DIGITAL SELF DEFENCE – TOWARD A HUMANIST CIVIC CYBER-SECURITY SYLLABUS

Andy Farnell
Solent University Southampton
United Kingdom

Abstract

The pressing necessity and significant challenges for a course in '*Digital Self Defence'* are explored in this paper. In light of widespread failure to usefully communicate deep technical knowledge necessary to protect citizens amidst an increasingly hostile and complex digital landscape, an alternative approach based on film, literature, psychology and game theory is developed. A description of the content and motivations for pilot lectures is offered along with commentary on successes and failures of certain methods and messages, and the course's impact on students' lives.

Introduction to Digital Self Defence

In the 1980s governments of many European countries began ambitious programmes of computer literacy. They perceived a looming crisis of innovation, and so created educational projects to prepare a generation of digital workers. As personal computing became a reality in the UK, the BBC gave us a 6502 microcomputer, books, magazines and nightly mainstream television programmes teaching BASIC programming. Teachers stressed the importance of computer science, so as 10-year-old children we all learned about RAM, ROM and how disk drives and CPUs worked. Many of us have had exciting, happy and rewarding careers in the technology industry. We have played our part in building the internet and the digital world we see today.

Forty years later a new crisis is looming. As the science fiction writers warned us, digital technology is turning from being our servant to being our master. Privacy, dignity and democracy are under sustained attack. The problem is not the technology *per se*, but the ends to which companies and governments have turned it. My generation heard from our grandparents how democracy was snatched back from the jaws of fascism in two world wars, at enormous cost. But in our enthusiasm as technologists we have been well meaning, unwitting accomplices to the reprise of enslavement. As for many computer scientists, my world changed in 2013 with the revelations of Edward Snowden. I put my life work in digital signal processing on a back burner to start figuring out how to save computer science for my children, how to preserve a world of digital technology compatible with intellectual enquiry, freedom and democracy.

Unlike the 1980's there is no grand social project backed by government and media. Since 2015, I have been developing a "civil and personal cyber-security" curriculum. Academically it would be described as a "philosophy of

human values and technology". Practically, the aim is to teach data hygiene, info scepticism, personal operational security and intellectual self-defence to students who do not have technical and mathematical pre-requisites. The hope is to educate a generation about their ownership and responsibility to steward technology. I see this as distinct from "digital literacy" which, for the most part, I feel is a project to teach people to accept and utilise established paradigms rather than continue to challenge them creatively. The first course ran for eight weeks in 2016 at SAE Institute London, generating extremely positive feedback, and was described as "life changing" by students. With encouragement from colleagues at Solent University, Southampton, I have polished and re-branded the lecture series as *Digital Self Defence*.

Enhanced Security Thinking

Our metaphor of martial arts works extraordinarily well on a number of levels. A real martial artist never goes out looking for fights, but cultivates inner security, self-discipline, mindful awareness and respect for others and the environment. We have explored running the classes as part of a women's self-defence series embedded within a programme of Kempo and street situational awareness to complement physical safety with an intellectual self-defence against cyber-bullying, stalking, tracking and surveillance. There are currently plans to deliver an updated version of the course at the University of Edinburgh and at the University of Central Sweden in 2019. An important goal is to resituate "security" as an idea, through a philosophically broader and deeper treatment than established accounts of the subject. We unpack and challenge ideas like "nothing to fear, nothing to hide", "freedom and security are a tradeoff" and apply quite rigorous philosophical analysis to the tension within security with regards to individual and collective good.

What do I mean by a "Humanist" approach? Much modern security thinking revolves around the objects of machines and systems, protocols, timing, utility, value and suchlike. As a lifelong student of Humanist philosophy, it strikes me that what's missing from this picture is the subject. I am of an anachronous mindset, an old Jedi sect who believe that computer science should be about Intelligence Amplification (IA as opposed to AI). It should enhance all areas of human experience, including arts, entertainment, medicine, exploration, care, social life, and the myriad other dimensions of life that are not conflict and acquisition – the Dark Side. Sadly, the origins of most cyber-security is in finance and warfare, which means that when translated into a reductionist neo-liberal civilian culture it has no connection with people (*qua* humans) except as "consumers" or "targets". A Humanist approach brings cyber-psychology and cyber-philosophy right to the heart of the project in an attempt to restructure attitudes and dispel those assumptions.

