistic." [15].

Quantum Physics is a century old and scientists and educators are still debating its meaning in terms of *Reality*, *causality*, *locality*, and *observer's independence* [62]. In 1965, Richard Feynman said: …*I can safely say that nobody understands quantum mechanics. So do not take the lecture too seriously, feeling that you really have to understand.* With all due respect and admiration, such an attitude is against the progress fired by understanding. What about those with a middle-skill job [63] who do not command the *mathematics* but will still have to install and troubleshoot QCS technology? What about K-12 teachers whose job is to inspire, discover, and kindle talent? And educators at all levels (Certificates, AAS, etc.)? In 1982, Karl Popper [64] said: *The denial that we can understand quantum theory has had the most appalling repercussions, both on the teaching and on the real understanding of the theory.* Alas, not much has changed since 1982 and, well into the 21st century, our students and educators deserve better. Education and workforce creation must go hand-in-hand for the successful transition to practice of novel technologies [65]. Ergo, didactic techniques involving interactive learning and novel pedagogical approaches [66] [67] [13] [68] [69] [70] [71] are paramount to improving student learning/retention in STEM, particularly for women and underrepresented students [15].

Based on those premises/facts, I have united the Salt Lake Community College and the University of Utah to conceive a 10-year/3-phase plan to develop a nationally-scalable curricula/infrastructure (K-12 to Ph.D.), as well as to outreach to the human capital (trainers/trainees/employers) necessary for creating the National Workforce for Quantum/Classical Cyber Security (QCS/CCS) and enhancing the public awareness and literacy. To start our Phase I -of which I would be the Project Director- on October 6, 2016, the Salt Lake Community College will submit a Collaborative Proposal to the NSF ATE (Advanced Technological Education) Program entitled *Creating the National Workforce for Quantum Cybersecurity, Phase I: Curricula/Infrastructure for K-12/College/University Career Pathways* [14]. Upon request, we will be pleased and honored to submit to the Commission the full-text of our NSF Proposal.

Phase-I aims to create a vigorous synergy between both Institutions and the High-School system to develop the QCS/CCS curricula/infrastructure needed for a rich cybersecurity-pathways structure, allowing students/prospective teachers to successfully navigate from High-Schools, through 2-year Colleges, to the University -- acquiring 21st century technical/employability skills [72] [73]. The long-term goal (Phases II and III) is to achieve a self-sustained capacity/infrastructure for outreaching, educating, mentoring, and training the workforce needed for QCS/CCS technologies up to the Ph.D. level -- while promoting the nationwide adoption of our curricula/pedagogics/pathways model.

A sizable part of our work plan involves *outreaching* to prospective students, teachers, employers and *educating* the general public. The SLCC has partnerships with over 500 businesses and school districts providing skills training, professional development, internships, etc. to employees and employers. Besides, our close partnership with the University of Utah's Division of Continuing Education will provide us with an additional and fluid liaison to employers, employees, and policy makers.

It is irrefutable that US prosperity and security does and will depend on cybersecurity, so we resolutely believe that -upon inaction in QCS/CCS workforce creation and education- the inevitable advent of *quantum computers* will turn our vital data instantly vulnerable, with dire consequences to our Society.

References Cited

[1] Symantec, "2016 Internet Security Threat Report, Volume 21," April 2016. [Online]. Available: https://www.symantec.com/security-center/threat-report.

[2] White House, "Cyber Security National Action Plan (CNAP," 9 February 2016. [Online]. Available: https://www.whitehouse.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan.

[3] White House - Office of Management and Budget, "Strengthening the Federal Cybersecurity Workforce," 12 July 2016. [Online]. Available: https://www.whitehouse.gov/blog/2016/07/12/strengthening-federal-cybersecurity-workforce.

[4] S. Loepp and W. K. Wooters, Protecting Information - From Classical Error Correction to Quantum Cryptography, New York: Cambridge University Press, 2006.

[5] SECOQC, "White Paper on Quantum Key Distribution and Cryptography," SECOQC, 2007.

[6] D. Hayford, "The Future of Security: Zeroing In On Un-Hackable Data With Quantum Key Distribution," 2 Sept. 2014. [Online]. Available: http://insights.wired.com/profiles/blogs/preparing-for-the-quantum-cryptography-world#axzz3CAQ1uBru. [Accessed 24 Oct. 2015].

[7] National Security Agency, "Cryptography Today," 19 August 2015. [Online]. Available: https://www.nsa.gov/ia/programs/suiteb_cryptography/index.shtml.

