# CLOSING THE CYBERSECURITY SKILLS GAP

Rebecca Vogel[‡]

ABSTRACT

The current consensus is that there is a worldwide gap in skills needed for a competent cybersecurity workforce. This skills gap has implications for the national security sector, both public and private. Although the view is that this will take a concerted effort to rectify, it presents an opportunity for IT professionals, university students, and aspirants to take-up jobs in national security—national intelligence as well military and law enforcement intelligence. This paper examines context of the issue, the nature of the cybersecurity skills gap, and some key responses by governments to address the problem. The paper also examines the emerging employment trends, some of the employment challenges, and what these might mean for practice. The paper argues that the imperative is to close the cyber skills gap by taking advantage of the window of opportunity, allowing individuals interested in moving into the cybersecurity field to do so via education and training.

**Keywords:** cybersecurity skills gap, intelligence, cyber threat

## INTRODUCTION

After the attacks of September 11, 2001, the focus on counterterrorism provided the within the national security and law enforcement communities with additional resources. Although the focus on counterterrorism remains, there are, however, other national security issues that have risen in importance, in particularly cybersecurity.

In December 2008, Australia's then-prime minister, Kevin Rudd, delivered Australia's first National Security Statement (NSS) to Parliament. The NSS articulated the security challenges facing Australia and the federal government's principles and priorities in relation to national security policy. Importantly, the 2008 NSS articulated an important move from a narrow national security approach to an all-hazards, whole-of-government approach. Strategically, this all-hazards approach signaled a shift in thinking about what constituted a national security issue. This change of focus away from counterterrorism, encompassed: organised

[‡] Corresponding author: rebecca.vogel@mq.edu.au

crime, transnational crime (including smuggling of people, drugs and arms), border security, regional stability, and cybercrime. Cybersecurity is an overarching concept for hacking, espionage, fraud, and attacks on critical infrastructure. As such, it is now listed as a key risk area for national security by all of the Five Eyes intelligence partners—Australia, Canada, New Zealand, United Kingdom, and the Unites States.

Traditional crime is increasingly being replicated online through the Internet of Things, therefore enabling criminals to conduct their operations in a covert manner. Organised crime groups, both domestically and internationally, are targeting Australians at an unprecedented rate, with the Australian Crime Commission (ACC) conservatively estimating that serious and organised crime costs Australia $15 billion every year. Though the actual figure is likely to be much higher (Australian Crime Commission, 2015b).

Cybersecurity has also received higher prominence militarily. In 2010, US Deputy Defense Secretary William Lynn, during a ceremony to officially establish the US Cyber Command at Fort Meade, Maryland, declared that cyberspace was as important a military domain as was land, sea, air and space. In January 2012, the former Director of the FBI, Robert Mueller, testified in congress that he expected the cyber risks were likely to surpass the risk of terrorism to national security (Office of the Inspector General, 2015). James Clapper, the US Director of National Intelligence, testified in congress in February 2016 that as a strategic global threat, "The consequences of innovation and increased reliance on information technology in the next few years on both our society's way of life in general and how we in the intelligence community specifically perform our mission will probably be far greater in scope and impact than ever" (ODNI, 2016).

The expansion of national security priorities to include a pronounced focus on cybersecurity has necessitated a change in practitioners' skills (S. Morgan, 2016). The cyber skills that are needed globally include the ability to maintain computer information systems' security, protect them from intrusions and attempts to steal intellectual property, neutralising hacking, malware, viruses, denial-of-service attacks, and phishing. Cybersecurity professionals often control who has access to information, so they need to be able to plan and administer information security programs and conduct computer forensics as well as penetration testing.

But globally, cybersecurity skills are in short supply (Evans & Reeder, 2010). This claim has implications for the intelligence community—including law

enforcement intelligence—to increase the skills of their practitioners in this area. This is because as national security issues—such as espionage, terrorism, financial crime, business insider threats, drugs and arms trafficking, and organised crime—become more complex with implementation of the Internet of Things (IoT), the intelligence community will need remain strategic in its approach to deal with these issues.