Why the branding of "Digital Self Defence"? Initial feedback from the students revealed that "cyber" and "security" are words they associate with unpleasant practices and things which are against their interests. Philosophically and psychologically *security* has many meanings. Those proffered by John Bowlby (Bowlby, 1988) and Eve Ensler (Ensler, 2006) are

among the more interesting interpretations we explore. A notable modern thinker with broad and intelligent interpretations of security is Bruce Schneier (Schneier, 2008), a proponent of "technology in the public interest". We pay some attention to the position of American software freedom pioneers Richard Stallman (Stallman, 1997) and Eric S. Raymond (Raymond, 2001), who remind us that computer security is immanently expansive, and must be absolutely open to scrutiny. Accessible, well written core texts such as Ross Anderson's *Security Engineering* (Anderson, 2008) create a broad foundation. To this mix we also bring elements of communication theory from thinkers as diverse as Claude Shannon and Herbert Marcuse, along with game theoretical, cybernetic, systems and modelling ideas from thinkers as different as Norbert Weiner, Dana Meadows, John Nash, Andrey Markov, Vilfredo Pareto, and Robert Axelrod, touching on subjects like equilibria, threat, percolation, diffusion, contagion, tipping points, and coordination problems.

A good question to open our discussion is "Security for who, from what, and to what ends?", because there is no meaningful *noun* sense of security. Security is not an '*add on*' product to buy, or a thing one can make and then sit on. We look at the idea of "toxic security", which comes from an "industry of security" which is never satiated, where profit derives from a perpetual situation of insecurity. With a disturbing likeness to Munchhausen syndrome by proxy, or factitious disorder, where "keeping the patient sick" is the goal, such thinking creates an ever-growing sphere of imagined new threats, and "solutions" that beget ever more problems. A salient formulation of this concludes Adam Curtis's acclaimed documentary *The Power of Nightmares* (Curtis, 2004). Clinical psychology and psychodynamics figure in this analysis, including the role of personality in security thinking.

The over-reach and failure of state security "collect it all" programmes is examined, as expansive financial black holes from which no light of metrics, impact or success can ever escape, devouring billions of public money while small businesses and individuals go, at best unprotected, and increasingly weakened by misguided state projects. We also analyse the recent swerve towards "offensive security" models, as championed by US military cyber-command. Under the maxim that "attack is the best form of defence", this credo promotes the active manufacture and distribution of new threats, engaging in pre-emptive hacking and the production of malware. On face value the objective is: *continuous offensive penetration and presence inside computers of the enemy*, to have "total information awareness" (TIA). Again, a psychological and historical context is used, with comparisons to 11th and 12th century witch hunts, inquisitions and US McCarthyism. This helps us to understand how a relatively small clique can dominate a society's security narrative.

Understanding threats, probability and motivations is another key area. Notional enemies that are "everywhere, everything and everyone" appear to be misguided and counterproductive. Models of trust and dependency are needed to approach the subject of 'Big Data Tech' and the ongoing abuses of companies like Google and Facebook before we can explore alternatives and strategies for disengagement. An historical context is useful too. The rise and

fall of the Kempeitai, NKVD, Stasi, KGB, Gestapo SS, help us see limits of security, and to understand the decline of societies where security dominates every aspect of human existence, where it strangles economies, creativity, trade, art and education, and eventually the political and military leaders who imagine themselves its masters (the lesson of Stalinism). Because there is no possibility of a healthy balance with that kind of security, mature security thinking must seek to identify and minimise it. Long term security involves defence against certain other kinds of "security thinking". To this end we follow Dana Meadow's wisdom (Meadows, 1997), to intervene in systematic values of security, to strive for a minimal security framework which is a maximiser of freedom and democracy rather than a threat to it.