[8] US Department of Homeland Security, "Science & Technology Directory's Transition to Practice Program," 2013. [Online]. Available: https://www.dhs.gov/science-and-technology/st-snapshot-st-announces-first-success-technology-transition-program. [Accessed 31 March 2016].

[9] R. Hughes and J. Nordholt, "Strengthening the Security Foundation of Cryptography with Whitewood Quantum-powered Entropy Engine," January 2016. [Online]. Available: http://www.whitewoodencryption.com/wp-content/uploads/2016/02/Strengthening_the_Security_Foundation.pdf. [Accessed March 2016].

[10] R. Brandom, "Building a globe-spanning quantum internet," The Verge, 18 November 2014. [Online]. Available: http://www.theverge.com/2014/11/18/7214483/quantum-networks-expand-across-three-continents.

[11] National Science Foundation - Press Release 16-091, "NSF invests $12 million in quantum technologies for secure communication," 8 August 2016. [Online]. Available: http://www.nsf.gov/news/news_summ.jsp?cntn_id=189436&org=NSF&from=news.

[12] White House - Interagency Working Group on Quantum Information Science, "Advancing Quantum Information Science: National Challenges and Opportunities," National Science and Technology Council, Washington D.C., 2016.

[13] Felix Alba-Juez, Publisher, "Praise for Felix Alba-Juez Pedagogical Skills," [Online]. Available: http://www.felixalbajuez.com/Reviews.html. [Accessed 13 June 2016].

[14] Salt Lake Community College and University of Utah, *Educational Proposal to NSF ATE Program 14-577*, Salt Lake City, 2016.

[15] S. Malcolm and M. E. Feder, Barriers and Opportunities for 2-year and 4-year STEM Degrees, Washington DC: The National Academies Press, 2016.

[16] InfoSecurity Magazine, "Congressional Report," 22 May 2013. [Online]. Available: http://www.infosecurity-magazine.com/news/congressional-report-us-power-grid-under/.

[17] DOE - Office of Electrictiy Delivery and Energy Reliability, "Energy Delivery Systems Cybersecurity," [Online]. Available: http://energy.gov/oe/services/technology-development/energy-delivery-systems-cybersecurity. [Accessed 12 April 2016].

[18] NIST Special Publication 800-160, "Building Security into Cyber-Physical Systems," May 2016. [Online]. Available: http://www.nist.gov/itl/csd/building-security-into-cyber-physical-systems-nist-researchers-suggest-approach-for-trustworthy-modern-infrastructure.cfm.

[19] ETSI, European Telecommunications Standards Institute, "Quantum Safe Cryptography and Security; An Introduction, Benefits, Enablers, and Challenges," ETSI, Sophia Antipolis, 2014.

[20] National Security Agency, "Utah Data Center," [Online]. Available: https://nsa.gov1.info/utah-data-center/. [Accessed 6 April 2016].

[21] NIST, "NIST Special Publication 800-56B," September 2014. [Online]. Available: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-56Br1.pdf.

[22] MIT Technology Review, "Google Researchers make Quantum Computer Components more Reliable," 4 March 2015. [Online]. Available: https://www.technologyreview.com/s/535621/google-researchers-make-quantum-computing-components-more-reliable/.

[23] IBM Press Release, "IBM Scientists Achieve Critical Steps to Builiding Practical Quantum Computer," IBM, 29 April 2015. [Online]. Available: http://www-03.ibm.com/press/us/en/pressrelease/46725.wss.

[24] MIT Technology Review, "Microsoft's Quantum Mechanics," 10 October 2014. [Online]. Available: https://www.technologyreview.com/s/531606/microsofts-quantum-mechanics/.

[25] MIT Technology Review, "The CIA and Jeff Bezos Bet on Quantum Computing," 4 October 2012. [Online]. Available: https://www.technologyreview.com/s/429429/the-cia-and-jeff-bezos-bet-on-quantum-computing/.

[26] Intel, "Intel Invest $50 Million to Advance Quantum Computing," Intel News Room, 3 September 2015. [Online]. Available: https://newsroom.intel.com/news-releases/intel-invests-us50-million-to-advance-quantum-computing/.

[27] University of South California News, "Cooling breakthrough could improve performance of quantum computers," 5 August 2016. [Online]. Available: http://news.usc.edu/104956/cooling-breakthrough-could-improve-performance-of-quantum-computers/.

[28] White House, "Realizing the Potential of Quantum Information Science and Advancing High-Performance Computing," 26 July 2016. [Online]. Available:

https://www.whitehouse.gov/blog/2016/07/26/realizing-potential-quantum-information-science-and-advancing-high-performance.

