2020

Neurodiverse Knowledge, Skills and Ability Assessment for Cyber Security

Joel Scanlan

Andrew Eddy

Teresa Thomas

Tele Tan

Yi-Ping Phoebe Chen

See next page for additional authors

Authors

Joel Scanlan, Andrew Eddy, Teresa Thomas, Tele Tan, Yi-Ping Phoebe Chen, Paul A. Watters, Michael Fieldhouse, Lawrence Fung, and Sonya Girdler

Neurodiverse Knowledge, Skills and Ability Assessment for Cyber Security

Joel Scanlan
School of Nursing
University of Tasmania
Tasmania, Australia
Email: joel.scanlan@utas.edu.au

Paul A. Watters
Cyberstronomy
Victoria, Australia
Email: ceo@cyberstronomy.com

Andrew Eddy
Untapped Holdings
Victoria, Australia
Email: andrew.eddy@untappedholdings.com

Michael Fieldhouse
DXC Technology
Australian Capital Territory, Australia
Email: michael.fieldhouse@dxc.com

Teresa Thomas
MITRE
Maryland, United States of America
Email: tdthomas@mitre.org

Lawrence Fung
Psychiatry and Behavioral Sciences
Stanford University
California, United States of America
Email: lkfung@stanford.edu

Tele Tan
School of Electrical Engineering, Computing and Mathematical Sciences
Curtin University
Western Australia, Australia
Email: T.Tan@curtin.edu.au

Sonya Girdler
School of Occ Therapy, Social Work and Speech Path
Curtin University
Western Australia, Australia
Email: sonya.girdler@curtin.edu.au

Yi-Ping Phoebe Chen
Computer Science and Information Technology
Latrobe University
Victoria, Australia
Email: Phoebe.Chen@latrobe.edu.au

Abstract

Cyber attacks have become commonplace and cause harm to IT systems operated by governments, businesses and citizens. As a result, there has been substantial job growth within the cyber security industry to try and meet the need for network defence. However, due to fierce competition for with the relevant skills there is a shortfall in skilled workers able to fill these roles. The goal of this project is to develop, validate and verify a novel solution for the recruitment of highly competent cyber security staff who can defend our nation against capable and well-funded adversaries. The proposed solution involves the development of a training scheme to train neurodiverse individuals for these roles. There is evidence for their interest and aptitude within the sector, but no research has been undertaken to establish how best to train them in the context of their individual differences.

Keywords Cyber Security, Education, Autism.

1 Introduction

The rapid digitisation of most of the systems we use in our personal and working lives means that the threat of cyber attack is a reality not only for governments or corporations, but for everyday individuals. In 2019, one in three Australian adults was impacted by cyber crime (NortonLifeLock 2020). We frequently hear of large-scale attacks occurring globally, and, in early 2020, we heard of sustained attacks against Australian systems by a state actor (Hitch and Probyn 2020).

Attacks against Australia and other modern western economies, with their sophisticated and interconnected financial markets, and open, democratic norms, aim to achieve tactical or strategic success (Watters et al. 2012). For the private sector, a system compromise is most likely; in the government sector, spear-phishing is the most likely threat (Australian Cyber Security Centre 2017). Losses from cyber events can be categorized as direct and indirect: research indicates that direct losses are typically in the range $1.5-2m for a single data breach (Eling and Wirfs 2019; Layton and Watters 2014). As attacks on important institutions such as hospitals, universities, and government departments become more frequent, a skilled workforce must be available to design, develop and deploy security countermeasures (Caldwell 2013).

The global cyber security "skills crisis" has been well-documented in the private sector (Fourie et al. 2014), affecting Australia's cyber capacity, and that of our allies in the United States. Numerous studies have indicated that, for a variety of reasons, training at all levels has not kept pace with industry demand. This is due to several factors:

- the lack of people with the right combination of aptitude and attitude for training;
- the rise of compliance regimes demanding more skilled workers, such as the General Data Protection Regulation (GDPR) in Europe (O'Gorman 2017), and mandatory data breach reporting in Australia (Abrahams and Griffin 2017); and,
- competition from other fields in ICT which may be perceived as more rewarding and entrepreneurial, such as the blockchain.

