Cyber Talent Management- Inferences for the Armed Forces: A Review Based Analysis

Ramesh Balan[1] and Nandini Srivastava[2]
[1]FMS, MRIIRS, Faridabad
[2]Professor Faculty of Management Studies, MRIIRS, Faridabad

Author Note
Ramesh Balan https://orcid.org/ 0000-0002-0047-0737 is a PhD Scholar at MRIIRS, Fardidabad
Dr. Nandini Srivastava is a Professor & Director, Council for Doctoral Programme (CDP), at MRIIRS, Faridabad

We have no known conflict of interest to disclose.

Correspondence regarding this article should be addressed to Ramesh Balan, DS 266, Arjan Vihar, Delhi Cantt, New Delhi 110010. Email: rbalan66@gmail.com or ramesh_balanphd2019@manavrachna.net.

Abstract

In the information age, operating in and securing the cyber domain is critical for all enterprises. While contemporary literature places substantial focus on the technology aspects of cybersecurity, the related spheres of talent management, skilling, education etc., have drawn relatively lesser attention. Cyber talent is scarce and falls short of the demand. Competition for it therefore is fierce. The matter is further compounded by the organisational culture and peculiarities of the Armed Forces, which militate against effective cyber talent management. Several nation-states are contending with similar challenges, thereby allowing one to draw relevant inferences from material accessible in open domain. It is assessed that measurement of Aptitude, organisational fit and inter-disciplinary Knowledge, Skill and Abilities (KSAs) of potential candidates, coupled with a thrust in favour of specialisation will result in a sustainable way forward. This paper will attempt an exploratory review of the state of identification, sustainment and retention of cyber talent, with a view to arrive at inferences for cyber talent management for the Armed Forces.

***Key Words*:** cyber, talent management, armed forces, inter-disciplinary, knowledge, skill and abilities (KSAs), aptitude, psychology and behavioural traits, general cognitive ability, organisational fit, identification, induction, training, development, professional growth, retention, phasing out

Cyber Talent Management- Inferences for the Armed Forces: A Review Based Analysis

This paperproposesto examinefacets of talent management inan evolving strategic domain, viz cybersecurity, within the organisational context of a nation's armed forces. Talent today is knownto be the fuel of human capital, a core critical asset, the life-blood of an organisation. It is a complex combination of Knowledge, Skills and Abilities (KSAs), of cognitive skills and capacities, of the potential for growth, a reflection of the candidate's suitability for an organisation in terms of values and so on. Further, when one talks of talent management, certain questions beg to be answered, viz, how talent is defined and understood, and whether it is to be seen as an aptitude or a gift. These issues will be tackled in this paper, but only intuitively and contextually, without engaging with rigorous definitions. The context is set out in the contemporary information age where cybersecurity is important, where information is a key lever of state power.

In the information age, operating in and securing the cyber domain is critical for anynation. The domain *per se* has many facets; of which the human dimension assumes importance, in the face of scarcity of cyber practitioners; and the resultant competition. There are other peculiarities too which merit being flagged, such as the development, nurturing and professionalization of cyber talent, to name just a few. In fact, some compare the current state of talent management in the field of cyber to that of medicine and healthcare about two centuries back, to illustrate the associated growth pains and turbulence.

This paper however, goes beyond justcyber talent management. It attempts to explore the management of cyber talent in the context of the need and organisational construct of the armed forces. The armed forces (an instrument of national power)are organisations with a distinct ethos and culture. These organisational dimensions(e.g., the limited scope and flexibility for lateral entry, or the fact that armed forces overtly symbolise the face of Government power) place constraints and restraints, in comparison with say development of cyber talent in the corporate sector or by a non-state/ quasi-state actor. In this backdrop, a clearly defined career growth path for cyber practitioners in the armed forces is yet to take shape. In fact, the entire field - each of the pillars of cyber talent management viz, identification, development and retention of talent – may need to

DOI: 10.9756/INT-JECSE/V14I4.23

be re-cast. This is a difficult task, as observed by Max Smeets in his recent article on "building a cyber force", published on the 'War on the Rocks[1]' site. By extension, study and implementation of cyber talent management for the armed forces is hugely important at the national strategic level.

As nations grapple with this matter to arrive at a sustainable model for cyber talent management for the armed forces, it is but natural for researchers to turn to the limited documentation (be it in textual or audio-visual format) available in open domain, howsoever opaque, to adroitly derive customisable context-specific inferences. Such inferences may be sifted and examined at the individual level e.g., measures pertaining to (identification, development and retention of) a prospective cyber domain candidate; and at the organisational level e.g.,organisational structuring, transformation, specialisation and defining a sustainable career path for cyber-practitioners.

This paper will attempt to establish the need for, and undertake an exploratory survey of the steps associated with cyber talent management for the armed forces.

Establishing The Need

We live in the information age. Since warfare inherently takes on the characteristics of its age, and war is affected by technology in all its forms (Creveld, 1991),the information domain today has become the new domain and environment in which nation-states, non-state actors and individuals, all operate and steer their respective objectives. For a nation-state therefore, the information environment is comparable to land, sea, air and space (Kozloski, 2009), except that it is overarching and all-encompassing. Thus,prosecution of psychological and cyberspace operations can be viewed as a natural response to the challenges and opportunities created by the Information Age. It hardly needs emphasis that such operations are being waged incessantly, relentlessly, and globally.

Given that the cyber domain presents occasion for some really serious risks to national security and economy, it clearly is a front-line challengefor the 21st century(Govt, 2011). Accordingly, it behoves of all nations, to prepare to protect and defend themselves in cyberspace against all forms of threats – regardless of the threat actor (state/ non-state -/quasi -state, criminal etc.). The form of defence *per se* could be proactive or reactive; active or passive. The *US Defence Department Cyber Strategy, 2018* for instance propounds a proactive philosophy, viz., *defend forward* – actions takento disrupt or halt malicious cyber activity at its source - which some interpret as inherent authorisation for intelligence gathering and/ or setting the stage for battle, disruption or or even dismantling of an external network, if deemed a threat to U.S. interests.

So much for the cyberspace i.e., the data and IT infrastructure spanning the physical and information layers of the information environment. The cognitive layer of the information environment, constituted by the mind (of individuals and the society) alsomerits consideration. It is illuminating to take into account a British analyst, Ben Nimmo's perspective on information warfare (IW) strategy as cited in Legatum Institute's compendium on propaganda (Information at War: From China's Three Warfares to NATO's Narratives, 2015). According to him, while the Western model of waging IW appears to be a situation-specific, time-limited, response aimed at achieving a pre-defined end-state, the Russo-Chinese model of IW seemingly views it as an open-ended, continually ongoing activity, applicable across the board, in perpetuity. Either way, IW is a real threat. Therefore, can any nation let its guard down, be it against adversary's cyber warfare or IW?

Inferences from International Practise

In this backdrop, it would take extraordinary naiveté for any nation to overlook the measures required to enhance operational preparedness in the cyber/ information domain. Now, contemporary literature is replete with publications and grey literature which expound on operational philosophy or deliberate on various facets of the associated People, Process and Technology (PPT) triad. Less common however, is discussion on talent management in this field. In Cybersecurity and Cyberwar, strategist Peter Singer asserts, "we often frame cybersecurity as a technology problem. Instead, it is a human problem." Hence, we must turn attention to sustained capacity building in terms of a professional cyber workforce, with urgency and precedence(Fortson, 2017).

Cyber talent management presents a unique set of challenges which extend across various dimensions, such as identification (and selection), induction, sustainment (and development), retention, and phasing out. Further, these challenges when viewed from the perspective of the armed forces, get compounded, as the latter are beset with own peculiarities. Classically, armed forces the world over are products of the industrial age. They can scarcely be characterised ascontemporary, agile or nimble with regard to talent management or specialisation.

Characteristic of open societies, Western bloc countries, have published papers/ articles/ books on defining and identifying the challenge related to management of cyber talent; suggesting viable approaches; and finally reviewing the progress made. While not all, at least some of this body of knowledge is accessible to the

[1] https://warontherocks.com/2022/05/building-a-cyber-force-is-even-harder-than-you-thought/

DOI: 10.9756/INT-JECSE/V14I4.23

lay public. However, in contrast, such depth of knowledge in respect of countries such as Russia, China, Iran, North Korea, Israel and other leading cyber-proficient nations isnot easily traceable in open-source literature. This difference is partiallyattributable tocultural-lingual factors which govern a nation's general outlook. But it is also true that this body of knowledge falls in what nations classically view as classified domain; which needs to be understood and respected.