The present cybersecurity skills gap that has been identified in the subject literature (Francis & Ginsberg, 2016; (ISC)$^{2,}$ 2015), has implications for security in both the security sector as well as the public sector (S. Morgan, 2016). It follows that this skills gap presents a unique opportunity for IT professionals, university students, and those aspiring to work in the national security industry to become proficient in cybersecurity.

The paper argues that the imperative is to close the cyber skills gap by taking advantage of the window of opportunity, allowing individuals interested in moving into the cybersecurity field to do so via education and training.

## CYBERSECURITY SKILLS GAP

The 9/11 shift in national security priorities focused on counterterrorism, but today other national security threats have increased in priority. Examples relating to cybersecurity are plentiful—e.g. Office of Personnel Management, Anthem, IRS, VTech, Ashley Madison—all occurring in one year—2015. Examples where hackers accessed government and private computer systems, at times, exploiting the vulnerabilities in the security architecture provided by subcontractors working with large organisations. The FBI noted a proliferation in cyber economic espionage cases, including DuPont, Lockheed Martin and Valspar (Federal Bureau of Investigation, 2015).

The speed at which cybercrimes such as fraud, online child exploitation, and payment scams are committed requires a twenty-four-hour international response (Interpol, 2016). Confronting the increase in the assessed level of cyber threats, however, is a gaping hole in the cybersecurity workforce, leading to a global shortage of cybersecurity professionals. As far back as 2010, a report by the US Commission on cybersecurity for the Forty-Fourth President described a "human capital crisis in cybersecurity," saying "there is neither a broad cadre of cyber experts nor an established cyber career field to build upon, particularly within the Federal government," citing a need to expand cyber education and build a

certification system involving large private sector companies, universities with cyber programs and federal agencies (Evans & Reeder, 2010).

Further evidence of the talent shortage is the 2013 report from the US Government Accountability Office which showed a vacancy rate of 22% in jobs within the Department of Homeland Security's National Protection and Program Directorate's Office of Cybersecurity and Communications (U.S. Government Accountability Office, 2013). In 2014, a special Parliamentary Select Committee in the United Kingdom's House of Lords predicted a global shortage of "no less than two million cybersecurity professionals" by the year 2017 (Morgan, 2014).

In 2015, the Global Information Security Workforce Study, a global survey of 14,000 information security professionals by $(ISC)^2$, found that by 2020, the global shortage would still remain at about 1.5 million ($(ISC)^2$, 2015). This aligns with a view from Michael Brown, CEO of Symantec security software, who said demand was expected to rise to six million by 2019, with a projected global shortfall of 1.5 million (Morgan, 2016). Forbes also indicated in a January 2016 article that the cybersecurity market is expected to more than double in size, from $75 billion in 2015 to $170 billion by 2020 (Morgan, 2016).

A 2016 Raytheon survey showed the demand for cybersecurity professionals is growing 3.5 times faster than the overall IT job market, and 12 times faster than the total labour market. This imbalance exists while the global economy is ever more dependent on computer networks as the economic engine, and cybersecurity is becoming an increasing national security concern (Raytheon, 2016).

Numerous factors have combined to create a gap between the number of cybersecurity jobs available and the requisite skills to fill these positions (ISACA, 2015). Some of the factors that have contributed to this void include the increased focus on cybersecurity, a dynamic cyber operating context, and a rapidly evolving cyber risk landscape. In 2015, ISACA and RSA surveyed 649 international cybersecurity professionals as to the depth of this skills gap problem. The results showed that 35% of organisations surveyed were unable to fill security jobs despite the fact that 82% expected attacks. What could be considered more worrying was that 52% of these organisations said that less than a quarter of all applicants had the necessary skills for the position (ISACA, 2015). Lastly, a US Bureau of Labor Statistics report stated that in 2015, more than 209,000 US cybersecurity jobs went unfilled, and postings were up 74% over the previous five years (Morgan, 2016).

