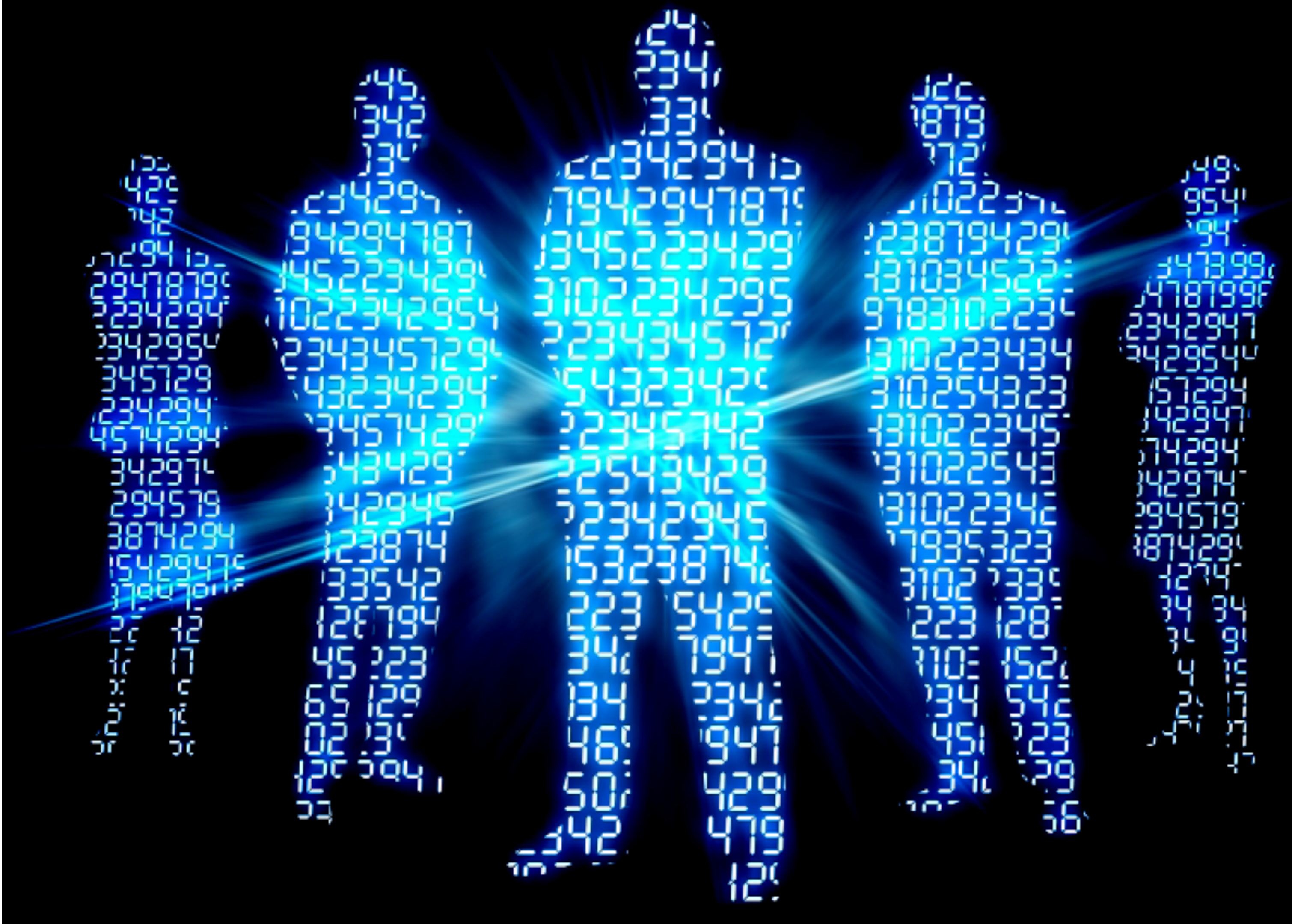
TINKER TAILOR SOLDIER CYBER



Ash J. Hunt

Tinker Tailor Soldier Cyber

The requirement to expand the MoD-sponsored Cadet Force initiative to include cyber and its wider activities of the fifth domain into the training programme.

