MIND THIS GAP: CRIMINAL HACKING AND THE GLOBAL CYBERSECURITY SKILLS SHORTAGE, A CRITICAL ANALYSIS

Stephen Cobb
ESET, USA

Email stephen.cobb@eset.com

ABSTRACT

This paper addresses a number of increasingly urgent questions about the defence of information systems against criminal hackers, the first of which is this: can the world produce enough appropriately skilled human defenders of digital systems to defeat the humans who seek to compromise such systems for nefarious purposes?

Multiple studies suggest that a significant 'cybersecurity skills gap' currently exists and is hampering efforts to defend information systems against criminal hackers. Based on this assumption, many countries are scrambling to increase the supply of cyber-skilled humans capable of making a worthwhile contribution to the defence of the digital infrastructure on which so many economies now depend. Massive education and recruitment efforts are being funded in numerous countries to attract more people to the profession. The success of these efforts is predicated on the assumption there will be an adequate supply of willing entrants who possess the necessary traits and abilities to become effective cybersecurity professionals. In other words, it is assumed that a wide range of people can be trained to become effective cybersecurity professionals, and that enough of them will want to do so.

In questioning that assumption, this paper provides a critical review of existing efforts to assess cyber-aptitude and ability, and considers the results of a number of experimental fast-track cybersecurity training programmes. The challenge of recruiting and retaining participants in a profession that can be both highly demanding and lacking in some traditional forms of job satisfaction is also discussed. To address the problems raised, the paper presents several positive scenarios for consideration in the areas of technology, economics and governance.

1. INTRODUCTION

As the world struggles to preserve the confidentiality, integrity, and availability of the information systems on which it so heavily relies, it faces an urgent question: can we produce enough appropriately skilled defenders of digital systems to defeat threats that range from natural disasters to user errors, from product defects to a growing cast of 'bad actors' who seek to compromise such systems for nefarious and often criminal purposes? This first section of this paper lays the groundwork for some answers and starts with acceptance of the assertion that 'the world struggles' with information security, a reality to which the steady stream of data breaches attests [1–3]. Also accepted is the assertion that the world relies on information systems. As the report titled *A Human Capital Crisis in Cybersecurity* [4] put it six years ago: 'That the nation and the world are now critically dependent on the cyber infrastructure is no longer a matter of debate.'

Section 2 scrutinizes the 'cybersecurity skills gap' and finds that it exists and that, although its exact dimensions and root causes are a matter of debate, it is hampering efforts to defend information systems [5]. In section 3, efforts undertaken to better understand the cybersecurity work that needs to be done are reviewed as a prelude to finding the right people to do the work. Initiatives to establish KSAs (Knowledge, Skills and Abilities) for cybersecurity roles are examined. Section 4 looks at aptitude, a person's propensity for, or affinity with, certain types of work. Aptitude with respect to cybersecurity roles is found to be under-researched.

Section 5 considers the role of personality in a profession that can be both highly demanding and lacking in some traditional forms of job satisfaction. In section 6 the paper looks at several 'gap-easing' scenarios and their implications for cybersecurity. Section 7 draws some conclusions, including recommendations for further research to improve the efficacy of efforts to close the cyber skills gap and to ensure that they are an effective and appropriate use of resources.

2. THE CYBER SKILLS GAP

For the purposes of this paper, the term 'cyber skills gap' is shorthand for the assertion that 'there are not enough people with the skills required to meet the cybersecurity needs of organizations'. There can be little doubt that many organizations today are finding it hard to fill cybersecurity positions and tap cybersecurity expertise. For example, in a 2016 global survey of IT spending, 46% of enterprises said they had a 'problematic shortage' of cybersecurity skills [6]. A 2016 *Spiceworks* study found that 59% of businesses with fewer than 500 employees had no access to a security expert (neither internally, nor externally via a third-party contractor or managed security provider) [7]. In its 2015 *Global Cybersecurity Status Report*, ISACA revealed that 86% of information security managers interviewed believe there is a shortage of skilled cybersecurity professionals [8]. However, it is important to ask whether or not all these problems and opinions really amount to a cyber skills gap, and if they do, we must ask: how wide is that gap?

Worrying numbers

When measuring anything cyber-related it should be noted that the computer security industry does not have the best track record when it comes to quantification [9]. Consider this statement in the *Cisco 2014 Annual Security Report*: 'It's estimated that by 2014 the industry will still be short [of] more than a million security professionals across the globe' [10]. No source or footnote is given for this number, despite the fact that *Cisco*'s annual security report authors are generally more diligent than others in this respect (the 2014 report has 37 endnotes). Furthermore, the statement 'will still be short' makes it seem as if the one-million gap is a prediction from the past, not a documented current reality. Nevertheless, 'one million' was

picked up and repeated not only by journalists and industry experts [11, 12], but by *Cisco* itself, which cited the number in several further reports without clarifying its origins.