What may be less well appreciated is the impact that the 'war for talent' has had on the public sector, including defence and law enforcement. Higher private sector salaries have lured many former public servants, resulting in a reduced capacity for public cyber operations. A number of universities have launched cyber programmes in recent years to try to meet the skill gap, including the Victorian government, who have moved to offer free Certificate IV enrolments in cyber security (Braue 2019).

Given the critical skills shortage, a range of stakeholders have worked hard to identify, and progress, novel strategies for increasing the cyber security workforce. These strategies include engaging more women and girls in cyber (Rowland et al, 2018), strategies focussed on retraining existing cyber workers (Locasto et al. 2011), establishing national cyber leagues (Tobey et al. 2014), and developing new courses designed for non-cognate graduates. While these strategies are individually worthy of pursing, it is likely that there is no single approach, or "silver bullet" likely to provide a solution.

This paper describes a proposed approach for the development, validation and verification of a novel solution to this urgent and pressing problem for Australia's national security: training neurodiverse individuals to fill cyber security roles. The paper will first discuss the justification for the proposed work before outlining the four phases of the work to be undertaken.

2 Justification and Background

Numerous, well-documented cases have come to light in which people diagnosed with Autism Spectrum Disorder (ASD), sometimes referred to in past research under the now-obsolete diagnosis of Asperger's Syndrome (AS), have been associated with successful hacking incidents (Ledingham and Mills 2015). Well-known hackers including Gary McKinnon, Ryan Cleary, Adam Mudd and Lauri Love, have relied on the so-called "autism defence" as an explanation for their behaviour (Davies 2018). What if, instead of losing some highly-skilled people with ASD to the "dark side" of black hat hacking, these individuals could be redirected to work as "white hats", employing the same dedicated focus and attention to detail to the work of protecting the Australian community from cyber-attacks?

Before we consider this possibility further, it is worth stepping back to first understand what ASD is, and the links between people with ASD and cyber security. According to the American Psychiatric

Association's Diagnostic and Statistical Manual, Fifth Edition (American Psychiatric Association 2013), ASD is characterized by a set of impairments, including:

- Social communicative and interaction deficits, including the inability to initiate or maintain shared interests, emotions and/or conversations, alongside a lack of eye contact, lack of facial expressions, and difficulties in understanding relationships; and
- The presence of restricted and repetitive behaviour patterns, including motor movements, insistence on sameness, ritualized behaviours, highly fixated interests, and hypo or hypersensitivity to the sensory environment (including the five senses plus proprioception and vestibular function);

These symptoms must be present from an early age and cause clinically significant impairments, and may co-occur with, but must not be explained by the presence of, intellectual disability.

The prevalence of autism in the US population is currently estimated to be 1:68, or 1.47% (Baio 2014), with a typical 4:1 ratio of males:females. There has been a marked increase in the prevalence of ASD; by comparison, in the 1960s and 1970s, estimates ranged from 0.04-0.2% (Fombonne 2018). While it was initially predicted that tightening the criteria for ASD in DSM-V would reduce prevalence rates (Matson et al. 2012), rates of diagnosis continue to rise. In Australia, 164,000 people have a diagnosis of ASD (Australian Bureau of Statistics 2015) representing a 42.1% increased since 2012, with a widely accepted consensus that this rate will continue its upward trajectory.