Written for the Conservative Science & Technology Forum.

'There are a number of very good points raised in this paper that deserve due consideration with a view to ensuring the cadet force is more relevant and accessible to our youth as an organisation. The notion of extending the training objectives of the cadet force, to include cyber activity, will go some way toward nurturing many of the skills required in a forward thinking, high tech society like the United Kingdom. I am also encouraged with the possibility of opening the cadet catchment, to those who may be currently disadvantaged on health reasons - in a similar way to our joint cyber reserves who add value as keyboard warriors. Finally, I cannot overstate the worth of increasing the opportunity to imbue more of our young people with the values and standards of our armed forces and therefore support moving this paper forward'.

Rt. Hon. The Lord Astor of Hever, DL, Under-Secretary of State (Ministry of Defence) and Lords Spokesman on Defence.

Warning - Cyber Attacks Ahead!

Cyber! Botnets! Malware! We are all well read into the fifth domain, the cyber sphere, the challenges of the ethernet - aren't we? Of course not! This is an esoteric and very real problem that needs addressing. It is a sad reality that most would doubt that cyber presents one of the most significant security challenges in our history. The digital skills gap coupled with the unending stream of public/private sector network vulnerabilities continues and increasingly puts sovereign security and success at an unacceptable risk. Perhaps addressing the reality of this cyber pill has been a hard one to swallow, but the nation's wealth and security demand a spoonful of sugar - peace of mind and real-time reassurance to assuage the nation's concerns. Current government spearheaded initiatives to secure the cyber frontier and grapple with the multitude of cyber risks and opportunities are to be applauded. Such efforts include the 2011 The UK Cyber Security Strategy[1] (a hand rail looking out to the public/private management of cyberspace), the £500 million 'cyber strike capability'[2] (an offensive military capability for future operations in cyberspace to ensure the security of our country) and the creation of the Joint Cyber Reserve Unit[3] (an MoD initiative to assist our military commanders in offensive and defensive cyber activities). This illustrates the government's intent to be serious, progressive and forward-thinking in safeguarding our national online assets, maintaing military preparedness and strategic advantage. Notwithstanding, we must not become complacent and join laissez-faire nations as they kick the cyber can down the street, leaving the balance of security drifting in the fifth domain.

The task of upholding a robust cyber defence posture demands consideration of all resources and talents - particularly from the workforces next generation. The government has actively 'encouraged many education and training initiatives to stimulate the development of relevant skills'[4] and laid out the requirement for 'the UK to have the cross-cutting knowledge, skills and capability it needs to underpin all our cyber security objectives'[5]. With youth engagement in mind, this paper sets out to highlight the benefits and requirement of extending the training programme of the MoD-sponsored Cadet Forces to include information security and cyber in-the-round. This would be a prudent step and initiative, both facilitating students with the necessary skills to succeed in the digital age whilst enhancing the country's future cyber security capacity. Marching our youth forward in tackling the complex intricacies of the fifth domain will help equip them with cutting-edge skills that will benefit industry, commerce and our security forces deep into the twenty-first century.

From Little Acorns Do Great Trees Grow

The MoD Cadet Forces is a well established initiative that has served students for over a century. At its core, it aims to 'provide a disciplined organisation in a school so that pupils may develop powers of leadership by means of training to promote the qualities of responsibility, self reliance, resourcefulness, endurance and perseverance'[6]. With MoD funding of around £28 million per annum, the Cadet Forces have become a popular, engaging and effective youth organisation and an

[1] Cabinet Office, 2014.

[2] Walters. The Daily Mail, 2013.

[3] Ministry of Defence, 2013.

[4] National Audit Office, 2014.

[5] Cabinet Office, 2014.