Claims about a cyber skills gap seem to originate, at least in the United States, within federal government circles, notably the military. In 2009, Defense Secretary Robert Gates, speaking at the Air War College about the need to 'increase the throughput of training of experts in cyber', admitted that: 'We are desperately short of people who have capabilities in this area in all the services and we have to address it' [13]. In 2010, the *Human Capital Crisis* report, produced by the non-partisan, non-profit Center for Strategic and International Studies (CSIS). framed the problem as one of both depth and breadth, quality as well as quantity [4]:

> 'We not only have a shortage of the highly technically skilled people required to operate and support systems already deployed, but also an even more desperate shortage of people who can design secure systems, write safe computer code, and create the ever more sophisticated tools needed to prevent, detect, mitigate and reconstitute from damage due to system failures and malicious acts.'

In 2009, the non-profit, non-partisan Partnership for Public Service had reported that CISOs and CIOs in a wide range of government agencies – not just the defence realm – were not getting enough good applicants for cybersecurity openings. Furthermore, the report found 'no strategic government-wide assessment of the current state of the cybersecurity workforce… no federal plan projecting how many cybersecurity specialists will be needed… what skills and certifications they should possess, how they should be trained, or how they should be recruited into federal service' [14]. The *Cyber IN-SECURITY* study put the federal cyber skills shortage on the map and, by the end of 2009, the problem was being reported in the mainstream media by journalists like Brian Krebs [15].

Cyber IN-SECURITY also highlighted the government's reliance on the private sector for data about cybersecurity (the report itself was not commissioned or funded by the government). The downsides of such reliance were discussed in a previously referenced *Virus Bulletin* paper [9]. In short, politicians looking for reasons not to increase funding for government activities – like fighting cybercrime or investing in cyber workforce development – can easily discount arguments that are backed by data from parties who stand to gain from that increased spending. Such parties include cybersecurity contractors, product vendors, consultants, as well as educational institutions and certification organizations, whether they are for-profit, like Phoenix University and *SANS Institute*, or non-profit, like Norwich University and *CompTIA*.

Workforce studies

Beyond the federal government and military, the US cyber workforce in general has arguably been experiencing a skills gap for some time. The 2013 *Global Information Security Workforce Study* (*GISWS*), produced by *(ISC)*^{2}, one of the largest non-profit cybersecurity certification organizations, found that: 'Even with past annual growth in the double-digits, workforce shortages persist – 56% of respondents believe there is a workforce shortage' [16]. The report went on to make an important point that will come up again: 'The impact of shortage is the greatest on the existing workforce.' The 2015 *GISWS* reported that the 'information security workforce shortfall' was growing wider [17]. The percentage of respondents who said that their organizations had too few information security professionals had risen to 62%. The study also cast doubt on the ability of market forces to close the gap, concluding that the hiring shortfall was 'less about money' and more about 'an insufficient pool of suitable candidates'.

Industry analyst *Frost & Sullivan* has assisted *(ISC)*^{2} with the *GISWS* for many years. In 2015, *Frost & Sullivan* felt confident in predicting that the cyber skills gap would be 1.5 million by 2020. This number was described as 'the difference between Frost & Sullivan's projection of the workforce needed to fully address escalating security staffing needs and our workforce projection that accounts for workforce supply constraints (e.g., a tightening labor market among security professionals).' [17].

Does that mean that in 2016 the one million mark from *Cisco*'s 2014 report has been reached? It is reasonable to assume as much, as the author has argued elsewhere [18]. In 2015, a news organization that is a project of the Stanford Journalism Program reported that its analysis of Bureau of Labor Statistics found at least 209,000 cybersecurity jobs unfilled in the US [19]. It also found that cybersecurity job postings had been rising rapidly, 'up 74% percent over the past five years'. That equates to a year-on-year growth rate of 15% in unfilled positions, consistent with numerous surveys of industry hiring intentions, census data on company size, and estimates of new entrants into cybersecurity [20]. It is at least plausible to translate 200,000 unfilled cybersecurity jobs in the US into one million globally because the US accounts for far less than one fifth of the world's digital technology users, arguably a useful metric for estimating the amount of cybersecurity work that needs to be done.

Having established that the global cyber skills gap is real, large, and probably still expanding, the paper now turns to the question of how that gap can be closed.

3. CLOSE THAT GAP

As countries around the world work to increase the supply of cyber-skilled humans, education and recruitment efforts are receiving more and more funding [21–23]. These efforts and expenditures raise numerous questions. Who is being trained and recruited? For which jobs? Performing what tasks? Requiring what skills?

Here come the NICE

To its credit, the US federal government has made an effort to answer these questions. In addition to funding sector-specific initiatives at the Department of Energy (DoE), the Department of Defense (DoD), and the Pentagon, the government created the National Initiative for Cybersecurity Education (NICE). The mission of this initiative, which got underway in 2009 and is coordinated by the National Institute of Standards and Technology (NIST), is: 'to improve the nation's cybersecurity education, including efforts directed at the federal workforce'

[24]. NICE has since worked with public and private experts and organizations, federal agencies, and industry partners to develop the National Cybersecurity Workforce Framework (the Workforce Framework) as a necessary first step[1].