Existing Projects

Many programmes exist with the aim of creating future cyber-security professionals. For example;

- In the USA, the DHS National Initiative for Cybersecurity Careers and Studies (NICCS) "Teaching Kids the Importance of Cybersecurity Through Games" (U.S. Department of Homeland Security, 2013). See also: "Hacker High" (Woerner, 2016)
- University of Tulsa: "Building Cybersecurity Capacity via Sustained Teacher Training" (2018, (Tulsa Regional STEM Alliance, 2016).
- In the UK, as reported by the BBC (Symonds, 2017), The Department for Culture, Media and Sport have recommended cyber-security lessons offered to schools in England. A 2014 press release reported "School children as young as 11 to get cyber security lessons" (Gov.UK, 2014) according to a government programme named "*The Cyber Security Skills: Business Perspectives and Government's Next Steps"*.
- Privately, many youth-clubs, schools, YMCA and PTA groups have taken initiatives to educate parents.
- Vodafone made a foray into corporate responsibility producing the *Vodafone Parents' Guide* (Vodafone, 2009), attempting to tackle subjects like cyber-bullying, fake-news, screen time limits, over-sharing, sexting and body-image issues.
- Universities offering Bachelor's and Master's degrees in cyber-security are becoming more common. In the UK, Cambridge, UCL, Kent, Derby, City, Birmingham, Southampton, Solent and Northumbria have some courses, while in the USA I have counted over 30 state and city universities offering courses.

Why We Need a New Approach

Teaching the value of data hygiene, anonymity, cryptography, device and code authenticity, offline computing, information scepticism and verification craft, gives a different perspective on cyber-security as an everyday life-skill, one that can be shared amongst friends and families. However, the above

programmes are intended to create a pipeline of capable cyber-defence for *industry*, based on threat models we know today. Many are network administrator courses dressed up with a bit of extra "intrusion detection" and "critical thinking" to make popular new course titles attractive to students in a competitive higher education market. Outside academia so-called "crypto-parties" (SBS, 2012) have emerged as pop-up educational projects aimed at journalists, therapists, doctors, small business owners and other professionals needing to protect themselves and their clients against surveillance and tracking. These tend to self-filter audiences to already well-educated persons with civic awareness. Programmes for parents, while commendable, are symptomatic relief, treating problems as if they were inevitable facts of nature rather than encouraging the kind of critical thinking in children that would arm them to change their digital world rather than meekly adapt to, or avoid it.

As top percentile hackers will attest, it's doubtful whether critical thinking about computer security can usefully be taught to adults anyway, it's really a mindset thing, one that begins when you are about 10 years old. Keeping pace with changing threats requires an endowment for anticipating them, not reading about them in books. More to the point, these kinds of courses are not generally aimed at a personal understanding or providing intellectual self-defence against manipulation and the negative social aspects of digital technology. They do not address inherent risks in some kinds of technologies or technologically mediated relationships. They contain little or nothing in the way of ethics or civics, although many courses deceptively misuse the title "*Ethical Hacking*" (by which they conflate ethics with parochial legality).

Issues of technological self-determination and freedom are becoming entangled with those of "cyber security" in an unhelpful way. Old ideas, rooted in property and criminal justice, perpetuate an increasingly unhelpful view that everything will be fine if we can just rid ourselves of the "bad stuff", iron out the bugs in some software and catch a few rogue cyber-criminals. Within the frame of classic cyber-security, perimeters, attribution, ownership and motive are all too blurred now to see clearly. Who the "bad guys" are is no longer clear, and we can no longer trust those who might tell us. The *raw technique* of cyber-security is no longer enough in the context of a moral free-for-all. Young people are ill equipped to deal with "fake news", tracking, doxing, intimidation, and extortion. They do not trust their devices or institutions, and these institutions and manufacturers are not the right people to be advising them. Further harm accrues with the rapid onset of Internet Balkanisation, disintegration of trust in systems, states and manufacturers which have all been unfolding since Snowden's revelations.

For my own generation, and back as far as my great-grandparents who fought in the Great War (1914-18), sceptical enquiry was the mark of an adult with worldly common sense. Today's technological culture infuses a palpably anti-intellectual and infantilising tone, where young people are inhibited from rational enquiry and from expressing their deeper needs or opinions. They are talked down to by "experts" and discouraged from exploration by those who gain from their stasis. For example, the Vodafone guide mentioned above is a mish-mash crafted by dozens of high-profile contributors associated with

Google, Facebook, Amazon, Apple (all predatory online marketers from whom we should be protecting young people). It seems to weave together every cliché about "digital natives", "Generation Y" and how adults are "in awe" of kids using technology. It is pushing candy while wagging a finger about bad teeth and getting fat. It is, frankly, naive tokenism of the *status quo,* which comedian and playwright Stewart Lee (Lee, 2019) mocks as "Mr. Fox's guide to chicken security". What should be worrying for those of us passionate about the potential for ICT in education is that technology *qua* hardware and software is inseparable from the culture and politics that envelope it, so unless current trends are arrested these wonderful tools of potential empowerment will surely become shackles of mind-control. In this sense we interpret security as '*security from...*'. Security from control and malinfluence is absolutely aligned with all senses of *freedom*.