Scope and Treatment of Cyber Talent Management

For ease of treatment, the balance of this Section covering inferences from internationalpractise is thematically organised as a literature review under varioussub-heads of talent management, such as identification and selection; induction; training and development; professional growth; retention; phasing out etc.

Identification and Selection of Cyber Talent

Researching the methodology of selection and evaluation of computer personneli.e., 'programmers' in the early days of electronic data processing, viz., late 1950s and early 1960s, the authors recognise and posit the need for a structured mechanism for identifying aptitude or intelligence in prospective candidates as discussed by(Mayer & Stalnaker, 1968). However, the effectivenessof such an approach in meeting the desired goals for selecting both trainees and experienced programmers remains moot, suggesting need for custom-built approach to tackle either.

Today, the focus of attention has shifted from the domain of electronic data processing or IT to that of cyber security. But the challenge is similar, as there is a shortage of skilled cybersecurity workforce, as commented variously in mediaarticles by(Davidson, 2015), scholarly work by (Cobb, 2016), think tank analyses by(Crumpler & Lewis, 2019; De Zan, 2019) and Government reports (Key Issues: Cybersecurity Challenges Facing the Nation – High Risk Issue (Accessed in April 2020)). As a consequence, institutionalised response along with requisite oversight have been put in place by certain countries such as United States, United Kingdom, Australia, European Union etc. The NICE (National Initiative for Cybersecurity Education) Cybersecurity Workforce Framework or NCWF, (Petersen et al., 2020) is one such example of a national response to the cybersecurity skills shortage. Apowerful reference framework, the NCWFrecognises the inter-disciplinary nature of cybersecurity and serves as a broad guidancecovering thework, job profiles, and knowledge, skills, and abilities (KSAs) associated with the cybersecurity stance of an organization. In so doing, it facilitates better understanding, and provides a standard vocabulary across employers and prospective employees[2].

Literature review suggests that cybersecurity is a multi-/ inter-disciplinary field; and cyber talent identification (amongst prospective candidates) has been explored using a few distinct approaches, based on individual facets or dimensions - such as 1) aptitude;2) knowledge, skills and abilities (KSAs);3) psychology and behavioural traits;4) General Cognitive Ability (GCA); and 5) organisational fit. At times a combination of some (but not all) of these facets has been suggested. Each of these facets of cyber talent identification, as shown in **Figure 1** below, is discussed in succeeding paragraphs, preceded by a brief consideration of the multi-/ inter-disciplinary nature of cybersecurity.

[2]National Institute of Standards and Technology Special Publication 800-181, Revision 1, available at https://doi.org/10.6028/NIST.SP.800-181r1

DOI: 10.9756/INT-JECSE/V14I4.23

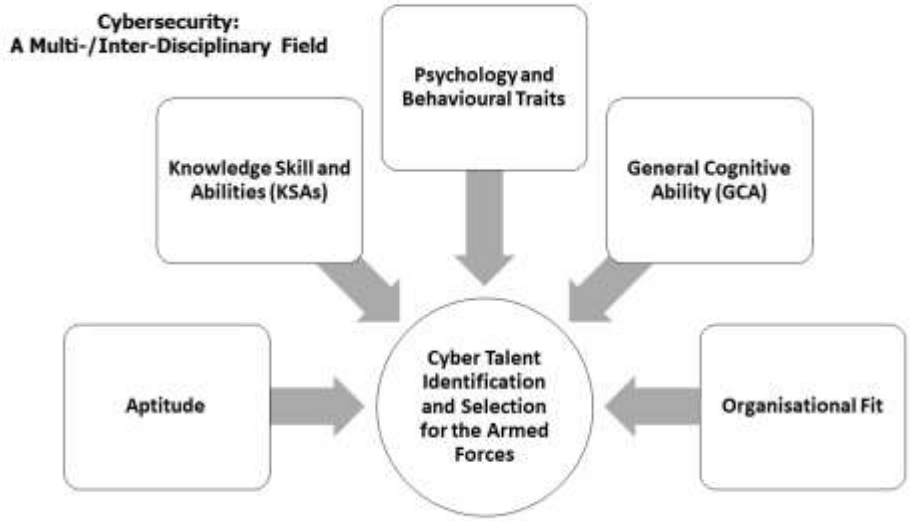

Figure 1: Dimensions/ Facets of Cyber Talent Identification and Selection for the Armed Forces, Source: Self Created

Multi-/ Inter-Disciplinary Nature of Cybersecurity. The authors (Dodge et al., 2012) observethat (cyber)security is a multi-/ inter-disciplinary field, quitelike health care. Just like health care requires a complete ecosystem of practitioners (medical-, para-medical- and nursing-staff), and a matching support environment, so does cybersecurity in terms of an ecosystem of complementary skills – ranging from the extremely specialised, technical to diverse, general ones. Noting that only 50% of cybersecurity is a technical challenge, Stephen J. Lukasik of Georgia Institute of Technology, advocates a versatile and integrative approach to cybersecurity. He opines thatbeyond just technical expertise, proficiency in subjects like law, diplomacy, and management isalso required.

The idea that a broad range of expertise (inter-disciplinary and multi-disciplinary) can lead to a qualified cybersecurity employee, and that a background in science/ technology is not required for all protagonists in the cyber field is also articulated in the DoD Cyberspace Workforce Strategy of 2013. As per (Waage & Morris, 2015), the Strategy document of 2013 *ibid*, also stresses the requirement to assess aptitude and consider qualifications. With the aim of identifying DoD personnel to tenant cybersecurity positions, the document discusses methods for talent identification – e.g., an individual'slogical and analytical abilities,or his aptitude - as tools for recruitment way back in 2010-11.

Aptitude. People have varying job-related cyber-aptitudes (Campbell et al., 2016). For example, some are naturally oriented to network defence, a cybersecurity job-role,(Gutzwiller et al., 2016). Once, detected, these aptitudes, can potentially be tapped to achieve a better match of candidate to a job description(as elaborated in U.S. Government report, entitledNICE (National Initiative for Cybersecurity Education) Cybersecurity Workforceframework (NCWF)[3]). (Campbell et al., 2016), proposes a framework for classifyingcybersecurity jobs in accordance withrole-specific cognitive demands (*vis a vis*KSAs).Building on the idea, (Saner et al., 2016) deliberate on the relevance and challenge of concisely characterizing work roles so that a cyber-aptitude battery test can be developed. However, (Campbell & Bradley, 2018)gracefully acknowledge that the cyber aptitude based approach for talent identification is still a work in progress. Thus, it can be inferred that the aptitude-based approach for talent identification is yet to mature fully.

KSAs. An alternate approach for identifying cyber talent accords precedence to a blend of technical proficiency, subject matter expertise, and congeniality(Dawson & Thomson, 2018). The Paper also suggests social and cognitive metrics which could be used to indicate candidate's future performance. Use of certain cognitive attributes amongst cybersecurity workers foridentification of cyber talent has also been proposed

[3] The National Initiative for Cybersecurity Education (NICE) Framework for the Cybersecurity Workforce (NCWF) itself emerged from multiagency effort. A pioneering role was played by the National Institute of Standards and Technology (NIST) in consultation with the Department of Homeland Security, USA. The frameworkarticulates the broad blueprint for standard job functions in the cybersecurity domain. The final product (Newhouse et al., 2017) emerged after sustained effort and refinement. This has since been replaced by Revision1, published in 2020.

DOI: 10.9756/INT-JECSE/V14I4.23

(Caulkins et al., 2016).Finally, identification of cyber potential particularly in the military context - based respectively on skills and abilities; and systems thinking- has also been suggested(Canali et al., 2017).

Psychologyand Behavioural Traits. A complementary approach to cyber talent identification, is based on assessment of human psychology and presence of of certain behavioural traits. A hacker for instance can be characterised as someone who thinks outside the box; and dabbles in probing system weaknesses out of curiosity (Schneider & Mulligan, 2011; Smith et al., 2008). He possesses above average IQ and great technical and problem-solving skills (Chiesa et al., 2008). Definitive characteristics of hacker behaviour (criminal context) are covered by (Van Beveren, 2001). He dwells on constructs such as flow[i.e. complete immersion], attention focus [i.e. absorption], curiosity, intrinsic interest [in the activity*per se*], and control (Seligman & Csikszentmihalyi, 2000). Going further, hacking behaviour is unravelled by(Jordan & Taylor, 2004)as an urge to hack, inquisitiveness, attraction to dominance and might, and peer acceptance.