The goal of the Workforce Framework, which should not be confused with the NIST Cybersecurity Framework [25], is to establish a standard taxonomy that can be used: 'to describe all cybersecurity work and workers irrespective of where or for whom the work is performed' [24]. By 2014, NICE had resolved cybersecurity work into 31 specialist areas organized into seven categories: securely provision; operate and maintain; protect and defend; investigate; collect and operate; analyse; and oversight and development. The next phase was to identify the knowledge, skills and abilities, the KSAs, required for each role. The combined results are available as an impressive 127-page hyperlinked PDF that enables employers and job seekers to drill down to the competencies required for different roles [24].

Suppose someone is interested in work involving anti-malware skills. Clicking on 'Investigate' in the list of seven categories reveals two specialist areas: investigation and digital forensics. The latter is described as: 'Collects, processes, preserves, analyzes, and presents computer-related evidence in support of network vulnerability mitigation and/or criminal, fraud, counter-intelligence, or law enforcement investigations.' Taking that path reveals three pages containing 39 numbered task descriptions, the first of which is 'Collect and analyze intrusion artifacts (e.g. source code, malware, and trojans) and use discovered data to enable mitigation of potential computer network defense (CND) incidents within the enterprise.' In addition to 'Tasks' there is a clickable tab for KSAs, of which there are 43 (knowledge: 25; skill: 17; ability: 1). Each is listed with the appropriate area of competency. For example, the 'Knowledge of encryption algorithms' entry lists examples and is assigned to the cryptography competency. The 'Skill in performing packet-level analysis' task is assigned to the vulnerabilities assessment competency.

While the Workforce Framework might seem mundane in some respects, it represents a big improvement over the disparate *ad hoc* taxonomies that it seeks to replace. The 2009 CSIS *Human Capital* report described earlier took a stab at this with something called the *Information Security Workforce Development Matrix* [4]. Although only two roles were analysed – CISO and Systems Operations and Maintenance Professional – the matrix included recommended credentials and suggested learning and development sources. This is where another federal government project comes in: the National Initiative for Cybersecurity Careers and Studies (NICCS). The NICCS has linked cyber roles to educational requirements and now hosts a web-based training catalogue that is aligned with the Workforce Framework. This website helps people find the course and education they need for specific roles.

Even before the KSA and training resource aspects of the Workforce Framework were built out, the US Department of Labor had incorporated the seven categories and 31 specialist areas into a broader Cybersecurity Industry Model that starts with 'Tier 1 – Personal Effectiveness Competencies' and builds from there to 'Tier 5 – Industry-Sector Functional Areas', which are the seven NICE categories [26]. The idea is to give employers and employees a broader picture of what a person needs to bring to a job in cybersecurity. Before digging deeper into this aspect of the cyber-staffing challenge, it is important to note other efforts aimed at better understanding the work that needs to be done in cybersecurity.

The smart gap?

In 2011, the DoE commissioned a study by Pacific Northwest National Laboratory (PNNL) into the cybersecurity workforce needs of the energy sector, specifically the KSAs required for securing the smart grid [27]. Evaluating the need for sector-specific workforce certification, such as a Secure Power Systems Professional (SPSP), was one of the goals [26]. The study tapped 28 subject matter experts (SMEs) and used a job analysis questionnaire (JAQ) deployed within the industry to identify 516 tasks as 'potentially relevant for determining the level of expertise and predicting performance' [26]. A collection of more than 100 'performance analysis' vignettes were discussed with employees as a method of job performance modelling (JPM) to 'distinguish the contributions of knowledge, skill, and ability factors in producing effective smart grid cybersecurity job performance'.

In a comprehensive 178-page report, published in 2012, PNNL 'outlined a multidimensional framework for understanding an individual's development and position along a learning trajectory from novice to master'. Dubbed the 'Competency Box', with axes for knowledge, ability and skills [26], this construct went well beyond basic KSAs to include adult intellectual development theory [28], and notions of personality, motivation and interests. The impressive 162-page final report of the project, released in 2014, was a body of knowledge that could 'immediately [be] applied by human resources professionals, recruiters and hiring managers to assist in the recruitment, selection, and training of SPSPs, as well as to identify needed skills to grow existing employees into SPSPs' [29]. To date, this is one of the most comprehensive studies of cyber work and its requirements in a sector-specific workforce context. To what extent the lessons of the study will be embraced by companies in the sector remains to be seen, but clearly they are now better equipped to pursue a coherent and consistent cyber workforce strategy.

As for organizations in general, some general indicators 'as to the kinds of attributes that make one successful in information security' can be found in the *GISWS* [17]. The study analysed thousands of responses from security professionals to the question: 'How would you rate the importance of each of the following in contributing to being a successful information security professional?' The top two items, consistently across multiple years, were: communications skills and a broad understanding of the security field. The study also asked: 'How significant were each of the following skills and competencies in information security in achieving your current position or level?' The top rated items were communication skills and analytical skills, both scoring well above the next item: risk assessment and management.

