Security Lancaster | LANCASTER UNIVERSITY

# The Future of Digital Disrupters
## Rethinking the Digital Divide

Dr Mark Lacy and Dr Daniel Prince

Security Lancaster: Security Futures

# Contents

# Abstract

*While we might want to keep a critical distance from the concept of Moore's law in debates on the future of technology and computing, it is clear we will continue to face radical and disruptive change as a result of technological change: disruptive change that takes all sectors of society by surprise (from the smart phone thief who posts 'selfies' that can be viewed by the owner on their iPad through to the politicians and security experts who confront the 'curse' of twitter in times of social unrest). What we call digital geopolitics confronts citizens, business, organized crime, politicians and activists with new opportunities – and new problems: the challenge is to work out what the potential 'black swan' events could be in societies that – by design or default – are digitizing all aspects of life. The messiness of digital life is compounded by the broader economic and political uncertainty of the times we live in, a time where geopolitical change is* accelerating *(the transition to a multipolar world of emerging economic superpowers outside of the West) and economic growth is – at least in Europe –* decelerating *(where there is uncertainty about the long term consequences of both financial crisis and broader geopolitical/economic transformations).*

*This report sets out to explore future social problems in a world of disruptive technological change and economic uncertainty. In particular, we are interested in thinking about what a 'digital divide' means in a world transformed by Moore's Law. What will the digital lives of people 'on the margins' look like in the coming years? What type of smart device will even the poorest sections of society be using by 2020? How could young people, confronted with economic uncertainty and insecurity, use their everyday 'tools'? As a way of opening up debate we imagine a future scenario about an event in 2020: a short story is a provocation to open up thinking about the future of technology and society. We suggest technical solutions to manage the young people of the future in Europe is unlikely to be effective; we might have to confront more profound social and economic questions about the future of society.*

# Introduction

*Security Futures, in conjunction with Digital Disruption, ran a workshop to explore what it would mean to be a 'Digital Disrupter' in the coming years; in light of the rapid socio-technological change we see accelerating around us, a critical discussion about the emerging problems and opportunities of new technologies – and their use (or abuse) by young people – was seen to be a useful element in debate over security and society in Europe.*

This discussion brought together academics from different disciplines with experts from the Digital Disruption Project and Bold Creative. Bold Creative is a media-technology company from London focusing on unlocking the potential of youth audiences by listening and understanding them in order to build more inspiring connections for brands and causes. This work led to the establishment of the Digital Disruption Project which has been working on the problems faced by young people negotiating both new technologies and inner city life. This has involved looking at the problems of radicalization and the Internet.

The plan was to see what problems and questions could emerge from a dialogue between academics, activists and business. The workshop was an opportunity to have a multi-disciplinary discussion on emerging trends in order to think through future security problems: problems policymakers might want to think about and problems on the margins of traditional thinking about security and policing. This paper presents those discussions and the dialogue and collaboration that followed. In following the spirit of the digital disrupter - and the approach of Security Futures- the authors have chosen to adopt a disruptive and unconventional methodology to present their findings. The mode of presentation is as provocative as some of the scenarios and questions contained in the paper – confronted with an 'accelerated reality' we think it is important to open up our thinking about the problems on the horizon.

*Would it be misguided to think that a Europe dealing with high levels of unemployment as a result of financial crisis and confronted with deeper geopolitical change would be one where marginalized young people would lack the technical skills to be digital disrupters?*

*Will the idea of a 'digital divide' seem out-dated in a time when technology continues to become cheaper and more powerful (and easier for 'digital natives' to use creatively)?*

These questions provided the starting point for the workshop. What emerged from the discussion was a complex series of interconnected trends woven together, a future scenario where more and more aspects of life are networked and digitalized, cultivating a terrain with increased opportunity for digital disruption.

This context raised a number of questions for the participants: would future disruption to society be limited because there wouldn't be the sufficient 'skill set' to cause serious disruption? But what if the technological culture was such that young people – even young people in the poorer sections of society- had the tools and the 'know-how' to cause complex disruption for the networked society? What if the digital literacy of the young was at a level where they could pose unprecedented problems for a highly networked (and vulnerable) society? Should policymakers be concerned about this possibility? What problems could be caused across Europe by a generation who aren't living the lives they see advertised – and a generation that have the tools (in their pockets) to generate disruption? What disruption could they cause? What if the 'digital divide'

imploded when even the poorest had technology far superior to what the richer members of society now consume? What if there was a 'digital underclass'? Is this an area where we are failing to grasp the radical implications?