[6] Letter Assistant Head Youth and Cadets, Reserves Forces and Cadets, 2014.

integral source for providing students with essential life skills and qualifications. Currently, approximately 140,000 students serve as cadets and in June, 2012, the Prime Minister, Rt. Hon David Cameron MP announced the government's intention to set up 100 new cadet units in state-funded secondary schools by 2015. This must be seen as an invaluable educational asset that is both extra-curricular to routine study whilst building and reinforcing character and is underpinned with the values and standards of our armed forces.

Currently, the Cadet Force administers to the conventional areas of military activity - marching, fitness, self-administration, drill, weapon handling and much, much more but it has yet to add the cyber dimension to the training programme. It is this new emerging, high-tech understanding of the cyber arena that needs to be imbedded in our institutions but particularly in our youth organisations. The development of introducing cyber skills should not be seen as a stand-alone unit. Instead, it will open the gate to integrating cyber activities into existing cadet force branches. Cyber, however, is ostensibly different to all other facets of traditional military force: it is a language all unto its own. Unlike other military activities, cyber intelligence in the human being is never nature but always nurture. Considering this, Cadet Forces must work with students to establish computer literacy and knowledge of network security whilst encouraging greater involvement with science, technology, engineering and mathematics (STEM) subjects in the curriculum. As cadet training activities are reinforced, our cyber-savy cadets will continue to be imbued with the ethos, mindset and philosophy of our armed services (providing a possible stepping stone for those who choose to pursue military service). Whilst cyber for the most part has been wholesome, we cannot turn a blind eye to its more destructive qualities. With the cyber reserves already in place, Cadet Forces are the natural next step in training our youth in the fifth domain. Akin to the cyber reserves, 'cyber cadets' would also open the door for a whole new swathe of young individuals (keyboard warriors) that may not have been considered hithertofore. Students previously sidelined, for character or health reasons, for conventional cadet activities may be well suited to cyber activities - you don't have to be 'action man' to work a computer! Adding the cyber dimension to the training programme would be a cost-effective, efficient and sustainable initiative that would crucially help to close the digital skills deficit. The task ahead is clear - governments must first plant its acorns if it wishes to see great trees grow.

Lessons In Cyber - Present and Future

As mentioned in the overview, the government has made concerted efforts in conjunction with private sector industry to expose the next generation to cyber. With a renewed focus on career opportunities in technology, the government has partnered with 'eskills UK' to 'help increase the number of cyber security apprenticeships' as well as initiating 'a new technical apprenticeship scheme through GCHQ and other intelligence agencies' - recruiting 'up to 100 apprentices for a tailored 2-year foundation degree course'[7]. Progressive changes to the curriculum, particularly with computing, further highlight the government's commitment to broadening the educational spectrum

[7] Office of Cyber Security and Information Assurance, 2013.

to incorporate cyber. As a result, students from the age of five will now be taught to code and by the age of seven, expected to 'understand what algorithms are [and to] create and debug simple programs'[8]. Moreover, students by the age of eleven will have to 'design, use and evaluate computational abstractions that model the state and behaviour of real-world problems and physical systems'[9]. A tall order, but a necessary one if we are to meet the challenges of the cyber era. Undertakings such as the St. Paul's Way Trust Science Summer School led by Professor Brian Cox, University of Manchester have already proved highly successful in exposing a whole new clutch of students to STEM subjects. Professor Cox, however, identifies the immediate requirement to instruct students in cyber when he states that 'the skills gap in STEM subjects will be between 1 and 2 million by 2020… we should be filling this gap from the pool of talent that is available. But in order to do that we need to go into schools and show these children that they can achieve in these fields'[10]. The professor has hit the nail on the head - or the enter button if you will! It is in all of our interests: social, economic, business and government - to provide students with the opportunities and capabilities to utilise the fifth domain.