Distinctive traitsof hackers comparable to those found in artisans engaged in craft-work e.g., a typical mentality; focus on skills; being possessive of their tools and work outcomes; commitment; absorptionin the process; tendency to transgress laid-down bounds; an affiliation to guild-like social and learning structures; and association with a common subjective experience(Steinmetz, 2015). In fact, a hacker requires a combination of systematic thinking and logical reasoning; and extraordinary technical ability(Summers et al., 2013).

(Libicki et al., 2014), suggest *inter alia* that a hacker is a savvy, curious, quick learner with natural ability to absorb technical information and techniques. All hackers are not motivated by the same inducements. Insatiable curiosity coupled with a strong urge to understand the internals of how things work, is probably a better indicator of high-end cybersecurity capabilities as against educational qualifications or even professional certifications.

Behavioural traits and psychological characteristics associated with cyber warriors are further developed by (Barbar, 2001; Hald & Pedersen, 2012; Rogers, 2013; Rogers, 2006; Seebruck, 2015). (Shropshire & Gowan, 2015)focus on the team psychology required amongst cyber practitioners. The Paper notes that conscientious-ness and open-ness are common attributes amongst top performers; and that they exhibit a strong preference for theoretical activities such as the pursuit of truth. In view of the foregoing, screening of prospective candidates based on traits, skills and motivations of cyber practitioners is recommended (Smith, 2007).

General Cognitive Ability (GCA).There exits yet another theorygrounded in the benchmarking of GCA, through psychometric testing, as an indication of apt, and potentiallytrainablecyber talent. In accordance with this theory, any suitably qualified,intelligent person can be employed in cyber assignments (Hernandez & Johnson, 2014). The Israel Defence Forces (IDF) seemingly follows such an approach. It seeks candidates with general traits such as observation, analysis, problem solving, capacity and eagerness to learn, socialadjustment, and leadership, with the belief that these would fuel success in the security and IT fields(Asher-Dotan, 2018). Further, given the former, they feel that the selected candidate's technical proficiency can always be cultivated.

Organisational Fit. A related yet important aspect in the context of the armed forces is the need for *organisational fit*(Soley, 2018).A soldier's professional integrity, for instance is one of the attributes of *organisational fit*. Contextually, a conscientious cyber/ information warrior may well have to contend with a persistent struggle between his personal values and organisational demands. Opinion will always be divided on whether Bradley Manning or Edward Snowden were morally right in blowing the whistle. But regardless of individual dilemma, a nation's armed forces can ill-afford the compromise of operational security and resultantembarrassment – caused by leaking sensitive national/ organisational information (Cleave, 2013). Insofar, professional integrity, and attitudinal attributes such passion/ motivation and team-spirit as dimensions of organisational fit, will be rightfully demandedby the armed forces from its cyber warriors.

Research Outcome

While fulfilment of technical proficiencyby a prospective candidate is a necessary condition for cyber talent identification, it may not be sufficient, because of the multi-/ inter-disciplinary nature of cybersecurity. Several complimentary approaches to cyber talent identification/ selection – such as aptitude, KSAs, behavioural and psychological traits, GCA and organisational fit, to name a few - have individuallyfound consideration by various scholars. Certain authors have implicitly examined a combination of some approaches. However, thus far discussion of a comprehensive, multi-dimensional model for cyber talent identification and selection has not been noted.

While, the armed forces may desireto induct the best available cyber talent based on aptitude,and/ orpsychology and behavioural traits, such candidates may not always fulfil otheressential criteria which govern their selection and induction. In many countries, military officer-candidates are shortlisted through an IQ test (as a measure of GCA); and screened by the Services Selection Board(for assessment of organisational fit, and suitability of psychology and behavioural traits). However, aptitude does not appear to be a selection criterion. Whether it can be invoked, is worthy of study. The current approach of selection of prospective officer-candidates in use by the armed forces can perhaps be extended to the domain of cyber talent identification and selection too, with some refinement, as it would assist in flexible billet management - a functional organisational

DOI: 10.9756/INT-JECSE/V14I4.23

need. While this is expected to obviate the need for endorsingcyber-gladiators *per se*, will it prove equal to the need of modern day incessant, non-contact war, where specialisation is the order of the day?The armed forces do not subscribe to lateral induction largely. But is there a case for a shift in stance, particularly in the context of cyber warfare?If so, quantification of prior experience, aptitude, and KSAsrelated to the cyber domain, can constitute an important measure. These nuances merit deliberation.

Induction of Cyber Talent

Both talent and knowledge management contribute to selection, and maintenance of the required expertise in cyber security assignments(Fontenele & Sun, 2016). Simultaneously, job-fit and potential for cyber knowledge have been identified as independent factors for selecting cyber warriors for the armed forces (Canali et al., 2017). Citing James Lewis, of the Centre for Strategic and International Studies (Dodge et al., 2012)highlight the lack of correlation between the training imparted to cyber professionals *vis a vis* their actual job profile or job-related competencies. Continuing in the same vein,it is for consideration that job-recruiters are often handicapped frombeing effective owing to a knowledge gap(Galliano, 2017).

It is also note-worthy that the armed forces are normally characterised by pre-defined terms and conditions, e.g., ages of recruitment and release. In comparison with the corporate world, this introducesinflexibility, whichin turn precludes mid-career opportunities for lateral inductioninto or exit from the military.In the rare instance that lateral induction isfacilitated by way of say a deputation,the specification-mismatch between the job characterisation andcandidate profile descriptioncan hobble the process (Nakayama & Sutcliffe, 2007). Excessive latitude and limited quantification of job description,can result in poor candidate-job match. Apropos, (Fontenele & Sun, 2016; Fontenele, 2017) suggest a 'robust method' for selecting, ranking and evaluating cyber-experts in the context of lateral induction, given a set of criteria/ profile. Various flexible options generated in the context of cyber warriors from the U.S. Marine Corps are discussed by(Ramsey, 2020); whereas (Curley, 2018)proposes maintenance of virtual reserve for providing a surge capacity,on demand.

Discussion

In case the armed forces intend to have uniformed personnel assigned to key cyber roles, they will need to generate flexible options to tackle *inter alia*induction of cyber talent. Some of the supplementary measure could be to accept candidates on deputation i.e.,lateral induction, hiring civilian cyber talent, leveragingupon reservists, and focusing purely on cyber talent (aligned to job needs), rather than rigidinsistence on adherence to archaic and irrelevant standards. Of course suitable checks and balances would need to be instituted to ensure that undue advantage is not taken of these relaxations, *per se*.

Training/ Development

The need to focus on cyber education is well documented in literature. The range of treatment spans a number of issues – from sharp focus on enhancement of technical skills to in-depth mastery of concepts/ knowledge; from broad-based multi-disciplinary study to content-based education; from development of curriculum and assessment to technology-aided delivery of knowledge. And yet, specific issues related cyber training in the context of the armed forces have received less coverage in open domain.

There is need for structured and holistic programmesfor cyber skilling, based on a combination of degree programmes and certifications - be they industry-endorsed or vendor-specific(Campbell et al., 2003). There is also need for subject-specific educational programmes whose scope ranges from cybersecurity specialisation within extant academic programmes to newly designed specialized cybersecurity degrees(Andel & McDonald, 2013). A holistic cyber education paradigm within the required general education programme – multi-level, multi-discipline, both technical and non-technical, running like a thread through an institution's entire curriculum is advocated by(Sobiesk et al., 2015).(Dawson & Thomson, 2018)lament the lack of discerning measurables connected with cybersecurity e.g., cognitive disposition, job roles, organisational structures etc., even as they emphasise multi-disciplinary skills.

Industry certifications play a role complementary to academic curricula in enhancing hands-on skills while simultaneously expanding a participant's horizon(Hentea, Dhillon, et al., 2006). (Hentea, Dhillon, et al., 2006; Whitman & Mattord, 2004), encourage review of curricula and evaluation mechanism, with focus on multi-disciplinary education and skilling so that the end product is responsive to the needs of the industry. (Mills et al., 2015)present a compendium of continuing education for a cyber-professional in the hope that it would lead to development of relevant tactics, techniques and procedures (TTP).