[29] IBM Cloud, "The World First Quantum Computing Platform delivered via the IBM Cloud," 4 May 2016. [Online]. Available: http://www.research.ibm.com/quantum/.

[30] M. Braithwaite, "Experimenting with Post-Quantum Cryptography," Google Security Blog, 7 July 2016. [Online]. Available: https://security.googleblog.com/2016/07/experimenting-with-post-quantum.html.

[31] W. Wootters and W. Zurek, "The no-clonning theorem," *Physics Today,* February 2009.

[32] J. Qiu, "Quantum Communications Leap out of the Lab," *Nature,* vol. 508, pp. 441-442, 24 April 2014.

[33] J. Chin and V. Pang, "China's Latest Leap Forward Isn't Just Great -- It's Quantum," The Wall Street Journal, 9 August 2016. [Online].

[34] A. Atashpendar, "Simulation and Analysis of QKD (BB84)," 2014. [Online]. Available: http://www.qkdsimulator.com/. [Accessed 20 May 2016].

[35] PQCRYPTO, "Post-Quantum Cryptography for Long-Term Security," 7 September 2015. [Online]. Available: http://pqcrypto.eu.org/docs/initial-recommendations.pdf.

[36] DOE - Office of Electricity Delivery and Energy Reliability, "Practical Quantum Security for Grid Automation," September 2013. [Online]. Available: https://www.controlsystemsroadmap.net/ieRoadmap%20Documents/Practical_QKD.pdf.

[37] ID-Quantique, "Acronis Partners with ID-Quantique to bring Quantum-Safe Encryption to Cloud Data Protection," 28 September 2015. [Online]. Available: http://www.idquantique.com/acronis-partners-with-id-quantique/.

[38] C. Elliott, "Building the quantum network," *New J. Phys.,* vol. 4, p. 46, 2002.

[39] Caltech & TU Delft, "Course on Quantum Cryptography," edX, [Online]. Available: https://www.edx.org/course/quantum-cryptography-caltechx-delftx-qucryptox. [Accessed 10 June 2016].

[40] Qubitekk, "Commercializing Quantum Technology Today," [Online]. Available: http://qubitekk.com/. [Accessed 7 June 2016].

[41] MagiQ Technologies, [Online]. Available: http://www.magiqtech.com/Products_files/QBox%20Datasheet-2011.pdf. [Accessed 7 Nov, 2015].

[42] NIST - NIST.IR.7977, "NIST Cryptographic Standards Development Process and Guidelines," March 2016. [Online]. Available: http://dx.doi.org/10.6028/NIST.IR.7977.

[43] NIST - NCCoE, [Online]. Available: https://nccoe.nist.gov/about_the_center. [Accessed 9 April 2016].

[44] A. Al Natsheh, S. A. Gbadegeshin, A. Rimpiläinen, I. Imamovic-Tokalic and A. Zambrano, "Identifying the Challenges in Commercializing High Technology," *Technology Innovation Management Review,* pp. 27-36, January 2015.

[45] A. Mink, X. Tang, L. Ma, T. Nakassis, B. Hershman, J. C. Bienfang and D. Su, "High Speed Quantum Key Distribution System Supports One-Time Pad Encryption of Real-Time Video," in *Quantum Information and Computation IV*, 2006.

[46] NIST, "NIST Randomness Beacon," 22 December 2015. [Online]. Available:

http://www.nist.gov/itl/csd/ct/nist_beacon.cfm.

[47] NIST - Workshop on QCS, "Cyber Security in a Post-Quantum World," April 2015. [Online]. Available: http://www.nist.gov/itl/csd/ct/post-quantum-crypto-workshop-2015.cfm.

[48] NIST, "NIST Kicks Off Effort to Defend Encrypted Data from Quantum Computer Threat," 28 April 2016. [Online]. Available: http://www.nist.gov/itl/csd/nist-kicks-off-effort-to-defend-encrypted-data-from-quantum-computer-threat.cfm.

[49] NICE (National Initiative for Cybersecurity Education), "Strategic Plan for the National Initiative for Cybersecurity Educationa (NICE)," 13 April 2016. [Online]. Available: http://csrc.nist.gov/nice/about/strategicplan.html.

[50] Network World, "Cybersecurity Skills Haves and Have Nots," 13 March 2014. [Online]. Available: http://www.networkworld.com/article/2226525/cisco-subnet/cybersecurity-skills-haves-and-have-nots.html.