# Workshop Methodology

Underpinning the workshop were two assumptions. First, given universities contain a variety of researchers working across many different disciplines, they provide a resource *ideal* for the creation of a multi-disciplinary dialogue - in collaboration with external partners - in order to explore current trends and problems. Many of the problems we confront – problems, for example, linked to cyber security and climate change – require this type of multi-party collaboration if we are to be able to generate the type of research and discussion needed across the worlds of policy and industry.

Second, one of the insights that emerged in the literature on risk in recent years is on how people become *habituated* to certain ways of seeing the world (Taleb, 2010). Human beings can become habituated to the values and ideas in an organization in a way that– while it might have short term value to the running of an organization – can limit critical thinking and ideas about problems. Certain questions or interpretations are not permitted to be asked; and some questions or interpretations are simply not generated due to organisational culture. This workshop created a space where we could bring together people working on the cutting edges of technology with people working on social, legal and political questions about the world we live in: an open space where we might begin to see the emergent problems we didn't even know were on the horizon.

The reason we think it is important to have a space to explore future problems stems from our view that the acceleration of power and capacity in technology is leading to exponential and disruptive change, change that impacts on all aspects of society. This fast, exponential growth leads to a 'non-linearity' that makes it even harder to think about the inevitable uncertainties of the future. What will personal computing look like in five or ten years? How will new technologies transform how we communicate, educate, do business, organize our lives? What will social networks look like in ten years? How will these networks transform how people organize politically across time and space? How will these social networks impact the worlds of consumerism and marketing? And what are the developments that might make our current interest in social networks or computing look 'quaint'?

Consider two of the most fundamentally changing technologies of the last three decades, the mobile phone and the tablet PC and their popularisation by the Star Trek TV series'. The original series of Star Trek was broadcast in 1966 and featured the "communicator". The first commercially available mobile phone was available in 1983, 17 years from fiction to fact. Star Trek: The Next Generation aired in 1987 and featured "Padds"; in 1999 the first commercially available tablet was released, 12 years from fiction to fact and also orders of magnitude more technologically advanced than a mobile phone. These fiction-to-fact examples demonstrates the power fiction has in the process of developing future scenarios and should therefore be included as a tool to explore the future: what are the products and ideas - in their infancy – that designers and technologists are beginning to imagine and develop?

One current concern is the digitalisation of all aspects of the state and business. There is a desire to use new technologies to enhance the speed and efficiency of all aspects of our complex state bureaucracies, from medical services to benefit payments to policing. But what are the glitches that could surface in our race to digitalise all aspects of life? How might our desire for digitalization lead to new vulnerabilities? If things go wrong – how 'messy' will an accident look like in a fast, networked world? What, for example, would cybercrime in our financial systems look like in coming years? How destructive could the impacts be? How would it be possible to orchestrate attacks on financial systems? How would you have to exploit human and technical vulnerability to create new types of cybercrime?

# The Way Forward

We believe the power of digital disrupters is set to increase and has the potential to create dramatic and unimaginable changes in the way society interacts with each other and in economic and political governance structures. From our perspective, the use of the term digital disrupter is ambiguous: creativity depends on disruptive thinking and practice; in some political and economic contexts we might welcome a generation of digital disrupters. Given the potential for disruptive change and the potential positive impact this might have, we believe it is important for policy makers to ensure that the responses they take in order to protect societal values do not simultaneously limit the creative benefits of the digital disrupter. At the same time, a new generation of Europeans might be able to cause digital disruption that will create serious challenges for all aspects of the network society: questions about the radical possibilities of technology might renew the need to open up radical thinking about social policy and social exclusion.

*We believe that any policy makers should consider the following set of principles in any response it might make to digital disrupters in order to maximise the benefit that they could create for society.*

- *Principle 1: Do not plan for a uniform digital divide, Moore's Law makes it messy and fragmented,*
- *Principle 2: In order to understand and benefit from digital disruption we need to adopt innovative digitally disruptive practices*
- *Principle 3: What we consider exceptional now will become the norm tomorrow*

# Background to the Future

*The idea behind the workshop on the Digital Disrupter emerged from a number of different events alongside our research on the impact that technology is having on society and in particular younger generations.*