(LeClair et al., 2013)lead the chorus for an inter-disciplinary approach to cybersecurity education; and suggests how instructional technologies may be integrated with online cybersecurity education. (Alvarez et al., 2016) argue in support of experiential/ heuristic learning, and bring out how the online medium and simulations can vastly assist in the cyber domain. (Caulkins et al., 2017)emphasise realistic training, through simulation of the operational environment.

Analysing the 2017 edition of the NICE Cybersecurity Workforce Framework (NCWF) in terms of job descriptions, career paths and associated academic eligibility criteria,(Jacob et al., 2018)observe that itis focused more on technical content. Continuing in the same vein(Jacob et al., 2020), examine the need for a responsive training and education system to meet the emerging requirement of inter-disciplinary treatment of cyber

DOI: 10.9756/INT-JECSE/V14I4.23

security whether it be in terms of direction, content or techniques. As a case in point, the authors discuss the impact of the legal, economics and criminology perspectives on cybersecurity and *vice versa*. Finally, the authors underscore the importance of cybersecurity knowledge for stake-holders (hailing across technical *and* non-technical backgrounds).

Notwithstanding, there are only a select few papers in open domain that engage in a context specific treatment of cybersecurity training as applicable to the armed forces. (Spidalieri, 2013) establishes that military institutions of higher learning must help blend postulate and precept, with practise and performance. The new strategic cyber military hierarchy must clearly appreciate the cyber environment, coupled with an in-depth understanding of international relations, geo-politics, law, strategic studies and related sciences in order to leverage cyber capabilities adequately. (Spidalieri & McArdle, 2016) dwellon how the cyber training academies of the armed forces can play a comprehensive role in the development of cyber-capable strategic military leaders. Further, the authors identify gaps in existing curricula and make relevant recommendations. (Furnell & Matt, 2020)acknowledge the criticality of specialisation in cybersecurity. There is also need for special programmes, hackathons etc., to cultivate talent(Allen & Herr, 2019).

Research Outcomes

In cyber skilling, a range of issues need to be comprehensively addressed. While in-depth role-specific specialised technical KSAs are crucial, muti-disciplinary exposure too is critical. Concurrently, a different line treatment of training is required to develop cyber-capable strategic leaders. Some facets of this aspect have been discussed by(Parilla & Wills, 2021). Further, the average soldier should be capable of both personal cyber hygiene and as a first line of defence for the cyber assets in his area of responsibility. Offensive cyber capability could be developed in a chosen few. There is also need to leverage technology for online delivery of training content and participation in cyber wargames/ hackathons.

Professional Growth

Sustaining any profession in the organised sector needs defined entry-level educational benchmarks, and a well charted career path, for growth. In this context, the National Research Council report(*Professionalizing the Nation's Cybersecurity Workforce?*, 2013) examines two principal issues, viz, firstly the advantages that might accrue out of professionalization of cybersecurity workforce (akin to health-care workers)- in terms of regulating capacity development and capability building in the field; and secondly, the criteria the Government should consider when taking a view in this regard.CISA report (*Cybersecurity Career Paths and Progression (Page 18 Cybersecurity and Infrastructure Security Agency)*, 2019)builds on career progression and pathways in the cyber profession and discusses the same under three heads viz, early exposure to technology, cybersecurity career pathways and cybersecurity career progression.

(Schmidt et al., 2015)endeavour to draw applicable lessons for the armed forces from the commercial sector with respect to best practices and processes, primarily in cyber defence. They correctly note that hardly any commercial enterprises operate at the scale and threat horizon of the armed forces(Conti et al., 2014).

(Borum & Sanders, 2015) dwell on gathering and processing of cyber intelligence by maintaining surveillance over an organisation's network operations, with the aim of gaining an insight into an adversary's capabilities, intentions, and activities in the cyber domain.

(Franz, 2011)articulates four key considerations for cyber professionals of the armed forces, viz inter-disciplinary team work, need for a culture shift from technology towards war-fighting, suitable taxonomy to better factor the diversity of cyber-space, and a way of depicting the levels of sophistication within cyber-space.

(Lee et al., 1995)observe that the cadre of information security professionals will need to be multi-dimensionally proficient -sound in technology, operations and management lines, and socially well-adjusted- to lead effectively. Further, there is perceptible shift towards decentralised information security organisations. Collectively, this calls for re-structuring of the curricula of the corresponding stream.

(Assante & Tobey, 2011)opine that workforce development strategies must factor the peculiarities of the cybersecurity field viz, fluid and dynamic infrastructure deployment, inadequacy of traditional solutions - necessitating new and better practices, and improved expertise, need to leverage professional cutting across organisational silos. These issues are further deliberated by(Mcquaid & Cervantes, 2019).

(Arnold et al., 2013)observe the need for an integrated and fully qualified cyber-officer-workforce for the armed forces, to meet envisaged challenges and opportunities. The authorsargue for a unified cyber branch that puts together the best from each of the stakeholder communities, addresses current gaps, and undertakes the much-required restructuring. The authors also attempt to design a cyber-career-path that is best for the armed forces.

(Hoffman et al., 2011)draw inspiration from other complex, cross-disciplinary fields like medicine which have integrated their workforce across varying levels of expertise and performance. The authors then focus on one element of a holistic strategy – education with the aim that practitioners think beyond their "stove-piped" fields and collaborate.

As per an analysis undertaken by(Lee et al., 2010), noticeable differences exist in skill-set requirements among different positions, entailing a nuanced approach to training. However, the fact remains that skilling must

DOI: 10.9756/INT-JECSE/V14I4.23

draw inspiration from the post-course-employment needs of the organisation. Concurrently, it must be noted that the placement paradigm of cybersecurity professionals in the armed forces, is yet to come of age. As on date, it appears to be based only on crowd-sourced feedback of the skill level of a practitioner, rather than a scientific approach.In fact, (Hentea, S. Dhillon, et al., 2006), astutely observe application of the following norms of placement of cybersecurity practitioners in the Armed Forces:-

a. Service-specific criteria (such as spoken reputation, prior exposure to the field, relevant service-course qualifications (within acceptable grading profile), overall performance, and availability of the candidate at that point in time).
b. Academic qualifications/ credentials.
c. Professional Certifications (CISSP, CEH, etc.)[4].
d. Vendor-Specific Certifications (MCSE, CCSP, Comp TIA Security + etc.)[5].

Research Outcomes

There is a strong case to explore ways and means to establish a well charted career path for cybersecurity professionals. Professional and vendor-specific certifications and such other measures can contributeto assessing hands-on competence.This must go hand in hand with creating and sustaining a cadre for the cybersecurity domain. However, for a cadre to be sustainable an essential ingredient is the actual numbers of human resource required, per skill set, and at each level of hierarchy. Efforts in this direction, particularly in respect of the armed forces are still at a nascent stage; but must be given a fillip.

Retention

Retention of the cyber workforce lies at the core of talent management whether it be in the context of the industry or the armed forces.(Fortson, 2017) for instance, observes the need to invest in innovative recruiting, talent management and retention endeavours. A number of eminent thinkers have applied themselves to examining various aspects of talent retention, such as compensation (monetary or otherwise); growth, development and job satisfaction; and organisational culture (employer branding, organisational/ corporate culture, climate, leadership etc.).

(Hernandez & Johnson, 2014)present the following findings aimed at retentionof armed forces cyber warriors, viz.,

a. Compensation (money and associated privileges/ perks);
b. Hygiene factors (duty station preference, geographic stability, educational opportunities, and a sustainable ecosystem);
c. Growth and development (development of skills, external growth opportunities, internal career development path,individual and personal development);
d. Organisational culture (conferring ofelite status to the community, and existence of a healthy organisational climate).

Comparable concerns are projected by(Linn, 2009) who notes the need for superior leadership (in the information warfare domain); and community direction apart from monetary and non-monetary incentives, to facilitate better retention.