[1] Disclaimer: the author has served on the NICE Industry Advisory Board.

4. AN APT GAP?

A clear statement of the KSAs required for a particular cybersecurity role is very helpful, as are indicators of how those may be acquired and evidenced (suitable education and certification). However, KSAs alone do not tell job seekers or employers what kind of person will be effective and happy in what role. In other words, KSAs do not address aptitude or personality. The challenge of measuring aptitude – fitting jobs to people and people to jobs – has fascinated generations of psychologists, sociologists, economists, and other assorted academics.

Alpha is for aptitude

One of the first instances of mass-administered aptitude testing was Army Alpha and its companion test for recruits with low literacy, Army Beta. These tests, developed to efficiently assign roles to US military recruits during World War I, were taken by more than one and half million men. Army Alpha built on the pioneering work of French psychologist Alfred Binet, who had sought ways of identifying children with special education needs after France instituted mandatory schooling for ages four to 14 at the end of the 19th century.

Unfortunately, what was developed as the Simon-Binet intelligence test in France and became the Stanford-Binet test in the US, was championed by Goddard, a psychologist who had worked on Army Alpha, but was also a promoter of eugenics. Goddard ignored many of the limitations regarding intelligence testing of which Binet himself had warned, including the observations that intellectual ability was influenced by environment and developed at varying rates. The latter point became central to debates over the relative merits of assigning children an intelligence quotient (for example, using IQ tests like Stanford-Binet) and assessing career aptitude in adults. Pioneers of aptitude testing were eloquent in advocating its benefits to people, society, and industry. Here is one of Army Alpha's developers, psychologist Walter Bingham, writing in 1937, two decades after its initial deployment [30]:

> 'To forge ahead in a field of activity presupposes aptitude for it. Capacity to become proficient in the work to be done, and to find in it a certain zest, is vital to happiness and health of mind, whether in school and college, in business and government, in trade or a profession.'

At the heart of much aptitude research is the two-factor theory of abilities, first proposed by English psychologist Spearman in 1904, which holds that people have both general cognitive ability (*g*) and specific abilities (*s*) [31]. To oversimplify, the latter are reflected in tests of specific abilities, like maths and language, whereas *g* is the kind of general intelligence measured by an IQ test. (Note that the literature refers to *g* as Spearman's *g*, general cognitive ability, and GCA).

Over time, researchers have found that people with high *g* tend to score well on multiple tests of *s*. The implication for aptitude testing is that GCA is a powerful predictor of job performance regardless of the job. As Schmidt put it in 2002: 'The purely empirical research evidence in I/O [Industrial/Organizational] psychology showing a strong link between GCA and job performance is so massive that there is no basis for questioning the validity of GCA as a predictor of job performance' [32]. The title of an extensive 1994 study using data from ASVAB (Armed Services Vocational Aptitude Battery) sums up this position: 'Predicting Job Performance: Not Much More than g' [33].

The implications of the above for cybersecurity recruitment are significant. If you screen applicants using tests that favour those who have pre-existing ICT knowledge, you risk rejecting people who have strong potential for taking on cybersecurity roles. While it can be argued that favouring those with prior knowledge reduces the need for training and speeds the onboarding process, failure to accord appropriate emphasis to *g* might short-change long-term success, given that cybersecurity involves defending a rapidly evolving technology. The ability to acquire new KSAs over time is likely to be critical.

Cyber aptitude

The US military continues to be one of the largest users of aptitude testing. The ASVAB was introduced in 1968 and in recent years it has been complemented by the ASVAB CT or Cyber Test, designed to 'predict training performance in entry-level cyber-related military occupations' [34]. ASVAB CIT is also an indirect measure of 'interest, intrinsic motivation, and skill in a particular area' [35]. In addition, the military has looked beyond ASVAB, funding research into different ways of identifying people who have what it takes to be good at cybersecurity, with several projects nearing maturity according to a comprehensive review by Morris and Waage [34].

One private sector initiative tested by the military is Cyber Talent Enhance, or CTE, from *SANS Institute*. A combined aptitude/skills exam, CTE is designed both to determine aptitude for cyber operations and to assess the current skill set of the test taker based on the *SANS* set of cyber training. Somewhat different is the CATA (Cyber Aptitude and Talent Assessment) test being developed by the University of Maryland Center for Advanced Study of Language (CASL). The goal is 'to predict cyber aptitude beyond assessing general intelligence' [34]. The CATA researchers recognized the need to 'assess aptitude in addition to current skills' because current skills may become obsolete [36]. They also grasped the multi-dimensional nature of different cyber careers, which can require very different requirements. These are mapped in Figure 1 on two axes: proactive/reactive and real-time/deliberate [37].

Work on the CATA is ongoing and its predictive capabilities are still being evaluated. For military and government purposes CATA offers potential advantages over CTE as the latter is a proprietary instrument, presumably with a per-use charge that could add up quickly. In terms of the need to expand our general understanding of what it takes to do well in cyber, there is clearly an academic bias toward open-source tools. Fortunately, some open-source tools are available when it comes to evaluating the factor missing from all of the cyber workforce testing discussed so far: personality.