In examining the crisis in human capital for the cybersecurity workforce, Fourie et al. (2014) suggested a two pronged approach that encompasses both short-term and strategic solutions. In the short-term, short courses for individuals already in the IT profession, as well as certification for those seeking a credential. For instance, graduate certificate programs (usually completed after one year of study) and graduate diploma programs (two years of study) would allow candidates to gain the necessary skills and transition into cybersecurity roles from other careers. Long-term solutions consist of collaboration between industry, academia and government to run workforce planning exercises with follow-up collaboration to ensure implementation. Fourie et al. (2014) called on academia to collaborate with the private sector to ensure ongoing relevance in the skills being taught; i.e., who could have predicted a decade ago the enormous challenges posed by the "bring your own device" protocols of today.

The responses seen in the Five Eyes intelligence alliance countries indicate an acknowledgement of the critical nature of the need to narrow the cybersecurity skills gap, with policies and strategies aimed at improving cyber skills amongst the national security community. There is a strategic focus within the broader Five Eyes intelligence community on the need to promote computing degrees regarding educational partnerships and increased workforce capability.

**Industry and Government Partnerships with Education/Training Providers**

One of the first examples of these initiatives was the Cybersecurity Challenge UK; its goal was to increase the number of cybersecurity professionals in the UK. Since 2010, Cybersecurity Challenge UK (a not-for-profit British company) has been running IT security-related competitions, specifically aimed at increasing numbers of people skilled in cyber security, to proactively address the skills shortage in the UK. The Challenge includes national competitions and networking initiatives which help identify those with appropriate IT skills, make them aware of educational and training opportunities, and provide career opportunities in the cybersecurity arena (Raytheon, 2015).

The UK government is also working with academia in developing cybersecurity programs—for example, GCHQ—the UK equivalent to the Australian Signals Directorate (ASD) and the American National Security Agency (NSA)—in 2014 gave its stamp of approval to six specific universities in the UK to train cyber experts to combat rising levels of cybercrime and build resilience in

its digital environment (Perry, 2014). In New Zealand there was the Cybersecurity Strategy (2011) that proposed collaboration with academia to meet the demand for graduates in cybersecurity (Fourie et al., 2014).

In 2012, the National Security Agency launched a Cyber Operations Program at four select universities to augment the cybersecurity curriculum and provide technical training (Gupta, 2012). The program was set-up specifically to train students for intelligence, military, and law enforcement jobs that require skills to operate protective networks against a hostile attack. The program was then expanded in 2014 by the NSA in conjunction with the Department of Homeland Security (DHS) to include 44 institutions designated as National Centers of Academic Excellence in Information Assurance and Cyber Defense. The purpose of the expanded program was to promote higher education in these areas and prepare a growing number of Information Assurance and Cyber Defense professionals to meet the need to reduce vulnerabilities in US networks (National Security Agency/Central Security Service, 2014). In January 2015. President Barack Obama and UK Prime Minister David Cameron delivered a joint statement regarding strengthening cybersecurity cooperation efforts and training in the largest companies, citing the "urgent and growing danger of cyber threats" (The Office of the Press Secretary, 2015).

The approaching "fourth industrial revolution" was the theme for the 2016 World Economic Forum, and a global report entitled, *Amplifying Human Potential* was released at the Forum. The report discussed the digital technologies young workers will need to navigate and the skills they will need. The report reiterated the importance of education—that "through education, there is an unassailable opportunity to prepare everyone for such a change (Infosys, 2016)."

The education system, both at a secondary level and the tertiary level, needs to be directly involved in programs to enhance cybersecurity skills. While the tertiary level appears to be moving in the right direction, in 2014, 64% of high school students America did not have access to computer science classes or other classes that would help prepare them for a career in cybersecurity (Raytheon, 2014). Industry experts consider that even if schools place a much stronger emphasis on cyber security, it may take up to twenty years for the skills gap to close (Morgan, 2014).

**Increased Workforce Capability**

In October 2012, the FBI launched its Next Generation Cyber Initiative, which was aimed at enhancing the Bureau's ability to deal with cybersecurity issues. To do this, the FBI sought to hire more computer scientists. While the FBI has made some progress toward this goal, recruitment and retention of qualified candidates is reported to remain a challenge; this is because there are higher salaries offered in private industry (Dunsmuir, 2015). Tellingly, a 2015 audit of the Next Generation Cyber Initiative showed the FBI was not able to hire 52 of the 134 computer scientists it was authorised to recruit, presumably because of the lower wages the Bureau offered (Office of the Inspector General, 2015).