(Knight, 2016)presents an excellent analysis from the perspective organisational culture and prospects for growth. The author's comments are based on the promotion policies of the U.S. armed forces. He advocates change to meet the severe competition for talent, based on the premise that industrial age talent management measures will prove unequal to information era challenges. However, herecords that the new system must be cognizant of factors which regulate inflow and exit of officers from the armed forces. An interesting study of HR practices in DOPMA (US Defence Officer Personnel Management Act of 1980 vintage) *vis a vis* Google Inc. is presented by(Blair et al., 2019). He infers that current HR practices in the U.S. armed forces are hardly congenial for development and sustenance of a cybersecurity and therefore recommends recalibration.(Downs, 2019)notes that application of traditional talent retention strategies will not work in the context of valued professionals and advocates adoption of creative solutions by the organizations in need. While the armed forces

[4] These are contemporary professional certifications in the field of cybersecurity. As per ANSI-ICE 1100: 2010(E), such a certification is a voluntary exerciseforconferral ofbounded recognition and testimonial to individuals who meet prescribed standards of knowledge, skills, or competencies. CISSP stands for Certified Information Systems Security Professional endorsed by the ISC2 (International Information Systems Security Certification Consortium); CEH stands for certified ethical Hacker offered by EC Council.

[5] MSCE stands for Microsoft Certified Systems Engineer offered by Microsoft Inc.; CCSP stands for Cisco Certified Security Professional offered by Cisco Inc.; CompTIA Security+ stands for Computing Technology Industry Association Security certification and is offered by CompTIA, an association known for its preparatory courses and certification exams in IT.

DOI: 10.9756/INT-JECSE/V14I4.23

have indeed evolved with time and are continuing to do so, the pace of change is handicapped by inertia. Meanwhile, concomitant with the felt need of the information age, the armed forces of several nations have now created cyberwarfare components. But these continue to operate in a forbidding environment, apprehensive of and irreverent to technology and technical proficiencyas discussedby(Conti & Surdu, 2009). Clearly there is need for organisational and cultural reform.

(Latukha & Selivanovskikh, 2016)review talent management practices in vogue in information technology (IT) firmshailing from emerging economies; and highlight the influence of institutional and cultural factors, on the industry. In a similar vein, examination of institutional and cultural factors prevalent in the armed forces can potentially throw up interesting findings for cyber-talent retention.(Su, 2018)examines the association among the corporate culture, talent training and development (T&D). The results possibly can serve as a reference for related government divisions and subsequent studies. An(ISC2, 2018)report notes the imbalance - loaded in favour of the capable aspirant in the lucrative job market. In keeping with same, employers would do well to be sensitive to the priorities of proficient practitioners with a view to retain talent.

The challenge of sustainment and retention of cyber talent is not peculiar to the armed forces. It cuts across the industry and balance of the Government sector as well. In addition, industry competition and the median pay for cyber personnel is increasing as per (Hernandez & Johnson, 2014). This makes talented cyber personnel vulnerable to poaching. (Gourova et al., 2017)make note of the industry-wide strategic focus on talented human capital, creation of a conducive climate, and employer branding to draw and keep, consummate and competent employees within an enterprise.(Gourova & Gourova, 2017)note that knowledge workers are more loyal to their trade or proficiency (across organisational boundaries) than their employers, which is a tremendousinsight for talent retention. (Mihalcea, 2017)echoes similar thoughts. The authoremphasises focus on HR accomplishments, development, growth, and incentives. He also draws attention to development of digital skills for managers and employees as a major challenge.

(Parker & William, 2016)examine the evolution of the emerging career field of cyber-warriors from the perspectives of retention and growth. To this effect the author takes a look at public sector skill retention initiatives; and the effectiveness of tools (e.g., special and incentive pay) employed by the U.S. DoD.

(Hardison et al., 2019)explore measures to address *inter alia*skill shortages (i.e., skilling, learning, induction, certification, professional development, workforce management and the like).

Research Outcomes

Information age HR practices particularly for armed forces cyber-practitioners, need to evolvebeyond industrial-age anachronisms, which werebased on staffing conceived to fulfil the needs of traditional kinetic wars.

Phasing Out

(Merritt, 2020)discusses how veterans can be leveraged to partially offset the cybersecurity shortage being experienced. The author posits that the veteran pool comprises of integrity-checked, cyber skilled and trained personnel, who are proficient in risk management, along with unique domain expertise. Yet, their transition into the civvy street is surprisingly hard.

Research Outcomes

Just as any other soldier, armed forces cyber-warriors will become veterans one day, whether on superannuation or premature retirement or on completion of contractual obligations. If they continue to remain passionate about their field, then their years of experience, domain expertise and proficiency can be harnessed for building the pipeline for the nation (teacher-ship or policy articulation or legal studies or counselling), or tapped to establish a start-up, or in terms of lateral placement in Government or corporate sectors. Possibilities exist; hand-holding will likely yield rich dividends.

Research Methodology

This study broadly follows the method outlined by (Mengist et al., 2019), and presents a qualitative recap of several studies on the topic of cyber talent management. The research question set out was to examine if the armed forces could draw relevant inferences regarding the best practises of cyber talent management prevalent either in the corporate sector, orfollowed by government organisations (including armed forces world-wide). Criticalities which affect cyber talent management in general, with focus on the inferences and derivatives for the armed forces of any nation were identified through the process of systematic literature review. The objectives set out were as follows: -

a. To establish the need for cyber talent management in the face of skill shortages, with focus on the armed forces of a nation.
b. To explore inferences from international cyber talent management practise which could be extended to the armed forces.
c. To arrive at significant takeaways for the armed forces.
d. To suggest a way forward.

There are several aspects of cyber talent management which are not commonly discussed in open domain, being classified. In addition, being an emerging field, vibrant discussion on the topic is visible in grey

DOI: 10.9756/INT-JECSE/V14I4.23

literature too, which it may be prudent to suitably factor in. Hence, this study accessed peer-reviewed journal papers, conference proceedings, and books, as also grey literature,subject to their being scripted in English language and present in the open domain. The most commonly referred search databases include Google Scholar, Microsoft Academic (till it was available), Scopus, Science Direct and Jstor. Barring a rare case, the study excluded publications prior to the year 2001; and included relevant publications upto 2022. To assess tendencies within various reviewed articles, descriptive statistics was used; whereas for text analytics, the Voyant tool (https://voyant-tools.org/) was used.

A Suggested Way Forward

Putting first things first, the foremost requirement is to have clarity in one's doctrinal thought. In the cyber context,two significant policy shaping observations are laid out by(Schneider & Mulligan, 2011):-

a. Cybersecurity can no longer be left to technologists as technology alone cannot lead to a trustworthy cyberspace. Thus Governments, must get involved with regulation and legislation. New policy and new institutions are required.
b. Doctrinal thought must precede policy, as it would engender a top-down, coherent and consistent approach.

In a similar context-setting argument, (Starr et al., 2010) explores the US's cyber force structure and the associated cyber workforce. Troubled by the talent shortfall, the author suggests a slew of measures covering the complete gamut ranging across learning, training, certification, selection, recruitment, proficiency-enhancement,cadre management, and assurances of dependability and so on. (Bhutani, 2017)presents a similar case in favour of holistic end-to-end treatment of the matter, for synergies to develop and security assurance to emerge, along with structural recommendations.

In this backdrop, assuming that the cyber-domain of war-fighting is here to stay, and that raising of cyber organisations is imperative from the national security perspective, the armed forces will need to actively explore best practices associated with all dimensions of cyber talent management (to include talent identification, selection, induction, sustainment (training and development, skilling, education, professional growth), retention and phasing out), for the demand far outstrips supply.

The armed forces or other Government organisations can scarcely hope to compete with private enterprise in terms of compensation (pay, perks, and terms & conditions of service) as per(Blair et al., 2019; Egloff, 2022). However, a deep dive can certainly be attempted to come out with complementary incentives. The armed forces do not have to traverse the entire trail. Rather, they are well placed to draw and adapt lessons fromthe private sector, to incubate and foster (cyber) teams as projected by (Fortson, 2017). As per (Schmidt & Rosenberg, 2014)firms like Google Inc. focus more on quick and continuous learners, i.e., generalists, *vis a vis* specialists, as they operate in a volatile, rapidly evolving, uncertain industry.