The rise in prevalence presents many support challenges, which have both an economic as well as social impact. For example, people with ASD are five times less likely to hold a Bachelor's degree or higher, compared to the rest of the population, and experience high levels of unemployment at a rate of 31.6% (Australian Bureau of Statistics 2015). People with ASD are often under-trained and under-employed, limiting their opportunities and contribution to society, and resulting in a significant financial burden for the government. According to the ABS, individuals with ASD require the greatest support in the areas of cognitive or emotional skills, communication, mobility, health care and self-care. However, too often these support needs go unmet, as evidenced by poor outcomes in major life areas such as employment, despite many people with ASD possessing skills and abilities highly valued by employers.

Given that people with autism have a range of cognitive and psychological skills highly valued in cyber, their ongoing underemployment, and Australia's critical shortage of cyber workers, can we develop a systematic approach to identifying potential cyber employees within the ASD population, who – with appropriate supports – could help solve the cyber skills crisis? The DXC Dandelion Program (DXC 2020), for example, has devised a program of supports enabling cohorts of people with autism to work at a number of large technology companies and banks, using a "pod" structure, where a support team of capability managers, service delivery managers and autism consultants work together to support a technical team. This program has demonstrated that people with autism, given appropriate supports, can deliver value as part of the cyber security and broader ICT workforce at two major Australian banks (ANZ and NAB) and the Australian Defence Organisation. A similar programme has been created by the the Israeli Defence Forces (IDF) called Ro'im Rachok (or "seeing in the future") where IDF members on the autism spectrum in Unit 9900 provide strength in image analysis, such as deciphering aerial and satellite media, looking for suspicious activities or movements (Lorenz et al. 2017). This task requires sustained focus and attention to detail, including being able to identify patterns in cluttered environments. A third example can be seen in Curtin's Autism Academy for Software Quality Assurance (AASQA), which was the first in the world to introduce an integrated program for high school students to transition to tertiary education and employment by adopting a strength-based approach (Curtin Univeristy 2020). It is now supporting close to 250 students in STEM training, industry certification, work integrated learning and internships. It has placed 40 tertiary students into paid internships with businesses including BHP, Woodside, Fortescue Metals Group, Bankwest, Deloitte, Hexagon Mining and State Government Departments.

Specialised programs for those with ASD are growing in number, and the goal of this project is to develop new processes, techniques and technologies to assess and strengthen the capacity of people on the autism spectrum to undertake cyber security work in a verifiable manner.

3 Proposed Work

We propose a four-stage model for this project focused on neurodiverse talent identification (Phase 1), talent development (Phase 2), workplace deployment (Phase 3) and workplace evaluation (Phase 4)

within a cyber security context. This research extends work on Integration of Workers on the Autism Spectrum by examining its application within the cyber workforce (Scheiner and Bogden 2017). We will examine the means by which cyber skills for workers with autism may be specified and developed with a focus on gamification in education as a paradigm to undertake this.

One of the complicating factors about ASD as it pertains to this research is the enormous variability in skill profiles: as Dr Stephen Shore once wrote, "If you've met one person with autism, you've met one person with autism." To address this issue, we need to develop an evidence-based approach to assessing cyber skills potential in a way which is informed by the DSM-V criteria, as well as cyber security education standards such as the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (Newhouse et al. 2017). The NICE Framework provides a highly detailed method to link job categories to specialty areas, work roles, Knowledge/Skills/Abilities (KSAs) and tasks. Situated knowledge has a significant impact on cyber security event detection (Ben-Asher and Gonzalez 2015), while cyber skills can be taught through gamification and similar approaches (Nagarajan et al. 2012). An empirical analysis of cyber abilities found 37 were essential to undertake the role of a cyber officer in a military setting (Diedrich et al. 2018). While cyber skills and knowledge can be readily assessed by traditional cyber tests, abilities are more subtle, and as yet, not well expressed within the NICE Framework at a basic, assessable level.