In Australia, the 2013 *Australian National Plan to Combat Cybercrime* identified two key priorities that were intended to strengthen its response to the cybersecurity skills shortage:

1) Improving the capacity and capabilities of agencies to address cybercrime, and

2) Partnering with industry to tackle the shared problem of cybercrime.

The imperative for cyber capacity and capability was explained in the report, saying, "…law enforcement agencies need to keep pace with evolving technologies if police are to perform their duties in the digital environment (Commonwealth of Australia, 2013). Similarly, the Australian Crime Commission (ACC), Australia's national criminal intelligence agency, in its *National Organised Crime Response Plan 2015–18*, cited the need to:

1) progress the priorities set out in the 2013 *Australian National Plan to Combat Cybercrime*, specifically, …improving the capacity and capability of government agencies, particularly law enforcement, to address cybercrime; and

2) develop a technical capability community of interest, comprising a national forum for relevant agencies and organisations to discover and understand the technical capability challenges facing law enforcement agencies nationally that impede investigations into cybercrime and technology-enabled crime, to identify mechanisms to mitigate or address these capability challenges. (Australian Crime Commission, 2015a).

In 2014, the Pentagon announced an initiative that it intended to create a 6,000 strong cyber workforce to defend against threats to American computer networks, citing a challenge to train a cyber workforce, which is expected to run through 2016 (Bottalico, 2014). The US Senate also passed the *Cybersecurity Skills Shortage Bill* in September 2014, granting authority to hire and retain qualified cybersecurity professionals in an expedited manner, pay recruits more competitive salaries, and provide more attractive benefits and incentives (Chabrow, 2014).

Later, in November, 2015, the UK government announced its *National Cybersecurity Plan* (previously known as the National Cybersecurity Programme) (NCSP) to bolster Britain's next generation of cyber security professionals. The plan involved an increase in spending on cybersecurity to £1.9 billion by 2020, and recruiting 1,900 new staff across the three intelligence agencies. The first National Cyber Centre will be established, which will house the UK's first dedicated cyber force. A £20 million competition will be run to open a new Institute of Coding to train cybersecurity students in high-level digital and computer science skills. In quite an innovative move, the plan targets the most talented 14 to 17 year olds, providing them with expert mentors, challenging projects, and summer school to identify and train potential future employees (UK Government, 2015).

## EMERGING EMPLOYMENT TRENDS

The US Bureau of Labor Statistics releases a biennial report on the fastest-growing occupations. Its 2013 report indicated that the information-security profession, including cybersecurity professionals, is expected to grow 36.5% by 2022. This profession is one of only twenty occupations with the highest expected percentage change of employment between 2012 and 2020 (Bureau of Labor Statistics, 2014).

Results of research conducted by KPMG are also indicative of the trend toward "upskilling" within the private sector to protect itself against cyber breaches. In 2014, KPMG surveyed 300 senior IT and HR professionals in the UK within organisations of between 500–10,000 staff and found that companies are "increasingly desperate" to in their quest to hire the right cyber people, with 70% admitting their company lacks the ability to assess incoming threats (KPMG, 2014).

There are positive trends being seen in bridging the gap in cybersecurity skills and reasons for optimism. The 2015 ISACA report showed enterprises are beginning to look at cybersecurity as an issue for the business itself, and not just

for the security manager. Security Operations Centres (SOCs) are being implemented, budgets are increasing, and executive support for security programs is more apparent, helping to elevate cybersecurity programs (ISACA, 2015). Another emerging trend in employment practice is to use Cyber Challenge competitions as a means to vet the cybersecurity skills and know-how of prospective employees. The US Cyber Challenge, in partnership with private industry, is creating "mini-challenges" to be piloted in late-2016, which will allow job applicants to demonstrate their cybersecurity abilities and potential employers to evaluate their skills in real-time (Chabrow, 2016).