Notwithstanding Professor Cox's flag of concern, the government has made substantial progress in bringing cyber into the classroom. Government and industry partnerships with non-profit organisations such as 'eskills UK' and 'Cyber Security Challenge' have made cyber an alluring possibility for many young students. The following are just a sample of the various public/private sector initiatives that are expanding the educational programme in this direction:

- **Girls Get <Coding>**

  As part of the joint government/industry campaign 'Your life', 'Girls Get <Coding>' is just one initiative aimed at increasing the number of students studying STEM subjects by 50% over the next three years. Organised by 'eskills UK' and the Parliamentary Internet Communications and Technology Forum (PICTFOR), 'Girls Get <Coding>' saw 100 girls aged 9 - 12 from 40 schools around the UK visit Westminster to teach MPs how to code a computer game. With the intention of improving female representation in the technology sector, the girls also had the opportunity to meet female role models from leading high tech companies such as: BT, Cisco, Accenture, Vodafone, HSBC, HP, Co-operative Group, and JP Morgan. Stephen Mosley, Co-Chair of Parliamentary Internet Communications and Technology Forum and Conservative MP for City of Chester reflected that 'it's very encouraging to see how Get Girls Coding is inspiring young women about tech. The excitement today has been palpable, and I'm glad to be a part of a valuable and enjoyable initiative that is focused on tackling the gender imbalance in tech education and careers'[11].

- **National Cipher Challenge**

  With sponsorship from both public and private sector institutions such as GCHQ and IBM, the 'National Cipher Challenge' is a nationwide competition to engage students in mathematics and computing. Organised by the University of Southampton School of Mathematics, thousands of students (18 years of age and below) each year take part in the online code-breaking competition; attempting to break a series of challenging cryptograms. Students also have the opportunity to attend a series of lectures concerning the Semantic

[8] Richardson. BBC News, 2014.

[9] *Ibid.*

[10] Gurney-Read. The Daily Telegraph, 2014.

[11] e-skills, PICTFOR. e-skills UK Sector Skills Council, 2014.

Web, World War II cryptography and computer programming at Bletchley Park as part of a wider effort to engage more pupils in STEM subjects.

- **Coder Dojo**

  A private sector organisation, 'Coder Dojo' is a global volunteer-led community that offers free programming clubs for youths. Born out of the requirement to propagate the teaching of computer/network programming, the club administers to children aged 7-17 years of age and instructs them on the practicalities of learning code, developing websites, apps, programmes, games and exploring technology.

- **Cyber Security Challenge UK**

  Operating as a non-profit organisation, the 'Cyber Security Challenge is a series of national competitions, learning programmes, and networking initiatives designed to identify, inspire and enable' more UK students 'to become cyber security professionals'. With the launch of its schools programme in May, 2013, 'Cyber Security Challenge UK' has reinvigorated the study of Computer Science in the curriculum with the purpose of filling the online 'security gap'. At present, over 700 secondary schools are involved and benefit from a range of materials such as touch screen games and infographics designed by UK cyber security leaders. Collegiate engagement is at the heart of the programme, encouraging students to develop 'uncrackable ciphers' which are then interchanged between other participating schools in order to crack each other's cipher. In tandem with the schools programme, the Cyber Security Challenge runs an additional project - 'Cyber Games 2.0'. The game requires student codebreakers to 'take on the role of counter-terrorism professionals and tackle a unique mixture of cyber security treasure hunts and code cracking exercises'. Students are also asked to manage both a cyber terrorism attack scenario and a game of cyber top trumps - matching cyber threat cards with cards representing an appropriate defensive solution.

Collectively, these examples provide a glimpse of the type of activities 'cyber cadets' could be involved in. Inter-collegiate competitions and coding are just a couple of the strands that form part of the wider cyber eduction agenda. Cyber exercises would expand the cadet training programme to include activities such as network security, ethical hacking (white hat)[12] and advanced computer literacy. As it stands, the government's direction in cyber education is sound but the speed and depth are questionable. Considering the means and methods for cyber tutelage already exist, it would require relatively little effort for the government to provide students with the space and time to acquire these much-needed skills. We must not rest on our laurels but rather look towards developing this invaluable tool for training the next generation of cyber-literate individuals.