3.1 Phase 1: Talent Identification and Selection

Our work begins with the conceptual framework for cyber skills developed by NICE, as shown in Figure 1. This framework incorporates a common lexicon of Knowledge, Skills and Abilities (KSAs), relates them to role criticality, and identifies the need to assess proficiency for the KSAs. While NICE proposes that organisations use training and examinations for proficiency assessment, the framework provides no guidance on how best this should be achieved. We propose to extend the conceptual framework by further defining a set of *fundamental* cognitive abilities which underlie the higher-level abilities defined within the framework. We will then validate this approach using confirmatory factor analysis and related statistical tests.

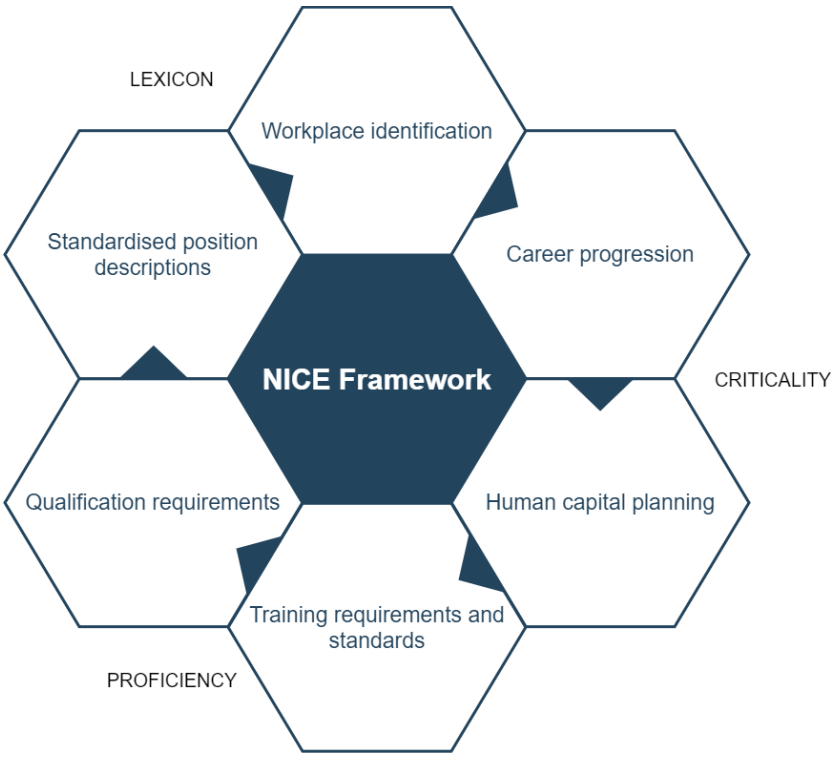

Figure 1. NICE Conceptual Framework

Drawing upon theories of cognition, we will use a *reasoning community of cyber security experts* approach (Kelarev et al. 2010) to identify the fundamental cognitive skills that underlie the 178 higher-level abilities identified under the NICE framework. While this represents a significant amount of effort, the usability of any assessment tool depends on its validity, and we feel that identifying and mapping these fundamental skills will advance the knowledge base of the discipline significantly. Furthermore, we will use a similar consultative process with a pool of adults with ASD to co-design

and validate our approach. "Screening in" individuals who have the potential and capacity to work in cyber security in a robust and scientifically valid way will ensure that those selected individuals will be able to progress their careers, and give confidence to potential employers. We will target both working age adults as well as teenagers who may be interested in cyber security as a career.

3.2 Phase 2: Talent Development

Given our focus on the ASD community, we will develop gamified approaches to enhance fundamental cognitive skills within the cyber security context. Gamification has been proposed as a way of engaging autistic learners that outperforms traditional instruction and assessment, since both intrinsic and extrinsic rewards can be incorporated to increase overall motivation (Ng 2016). There is significant overlap between the goals of Serious Games and some current practices in cyber security training – the use of red-teaming and blue-teaming to simulate cyber security incidents, assess the effectiveness of responses, and improve these through targeted training, is one example (Steinke et al. 2015). By providing a gamified environment, social stress and pressure in the assessment and instruction can be reduced, which may lead to more enhanced approach for an autistic individual's true abilities.