For most of us though, encounters with "security" are overwhelmingly negative. As Ensler writes in *Insecure at Last* (Ensler, 2006), it's "authentic insecurity" that's missing today. The kind that builds awareness and real strength. The paradox here is that real security is like exercising for health - someone else cannot do it for you. The more dependent one becomes on outsourcing responsibility, the weaker one grows. Schools and even universities now spy on their students ostensibly to monitor bullying, alcohol, gangs, underage sex and terrorism. While this seems justified to a minority crippled by fear, the reality is that we are naively pouring fuel onto a bonfire of trust, undermining earned maturity and genuine social awareness - ultimately the most important things that formative education can offer.

Obviously, schools and universities, even in legal *loco-parentis*, have no legitimate role as quasi-police. In the US and UK tragically misguided government regulation aligns with corporate profit motives to put armed cops in classrooms, metal detectors, barbed wire and CCTV at school gates. We inflict upon our young people a culture of over-monitoring, highly corrosive to learning relationships. RFID badges track student location, building intricate behavioural profiles. Parents in the UK are fined if they take their stressed kids for a day at the beach, as relief from relentless standardised test drills. Childhood depression and university student suicides grow each year. Schools, embracing the worst technological indulgences of Bentham's micro-managerial control (see Brunon-Ernst, 2012 for a modern account) are little more than prisons, and the solution for children with higher human aspirations, who do not fit into the machine, is to medicate them.

We are raising a generation who will be turned easily against occidental liberal culture, towards a deflated, one-dimensional conceit of 'progress'. For example; the anti-vaccine movement highlights a growing neo-Luddite trend amongst the young, middle-class, and well educated. It is not as the press might have us believe "uneducated idiots" leading this catastrophe, but those intelligent enough to rightly suspect their trust in institutionalised technology is being abused. Those who doubt the sincerity of institutional care find a lucrative market for "alternative science" exists to comfort them. Attacking the pushers of junk science is picking the wrong target. Plenty more peddlers of alternative facts will spring up in their place to meet demand. Security in

this sense is about rebuilding trust, not imposing truths.

This kind of reaction is one which we are starting to see in digital technology. Educational information about complex balances of threats and benefits, at an individual citizen level, must be re-aligned with liberal interests, by treating citizens as adults. It must not be deceptive. It must not be unverifiable in principle (such as hiding behind secrecy). Failure to achieve this basic quality standard is a collective societal suicide. Since Edward Bernays (Bernays, 1928) misused psychoanalytic theory for advertising, and governments in the 1950's and 60's embarked on Cold-War mass mind control projects, systematic deception became an expected norm. Systematically distorted communication is part of everyday life now, while real science and reasoned discourse, which has always been a marginal exception rather than the rule, is increasingly on the back foot. The disingenuity of politicians and intelligence agencies who sow discord and confusion to serve their parochial interests now constitutes an additional *real* threat to existing *actual* security problems. These actors are unlikely to take the moral high ground any time soon.

As teachers and parents, we disappoint our young men and women by failing to stand up to, and set a good example in contrast to, predatory corporations and misguided governments. This also threatens our economic future. My experience of talking to young people in universities indicates they have no desire to grow up to work for government or for the likes of Google, Facebook, the NSA or GCHQ (and if people in those places don't know that, they should urgently spend time talking to their kids). This is a tragedy on many levels, because while civic and commercial structures need fresh blood a huge recruiting crisis is emerging. Thus the advantages of scale, and the positive, even necessary aspects of big-tech and state apparatus, are subverted and sabotaged by the likes of James Clapper lying under oath (Fung, 2014) about the misdeeds of the NSA, and Mark Zuckerberg showing sneering disrespect by calling his Facebook users "Dumb fucks" (Tate, 2010). In this sense, another security problem is *contempt.* It's a problem because most real security solutions are long-term compromises between competing interests, and there can be no compromise so long as there is a lack of *good faith* arising from arrogance. In the 20th Century, the Northern Irish, Arab-Israeli and many other conflicts should have taught us that superior strength or even outright victory are insufficient to win security.