## EMPLOYMENT CHALLENGES

There are challenges surrounding developing and maintaining a robust cybersecurity workforce within the national security community, encapsulated in a 2015 article from *The Times of London*:

> Technological skills are at a premium, and the Confederation of British Industry calculates that in three years there will be 600,000 vacant slots for able technological graduates. People who work at GCHQ are on government pay; many could earn far more outside. 'Cheltenham is not much like San Francisco. If you're a techie, this might not be the first place you would want to come,' the head of personnel says (MacIntyre, 2015).

Across the Atlantic, a US report (2016) reiterated similar challenges seen in the Federal Cybersecurity Workforce, namely: 1) demand outstripping supply for cybersecurity professionals, 2) skills gap in cybersecurity positions, and 3) agency strategic workforce plans that do not specifically address cybersecurity workforce needs (Francis & Ginsberg, 2016). Compounding the challenges faced by the cybersecurity skills shortage are those of enticing and retaining the information security experts needed within the National Security space and public sector space more broadly.

The 2014 KPMG survey mentioned earlier indicates a higher "churn" rate for cyber professionals than for IT professionals, and 52% of those IT and HR professionals surveyed agreed there is aggressive headhunting in this field (KPMG, 2014). This presents an obvious challenge to the public sector, as the public sector, with its historically lower salaries, will surely struggle to retain cyber-skilled individuals who can and will be easily headhunted by the private sector, with its much more robust capability to offer attractive pay packages. Private sector entities, including the large Professional Services, Technology and

Financial Services firms, will no doubt increase salaries and compensation packages offered to public sector cybersecurity specialists, effectively cherry picking many of the best potential employees.

A 2015 report by the US Department of Justice highlighted the struggle facing the FBI in attracting computer science recruits, mainly due to low pay (Dunsmuir, 2015). The FBI, responding to the report, said "the cyber workforce challenge runs through the federal government" and that it was necessary to develop "aggressive and innovative recruitment and retention strategies" (Dunsmuir, 2015). An encouraging move to address the pay gap issue was the introduction of US legislation (S.1,691—*Border Patrol Agent Pay Reform Act of 2014*), which incorporated the Department of Homeland Security's Workforce Recruitment and Retention Act, aimed at mitigating the significant problems of successful retention and recruitment, which was passed in December 2014, enabling qualified recruits to be paid more competitive salaries, benefits and incentives.

## IMPLICATIONS FOR PRACTICE

The global cybersecurity skills gap has important implications for the private and public sectors. There is a critical need to address the talent shortage by increasing the number of individuals who have cybersecurity skills. While problematic, this situation presents a unique window of opportunity for those individuals looking to work in the national security community. Current IT professionals, university students and others interested in the cyber domain have abundant opportunities to upskill in cybersecurity areas such as forensic computing, social media exploitation or threat intelligence reporting, and move into this dynamic, growing field.

Numerous government initiatives are in place to address the cyber skills shortage, as well as legislation which will provide the means for the public service to become more competitive in attracting and retaining the best and brightest individuals.

The public service, facing challenges of competition from the private sector in recruitment and personnel retention, will need to innovate and respond in a much more agile way to market forces in order to attract and keep the best cyber personnel. Given the challenges in competing on remuneration, organisations that offer additional benefits on the job, such as ongoing training and professional development, a clear career path within the cybersecurity field, ongoing

engagement with outside stakeholders, vendors and academia, to inform their employees' cybersecurity expertise, will likely have a stronger case for retaining their cybersecurity professionals. These aspects of a strategic workforce planning and retention program will ensure that the next generation of cybersecurity professionals remain engaged in the national security sector to combat the cyber threats of the future.

The implications of the ongoing and growing threat posed by criminal and foreign adversaries are clear for cybersecurity operations and intelligence practice. The gap between the need for individuals highly skilled in cyber and the numbers of cyber-trained intelligence analysts within the National Security and Law Enforcement communities provides a challenge, but also numerous opportunities. Reskilling and upskilling in cyber expertise within the national security community will be important in dealing with dynamic, technically savvy cyber opponents. Creating an agile, skilled cybersecurity workforce is the current challenge. The bottom line is that national security communities will need to invest in their workforce, to improve the cybersecurity capability and capacity of their people through further education and training.