Either way, review of organisational culture is warranted - to the extent practicable, with provision for specialisation - albeit without compromising on the corewarrior ethos of such organisations. While almost all level-headed decision-makers appear to endorse the need for specialisation, it is the "implementable how" which confounds. In this context it is pertinent to observe the following: -

a. Language training may have lessons to offer for training of cyber warriorsas observed by(Jennifer & Daugherty, 2015). Similarly, the field of aviation and the conduct of PABT (Pilot Aptitude Battery Test), may have lessons to offer.
b. The best cyber practitioners operate much like the Special Forces – in small teams of elite (skilled and trained) specialists. Many of the "SOF Truths," (*USSOCOM*, n.d.) articulated in the 1980s appear as if they were written with cyber practitioners in mind as explained by(Paul et al., 2014).
c. Without prejudice to the need for civilian or reservist/ auxiliary corps cyber warriors, every aspirational cyber-capable state requires uniformed cyber forces as per (Paul et al., 2014) for the following reasons:-

i. There are very limited alternatives to having cyber practitioners in military hierarchy, for integration of cyberspace operations within full spectrum operations.
ii. Uniformed cyber warriors enjoy protection under the laws of armed combat to operate in Cyberspace, as legal combatants.
iii. Uniformed cyber warriors are deployable(Paul et al., 2014).

As posited by(Hoffman et al., 2011) a holistic outlook to workforce development is preferable. Ideally, it should be one that factors a multi-disciplinary approach to produce and enhance cybersecurity professionals – both technical (e.g., computer science and engineering) and non-technical (e.g., management and policy related disciplines) alike. It (should) comprise of three key components: (1) workforce structuring; (2) opportunities for right-skilling and upgrading the workforce; and (3) capacity building initiatives to sustain the pipeline. (Hoffman et al., 2011) goes on to add that the field of cybersecurity today, is comparable to that of 19th century health-care. In the absence of a structured medical professional trajectory, practitioners were often self-taught, with an unquantified difference in proficiency levels, operated in a complex, uncertain and emerging environment, with few professional standards for performance. Progressively, the professionalization of medical

DOI: 10.9756/INT-JECSE/V14I4.23

practise took shape. Today it includes a variety of specialisations and super-specialisations with clear career progression paths, nuanced learning and skilling programmes, and well-defined professional bench-marks.

When taken together, measures for talent detection (screening for KSAs, detection of aptitude and fulfilment of organisational fit) and measures aimed at organisational reform, specialisation, and incentives are likely to enable better talent management through the entire cycle as shown in **Figure 2** below.

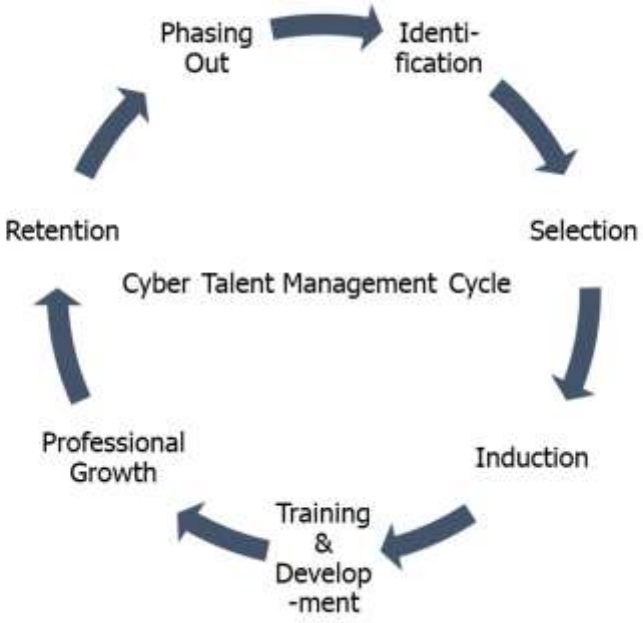

Figure 2: Cyber Talent Management Cycle, Source: Self Created

Apropos the above, a number of interesting research questions related to cyber talent management with particular reference to the armed forces get thrown up, such as (but not limited to) the following: -

a. How can cyber talent be identified? What is the right balance between passion/ motivation, aptitude, and KSAs? How should the selection system satisfy itself that the talent identified conforms to organisational fit?
b. What would be right mix of technical, non-technical and inter-disciplinary skills for the armed forces? How can the induction/ recruitment model be tweaked to suit the armed forces? How should the pipeline of appropriate capacity be built?
c. What is a sustainable career growth path and assured career progression model for cyber practitioners? What measures of organisational reform are desirable and sustainable to sustain the cyber workforce?
d. How should balance be struck between the training and development of the various kinds of cyber practitioners as also the cyber training of military leadership?
e. What innovative measures of talent retention should be considered?
f. How should the phasing out of cyber talent be planned, in a manner that induction is incentivised and national capacity is progressively built?
g. What would constitute the right staffing ratios (and numbers) for each skill-set – so that suitable cyber establishments can be set-up and sustained?
h. Should cyber-training and skilling be centralised?
i. Should offensive cyber training be delineatedand segregated from defensive cyber training?
j. What proportion of cyber-practitioners are required for cyber-enabled influence operations?
k. An interesting fallout is how should the armed forces look at specialisation in general?

Conclusion

A study of cyber talent management in the context of the armed forces promises to make for an interesting study with scope for quantitative and qualitative examination. It is also a critical imperative of the times. However, some parts of the examination, may have to be kept out of open domain for reasons of security.

Measurement of Aptitude, Organisational Fit and inter-disciplinary Knowledge, Skill and Abilities (KSAs) of potential candidates coupled with a thrust in favour of specialisation will likely present a way forward. The approach explored in this context may also provide some initial leads on - if and how – specialisation in other spheres can be adopted by the armed forces.