[51] United States Department of Labor, "Computer and Information Technologies Occupations," 17 December 2015. [Online]. Available: http://www.bls.gov/ooh/computer-and-information-technology/home.htm.

[52] NIST-NICE, "Cybersecurity Workforce Demand," [Online]. Available: http://csrc.nist.gov/nice/NICE_Workforce_Demand.pdf. [Accessed 3 June 2016].

[53] NSF InfoBrief, "ICT Industries Account for $133 Billion... in 2013," National Center for Science and Engineering Statistics - NSF 16-309, Washington DC, April, 2016.

[54] Government Technology Magazine, "10 Cybersecurity Issues to expect in 2016 (Industry Perspective)," 19 January 2016. [Online]. Available: http://www.govtech.com/opinion/10-Cybersecurity-Issues-to-Expect-in-2016.html.

[55] UK National Quantum Technologies Programme, "Quantum Technologies: a £1 Billion future industry for the UK," 1 March 2016. [Online]. Available: http://uknqt.epsrc.ac.uk/.

[56] Nature, "Europe plans giant billion-euro quantum technologies project," 21 April 2016. [Online]. Available: http://www.nature.com/news/europe-plans-giant-billion-euro-quantum-technologies-project-1.19796.

[57] Qurope -Quantum Information Processing and Communications in Europe, "Quantum Manifesto - A New Era of Technology," May 2016. [Online]. Available: http://qurope.eu/system/files/u7/93056_Quantum%20Manifesto_WEB.pdf. [Accessed 22 August 2016].

[58] Phys.org, "Quantum Photonic researchers start new company, Sparrow Quantum," 30 May 2016. [Online]. Available: http://phys.org/news/2016-05-quantum-photonic-company-sparrow.html#jCp.

[59] Computer World, "Government sees potential 'quantum ecosystem' in Australia," 29 August 2016. [Online]. Available: http://www.computerworld.com.au/article/605716/government-sees-potential-quantum-ecosystem-australia/.

[60] U.S.News, "Op-Ed: The Time Is Now to Prevent a Cybersecurity Workforce Crisis," 8 June 2016. [Online]. Available: http://www.usnews.com/news/articles/2016-06-08/op-ed-the-time-is-now-to-prevent-a-cybersecurity-workforce-crisis.

[61] Community College Research Center, "Community College FAQs," [Online]. Available:

http://ccrc.tc.columbia.edu/Community-College-FAQs.html. [Accessed 10 June 2016].

[62] R. Omnès, Quantum Philosophy - Understanding and Interpreting Contemporary Science, Princeton and Oxford: Princeton University Press, 2002.

[63] C. Dortch, "Career and Technical Education (CTE): A Primer," Congressional Research Service, Washington DC, 2014.

[64] K. R. Popper, "Quantum Mechanics without the Observer," [Online]. Available: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.473.23&rep=rep1&type=pdf. [Accessed 2 February 2016].

[65] NSF, "Investing in Science, Engineering, and Education for the Nation's Future - Strategic Plan for 2014-2018," National Science Foundation, Arlington, Virgina, USA, 2014.

[66] J. L. Bishop and M. A. Verleger, "The Flipped Classroom: A Survey of the Research," in *120th ASEE Annual Conference & Exposition*, Atlanta, USA, 2013.

[67] C. J. Brame, "Flipping the Classroom," Center for Teaching, Vanderbilt University, [Online]. Available: https://cft.vanderbilt.edu/guides-sub-pages/flipping-the-classroom/. [Accessed 5 June 2016].

[68] C. Furse, "Teaching Flipped," University of Utah, [Online]. Available: https://utah.instructure.com/courses/356979. [Accessed 13 May 2016].

[69] C. Furse and B. S. Ziegenfuss Donna, " Using a MOOC as a Faculty Development Tool and/or Learning Community for STEM Faculty Teaching Flipped Classes," in *MOOCs in STEM: Exploring New Educational Technologies*, San Jose State University, San Jose, CA, June 6, 2014.

[70] Sciencedaily.com, "Flipped classrooms turning STEM education upside down," 7 June 2016. [Online]. Available: https://www.sciencedaily.com/releases/2016/06/160607151512.htm.

[71] University of Utah, "Teaching Flipped," [Online]. Available: www.teach-flip.utah.edu. [Accessed 15 May 2016].

[72] Partnership for 21st Century Learning, "P21," [Online]. Available: http://www.p21.org/. [Accessed 9 July 2016].

[73] Department of Education, "Employability Skills Framework," [Online]. Available: http://cte.ed.gov/employabilityskills/. [Accessed 7 July 2016].