Another obvious disconnect concerns the role of women in tech, which has received significant press lately. We pretend to wonder why there are few women in tech, proffering silly theories about the workings of women's brains for engineering, or bemoaning the patriarchal structures that discourage women. But if, as a large body of research indicates, it's true that women have increased emotional attunement to negative behaviours, then their representation may have an entirely different explanation… namely that much of "tech" these days is a circus of thinly veiled abuses dressed up as business. It's not that tech doesn't interest women they just feel they can do better than that in life. What if it's our Western "enlightenment" narrative about the liberation and empowerment of technology that is wearing thin? Are women looking at the most visible *ends* of digital technology, seeing systems of

control and domination, and looking for other paths in life? If so, we need them in technology more than ever.

What future is there for industries that are increasingly predicated upon deceiving and spying on each other? I believe they will be exclusively staffed by over-40s before long. A substantial reactionary disconnect from technology by young people is looming. It's no secret that Silicon Valley tech leaders keep their own children far away from mainstream online social media, and that "the next cool thing" for young people will be going "no tech". Will we support them in that? Will we stand behind our teenagers when *they* decide that carrying a smartphone is something only for "silly old people whose brains stopped working"? If we want to preserve the advantages of a technologically enabled society then we have a generation that needs urgent help re-imagining technological relationships and building free, open, distributed alternatives for every kind of digital technology. We need to keep them on board with computer science as a progressive rather than oppressive project.

Finally, there is the most frightening prospect that as we are losing control of digital technology corporations and governments are experimenting with AI in ever more adventurous ways. That is not to say that AI cannot serve humanity with immense benefits, but in all likelihood, it will amplify our existing problems first, and we will not survive that. Humans must face the fact that we will have to fight machines at some point. Most thinkers consider that an unwinnable battle, in the same effective category as nuclear war.

Fools who think they can infallibly control the machines, and so act recklessly, must be considered themselves as a new class of threat toward which Humanists should direct a counter-social-engineering effort to challenge foolish utopian ideologies. If history has taught us anything, it is that when we hear the word "safeguards" from corporations or governments it is time to *really* worry. Safeguards are only ever sticking plasters applied to give a token veneer of action after it is already way too late. We know that neither the capital projects of corporations nor the social aims of governments are sufficient to steer the course ahead of us, not without a third arm of powerful civic mobilisation rooted in early education. If we can give people the ability and will to understand and control technology, and, if necessary, turn it off until it is (or we are) ready, the future may be very much brighter.

Challenges and Funding

A difficulty in getting support for a project of civic cyber-security is presumably that governments, corporations and other potential funding sources are ambivalent about it. They rely on weakness for their own ends. Official cyber-security projects are designed to maintain the corporate status-quo. For freedom and democracy, the issue is that these institutions are part of the problem. Cyber-security *from* the corporate surveillance state is needed as well as cyber-security *for it*. An obvious conflict of interest exists, and it seems reasonable to suspect that while vigilant elements of government do

acknowledge cyber-security as a national interest, neither government nor industry in general really want it widely taught. Or rather; a hopelessly limited interpretation of it is begrudgingly supported.

There is a fledgling movement around “Technology in the Public Interest” (Schneier, 2019; Slaughter, Walker, & Kramer, 2019) which is promising, because it offers a banner for a swelling group of deeply concerned scientists and developers who have until now been marginalised and even ridiculed. However, it remains to be seen whether any centre of this association, which is ostensibly funded by the Ford Foundation, can hold loyal to “the public” once the required opposition to entrenched power becomes clear and urgent to those involved. So long as powerful individuals believe strong civic culture of technologically informed citizens would subtract from their power, the only entities worthy of defence will remain giant businesses, not citizens.

Whereas the UK created a very promising looking new agency as an adjunct to GCHQ, the NCSC disappointingly turns out to involve an alliance with a questionable (Salcito, 2019) US defence corporation, Northrop Grumman. Although several people have suggested we obtain funding from them, there seems little hope that would work out well given the Northrop Grumman's record, so we must presently look elsewhere for assistance with the project. In 2018 I wrote a research proposal trying to cement links between British Army 77 brigade, where I had a reliable colleague, and Solent University. The idea was that since education and positive influence campaigns can fall quite nicely under the remit of "positive psychological operations", we might be able get a grant for research on a set of powerful taglines, slogans and accessible maxims - all aimed at raising awareness of collective cyber-security obligations and rights. Unfortunately, Solent University rejected the proposal as "too complex to understand", so we were unable to progress.