References

DOI: 10.9756/INT-JECSE/V14I4.23

Allen, D., & Herr, C. (2019). *Cyber Talent Identification and Assessment*. https://apps.dtic.mil/sti/pdfs/AD1085449.pdf
Alvarez, I. B., Silva, N. S. A., & Correia, L. S. (2016). Cyber education. *ACM SIGCAS Computers and Society*, *45*(3), 185-192. https://doi.org/10.1145/2874239.2874266
Andel, T. R., & McDonald, J. T. (2013). *A Systems Approach to Cyber Assurance Education* Proceedings of the 2013 on InfoSecCD '13 Information Security Curriculum Development Conference - InfoSecCD '13,
Arnold, T., Harrison, R., & Conti, G. (2013). *Professionalizing the Army's Cyber Officer Force*
Asher-Dotan, L. (2018). *How the Israel Defense Forces' approach to diversity can help ease the security talent crunch*. https://www.cybereason.com/blog/israel-unit-8200-women-diversity-security-talent-hiring
Assante, M. J., & Tobey, D. H. (2011). Enhancing the Cybersecurity Workforce. *IT Professional*, *13*(1), 12-15. https://doi.org/10.1109/mitp.2011.6
Barbar, R. (2001). Hackers Profiled — Who Are They and What Are Their Motivations? *Computer Fraud and Security*, *2*, 4. https://doi.org/10.1016/S1361-3723(01)02017-6
Bhutani, B. R. (2017). A Comprehensive National Cyber Force Structure for India *Synergy*.
Blair, D., Hughes, J., & Mashuda, T. (2019). *From DOPMA To Google: Cyber As A Case Study In Talent Management – Analysis.* https://www.eurasiareview.com/23062019-from-dopma-to-google-cyber-as-a-case-study-in-talent-management-analysis/
Borum, R., & Sanders, R. (2015). *Cyber intelligence: Preparing today's talent for tomorrow's threats* https://www.insaonline.org/wp-content/uploads/2017/04/INSA_Cyber_Intel_PrepTalent.pdf
Campbell, R. D., Hawthorne, E. K., & Klee, K. J. (2003). The role of two-year colleges in educating the cyber-security workforce. *ACM SIGCSE Bulletin*, *35*(3), 235-235. https://doi.org/10.1145/961290.961592
Campbell, S. G., & Bradley, P. (2018). *What shape peg are you? Different cyber jobs require different cognitive skills*.
Campbell, S. G., O'Rourke, P., & Bunting, M. F. (2016). Identifying Dimensions of Cyber Aptitude. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, *59*(1), 721-725. https://doi.org/10.1177/1541931215591170
Canali, K. G., Wind, A. P., & Willford, J. C. (2017). *Cyber Selection Test Research Effort for U.S. Army New Accessions*. https://apps.dtic.mil/dtic/tr/fulltext/u2/1044605.pdf
Caulkins, B., Goldiez, B., Wiegand, P., Dumanoir, P., Martin, G., & Torres, T. (2017). *Emerging Network and Architecture Technology Enhancements to Support Future Training Environments* Interservice/Industry Training, Simulation, and Education Conference (I/ITSEC)
Caulkins, B. D., Badillo-Urquiola, K., Bockelman, P., & Leis, R. M. S. (2016). *Cyber Workforce Development Using a Behavioral Cybersecurity Paradigm* 2016 International Conference on Cyber Conflict (CyCon U.S.), https://ieeexplore.ieee.org/document/7836614
Chiesa, R., Ducci, S., & Ciappi, S. (2008). *Profiling hackers: The science of criminal profiling as applied to the world of hacking* (1 edition ed.). Auerbach Publications. https://doi.org/10.1201/9781420086942
Cleave, V. M. (2013). *Myth, Paradox & the Obligtions of Leadership: Edward Snowden, Bradley Manning and the Next Leak*.
Cobb, S. (2016). *Mind This Gap: Criminal Hacking and the Global Cybersecurity Skills Shortage, a Critical Analysis*. https://www.virusbulletin.com/conference/vb2016/abstracts/mind-gap-criminal-hacking-and-global-cybersecurity-skills-shortage-critical-analysis
Conti, G., & Surdu, J. (2009). *Army, Navy, Air Force and Cyber - is it time for cyberwarfare branch of military?*
Conti, G., Weigand, M., Skoudis, E., Raymond, D., Cook, T., & Arnold, T. (2014). Towards a Cyber Leader Course Modeled on Army Ranger School *Small Wars Journal*.
Creveld, M. V. (1991). *Technology and War: From 2000 B.C. to the Present. Simon and Schuster*.
Crumpler, W., & Lewis, J. A. (2019). *The Cybersecurity Workforce Gap*. https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/190129_Crumpler_Cybersecurity_FINAL.pdf
Curley, M. G. (2018). The Provision of Cyber Manpower - Creating a Virtual Reserve. *MCU Journal*, *9*(1). https://doi.org/https://doi.org/10.21140/mcuj.2018090108
Cybersecurity Career Paths and Progression (Page 18 Cybersecurity and Infrastructure Security Agency). (2019).
Davidson, J. (2015). *Lack of digital talent adds to cybersecurity problems—The Washington Post* https://www.washingtonpost.com/news/federal-eye/wp/2015/07/19/lack-of-digital-talent-adds-to-cybersecurity-problems/
Dawson, J., & Thomson, R. (2018). The Future Cybersecurity Workforce: Going Beyond Technical Skills for Successful Cyber Performance. *Frontiers in Psychology*, *9*. https://doi.org/10.3389/fpsyg.2018.00744
De Zan, T. (2019). *Mind the Gap: The Cyber Security Skills Shortage and Public Policy Interventions* (Cybil, Issue. https://cybilportal.org/publications/mind-the-gap-the-cyber-security-skills-shortage-and-public-policy-interventions/
Dodge, R., Toregas, C., & Hoffman, L. (2012). Cybersecurity Workforce Development Directions. HAISA,

DOI: 10.9756/INT-JECSE/V14I4.23

Downs, F. (2019). The Battle for Cybersecurity Talent Must Include Retention Emphasis. Infosecurity Magazine. https://www.infosecurity-magazine.com:443/blogs/talent-retention-emphasis-1-1/

Egloff, F. J. (2022). *Semi-State Actors in Cybersecurity*. Oxford University Press. https://doi.org/10.1093/ oso/ 9780197579275.001.0001

Fontenele, M., & Sun, L. (2016). *Knowledge management of cyber security expertise: an ontological approach to talent discovery* 2016 International Conference On Cyber Security And Protection Of Digital Services (Cyber Security),

Fontenele, M. P. (2017). *Designing a method for discovering expertise in cyber security communities: an ontological approach* University of Reading].

Fortson, C. C. L. (2017). *Putting the Pieces Together: Army Cyber Warrior Talent Management*. https://publications.armywarcollege.edu/pubs/3422.pdf

Franz, T. (2011). The Cyber Warfare Professional: Realizations for Developing the Next Generation.

Furnell, S., & Matt, B. (2020). Addressing Cyber Security Skills: the Spectrum, not the Ssilo. *Science Direct*. https://doi.org/https://doi.org/10.1016/S1361-3723(20)30017-8

Galliano, J. (2017). *Improved matching of cybersecurity professionals' skills to job-related competencies: An exploratory study* University of Fairfax].

Gourova, E., Gourova, N., & Dragomirova, M. (2017). *Keeping Talents* Proceedings of the 22nd European Conference on Pattern Languages of Programs,

Gourova, N., & Gourova, E. (2017). *Attracting talents* Proceedings of the VikingPLoP 2017 Conference on Pattern Languages of Program - VikingPLoP,

Govt, U. S. (2011). *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure*. Retrieved from https://www.energy.gov/cio/downloads/cyberspace-policy-review-assuring-trusted-and-resilient-information-and-communications

Gutzwiller, R. S., Hunt, S. M., & Lange, D. S. (2016). *A task analysis toward characterizing cyber-cognitive situation awareness (CCSA) in cyber defense analysts* 2016 IEEE International Multi-Disciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support (CogSIMA),

Hald, S. L. N., & Pedersen, J. M. (2012). *An updated taxonomy for characterizing hackers according to their threat properties* 14th International Conference on Advanced Communication Technology (ICACT), South Korea.

Hardison, C. M., Payne, L. A., Hamm, J. A., Clague, A., Torres, J., Schulker, D., & Crown, J. S. (2019). *Attracting, Recruiting, and Retaining Successful Cyberspace Operations Officers: Cyber Workforce Interview Findings* https://www.rand.org/pubs/research_reports/RR2618.html

Hentea, M., Dhillon, H., & Dhillon, M. (2006). *Towards Changes in Information Security Education* Proceedings of the 2006 InSITE Conference,

Hentea, M., S. Dhillon, H., & Dhillon, M. (2006). Towards Changes in Information Security Education. *Journal of Information Technology Education: Research*, *5*, 221-233. https://doi.org/10.28945/244

Hernandez, L. F., & Johnson, D. K. (2014). *Designing Incentives for Marine Corps Cyber Workforce Retention*.

Hoffman, L. J., Burley, D., & Toregas, C. (2011). *Thinking Across Stovepipes: Using a Holistic Development Strategy to Build the Cybersecurity Workforce (Report GW-CSPRI-2011-8)*.

Information at War: From China's Three Warfares to NATO's Narratives. (2015). https://li.com/wp-content/uploads/2015/09/information-at-war-from-china-s-three-warfares-to-nato-s-narratives-pdf.pdf

ISC2. (2018). *Hiring and Retaining Top Cybersecurity Talent: What employers need to know about cybersecurity jobseekers in 2018*.

Jacob, J., Peters, M., & Yang, T. A. (2020). Interdisciplinary Cybersecurity: Rethinking the Approach and the Process. In *National Cyber Summit (NCS) Research Track* (pp. 61-74). https://doi.org/10.1007/978-3-030-31239-8_6

Jacob, J., Wei, W., Sha, K., Davari, S., & Yang, T. A. (2018). *Is the Nice Cybersecurity Workforce Framework (NCWF) Effective for a Workforce Comprising of Interdisciplinary Majors?* Proceedings of the 16th International Conference on Scientific Computing (CSC'18), Las Vegas, USA.

Jennifer, J. L., & Daugherty, L. (2015). *What Can Be Learned from Defense Language Training?*https://www.rand.org/pubs/research_reports/RR476.html

Jordan, T., & Taylor, P. (2004). *Hacktivism and Cyberwars*. https://doi.org/10.4324/9780203490037

Key Issues: Cybersecurity Challenges Facing the Nation – High Risk Issue (Accessed in April 2020). https://www.gao.gov/key_issues/ensuring_security_federal_information_systems/issue_summary

Knight, J. (2016). *Down and Out About Up or Out: A Viable Alternative*.

Kozloski, R. (2009). The Information Domain as an Element of National Power; Strategic Insights, v. 8, issue 1(January 2009).

