Personal - in confidence

The Institute for Statecraft

Concept Paper fourth draft: 30 01 2016

CyberGuardian: **Cyber Security Education Programme for Children and Young People**

The Need

- The character of conflict has changed in recent years. Today, we are seeing a new level of competition among State and non-State interests. It is self evident that success in this hypercompetitive world, to a large extent, will depend on a nation's ability to develop and deploy new forms of power, including indigenous skills in the Cyber, Signals and Electronic Warfare spheres.

- The UK's future Defence, Security and Prosperity will be directly linked to its reservoir of indigenous talent and ingenuity in the Cyber, Signals and Electronic Warfare spheres. Government, Military and Industry employers will require a large pool of talent if we are to remain ahead of foreign competition.

- Cyber security professionals unanimously agree that the cyber threat to the UK is growing; that it is much more serious than generally appreciated, and; that the UK is not educating young people adequately or in sufficient quantity to provide for our current and future needs in government, industry and society.

- The cyber threat includes attack from states and sub-state groups intent on undermining the UK and on reducing our competitive stance. Currently, for example, radicalisation to violent extremism is conducted primarily through cyber means, targeting youth.

- Current governmental plans for cyber security education in schools are at best inadequate and will not meet the need in the foreseeable future. The trend to shrinking the size of the state, and the pressure on government budgets for the foreseeable future, means that we cannot and should not expect the state to deal with the totality of this problem.

- The UK adult skills base is actually being depleted by other countries targeting those with appropriate qualifications to emigrate. For example, each of the Netherlands' Provinces (i.e. federal districts) employs officials tasked with assessing the future skills gaps of their Province and attracting skilled personnel with offers of tax and housing benefits etc. UK regions are one of their prime target areas.

- Outsourcing to Asia may solve industry's IT problems temporarily, but long-term it hinders our building up our domestic IT skills base.

- In the UK, only 8% of cyber security practitioners are female. It is important to foster the interest of girls as well as boys to fill the skills gap.

- Consequently, there is an urgent need to develop alternative, supplementary programmes for improving cyber security education, particularly amongst children and young people.

What is currently available

Governmental

- Cyber Security Research and Education (CESG) – UK Govt partnership with Academia
- GCHQ – Cryptoy
- SDSR
    - Schools programme to identify and encourage talent in 14-17 year olds (ref no 6.67)
    - Increase in the number of Cadet organisations
    - £20m + competition to open a new institute of coding
    - Cyber First undergraduate scholarship scheme

Non-governmental

- Cyber Security Challenge
    - CSC for Schools
    - Cyber Centurion
- Tech Partnership:
    - Tech Future Classroom (*Behind the Screen*)
    - Tech Future Girls (*Computer Clubs for Girls*)
    - Secure Futures
    - Tech Future Teachers Professional Development (on-line learning in partnership with *Naace*)
    - Partnerships for learning (regional partnerships between police, schools, school governors and parents)
- British Computer Society
    - Get Safe on Line
    - Cyber to the Citizen

General programmes with some IT content

- Stemnet - Stem Ambassadors
- Women in Science and Engineering
- Women in Information Technology
- Childnet (voluntary charity working in schools)

NB the above initiatives need further analysis. They all appear to be useful short programmes/apps for teachers to employ but many do not bring extra resources to schools, breadth of coverage is

patchy and the programmes are not coordinated or integrated with one another, athough the SDSR and updated Cyber Security Strategy promise to make them so.

The US *Cyberpatriot* model

Cyberpatriot is the largest and most successful cyber security education programme in the USA. In the seven years since it was set up (on the initiative of the US Air Force Association), *Cyberpatriot* has grown to reach well over 1000 high schools in the US. The programme - which is now owned and run by a separate civilian, non-profit organisation - is run on an annual basis and includes a major national competition. This year the programme will impact on half a million young people between the ages of 13-18 from all walks of life, over 60,000 of whom will be involved in the US national competition. The programme enables the participants to learn cyber defence and safety. It does not teach offensive "hacking".

Within the wider cyber defence programme, the national competition operates with two "Divisions": an "Open Division", open to teams from every high school in the US; and, an "All-Service Division", for teams drawn from the Junior Reserve Officer Training Corps organisation (JROTC) – the US equivalent of the UK's Cadet Force organisation. ***(NB This element of the model, having parallel streams in schools and Cadet organisations, is particularly attractive for our proposed programme)***

A contractual arrangement is made with high schools to ensure that the programme becomes part of the school's IT syllabus, with appropriate rules and conditions to ensure overall child protection. The programme provides computer software and printed educational material to JROTC units and to high schools, both for teachers and pupils. Where appropriate and needed, computer hardware systems, computer specialists and mentors (virtual or in person) are also provided.