Philosophy and Methodology

Cybersecurity is better understood, not as a set of technical problems pitting attackers against defenders, but as a set of socio-political tensions around identity, accountability, loyalty, commonality, convenience, efficiency, sharing and much more. Within this multi-dimensional space, the positions of governments, corporations and citizens have diverged. Power asymmetries have evolved around intellectual property, the financialisation of personal data, and ownership of the means of communication and payment. The idea of digital technology as “a tide that raises all ships”, something that ultimately benefits all of humanity, must be re-examined. Schneier suggests that technology always offers a first advantage to progressive forces (Schneier, 2012), but then empowers conservative ones after a phase lag. This seems only partially correct, in that we see more than a simple question of flexibility versus inertia. There are many malevolent progressive forces that are enabled, and many positive conservative forces that do not benefit.

There is some element of zero-sum dynamics at play. Security for one group is insecurity for another. Technologies that enable one group can disable or

suppress another. In light of Edward Snowden's revelations of ubiquitous illegal mass surveillance, the Cambridge Analytica scandal, and Trump and Brexit elections, we've entered an era where the internet's benefits are leveraged by well-resourced minorities against the remainder. Familiar tools we use daily are now identified as a threat to democratic life, and even to individual mental health. An impending implosion of social media is overdue as polarisation and partisan censorship grows. There are no credible authorities to turn to. Those vying for moral high-ground are all visibly, often unashamedly, hypocritical. With national firewalls, walled gardens, blacklists, kill-lists, purges, payment blockades and takedowns, the internet has never seemed more divided into hostile fragments.

The early internet was based on egalitarian assumptions, which were never explicitly examined. So, they were never truly valued. How do we now recover what is in all of humankind's interest? The necessary insights and answers cannot be obtained by technical analysis. I have tried and failed to reach more than a few percent of already technically literate high IQ students through treatments of cryptography, graphs and routing, protocols, exploits, game theory and trust models - and I immodestly consider myself a versatile and capable teacher. Somehow computer science became “everybody's problem” but rather few of us are adept at grasping computer science.

Reflection upon course feedback from the first Digital Self Defence classes indicated which bits of the lectures were reaching students. I soon realised a complete change of tactics was needed. Just as we had to learn by analogy in 1980 that “computer memory is like a box”, the key elements of cyber-security need an approachable formulation.

New Problems, Old Solutions

So, it is through drama, poetry, literature, film, classic tales, anecdotes and metaphors that a powerful understanding of modern cyber-security concepts can be obtained. Medical analogies from infection control, immunology and contagion models are also valuable. So are concepts from biological, evolutionary and genetic science.

Our problem, and opportunity, is that real life is converging with dystopian fiction. Rather obviously, insights and answers are close to hand in the writings of Goethe, Ibsen, Mary Shelley, H.G Wells, E.M Forster, George Orwell, Kurt Vonnegut, Philip K. Dick, Ursula Le Guin, Issac Asimov, Arthur C. Clarke, Aldous Huxley and so many more. As for Machiavelli's *The Prince* (Machiavelli, 1513), the material can also be read as a warning and means of disarmament. The ‘manuals’ that opponents of freedom have used to build a dystopia also contain the knowledge to dismantle it.

Alas it seems that few people read books these days, but we do have film. Since Georges Melies 1902 screen version of Jules Verne's *A Trip to the Moon*, from *Metropolis* to *The Matrix* we've had wonderful cinematic worlds conveying important messages about technology. Thanks to Kubrik,

Rodenberry, Cronenberg, Scott, Gilliam, Godard, Lynch, Zemeckis, and so many talented directors, difficult technical issues can be made beautifully clear so long as we know how to interpret and present them to students. Television gives alternative accessible forms via programmes like *The Outer Limits*, *Twilight Zone*, *Dr Who*, by screenwriters like Terry Nation. One of the freshest is Charlie Brooker's *Black Mirror* series.