3.3 Phase 3: Workplace Deployment

To validate our approach, using a related topic, one of the authors recently developed an attitudinal test for cyber recruits on the autism spectrum, finding that the results of an attitudinal test battery matched the predicted outcome for participants in around 66% of cases (Watters 2020). The use of serious gamification is novel, and matches our aim of being able to assess fundamental abilities for cyber staff, especially those on the autism spectrum. To manage risk in the project, we will conduct a small pilot study in the first year, building on the success of the work already undertaken. This will be followed by a large-scale deployment with a range of end-user organisations, such as BHP. Working with these end-users, we will provide a range of supports to ensure success, including manager training, provision of training and skill development resources, expectations (such as time commitments), obtaining appropriate buy-in from executives, as well as determining current and future staffing needs in cyber security. Position descriptions will be developed using NICE, and cross-referenced with the norms established for people on the autism spectrum arising from our research in Phase 1. We expect this approach to show immediate success, since the process of recruiting people with ASD can often fail in the early stages, especially where they do not meet social or behavioural norms, such as avoiding eye contact at interviews. Furthermore, by providing the prospect of talent development (through Phase 2 of this project), we believe this will act as an incentive to encourage more people with ASD to engage and develop their knowledge, skills and abilities. A program to promote workplace understanding of neurodiverse talent will also be developed and deployed through this stage.

3.4 Phase 4: Workplace Evaluation

We will implement a range of evaluations throughout the process, from recruitment, talent identification, and workplace deployment. We will build a statistical model of success, including a range of demographic, social and cognitive factors. Over the long term, we intend to do follow-up studies with the cohorts we recruit to establish the impact of the program. In parallel, and depending on the staffing needs of the end-user organisation, we will compare the outcomes achieved through traditional talent selection and recruitment, versus our scientifically-validated approach for people on the autism spectrum. Based on prior experience with the Dandelion Program, we expect to be able to demonstrate not only economic benefits for end-user organisation, but also quantifiable knowledge, skill and ability improvements for our autistic cohort, which ultimately will improve their quality of life and self-esteem whilst reducing reliance on government benefits.

4 Discussion

This research is significant because, for the first time, we will develop an integrated approach to design new processes, techniques and technologies to assess and grow motivation, knowledge, skills and abilities within this new cyber security workforce. We propose a four-stage model of talent identification, talent development, workplace deployment and workplace evaluation; within each stage, there is significant scientific work that needs to be undertaken, building on what has already been established through DXC Dandelion and Ro'im Rachok.

We will identify a comprehensive set of crystallised and fluid cyber abilities and develop an instrument to test these abilities among the ASD population. We aim to advance the knowledge base of cyber security skills assessment by providing better mapping between crystallised and fluid cognitive

abilities, and the knowledge/skills/ability framework adopted by NICE. There is a clear lack of systematized knowledge which needs to be conceptualised, validated and verified before robust cyber ability assessments can be reliably obtained. Our proposed approach of focusing on the identification and fostering of key abilities not uncommonly found among those with ASD is novel and innovative, and allows our partners to identify talent from a group in our communities who are largely under-employed, and yet who, ironically, can be highly skilled in specific areas of interest to cyber security.

Furthermore, we will develop new approaches to the development of these specific skills and abilities using gamified technologies (especially Serious Games), which can be undertaken concurrently with formal study in cyber security. Serious Games may have a range of benefits for individuals on the autism spectrum over traditional computer-based interventions, since they hold greater potential to enhance skills, including those relating to interpersonal communication.

5 Conclusion

This project is aiming to develop, validate and verify a novel solution to an urgent and pressing problem for Australia's national security - the ready supply of the most-skilled cyber security staff who can defend our nation against highly capable and well-funded adversaries. This project is aiming to provide job opportunities for neurodiverse individuals with a career within the cyber security industry.