5. A PERSONALITY GAP

To varying degrees, people can be cheerful or fearful, trusting or suspicious, caring or self-interested. These are all aspects of

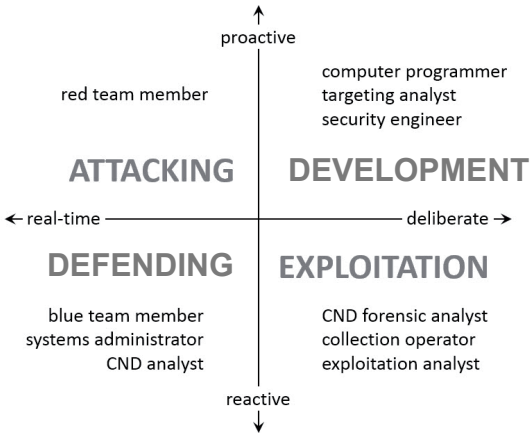

Figure 1: Cyber career dimensions, from Campbell et al. [37].

personality, and numerous studies have looked at how personality traits impact cybersecurity. However, almost all of these studies have focused on users who undermine security, for example by opening infectious email messages. The personality traits of information system defenders have received scant attention. This is not true of some other 'security roles' within society, such as civilian police officers and detectives.

An early example of this type of study, published in 1975, found that 'good police [officers] are characterized by functional intelligence, achievement motivation, and social poise' [38]. Later research into police and personality was reluctant to make such definitive pronouncements. In a 2007 study, Sanders found that 'personality characteristics had no direct bearing on individual officer performance' [39].

Sanders employed 'the Big Five' to determine personality traits. Also known as the five-factor model of personality (FFM), this model transformed personality research in the 1990s and has evolved as an open-source research tool. FFM is focused on five basic personality traits: openness to experience, conscientiousness, extroversion, agreeableness, and neuroticism (acronym OCEAN). FFM has proven consistently useful in a wide range of personality tests, many of which use a set of questions from what is called the IPIP NEO (International Personality Item Pool – Neuroticism, Extroversion & Openness, openly accessible at ipip.ori.org). Frequent testing of these items has enabled a shorter assessment instrument to be fielded while maintaining consistent results. The IPIP NEO Short Form is 120 items as opposed to the original 300, and even 20-item versions have successfully been fielded [40].

When studying federal criminal investigator performance in 2011, Ono *et al.* used FFM along with cognitive ability and emotional intelligence [41]. They found neuroticism (emotional stability) to be the strongest FFM predictor of good performance. In his 2012 thesis, Funicelli found that conscientiousness and extroversion were positive performance indicators in criminal interrogators [42]. In their FFM study of Special Force police officers, Garbarino *et al.* replicated previous findings of law enforcement studies that showed 'police officers are highly extroverted, conscientious and emotionally stable' [43]. At the same time, they found that, contrary to expectations, all officers did not share the same profile and in fact fell into several different personality groups.

FFM is a useful tool with which to examine the relationship between personality traits and job aptitude/performance, even if the findings sometimes show that a wide range of personalities can perform equally well in a particular role. Yet a literature search located only two studies that have applied FFM in a cyber-defender context. The first of these, conducted by Whalen and Gates, involved attendees at a 2004 computer security conference. The researchers found that participants achieved high scores for conscientiousness and low scores for openness [44]. Researchers noted that this might indicate limited ability to respond quickly to emerging security situations, but also observed that this might not be problematic because these particular study participants were less likely to be in operational roles due to the nature of the conference. Indeed, the major accomplishment of the study was to point the way for further research.

Such research appeared in the form of a 2014 Master's thesis by Freed which examined personality characteristics in both cybersecurity and information technology professionals [45]. Freed found that:

> 'Cybersecurity specialists differ from regular information technology employees on six narrow traits from the IPIP NEO Short Form: Trust, Intellect, Vulnerability, Self Consciousness, Assertiveness, and Adventurousness.'

Those six items are facets of the Big Five, and differences between demographic groupings are identified through statistical analysis of survey responses. That these particular differences were identified suggests that, at the very least, the personalities of cybersecurity people may differ from those of IT people. Freed appears justified in her conclusion that: 'These results can be useful in creating training programs specifically geared towards cybersecurity professionals' unique personality characteristics.' [45].

In other words, further research into personality has the potential to improve the ability of organizations to recruit and train for cybersecurity roles. Conversely, research may show that encouraging people to work in cybersecurity just because job openings are plentiful and salaries are high is not likely to be a sustainable strategy for closing the cyber skills gap. After all, what the industry really needs are people who enjoy the work, are good at it, well-suited to doing it, and motivated to keep doing it.