## ABOUT THE AUTHOR

**Rebecca Vogel**, BA, MPICT, Cert HE, is a lecturer in intelligence at the Department of Security Studies and Criminology at Macquarie University, Sydney. Prior to receiving her master's degree, she worked for Dun & Bradstreet as a senior business analyst and fraud investigator assessing high risk businesses. Ms Vogel was also a government licensed private investigator in the US state of Wisconsin. She is a member of the board of the Australian Institute of Professional Intelligence Officers, and the editor of the Institute's journal—the *Journal of the Australian Institute of Professional Intelligence Officers.*

## REFERENCES

(ISC)$^2$. (2015). *Global Information Security Workforce Study*. Retrieved from https://www.isc2cares.org/uploadedFiles/wwwisc2caresorg/Content/GISWS/FrostSullivan-%28ISC%29%C2%B2-Global-Information-Security-Workforce-Study-2015.pdf

Australian Crime Commission. (2015a). *National Organised Crime Response Plan 2015-18*. Retrieved from

http://www.ag.gov.au/CrimeAndCorruption/OrganisedCrime/Documents/NationalOrganisedCrimeResponsePlan2015-18.pdf.

Australian Crime Commission. (2015b). *Organised Crime in Australia 2015*. Retrieved from https://www.crimecommission.gov.au/sites/default/files/FINAL-ACC-OCA2015-180515.pdf.

Bottalico, B. (2014). Pentagon creating 6,000-strong cyber force. *Maryland Gazette*. Retrieved from http://www.capitalgazette.com/maryland_gazette/news/ph-ac-gn-cyber1001-20141001-story.html

Bureau of Labor Statistics. (2014). *Occupational Outlook Handbook*. Retrieved from http://www.bls.gov/ooh/fastest-growing.htm.

Chabrow, E. (2014). Senate Passes Cybersecurity Skills Shortage Bill. Retrieved from http://www.bankinfosecurity.com/senate-passes-cybersecurity-skills-shortage-bill-a-7340/op-1

Chabrow, E. (2016). Adapting Cybersecurity Contests as a Recruitment Tool. *Careers Info Security*. Retrieved from http://www.careersinfosecurity.com/interviews/adapting-cybersecurity-contests-as-recruitment-tool-i-3092

Commonwealth of Australia. (2013). *National Plan to Combat Cybercrime*. Retrieved from https://www.ag.gov.au/CrimeAndCorruption/Cybercrime/Documents/National%20Plan%20to%20Combat%20Cybercrime.pdf.

Dunsmuir, L. (2015). The FBI can't hire enough cyber specialists because it doesn't pay enough. *Business Insider*. Retrieved from http://www.businessinsider.com/r-fbi-understaffed-to-tackle-cyber-threats-says-watchdog-2015-7?IR=T

Evans, K., & Reeder, F. (2010). *A Human Capital Crisis in Cybersecurity*. Retrieved from http://csis.org/files/publication/101111_Evans_HumanCapital_Web.pdf

Federal Bureau of Investigation. (2015). *Economic Espionage - FBI Launches Nationwide Awareness Campaign*. Retrieved from

https://www.fbi.gov/news/stories/2015/july/economic-espionage/economic-espionage.

Fourie, L., Pang, S., Kingston, T., Hettema, H., Watters, P., & Sarrafzadeh, H. (2014). *The global cyber security workforce : an ongoing human capital crisis*.

Francis, K. A., & Ginsberg, W. (2016). *The Federal Cybersecurity Workforce: Background and Congressional Oversight Issues for the Departments of Defense and Homeland Security*. Retrieved from https://fas.org/.

Gupta, U. (2012). NSA Launches Cyber Operations Program. Retrieved from http://www.careersinfosecurity.com/nsa-launches-cyber-operations-program-a-4860

Infosys. (2016). *Amplifying Human Potential - Education and Skills for the Fourth Industrial Revolution*. Retrieved from http://www.experienceinfosys.com/humanpotential

Interpol. (2016). *Coordinating Efforts to Better Combat Cybercrime Focus of INTERPOL Working Group*. Retrieved from http://www.interpol.int/News-and-media/News/2016/N2016-040.