'Sinkhole Their Botnets'

In its entirety, cyber presents as much of a real and present danger as it does a force for good. Targeted network attacks such as the Stuxnet attack and the Shamoon virus on Saudi Aramco only begin to demonstrate the ruinous, tangible realities of cyber malice. Preventive measures against sinister cyber aggression are just one half of the equation, the capacity to instigate an offensive cyber response is the other. At last, the narrative of online battleships has begun! Unfortunately, the digital skills gap has left us with only a handful of capable individuals who can manage these tasks -

[12] A white hat hacker is a computer security specialist who breaks into protected systems and networks to test and asses their security. White hat hackers use their skills to improve security by exposing vulnerabilities before malicious hackers (black hat hackers) can detect and exploit them.

a stark contrast to the vast pool of future talent that lies across the student community. It is this reservoir that the government needs to tap into. The ability to ably manage our future cyber capabilities will rely upon a systematic approach towards training the first generation of cyber warriors. Students need to be imbued with a working knowledge of information security from an early age to allow them time to hone their online skills - after all, Rome was not built in a day! This new cadre of young cyber security professionals will provide the UK with a more agile, flexible and capable presence in the fifth domain and help bring cyber to the fore of the national security consciousness.

Cadet Forces, however, may not be enough. Cyber is not solely a defence matter but also a civilian one. Building upon our efficacious and robust police force, the government should lend full consideration to creating a youth branch of cyber-savy police cadets (a potential starting point for those who wish to pursue a career with the police forces's 'cyber-specials')[13]. In a similar vein to the MoD cadets, the police cadet force would be an invaluable tool in helping SMEs, public and private sector organisations and the wider community at large to deal with the daily onslaught of cyber crime. Students who may not fit the conventional police profile would be given the opportunity to play their part in contributing to the safety of our nation. In essence, this is a win-win for everyone: government, business and the students.

Forward March!

The cadet initiative in the UK is a strong one. Until now, it has recognised and adapted accordingly to the emerging domains of military activity; furnishing cadets with the values, standards and ethics of the Armed Forces. Cyber is the next logical step. Lets not waste any more time and get on with it.

[13] Cabinet Office, 2014.

Bibliography

- Computing, Academy of (N/A) *National Cipher Challenge*, BCS.
- Cyber Security and Information Assurance, Office of (20 February, 2013). *Improving cyber skills, education and professional opportunities*, gov.uk.
- Defence, Ministry of (12 December, 2012). *The Cadet Forces and MOD youth work*, gov.uk.
- Defence, Ministry of, Command, Joint Forces, Hammond MP, Rt. Hon Phillip (29 September, 2013). *New cyber reserve unit created*, gov.uk.
- Gurney-Read, Josie (28 August, 2014). *Brian Cox: universities need to play a bigger role in society*, The Daily Telegraph.
- Haggerty, Angela (22 August, 2014). *Traversing the digital skills gap – how can businesses ensure they have the know-how to survive?*, The Drum.
- N/A (8 August, 2014). *Letter Assistant Head Youth and Cadets, Reserves Forces and Cadets, D/DRFC/4/1/5.*
- Office, Cabinet (10 September, 2014). *Update on the National Cyber Security Programme*, National Audit Office.
- Office, Cabinet (November, 2011). *The UK Cyber Security Strategy - Protecting and promoting the UK in a digital world*, Crown copyright.
- Paton, Graeme (5 September, 2014). *Private school cadet forces 'facing closure' in funding shift*, The Daily Telegraph.
- Richardson, Hannah (1 September, 2014). *Pupils begin 'tough' new national curriculum*, BBC News.
- UK, e-skills, PICTFOR (8 July, 2014). *Girls Get Coding 2014*, e-skills UK Sector Skills Council.
- Walters, Simon (29 September, 2013). *Hammond's £500m new cyber army: As he reveals top-secret Whitehall bunker for the first time, Defence Secretary says future wars will be fought with viruses*, The Daily Mail.

Ash J. Hunt is a researcher on transnational cyber policy. He has authored several articles and publications including the paper ‘Cyber - a real and present danger’. In 2013, he was the sole British delegate to the UN Conference on the Development of Communication and Technology Policies. He has also worked for the Under-Secretary of State, Lord Astor, the Ministry of Defence and the Cabinet Office.