6. SCENARIOS AND SUGGESTIONS

Daunting as the cyber skills gap may seem, closing it has to be considered as one possible scenario when mapping future cybersecurity strategy. Indeed, a closed gap was predicted in the *H4ckers Wanted* report published in 2014 by US think tank *RAND* [46]. The report concluded that existing government efforts and market forces would eliminate the cyber skills gap over time. Unfortunately, that time was put at five to 10 years – hardly helpful to those people who are currently working flat out to protect organizations from today's cyber threats. As the 2015 *GISWS* noted: 'The impact of shortage is the greatest on

the existing workforce' [17]. There is ample reason to think that the current gap is undermining security right now [5].

A growing supply of cyber-skilled workers was not the only factor in *RAND*'s gap-closing scenario. *RAND* also speculated about changes to the demand side of the equation, explained like this: 'By then [meaning the 5–10 year timeframe], the current concern over cybersecurity could easily abate, driven by new technology and more secure architectures' [42]. While many information security professionals would welcome concern abatement – having other interests in life that they would like to pursue – relying on 'new technology and more secure architectures' to solve the cybersecurity problem is arguably a risky strategy. The impact of unchecked cybercrime and cyberconflict prior to any abatement has to be acknowledged, with its potential to erode trust in digital technology, cripple critical infrastructure, foster global instability, and generally retard economic growth.

A scenario in which new technology improves an organization's ability to defend systems to the extent that it can substantially reduce its cyber workforce also begs the question of how this will impact the level of criminal activity in cyberspace. Fighting cybercrime is perennially described as an arms race between defenders and attackers. Improvements to defensive technology typically result in new methods of attack. Disruption of this cycle is not a technical problem; it is a people and policy problem. Criminology research suggests that swifter justice for criminals can have a deterrent effect, reducing the amount of criminal activity that must be defended against. During the last ten years very few serious cybercriminals have been prosecuted within a short time of committing their crimes. During the same period cybercrime has been flourishing. Directing more public resources toward better cybercrime deterrence seems at least worth a try.

One way in which the cyber skills gap could be shrunk without new developments in technology or public policy is through major improvements in human resource (HR) management. There is plenty of anecdotal evidence that qualified applicants for cybersecurity roles are thwarted by HR departments that have not yet embraced the Workforce Framework. They still structure job descriptions unrealistically, while erecting inappropriate skill, experience, and certification barriers to application and entry [47–49]. HR would also serve its customers better if it championed the movement to adopt more inclusive attitudes toward new hires [50], and embrace a reality that even the military has acknowledged [51]:

> 'Genius could arise from various backgrounds. Younger, physically or mentally handicapped, elderly, or overweight people ... could all develop their own genius beside able-bodied military or non-military leaders.'

There are plenty of other measures that could improve an organization's cyber skills acquisition, like encouraging training and development of current employees who exhibit interest in, and aptitude for, cybersecurity roles [52].

6. CONCLUSIONS

This paper concludes that a cyber skills gap – a shortage of people with the KSAs needed to defend information systems against the current level of threats – does exist, and it could exceed one million unfilled positions globally. This gap has the potential to undermine the security of, and trust in, the information systems upon which our world is heavily reliant. So far, efforts to close the gap have improved our understanding of cybersecurity roles and the KSAs required to perform them. However, there is still a lack of research into what constitutes an aptitude to perform effectively in these roles over a sustained period of time. This paper has made the case for such research, from exploring what kind of personality works best in the different cyber roles, to understanding job satisfaction in cybersecurity.

One final thought: there is definitely untapped cybersecurity aptitude and potential out there. Unfortunately, the number of people who can perform effectively over time in key cybersecurity roles may be limited. Further research is needed to determine this, but potentially the number of viable candidates could be lower than the number needed to close the cyber skills gap, unless demand is substantially reduced by major advances in security technology and crime deterrence.

REFERENCES

[1] Chideya, F. Your data is showing: breaches wreak havoc while the government plays catch-up. The Intercept, May 2015. https://theintercept.com/2015/05/27/data-breaches-wreak-havoc/.

[2] Lewis, P. Hackers wreaking havoc in healthcare. IT Canada. May 2016. http://www.canadait.com/index.php/c-level-insight/security/1638-hackers-wreaking-havoc-in-healthcare.

[3] Information is Beautiful. World's Biggest Data Breaches: Selected losses greater than 30,000 records. May 2016. http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/.

[4] Evans, K.; Reeder, F. A human capital crisis in cybersecurity: A report of the CSIS commission on cybersecurity for the 44th presidency. Center for Strategic & International Studies. 2010. https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/100720_Lewis_HumanCapital_WEB_BlkWhteVersion.pdf.

[5] Drinkwater, D. Cyber-security pros blame breaches on skills gap. SC Magazine. April 2015. http://www.scmagazineuk.com/cyber-security-pros-blame-breaches-on-skills-gap/article/409393.

[6] Oltsik, J. High-demand cybersecurity skill sets. Network World. May 2016. http://www.networkworld.com/article/3068177/security/high-demand-cybersecurity-skill-sets.html.

[7] Lemos, R. IT Security Skills Gap More Harmful for SMBs Than Larger Firms. eWeek. July 2016. http://www.eweek.com/security/it-security-skills-gap-more-harmful-for-smbs-than-larger-firms.html.