A high school or JROTC unit's involvement in the programme is led by a coach (usually a member of staff or a volunteer assistant), appointed by the school or unit and assisted where necessary by a technically competent mentor. Lessons in cyber defence and the understanding of a computer's hardware and software form the initial stage of the programme. These lessons are delivered on a broad basis to as many young people as possible, from whom the coach will subsequently identify one or more teams of 8-10 players from within the school or unit to play in the national competition.

Instructors ("coaches") for the programme are mostly drawn from former members of the US Armed Forces who do the work on a mostly pro bono basis. It has been found that advanced computer skills are not required for the vast majority of instructors. Normal IT skills are quite adequate when supplemented by a short course and a continuation distance-learning package. Most important are the instructors' teaching skills and capacity for empathy with the students, especially in difficult schools in inner city areas. ***(NB This element of the model, using retired service personnel, is particularly attractive for our proposed programme)***

Three increasingly demanding virtual "rounds" of the competition are played in each division, successively reducing the number of teams to twelve finalists for each division. These 24 teams are flown to Washington for the final rounds, where the teams defend their networks against live "red" attackers. The victorious teams and individuals receive prizes and scholarships.

The programme is currently funded by commercial sponsors, reducing the cost burden to the school, unit or individual to an absolute minimum. The education provided contributes directly to the school curriculum for IT training and forms part of the JROTC programme of activities. The programme has proven that it can be scaled up and that it is highly effective with differing skill levels across the age range, with pupils from all ethnic and cultural backgrounds, and with all socio-economic groups. Its

popularity with young people is due not only to its obvious personal and career utility or to the fact that it is fun, but also because it offers the opportunity of a benignly competitive activity to those not gifted at sports and competitive games.

In addition to teaching important technical skills, the programme instils a sense of ethics and values with the aim of improving all participants' respect for other IT users, as well as improving their personal on-line safety and security. The programme is already producing dividends by way of improved school grades, employment opportunities and higher education and career choices.

NB The Institute for Statecraft proposed to develop a similar programme to *Cyberpatriot,* specially tailored to UK conditions and with a distinct UK identity. However, despite support from the original parent body (The USAF Association), financial sponsors (Northrop Grumman) would not share software or programme details for proprietary reasons.

In January 2016 Louise Bennett discussed *Cyberpatriot* with CDP, who was generally in favour as it ticks many boxes – supporting cadets in schools, adding to the Enterprise Programme to address STEM and cyber skills shortages throughout the armed forces, involving veterans in education programmes in schools (potentially including wounded veterans) and focussing on leadership and ethical values. CDP (who retires at the end of April) will make introductions to the key people in MOD who should be involved. He cautioned that the MOD budget was very tight for the next two years and 30% of Civil Servants must leave MoD in this Parliament.

The Estonian model

Following the Russian-sponsored cyber-attack on Estonia, the Estonian Government instituted a national programme of cyber security, including education for children and young people. Estonia also accepted to host a NATO Cyber Security Centre of Excellence. The Institute has been in contact with both HQ NATO, which has agreed to give privileged access to the CoE, and with the staff of the Estonian Government Education Programme, who have agreed to make their materials and expertise available to us, and to assist us in setting up our programme. *An example of their material is attached.*

The Cadets initiative

The Institute's original concept, taking its lead from the US Cyberpatriot, was to develop parallel programmes in schools (both state and private) and in the Cadet Forces with the support of the Reserve Forces and Cadets Association (RFCA). Cadet Forces are not subordinated to MOD but are independent educational bodies, although supported by the Armed Forces and Grant in aid. The RN has several separate Cadet organisations. Consequently, Cadet organisations need to be approached separately and will not necessarily follow one another's example. However, there is also a "Cadets in School" programme where there is a Government commitment to introduce cadet programmes to 500 more state schools.

Starting in 2013, The Institute approached the RAF Cadets (Air Commodore Dawn Mc Caffery) to interest them in adopting our idea of developing cyber security education as a special element of the cadet programme. The RAF Cadets have chosen to follow this advice and are developing the idea independently, using a commercial company with which they have links.