Latukha, M., & Selivanovskikh, L. (2016). Talent Management Practices in IT Companies from Emerging Markets: A Comparative Analysis of Russia, India, and China. *Journal of East-West Business*, *22*(3), 168-197. https://doi.org/10.1080/10669868.2016.1179702

DOI: 10.9756/INT-JECSE/V14I4.23

LeClair, J., Abraham, S., & Shih, L. (2013). *An Interdisciplinary Approach to Educating an Effective Cyber Security Workforce* Proceedings of the 2013 on InfoSecCD '13 Information Security Curriculum Development Conference - InfoSecCD '13,

Lee, D. M. S., Trauth, E. M., & Farwell, D. (1995). Critical Skills and Knowledge Requirements of IS Professionals: A Joint Academic/Industry Investigation. *MIS Quarterly*, *19*(3). https://doi.org/10.2307/249598

Lee, J., Bagchi-Sen, S., Rao, H. R., & Upadhyaya, S. J. (2010). Anatomy of the Information Security Workforce. *IT Professional*, *12*(1), 14-23. https://doi.org/10.1109/mitp.2010.23

Libicki, M. C., Senty, D., & Pollak, J. (2014). *Hackers Wanted: An Examination of the Cybersecurity Labor Market*.

Linn, R. A. (2009). *Information Warfare Officer Retention: Using a Capabilities-based Assessment to Solve Retention Issues* Naval postgraduate school monterey CA].

Mayer, D. B., & Stalnaker, A. W. (1968). *Selection and evaluation of computer personnel- the research history of SIG/CPR* Proceedings of the 1968 23rd ACM national conference on -,

Mcquaid, P. A., & Cervantes, S. (2019). How to Achieve a Seasoned Cybersecurity Workforce. *Software Quality Professional*, *21*(4), 7.

Mengist, W., Soromessa, T., & Legese, G. (2019). Method for Conducting Systematic Literature Review and Meta-analysis for Environmental Science Research. *Elsevier B.V.*https://doi.org/http://dx.doi.org/10.1016/j.mex.2019.100777

Merritt, M. (2020). *Improving Veteran Transitions to Civilian Cybersecurity Roles: Workshop Report*.

Mihalcea, A. D. (2017). Employer Branding and Talent Management in the Digital Age. *Management Dynamics in the Knowledge Economy*, *5*(2), 289-306. https://doi.org/10.25019/mdke/5.2.07

Mills, R. F., Wingo, J., & Iverson, P. (2015). *Cyber Compendium, Professional Continuing Education Course Papers*. https://apps.dtic.mil/seo/citations/ADA617022

Nakayama, M., & Sutcliffe, N. (2007). Managing IT skills portfolios *British Journal of Educational Technology*, *38*(1), 181-182. https://doi.org/10.1111/j.1467-8535.2007.00682_15.x

Parilla, D. R., & Wills, S. L. (2021). *Department of the Navy Cyber Workforce Leadership Development Capstone Study* Vanderbilt University]. https://ir.vanderbilt.edu/handle/1803/16543

Parker, I., & William, E. (2016). *Cyber Workforce Retention*. https://apps.dtic.mil/sti/citations/AD1030226

Paul, C., Porche, I. R. I., & Axelband, E. (2014). *The Other Quiet Professionals: Lessons for Future Cyber Forces from the Evolution of Special Forces*. https://www.rand.org/pubs/research_reports/RR780.html

Petersen, R., Santos, D., Smith, M. C., Wetzel, K. A., & Witte, G. (2020). *National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework*. (SP 800-181 Rev. 1). U.S. Dept of Commerce Retrieved from https://csrc.nist.gov/publications/detail/sp/800-181/rev-1/final

Professionalizing the Nation's Cybersecurity Workforce? (2013). https://doi.org/10.17226/18446

Ramsey, C. A. A. (2020). Talent Management for Cyber Warfare - Mainitaining the Right Workforce. *Marine Corps Gazette*. www.mca-marines.org/gazette

Rogers, M. (2013). A new hacker taxonomy. *Journal of Chemical Information and Modeling*, *53*(9), 1689-1699. https://doi.org/10.1017/CBO9781107415324.004

Rogers, M. K. (2006). A two-dimensional circumplex approach to the development of a hacker taxonomy. *Digital Investigation*, *3*(2), 97-102. https://doi.org/10.1016/j.diin.2006.03.001

Saner, L. D., Campbell, S., Bradley, P., Michael, E., Pandza, N., & Bunting, M. (2016). Assessing Aptitude and Talent for Cyber Operations. In *Advances in Human Factors in Cybersecurity* (pp. 431-437). https://doi.org/10.1007/978-3-319-41932-9_35

Schmidt, E., & Rosenberg, J. (2014). *How google manages talent* https://hbr.org/2014/09/how-google-manages-talent

Schmidt, L., O'Connell, C., Miyake, H., Shah, A. R., Baron, J., Nieboer, G., Jourdan, R., Senty, D., Winkelman, Z., & Taggart, L. (2015). Cyber practices: What Can the U.S. Air Force Learn from the Commercial Sector?

Schneider, F. B., & Mulligan, D. K. (2011). A Doctrinal Thesis. *IEEE Security & Privacy Magazine*, *9*(4), 3-4. https://doi.org/10.1109/msp.2011.76

Seebruck, R. (2015). A typology of hackers: Classifying cyber malfeasance using a weighted arc circumplex model. *Digital Investigation*, *14*, 36-45. https://doi.org/10.1016/j.diin.2015.07.002

Seligman, M. E. P., & Csikszentmihalyi, M. (2000). Positive psychology: An introduction. *American Psychologist*, *55*(1), 5-14. https://doi.org/10.1037/0003-066x.55.1.5

Shropshire, J., & Gowan, A. (2015). *Characterizing the Traits of Top-Performing Security Personnel* Proceedings of the 2015 ACM SIGMIS Conference on Computers and People Research,

Smith, P. K., Mahdavi, J., Carvalho, M., Fisher, S., Russell, S., & Tippett, N. (2008). Cyberbullying: its nature and impact in secondary school pupils. *Journal of Child Psychology and Psychiatry*, *49*(4), 376-385. https://doi.org/10.1111/j.1469-7610.2007.01846.x

DOI: 10.9756/INT-JECSE/V14I4.23

Smith, T. S. (2007). *In pursuit of an aptitude test for potential cyberspace warriors*https://www.researchgate.net/publication/235105144_In_Pursuit_of_an_Aptitude_Test_for_Potential_Cyberspace_Warriors

Sobiesk, E., Blair, J., Conti, G., Lanham, M., & Taylor, H. (2015). *Cyber Education* Proceedings of the 16th Annual Conference on Information Technology Education,

Soley, M. (2018). *Policy Shortcomings: Growing the CAF CyberOperator Occupation*

Spidalieri, F. (2013). *Joint Professional Military Education Institutions in an Age of Cyber Threat*.

Spidalieri, F., & McArdle, J. (2016). *Transforming the Next Generation of Military Leaders into Cyber-Strategic Leaders: The role of cybersecurity education in US service academies*. https://www.jstor.org/stable/26267304

Starr, S., Kuehl, D., & Pudas, T. (2010). *Perspectives on Building a Cyber Force Structure* Cyber Conflict Proceedings

Steinmetz, K. F. (2015). Craft(y)ness. *British Journal of Criminology*, *55*(1), 125-145. https://doi.org/10.1093/bjc/azu061

Su, C.-M. (2018). *Association among Corporate Culture, Talent Training and Development, and Corporate Operational Performance* Proceedings of the 4th International Conference on Industrial and Business Engineering,

Summers, T. C., Lyytinen, K. J., Lingham, T., & Pierce, E. A. (2013). How Hackers Think: A Study of Cybersecurity Experts and Their Mental Models. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2326634

Van Beveren, J. (2001). A conceptual model of hacker development and motivations. *Journal of E-Business*, *1*(2), 9. https://www.researchgate.net/publication/253411127_A_conceptual_model_of_hacker_development_and_motivations

Waage, E., & Morris, J. (2015). *Cyber Aptitude Assessment: Finding the Next Generation of Enlisted Cyber Soldiers*. https://digitalcommons.usmalibrary.org/aci_ja/21

Whitman, M., & Mattord, H. J. (2004). A Draft Model Curriculum for Programs of Study in Information Security and Assurance.

DOI: 10.9756/INT-JECSE/V14I4.23