By exploring archetypes of the Mad scientist, the Monster, the Overreacher, the Faustian Bargain, Medusae and Hydras, we can situate abstract digital concepts in accessible narratives. Some obvious classic choices are *Dr. Strangelove*, *Gattaca*, *Eraserhead*, *Frankenstein*, *They Live*… but marginal films and books are useful too. For example; we often start a lesson with a clip from the opening scenes of Spielberg's *Schindler's List* (Spielberg, Zaillian, & Keneally, 1993). When asked about the film most people recall a scene of horror, of Nazis shooting children. But in fact, the first scene is a careful choice by the director. It is a mundane shot of a small, innocuous table with a bottle of ink, and an official asking a line of Jews, "Name please?!".

This leads us easily into a discussion of lists, data and identity, which are powerful story themes, and then to a discussion of Edwin Black's 2001 text *IBM and the Holocaust*. This technique allows us to explore themes which cannot be approached “head-on” in their present technological context. For example; the tension between ancient mores and superficial legal tyranny in Sophocles’ representation of Antigone's dialogues with Creon is a wonderful way to show young people that such struggles have existed for millennia. It releases them from compliance and parochial fear of authority - to become technological freethinkers capable of asserting their own ideas onto their digital world.

Other-worldly stories also help to overcome the considerable psychological barrier of closed-mindedness and anti-intellectualism of western culture. Our nonchalant dismissal and urbane detachment make us quite resistant to difficult messages. When they clash with our cherished worldviews, they cause cognitive dissonance. The so-called "snowflake" mindset is an extreme form of this fragility. However, when unpalatable morsels are flavoured as ancient stories young people have more appetite. Now they see why history and literature are such dangerous subjects, because they can give clear voice to perennial complex issues otherwise dismissed as "conspiracy theories", "politically incorrect" or "too scary to think about". The strength of the cannon is that it blasts through all petty and parochial guises of fascism.

Positive Messages

The aim must not be bleak technological critique in the vein of Ellul, Postman, and McLuhan but a clear call to “take back technology”. Neither must it be an exhortation to abandon technologies or attack its proponents, lest we become disaffected Ted Kaczynski type recluses living in woodland shacks. The need for a new social contract that puts technological development in the hands of citizens is a key theme. Organisations like the Free Software Foundation

(FSF) are on the right track, but championing Free software, or ubiquitous strong encryption is not enough (it leads to its own problems). Mature new understandings of hardware and data as pollution problems have resonance with students already disgusted by environmental destruction. The idea that there is a “digital environment” which is an extension of our physical ecosystems, makes sense. So do treatments of convenience and dependency as drug-like vulnerabilities. Messages already understood by students about drugs and addiction are easily adapted once digital technologies are understood analogously. We wish to replace starry-eyed cargo-cult fawning and fetishisation of technology with measured scepticism.

Restoring our technology to serve us once again is the goal. In a wider sense, we also hope to explore general counter-influence tactics. And, without any pretence at value neutrality, to bolster liberal European values and traditional ideas of the "good life". The kind of obsequious technological deference that allowed companies like Apple and Google to become so powerful, needs burying. For Europeans, the destabilising, discordian techniques of Russia and the USA dazzle us as we try to navigate the interregnum of technological "post-truth". We are no longer experiencing Baudrillard’s *Ecstasy of Communication* (Baud, 1988), rather Owen's “Ecstasy of fumbling” (Owen, 1920). Arthur C. Clarke (Clarke, 1962) got something half right when he said; “Any sufficiently advanced technology is indistinguishable from magic”. He should have added “to sufficiently lazy minds”. Those who let themselves be governed by magicians have, historically, fared no better than those ruled by jugglers and jesters.

An interregnum is a period when many people are confused about the meanings of ideas like security, community, freedom, truth, debate, privacy, public spaces, experts, opposition, hate and news. Nobody can hope to challenge such powerful tides of history, but sensible realism is not the same as giving up on navigating a way through the storm. The currently parochial project of "cyber-security" needs reconsidering, as a much bigger game, as a grand civic, Humanist undertaking. It needs updating to include propaganda and disinformation as first-class threats. It needs modernising, to recognise certain architectural patterns of political and business logic (so called Dark Patterns) as intrinsically harmful. It requires introspection, to see how some of its own practices can be harmful and its goals dishonest. This can be achieved by massively widening the audience in a project similar to the "computer literacy" projects of the 1980s. Without a will of the people to retake charge of our digital technology it’s not only money, personal data, business secrets, computing assets and military infrastructure that are targets - but our culture itself is at risk from threats within as well as outside.