[8] ISACA. 2015 Global Cybersecurity Status Report. http://www.isaca.org/cyber/Documents/2015-Global-Cybersecurity-Status-Report-Data-Sheet_mkt_Eng_0115.pdf.

[9] Cobb, S. Sizing Cybercrime: Incidents and accidents, hints and allegations. Proceedings of the 25th Virus Bulletin International Conference. 2015. https://www.virusbulletin.com/uploads/pdf/conference/vb2015/Cobb-VB2015.pdf.

[10] Cisco. Cisco 2014 Annual Security Report. http://www.cisco.com/web/offer/gist_ty2_asset/Cisco_2014_ASR.pdf.

[11] Morgan, S. One Million Cybersecurity Job Openings In 2016. Forbes, January 2016. http://www.forbes.com/sites/stevemorgan/2016/01/02/one-million-cybersecurity-job-openings-in-2016/#1ed106a77d27.

[12] Bednarz, A. Cisco estimates a million unfilled security jobs worldwide. Network World. March 2015. http://www.networkworld.com/article/2893365/security0/shortage-of-security-pros-worsens.html.

[13] Real Clear Politics. Secretary Gates Talks to Troops in Alabama. 2009. http://www.realclearpolitics.com/articles/2009/04/15/gates_talks_to_troops_in_alabama_96023.html#ixzz4DNvqTeHg.

[14] Partnership for Public Service. Cyber IN-SECURITY: Strengthening the Federal Cybersecurity Workforce. Booz Allen Hamilton. 2009. https://www.boozallen.com/content/dam/boozallen/media/file/CyberIn-Security_2009.pdf.

[15] Krebs, B; Nakashima, E. As attacks increase, U.S. struggles to recruit computer security experts. Washington Post. December 2009. http://www.washingtonpost.com/wp-dyn/content/article/2009/12/22/AR2009122203789.html.

[16] (ISC)² 2013 Global Information Security Workforce Study. 2013. https://www.isc2cares.org/uploadedFiles/wwwisc2caresorg/Content/2013-ISC2-Global-Information-Security-Workforce-Study.pdf.

[17] (ISC)² 2015 Global Information Security Workforce Study. 2015. https://www.isc2cares.org/uploadedFiles/wwwisc2caresorg/Content/GISWS/FrostSullivan-(ISC)%C2%B2-Global-Information-Security-Workforce-Study-2015.pdf.

[18] Cobb, S. Sizing the Cyber Skills Gap: A white paper. S. Cobb on Security. 2016. http://scobbs.blogspot.com/2016/07/sizing-cyber-skills-gap-white-paper.html.

[19] Satelvad, A. Demand to fill cybersecurity jobs booming. Peninsula Press. March 2015. http://peninsulapress.com/2015/03/31/cybersecurity-jobs-growth/.

[20] ISACA. 2016 Global Cybersecurity Status Report. http://www.isaca.org/cyber/Documents/2016-Global-Cybersecurity-Snapshot-Data-Sheet_mkt_Eng_0116.pdf.

[21] White House. FACT SHEET: Cybersecurity National Action Plan. 2016. https://www.whitehouse.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan.

[22] Curtis, J. UK Gov will double cybersecurity funding to fend off 'ISIS cyber attacks'. IT Pro UK. November 2015. http://www.itpro.co.uk/security/25611/uk-gov-will-double-cybersecurity-funding-to-fend-off-isis-cyber-attacks.

[23] Peters, S. New White House Cybersecurity Plan Creates Federal CISO. Dark Reading. February 2016. http://www.darkreading.com/risk/new-white-house-cybersecurity-plan-creates-federal-ciso---/d/d-id/1324243.

[24] NICE. National Cybersecurity Workforce Framework, website and link to the interactive version. http://csrc.nist.gov/nice/framework.

[25] NIST. Cybersecurity Framework NIST website. http://www.nist.gov/cyberframework/ and NIST Framework document accessed at http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf.

[26] PNNL. Smart Grid Cybersecurity: Job Performance Model Report. 2012. http://energy.gov/sites/prod/files/2013/05/f0/SGC-Report.pdf.

[27] DoE Smart Grid (2016) website. http://energy.gov/oe/services/technology-development/smart-grid.

[28] Ackerman, P. L. A theory of adult intellectual development: Process, personality, interests, and knowledge. 1996. Intelligence, vol. 22, no. 2, pp.227–257.

[29] O'Neil, L. R.; Greitzer, F. L.; Conway, T. J.; Dalton, A. C.; Tobey, D. H.; Pusey, P. K. Secure Power Systems Professional Phase III Final Report: Recruiting, Selecting and Developing Secure Power Systems Professionals. 2014. https://www.controlsystemsroadmap.net/ieRoadmap%20Documents/SPSP_Phase3.pdf.

[30] Bingham, E. V. Aptitudes and Aptitude Testing. Harper Brothers, New York, p.vii. 1937.

[31] Spearman, C. General Intelligence, Objectively Determined and Measured. The American Journal of Psychology, Vol. 15, No. 2. April 1904. pp.201–292. http://www.jstor.org/stable/1412107.