6 References

Abrahams, N., and Griffin, J. 2017. "Privacy Law: The End of a Long Road: Mandatory Data Breach Notification Becomes Law," *Law Society of NSW Journal* (32:32), pp. 2017–2018.

Association, A. P. 2013. *Diagnostic and Statistical Manual of Mental Disorders (DSM-5®)*, American Psychiatric Pub.

Australian Bureau of Statistics. 2015. *Disability, Ageing and Carers, Australia: Summary of Findings*, Australian Bureau of Statistics Canberra.

Australian Cyber Security Centre. 2017. "ACSC Threat Report 2016," *Australian Cyber Security Centre*.

Baio, J. 2014. "Prevalence of Autism Spectrum Disorder among Children Aged 8 Years - Autism And Developmental Disabilities Monitoring Network, 11 Sites, United States, 2010," *MMWR Surveillance Summaries* (63:2), p. 6. (https://doi.org/10.15585/mmwr.ss6904a1).

Ben-Asher, N., and Gonzalez, C. 2015. "Effects of Cyber Security Knowledge on Attack Detection," *Computers in Human Behavior* (48), pp. 51–61. (https://doi.org/10.1016/j.chb.2015.01.039).

Braue, D. 2019. "Victoria to Upskill Workers in Tech," *Information Age*, Australian Computer Society. (https://ia.acs.org.au/article/2019/victoria-to-upskill-workers-in-tech.html).

Caldwell, T. 2013. "Plugging the Cyber-Security Skills Gap," *Computer Fraud and Security* (2013:7), pp. 5–10. (https://doi.org/10.1016/S1361-3723(13)70062-9).

Davies, G. 2018. "Court of Appeal High Court: Extradition, Forum Bar and Concurrent Jurisdiction: Is the Case of Love a Precedent for Trying Hackers in the UK? Lauri Love v (1) The Government of the United States of America (2) Liberty [2018] EWHC 172," *The Journal of Criminal Law* (82:4), pp. 296–300. (https://doi.org/10.1177/0022018318791670).

Diedrich, T., Cordiero, L., and Coradesque, F. 2018. *Required Abilities for a Cyberwarfare Officer in an Air Flight Squadron: A Curricular Analysis*, Air & Space Power Journal.

DXC. 2020. "The DXC Dandelion Program." (https://www.dxc.technology/au/ahp/142235-the_dxc_dandelion_program).

Eling, M., and Wirfs, J. 2019. "What Are the Actual Costs of Cyber Risk Events?," *European Journal of Operational Research* (Vol. 272), European Journal of Operational Research. (https://doi.org/10.1016/j.ejor.2018.07.021).

Fombonne, E. 2018. "The_rising_prevalence_of_diabe.PDF," *Journal of Child Psychology and Psychiatry* (59:7), pp. 717–720.

Fourie, L., Sarrafzadeh, A., Pang, S., Kingston, T., and Watters, P. 2014. "The Global Cyber Security Workforce - An Ongoing Human Capital Crisis.," in *2014 Global Business and Technology Association Conference*, pp. 173–184.

Hitch, G., and Probyn, A. 2020. "China Believed to Be behind Major Cyber Attack on Australian Governments and Businesses," *ABC News*. (https://www.abc.net.au/news/2020-06-19/foreign-cyber-hack-targets-australian-government-and-business/12372470).

Kelarev, A. V., Brown, S., Watters, P., Wu, X. W., and Dazeley, R. 2010. "Establishing Reasoning Communities of Security Experts for Internet Commerce Security," in *Technologies for Supporting Reasoning Communities and Collaborative Decision Making: Cooperative Approaches*, J. Yearwood and A. Stranieri (eds.), pp. 380–396.

Layton, R., and Watters, P. A. 2014. "A Methodology for Estimating the Tangible Cost of Data Breaches," *Journal of Information Security and Applications* (19:6), pp. 321–330. (https://doi.org/10.1016/j.jisa.2014.10.012).