References

Anderson, R. (2008). *Security engineering (2nd ed.).* Hoboken NJ: John Wiley & Sons.

Baudrillard, J. (1988). *The ecstasy of communication—Semiotex (e)* (B. and C. Schutze, Trans.). New York: Autonomedia.

Bernays, E. (1928) *Propaganda.* New York NY: Liveright.

Black, E. (2001). *IBM and the Holocaust: The strategic alliance between Nazi Germany and America's most powerful corporation*. New York, NY: Random House Inc.

Bowlby, J. (1988). *A Secure base - Clinical applications of attachment theory.* Routledge: London

Brunon-Ernst, A. (2012). *Beyond Foucault - New perspectives on Bentham's panopticon*. London: Routledge

Clarke, A. C. (1962). Hazards of prophecy: The failure of imagination. *Profiles of the Future, 6*, 36.

Curtis, A. (2004) *The power of nightmares: The rise of the politics of fear* (Vol. 20). UK: BBC Television

Ensler, E. (2006) *Insecure at last: Losing it in our security-obsessed world.* New York NY: Villard Books.

Fung, B. (2014, January 14). Darrell Issa: James Clapper lied to Congress about NSA and should be fired. *Washington Post,* retrieved from https://www.washingtonpost.com.

Gov.UK. (2014, March 13). School children as young as 11 to get cyber security lessons. Retrieved from https://www.gov.uk/government/news.

Lee, S. (2019) *Stewart Lee's comedy vehicle (Series 3,* Episode 1*).* UK: BBC Television

Machiavelli, N. (1984). The prince (1513). *New York: Bantam*.

Meadows, D. H. (1997) Places to intervene in a system. *Whole Earth, 91*(1), 78-84.

Méliès, G. (1902). *A trip to the moon*. Star Film [empresa de producció].

Owen, W. (1920). Dulce Et Decorum Est. *Compendium of World War I*. UK: British Library

Raymond E. S. (2001). *The cathedral and the bazaar. Sebastopol CA:* O'Reilly Media, Inc.

Salcito, K. (2019, May 13). Shareholder resolution asks how Northrop Grumman implements its human rights policy. *Just Security* (New York University School of Law). Retrieved from https://www.justsecurity.org

SBS. *(2012).* Cryptoparties teach data privacy to the public. *Cryptoparty Sydney.* Sydney: SBS World News. Retrieved from https://www.sbs.com.au/radio/video/

Schneier, B. (2008) *Schneier on security.* Hoboken NJ: John Wiley & Sons.

Schneier, B. (2019, Jan/Feb). Cybersecurity for the Public Interest. *IEEE Security and Privacy Magazine*.

Schneier, B. (2012) *Liars and outliers*: *Enabling the trust that society needs to thrive.* Hoboken NJ: John Wiley & Sons.

Slaughter, A., Walker, D. and Kramer, L. (2019, March 12). Building the field of public interest technology. *Inside Higher Ed*. Retrieved from https://www.insidehighered.com/

Spielberg, S., Zaillian, S., & Keneally, T. (1993). *Schindler's list.*

Amblin/Universal.

Stallman, R. (1997). The right to read. *Communications of the ACM, 40*(2), 85-77.

Symonds, T. (2017, Feb. 11). Cyber security lessons offered to schools in England. UK: BBC. Retrieved from https://www.bbc.com/news/

Tate, R. (2010, September 13). Facebook CEO admits to calling users 'Dumb Fucks'. *Gawker,* retrieved from https://gawker.com.

Tulsa Regional STEM Alliance. (2016). GenCyber Tulsa – The University of Tulsa**:** GenCyber teacher workshop: Building cybersecurity capacity via sustained teacher training. Retrieved from https://tulsastem.org/gencyber-tulsa/

U.S. Department of Homeland Security. (2013, Feb. 21). DHS launches national initiative for cybersecurity careers and studies. Retrieved from https://www.dhs.gov/

Vodafone. (2009, Nov. 15). Vodafone launches first comprehensive website to help parents get to grips and get involved with the 'Twitter Generation'. Retrieved from https://www.vodafone.com

Woerner, R. (2015, July 6). Hacker high: Why we need to teach hacking in schools. *Tripwire*. Retrieved from https://www.tripwire.com

Author Detail

Dr. Andy Farnell
sol@aspress.co.uk