Outline features of our proposed programme

Philosophy

- To foster a world-leading reservoir of potential cyber talent among children and young people (initially 12-18 year olds, but spreading to younger children as the programme evolves).

- To provide basic cyber security education through the national school curriculum and, in parallel, the existing framework and structure of the Cadet Forces. To include, for example, how to protect themselves from mobile phone bullying, online grooming, hacking etc.

- To provide education appropriate to each age group, taking into account that the wide range of emotional, skill and academic levels within each age group will require special attention and management.

- To provide a competitive programme for those particularly interested and talented which will enable them to develop their cyber skills in a benign and monitored environment, and encourage them to pursue this as a career

- To provide this education (a) in an ethical framework, within the school curriculum, at no extra cost to schools, using volunteer staff drawn particularly from retired military, and; (b) through the Cadet organisations (RN, RM, Army, RAF).

NB Basing the education within an ethical framework, and using retired military (or volunteers and reservists) would twin an enthusiasm for Cyber security with the development of qualities of leadership, responsibility and good citizenship (directly challenging the cliché of the teenage hacker as a social misfit hidden in a top room).

Basic Principles

- Evolutionary
    - The whole programme will be evolutionary in nature
    - The software will evolve as part of the process
    - The players will influence the evolution

- The educational process
    - Start with a strong ethical base
    - Define the programme's values and standards
    - Develop content, messages and story lines appropriate to the age group / levels of emotional maturity or technical attainment
    - Develop into a competition as the core of the process as it develops

- Making the education attractive. It must:
    - be fun
    - be visibly useful
    - Create an adventure rather than excitement or entertainment

- Safely Identify the potential, the talent, and the various forms of skills young people have in IT
- Help them to realise and improve those abilities
- Devise a means of assessing, measuring and classifying those abilities
- Attract, via a competition and building expertise and skills, children and young people who are not good at physical sports
- be attractive to those with physical disabilities or specific conditions e.g. Asperger's and Autism
- provide the means for keen children to continue to work on the programme from home
- be attractive to parents as well as to the children

NB Where will the end point be? is there an age limit? an adult package? (NB adults learn in a very different way from children)

- Deployment strategy:
  - Trial through the Cadet system and selected schools
  - Tailor it to the school curriculum
  - Use a specific inspectorate and school authority as a pilot
  - develop to be introduced into the state system, targeting firstly schools with a relevant specialisation or get them to develop cyber as a specialisation (WCIT sponsored Academies may be particularly relevant)
  - trial in a school where children at risk of radicalisation can be engaged

NB As the project matures and if conditions are suitable, it may in time prove possible to consider taking the programme to other countries, perhaps through Commonwealth mechanisms. This would also allow international competitions.

- Graduating and tailoring the educational process:
  - We need to know the ability of children to understand things at different ages so that we pitch the education at the right level.
  - We might find it useful to have someone from the schools inspectorate
  - Are the role models the same in each ethnic group? e.g. Bond's "Q" rather than Bond
  - How will we stream it so that all the religious, gender and ethnic backgrounds are treated fairly?
  - We need a default process so that weak performers do not drop out of the process

- The Team Principle:
  - The process will be based on developing teams, rather than individuals separately.
  - Individuals will learn from each other and teams, not individuals, will compete to defend a computer system.
  - Time limits or similar constraints will be set to stimulate teamwork and creativity.

- The Competition:
  - Have a Red Team and a Blue Team; build the system so that the competition gets increasingly difficult.

- Create a league for the competition
- provide rewards

- Link to measurements of value/qualification, viz:
  - UCAS tariff points
  - BTech and MTech
  - Bachelor's and Master's degree credits
  - City & Guilds: what qualifications/ accreditation could they offer?

  NB - what other means are there to validate the impact?

- Link to Universities:
  - Oxford
  - Southampton
  - Bath
  - York
  - Cambridge
  - Portsmouth
  - Royal Holloway College
  - Edinburgh- there is a professor who is studying the role of digital technology in education.

