Personal - in confidence

The Institute for Statecraft

Executive Summary: 26 02 2016

Cyber Security Education Programme for Children and Young People

The Need

In the modern world our prosperity and security will depend on our cyber skills. We need a large pool of cyber talent if we are to remain ahead of foreign commercial competition. The cyber threat to the UK is growing. We are constantly under attack from hackers and propagandists. Radicalisation to violent extremism is now conducted primarily through cyber means.

However, the UK is not educating young people adequately or in sufficient quantity to provide for our current and future needs. Budgetary pressure means that we cannot expect the state to solve this problem alone. We urgently need to develop additional programmes on cyber and cyber security education for children and young people from 11-16, where the shortfall is greatest. It is especially important to foster the interest of girls as well as boys to fill the skills gap.

What is currently available

Most governmental and private initiatives target people in their late teens. For school age children the national curriculum is inadequate to ensure online responsibility. A variety of useful educational programmes/apps are available 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.

Other countries have introduced successful programmes to address these issues. Staff of the Estonian Government's extensive Cyber Education Programme have agreed to make their materials and expertise available to the Institute. But the US *Cyberpatriot* programme provides the best model for the UK to emulate. Details are at Annex A.

Outline features of our proposed programme

- 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 in an ethical framework through the national school curriculum and, in parallel, the existing framework and structure of the Cadet Forces.
- 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 and provide career and training opportunities.
- To provide this education at no extra cost to schools, using volunteer staff drawn particularly from retired military.

The programme will be evolutionary in nature with a strong ethical base. It will develop content, messages and story lines appropriate to different age groups / levels of emotional maturity or

technical attainment. Over time it will develop into a competition as the core of the process. The outline deployment strategy is at Annex B.

Attachments

Annex A - Details of *Cyberpatriot*

Set up on the initiative of the US Air Force Association seven years ago in the face of the problem of hacking from China, this programme - which is now owned and run by a civilian, non-profit organisation, reaches well over 1000 high schools plus units of the Junior Reserve Officer Training Corps (JROTC) – the US equivalent of the UK's Cadet Forces. It impacts on nearly a million young people between the ages of 13-18 from all walks of life. The programme enables the participants to learn cyber defence and safety. It does not teach offensive "hacking".

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 for teachers and pupils. Where needed, hardware, computer specialists and mentors (virtual or in person) are also provided. Lessons are tailored to the needs of the age group. In addition to teaching important technical skills, the programme instils a sense of ethics and values to improve participants' respect for other IT users, as well as improving their personal on-line safety. The programme actually improves school grades, employment opportunities and higher education and career choices.

Starting by addressing the ethics of smartphone use and defeating cyber-bullying, cyber defence, and; the understanding of a computer's hardware and software; the programme develops into a large-scale competition, which culminates with teams defending their networks against live "red" attackers. The victorious teams and individuals receive prizes and scholarships.

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. Most important are the instructors' teaching skills and capability to empathise with the students.

The programme is currently funded by commercial sponsors, reducing the cost burden to the school, unit or individual to an absolute minimum. 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.

Annex B – Outline deployment strategy:

- Engage an academic partner to develop and maintain the required educational software and printed material for the UK based on the material from the Estonian Cyber Education Programme
- 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 the programme 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
- Feed into the stream that is preparing for work through apprenticeships and industry sponsorship providing work experience
- Link competitions with the existing CyberCenturion programme in the Cyber Security Challenge.

The programme provides an opportunity for collaboration between government, academia, and the private sector. It already has the support of government and industry. It fits well into government plans to expand Academies and the Cadet Force. In addition to the students, the Departments for Education and of Business, Innovation and Skills are the main potential beneficiaries. 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.

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.). 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.

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.