ISACA. (2015). *State of Cybersecurity: Implications for 2015 - An ISACA and RSA Conference Survey*. Retrieved from http://www.isaca.org/cyber/Documents/State-of-Cybersecurity_Res_Eng_0415.pdf

KPMG. (2014). 'Hire a hacker to solve a cyber skills crisis' say UK companies [Press release]. Retrieved from http://www.kpmg.com/uk/en/issuesandinsights/articlespublications/newsreleases/pages/hire-a-hacker-to-solve-cyber-skills-crisis-say-uk-companies.aspx

MacIntyre, B. (2015, ). GCHQ's secret weapons for tracking enemy terrorists and child abusers. *The Times*. Retrieved from http://www.theaustralian.com.au/news/world/the-times/gchqs-secret-weapons-for-tracking-enemy-terrorists-and-child-abusers/news-story/a2381cfb3a695272734fcff7f66690a0

Morgan, L. (2014). Global Shortage of Two Million Cyber Security Professionals by 2017. *IT Governance.* Retrieved from

http://www.itgovernance.co.uk/blog/global-shortage-of-two-million-cyber-security-professionals-by-2017/

Morgan, S. (2016). One Million Cybersecurity Job Openings in 2016. *Forbes.* Retrieved from http://www.forbes.com/sites/stevemorgan/2016/01/02/one-million-cybersecurity-job-openings-in-2016/#17a1fb107d27

National Security Agency/Central Security Service. (2014). National Centers of Academic Excellence in Information Assurance (IA)/Cyber Defense (CD). Retrieved from https://www.nsa.gov/ia/academic_outreach/nat_cae/

ODNI. (2016). *Statement for the Record Worldwide Threat Assessment of the US Intelligence Community Senate Armed Services Committee*. Retrieved from http://www.dni.gov/index.php/newsroom/testimonies/217-congressional-testimonies-2016/1313-statement-for-the-record-worldwide-threat-assessment-of-the-u-s-ic-before-the-senate-armed-services-committee-2016.

Office of the Inspector General. (2015). *Audit of the Federal Bureau of Investigation's Implementation of its Next Generation Cyber Initiative*. Retrieved from https://oig.justice.gov/reports/2015/a1529.pdf.

Omand, D., Bartlett, J., & Miller, C. (2012). Introducing Social Media Intelligence (SOCMINT). *Intelligence and National Security, 27*(6), 801-823. doi:10.1080/02684527.2012.716965

Perry, K. (2014). GCHQ Endorses New Degrees for Tomorrow's Spooks. *Telegraph*. Retrieved from http://www.telegraph.co.uk/education/educationnews/11007644/GCHQ-endorses-new-degrees-for-tomorrows-spooks.html

Pherson, R. H. (2016). Strategic Foresight - Nine Techniques for Business and Intelligence Analysis. Retrieved from http://www.globalytica.com/wp-content/uploads/2016/03/Strategic-Foresight_Nine-Techniques.pdf

Raytheon. (2014). *Preparing Millennials to Lead in Cyberspace*. Retrieved from http://www.consumer-action.org/recommended/articles/preparing_millennials_to_lead_in_cyberspace

Raytheon. (2015). Mission Possible: From Cyber Geeks to Superheroes. Retrieved from http://www.raytheon.co.uk/news/feature/cyber_geeks.html

Raytheon. (2016). Cyber Help Wanted. Retrieved from http://www.raytheoncyber.com/news/feature/blog-cyber60-helpwanted.html

The Office of the Press Secretary, The White House. (2015). Remarks by President Obama and Prime Minister Cameron of the United Kingdom in Joint Press Conference [Press release]. Retrieved from https://www.whitehouse.gov/the-press-office/2015/01/16/remarks-president-obama-and-prime-minister-cameron-united-kingdom-joint-

UK Government. (2015). Spending Review and Autumn Statement 2015. Retrieved from https://www.gov.uk/government/news/chancellor-sets-out-vision-to-protect-britain-against-cyber-threat-in-gchq-speech

- o O o -