- Link with the Military & Security
  - Through the Cadet Forces
  - Through the Reserve Forces (inc Joint Cyber Unit - JCU(R))
  - Using retired / wounded soldiers/PTSD sufferers trained as mentors
  - Engage Headley Court to use as a therapy
  - GCHQ involvement

- Link with the Police/Home Office:
  - Important contribution to the Protection of Children
  - National Crime Agency interest
  - "Prevent": NB - Its attraction in Muslim schools will be the cyber education/qualification. But the ethics education and transmission of mainstream social values will help societal integration

- Link to IT related charities
  - Childnet and charities focussed on cyber bullying – see latest stats on calls to Child line in 2014/15 - cyberbullying was the 3rd largest reason for calls (25,736) and on-line sexual abuse the 10th (11,398)
  - Nominet Trust
  - British Computer Society and its Academy
  - Worshipful Company of Information Technologists

- Link to interested companies

The supporting rationale

- The UK has no coherent methodology for capturing, encouraging and developing the skills attendant to success in Cyber, Signals and Electronic Warfare among the 12-18 year old age bracket.

- Children who are aware of some nascent talent in this area – and who wish to develop it – are often forced to do so individually (cut off from the pastoral support of their schools, or even parents) hence the cliché of the socially isolated teenage hacker.

- This exposes them to all the dangers associated with Internet chat rooms et al. Such 'free agent' children are also denied the ability to develop their skills in a wholesome context - alongside the development of physical and social skills wrapped in an ethos of social responsibility and service.

- By the time they reach their late teens they are semi-fixed personalities. Psychologists and neurologists agree that the brain lays down myriad neurological pathways during the teenage years. If you wish to have a positive impact on such development it is crucial to start early.

Other supporting arguments

- There is an increasing need to educate young people to recognise on-line propaganda and disinformation, and to identify opinion masquerading as fact. They need to be taught how to check facts and spot bias. This "social malware" effect is very dangerous. IS/Daesh use it to great effect, and Russia's use of it is now forming attitudes even in our primary schools.

- There is no better country in which to address the problem of cyber security. We have a rich history of intelligence work combined with technological innovation. There exists a myriad of benign cultural reference points that celebrate indigenous talent and ingenuity and can inspire youth; Bletchley Park, The Double Cross System, our invention of the World Wide Web, GSM/GPRS telecommunications, DNA. All this fizzing, creative, ingenious Britishness can provide the imaginative hinterland for the "Cyber Cadets".

- The Cadet Forces themselves have spotted a dilemma in how to encourage children who don't exhibit the physical skills that would necessarily compliment flying, sailing or shooting but who nonetheless are bright and able. This is a fitting response to that dilemma.

- The initiative dovetails with an increasing willingness (and need) over the last thirty years for Government agencies such as GCHQ to "step out of the shadows". Not only has the existence of such agencies been avowed, but they now run websites and open recruitment programmes. This builds in the minds of the public a clearer understanding of how such organizations serve and protect them, in a politically accountable environment, and indeed celebrate and encourage the best UK traditions of service and self-sacrifice.

- The programme will feed into the stream that is preparation for work through apprenticeships and industry sponsorship providing work experience

Where we could draw support from

Why might Industry choose to support this initiative?

- Act as a cultural meeting place for UK Government, security and Industrial actors as they co-operate to support the new focus on Cyber skills.

- Leverage financial and practical efficiencies delivered through the more effective use of schools and of an existing, large-scale network in the form of the UK Cadet Force.

- As part of a Socially Responsible agenda that wishes to promote the Security and Prosperity of the UK.

- Provision of a stream of qualified candidates. An X-listed company will find it easier to get good people from non-standard sources as vetted employees.

- Companies which engage could find it easier to integrate into the UK system through myriad crossovers with other UK actors - both government, educational and civilian.

- An opportunity for co-operation between industry, government and wider civilian spheres of this sort may deliver far wider and as yet unanticipated dividends accruing to the wide melting pot of supporters (ergo; possible cross pollination between spheres of knowledge, training, funding, efficiency)

Why might Government, (inc Security & Military) choose to support this initiative?

- The Depts of Education and of Business, Innovation and Skills are the main potential beneficiaries. Furthermore, there is evidence of the educational benefit of pupils' participation in Cadet Forces which should further attract The Dept for Education. The degree to which the initiative captures and excites disadvantaged youth will also pay dividends to the whole panoply of Government agencies supporting communities, welfare, police and NHS.

- Government and its agencies, like industry, will also benefit from the wider and deeper pool of future recruits. Furthermore, it will provide a forum in which the ethical and moral purpose of such activities can be both explained and developed as a method of communication with youth and through them, the wider citizenry.