Ledingham, R., and Mills, R. 2015. "A Preliminary Study of Autism and Cybercrime in the Context of International Law Enforcement," *Advances in Autism* (1:1), pp. 2–11. (https://doi.org/10.1108/AIA-05-2015-0003).

Locasto, M. E., Ghosh, A. K., Jajodia, S., and Stavrou, A. 2011. "Virtual Extension the Ephemeral Legion: Producing an Expert Cyber-Security Work Force from Thin Air," *Communications of the ACM* (54:1), pp. 129–131. (https://doi.org/10.1145/1866739.1866764).

Lorenz, T., Heinitz, K., and Reznik, N. 2017. "A Different Point of View: The Neurodiversity Approach to Autism and Work," *Autism: Paradigms, Recent Research, and Clinical Applications*.

Matson, J. L., Hattier, M. A., and Williams, L. W. 2012. "How Does Relaxing the Algorithm for Autism Affect DSM-V Prevalence Rates?," *Journal of Autism and Developmental Disorders* (42:8), pp. 1549–1556. (https://doi.org/10.1007/s10803-012-1582-0).

Nagarajan, A., Allbeck, J. M., Sood, A., and Janssen, T. L. 2012. "Exploring Game Design for Cybersecurity Training," *Proceedings - 2012 IEEE International Conference on Cyber Technology in Automation, Control, and Intelligent Systems, CYBER 2012*, pp. 256–262. (https://doi.org/10.1109/CYBER.2012.6392562).

Newhouse, W., Keith, S., Scribner, B., and Witte, G. 2017. "National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework," *NIST Special Publication* (800:2017).

Ng, L. E. 2016. "The Gamification of Learning and Research : Technology , Autism and Social Skills," in *Proceedings of the AARE Conference*, Melbourne, pp. 1–12.

NortonLifeLock. 2020. "2019 Cyber Safety Insights Report Global Results." (https://now.symassets.com/content/dam/norton/campaign/NortonReport/2020/2019_NortonLifeLock_Cyber_Safety_Insights_Report_Global_Results.pdf).

O'Gorman, Á. 2017. "Awareness and Perceptions of the Role of Information Management Professionals and Graduates in the Context of Organisational Implementation of the General Data Protection Regulation."

Scheiner, M., and Bogden, J. 2017. *An Employer's Guide to Managing Professionals on the Autism Spectrum*, Jessica Kingsley Publishers. (https://www.amazon.es/Employers-Managing-Professionals-Autism-Spectrum-ebook/dp/B0746TDCFB).

Steinke, J., Bolunmez, B., Fletcher, L., Wang, V., Tomassetti, A. J., Repchick, K. M., Zaccaro, S. J., Dalal, R. S., and Tetrick, L. E. 2015. "Improving Cybersecurity Incident Response Team Effectiveness Using Teams-Based Research," *IEEE Security and Privacy* (13:4), pp. 20–29. (https://doi.org/10.1109/MSP.2015.71).

Tobey, D. H., Pusey, P., and Burley, D. L. 2014. "Engaging Learners in Cybersecurity Careers: Lessons from the Launch of the National Cyber League," *ACM Inroads* (5:1), pp. 53–56. (https://doi.org/10.1145/2568195.2568213).

Univeristy, C. 2020. "Autism Academy." (https://research.curtin.edu.au/projects-expertise/institutes-centres/autism/).

Watters, P. 2020. "Neurodiversity and the Cyber Attitude Test (CAT-B)." (https://profwatters.blogspot.com/2020/08/neurodiversity-and-cyber-attitude-test.html).

Watters, P. A., McCombie, S., Layton, R., and Pieprzyk, J. 2012. "Characterising and Predicting Cyber Attacks Using the Cyber Attacker Model Profile (CAMP)," *Journal of Money Laundering Control* (15:4), pp. 430–441. (https://doi.org/10.1108/13685201211266015).

Copyright