[32] Schmidt, F. L. The role of general cognitive ability and job performance: Why there cannot be a debate. Human performance, 15(1-2), 187–210. 2002.

[33] Ree, M. J.; Earles, J. A.; Teachout, M. S. Predicting Job Performance: Not Much More Than g. Journal of Applied Psychology, vol. 79, no. 4, pp.518–524. 1994.

[34] Morris, J.; Waage, E. Cyber Aptitude Assessment: Finding the Next Generation of Enlisted Cyber Soldiers. The Cyber Defense Review. November 2015. http://www.cyberdefensereview.org/2015/11/16/cyber-aptitude/.

[35] Trippe, D. M.; Reeder, M. C.; Brown, D.; Jose, I. J.; Heffner, T. S.; Wind, A. P.; Canali K. G.; Thomas, K. I.

Validation of the information/communications technology literacy (ICTL) test. 2015. US Army Research Institute.

[36] Campbell, S. G.; Saner, L. D.; Bunting, M. F. Characterizing cybersecurity jobs: applying the cyber aptitude and talent assessment framework. Proceedings of the Symposium and Bootcamp on the Science of Security April, pp.25–27, ACM. 2016.

[37] Campbell, S. G.; O'Rourke, P.; Bunting, M. F. Identifying Dimensions of Cyber Aptitude The Design of the Cyber Aptitude and Talent Assessment. Proceedings of the Human Factors and Ergonomics Society Annual Meeting, Vol. 59. 2015.

[38] Hogan, R.; Kurtines, W. Personological Correlates of Police Effectiveness. The Journal of Psychology, vol. 91, no. 2, pp.289–295. 1975.

[39] Sanders, B. A. Using personality traits to predict police officer performance. Policing: An International Journal of Police Strategies & Management, vol. 31, no. 1, pp.129–147. 2008.

[40] Donnellan, M. B.; Oswald, F. L.; Baird, B. M.; Lucas, R. E. The Mini-IPIP Scales: Tiny-Yet-Effective Measures of the Big Five Factors of Personality. Psychological assessment, vol. 18, no. 2, pp.192–203. 2006.

[41] Ono, M.; Sachau, D. A.; Deal, W. P.; Englert, D. R.; Taylor, M. D. Cognitive ability, emotional intelligence, and the big five personality dimensions as predictors of criminal investigator performance. Criminal Justice and Behavior, 38(5), 471–491. 2011.

[42] Funicelli, M. Personality, Competency and Communicative Suspiciousness Profile of Canadian Police Interrogators of Criminal Suspects, Concordia University Master's Thesis. 2012. http://spectrum.library.concordia.ca/974616/4/Funicelli_MA_F2012.pdf.

[43] Garbarino, S.; Chiorri, C.; Magnavita, N.; Piattino, S.; Cuomo, G. Personality Profiles of Special Force Police Officers Journal of Police and Criminal Psychology, vol. 27, no. 2, pp.99–110. 2012.

[44] Whalen, T.; Gates, C. A psychological profile of defender personality traits. Journal of Computers, 2(2), 84–93. 2007.

[45] Freed, S. E. Examination of personality characteristics among cybersecurity and information technology professionals. University of Tennessee Master's Thesis. 2014. http://scholar.utc.edu/cgi/viewcontent.cgi?article=1126&context=theses.

[46] Libicki, M. C.; Senty, D.; Pollak, J. Hackers Wanted: an examination of the cybersecurity labor market. RAND Corporation. 2014. http://www.rand.org/content/dam/rand/pubs/research_reports/RR400/RR430/RAND_RR430.pdf.

[47] Cobb, S. What the CISSP? 20 years as a Certified Information Systems Security Professional. We Live Security. May 2016. http://www.welivesecurity.com/2016/05/28/cissp-certified-information-systems-security-professional.

[48] Turgeon, W. The IT skills shortage – fact or myth? IT World Canada. March 2016. http://www.itworldcanada.com/blog/the-it-skills-shortage-fact-or-myth/381501#ixzz4Dx4NsFVl.

[49] Sorebo, G. The Cybersecurity Skills Gap: A Real or Manufactured Crisis? RSA Conference. May 2014. http://www.rsaconference.com/blogs/the-cybersecurity-skills-gap-a-real-or-manufactured-crisis#sthash.hGtWCjcA.dpuf.

[50] Schwartau, W. Hiring the Unhireable. RSA Conference (video). March 2016. https://www.rsaconference.com/videos/hiring-the-unhireable.

[51] Alfonso, K. L. A cyber proving ground: the search for cyber genius. Air Univ Maxwell AFB AL Air Force Research Institute. 2010. http://www.dtic.mil/cgi-bin/GetTRDoc?Location=U2&doc=GetTRDoc.pdf&AD=ADA595976.

[52] Florentine, S. 8 tips for recruiting cyber security talent. InfoWorld. January 2016. http://www.infoworld.com/article/3026319/it-careers/8-tips-for-recruiting-cyber-security-talent.html.