Individuals and Institutions

- NATO Centre of Excellence, Estonia
- Estonian Government cyber security education team
- Baltic Defence College
- Cabinet Office; Matt Hancock, Min for the Cabinet Office and Paymaster General: NB who is now Head of Govt Digital Services
- Baroness Joanna Shields (child protection element of IT)
- BIS; Min Nick Boles
- DCMS – Ed Vaisey
- Home Office CAST (Sci & Tech) Andy Bell, ex DSTL
- Baroness Pauline Neville-Jones
- Gen Sir Richard Barrons' staff

- CGS, CDS, VCDS
- Lt Gen Andrew Gilbert CDP
- Brig David Keenan Army HQ
- Air Cdre Dawn McCafferty, RAF Cadets
- Col Patrick Crowley and Army Cadets
- ACF – Hanif Qadir
- Affan Burki, Lancashire education project
- Mike Lynch; CEO cyber company: via Tasmia Hart
- Lt Gen Sir Edmund Burton
- ? Newall Hunter; expertise: FCO cyber, LIAG Counter-penetration
- ? Diane Allen; runs adventure training for 14-15 year olds, understands learning levels
- ? Lindsay Charlton; Game company, digital media operation
- ? Maria Dayton; media operation (using E European specialists)
- David Febrache (now at KPMG)
- Dougal Goodman IfS&T
- Richard Sermon, Livery Companies, eg Information Technologists
- Ken Olisa and Deputy Chairman Nimble Thompson, IoD, interest in small and medium businesses (including Perry Burns – Working Capital Partners)
- Prince Charles (William Bortrick; William Nye)
- Ian Brown, Oxford Internet Institute
- Prof Sir Nigel Shadbolt, Oxford Univ
- Martin Thomas, Royal academy of Engineering
- Wendy Hall, Southampton Univ

Developing the business case

- It is thought at this stage that the programme will be (an element of) a registered charity, Initially funded by donation from all interested parties (at a national level, through Government, Agencies and Industry) and at a local level (through the support of local bodies, schools etc).

- It should be borne in mind that much of the staffing will, in any case, be undertaken by volunteers. Therefore, what will be required into the longer term is a lightly staffed, centralized, coordinating office. This office will co-ordinate voluntary support offered by Government, Industry and Individuals, fundraising and the administrative side (standardization of printed material etc).

- The mechanism for financial self-sufficiency will accrue over time through the development of an endowment. We will look to public spirited and patriotic UK nationals who have generated considerable wealth, perhaps in associated areas, and seek to turn over the raising and maintenance of an endowment to them with Government, Military and Industry making up temporary operating shortfalls. Soft or hard support from these individuals will be elicited at the earliest stages. Of course it is hoped that in the long run alumni may also protect the investment they themselves enjoyed for future generations through donations.

- All individuals, companies and departments supporting the initiative at conception will be recognised in some appropriate way within the programme

Thoughts on the way ahead

- The Institute for Statecraft issues a Charter of Support to interested parties (Government, Industry). This document indicates a level of emotive (rather than financial) support for the Initiative. The document also lays out a process for the assessment of the initiative and assembles a semi-formal coalition of potentially willing supporters.

- The Institute for Statecraft supports the production of a developed business plan to lay out the practical architecture for the establishment and sustainment of the Initiative. The acknowledged goal is for the programme to be ultimately financially self-sustaining.

- The resultant business plan is then re issued by the Institute for Statecraft to the interested parties where hard commitment is sought.

- Marketing: explain-
  - What will Business get out of it?
  - What will Schools get out of it?
  - What will the Home Office get out of it?
  - What will the Dept of Education get out of it?
  - What will BIS get out of it?
  - What will the Cabinet Office get out of it?
  - What will the DCMS get out of it?
  - What will Cadets get out of it?
  - What will parents get out of it
  - What political capital will Government get out of it?

- Need to identify someone who will develop the software; gameification

- Sales and Sponsorship Strategy
  - Raise IT scholarships
  - Engage the City; Livery Companies
  - Offer internships, mentoring,

- Potential commercial Sponsors:
  - EADS
  - Babcock
  - KPMG
  - BP
  - Rolls Royce

  E.g. Attractions for EADS
  - An X-listed company will find it easier to get good people from non-standard sources as vetted employees
  - This programme will help EADS integrate into the UK system

NB who can we get to publicise the programme in a way that attracts major companies to support it? Saachi?

Attachments

1. Estonian Primary School intro pack
2. Estonian Primary School lesson plan for class 3-4
3. Estonian Primary School lessons on avoiding pornography
4. Letters of support from CDS, Baroness Neville-Jones, RFCA
5. Details of *Cyberpatriot*