## *The Digital Divide does not exist.*

At least not in the way that it is commonly perceived. Much is made of the 'digital divide' in the context of societal groups within a nation or in comparison between nations in a global context. The divide is an attempt to measure the disparity in the access to- and understanding of - information communication technology- between these groups. We argue that Moore's Law actually helps to bridge (or destroy) this divide rather than the general perception that the introduction of new technology increases it. Defined in 1965 by Gordon Moore, Moore's Law (Moore, 1965) is both a predictor of the average growth in the number of components that can be placed on an Integrated Circuit (IC), which is a measure of the computation potential a device has, and also an evolutionary indicator for those societies at the cutting edge of technology development. The predictive capabilities of Moore's Law can be viewed in two fundamental ways; either the computational power of devices doubles every 18 months, in line with the number of components available on the IC -or the price for the same computing power halves every 18 months. To put this into context: the Lawrence Livermore National Laboratory in 2012 reportedly spent roughly $250M to create the world's fastest supercomputer the IBM Sequoia (Brodkin, 2012). According to Moore's Law, before a child born in 2013 turns 30 they will be able to purchase this cutting edge technology for the same price that we can buy an iPad for today. What we consider super-computing today will be what our grandkids will play Angry Birds on tomorrow.

However, there are some important caveats to Moore's Law that are worth mentioning. First, Moore's Law is commonly interpreted as an increase in computing power rather than the actual statement regarding the number of components on an IC, due to the link between the IC component count and the potential this provides for computational functionality: this correlation, however, may not always follow. For example, advances in parallel computing architectures have accelerated the rate of computation beyond that which Moore's Law predicts. Given this, and for the purposes of this paper, we will use the increase in IC component count as an indicator of computational capacity. Second, as the law states it is an average, an average of the rate of change in component count and therefore computing power. It therefore smooth's out the rapid increases and the slowdowns. As we will argue later it is these transitions in pace that can cause some of the most radical disruption in society: Moore's Law hides this from our consideration. Finally, it is important to understand that the law only really holds for mainstream consumer electronics and does not necessarily hold for all forms of digital equipment (Meyer, Zhang, & Fall, 2007). This last point identifies that not all technology evolves in lock step. Arguable some of the more interesting and niche technology developments evolve at rates very different to those of the mainstream evolutionary branch. It is these discrepancies which again can provide grey areas where disruption can thrive.

These tendencies can have a big impact on the digital divide between groups within nations. The rapidly falling price enables access to sophisticated technology for all socio economic groups. While the Law of the diffusion of innovations (Rodgers, 2003)tells us that there will always be a set of "early adopters", the early and late majority will always have access to technology in order to support common daily activities. Rather than

underpinning the technological access interpretation of the Digital Divide, Moore's Law undermines it. Moore's Law is has the potential to be the great equaliser, enabling access to technology quickly and easily for all demographics. Further, the digital divide argument is now not about how much personal computing power and storage an individual owns but how much can they access. Relatively low powered devices with limited storage can access large processing and storage clusters from any geographical location facilitated by our complex and high speed telecommunications systems as a pay for service. Why would a digital disrupter need all the equipment in their bedroom, when they can obtain the latest high powered computer, with considerable storage, high speed network access and full business continuity for free from the Amazon EC2 (Amazon Inc, 2013), accessed via an Internet enabled mobile phone on the cheapest mobile phone contract, which would run at £10 a month? So for the price of 22 Big Mac Meals from McDonalds it is possible to set up a sophisticated technological platform today.

The final element of Moore's Law that needs to be considered in relation to the global digital divide is the fact it only relates to the evolution of technology with regards to those at the cutting edge of its development. If you are not at the cutting edge of development you can make leaps through the evolutionary timeline without having to take every step of the development. This can be evidenced by the rapid adoption of mobile phone technology in Africa, rather than the rollout of hard wired land line systems (Acker & Mbiti, 2010). This bypassing of evolutionary steps creates significant social change as the speed of transition is immense, giving society little time to adapt but significant opportunities for growth and beneficial change.

One of the key issues is whether 'digital capitalism' is creating a new economy where technology is bringing more and more people around the planet into the information age, with better employment prospects, health and education – or whether a global economy is emerging where opportunity and profit is increasingly centralized among those who are designing digital capitalism, with technology erasing jobs that have yet to be replaced (Lanier, 2013). In the context of Europe and North America, it could be argued that the problem is the emergence of digital capitalism during a time when geo-economic power shifts to China/India: all underpinned by an economy responding to years of financial crisis. To be sure, the opportunities for young people might deliver possibilities unimaginable for previous generations (and across the planet). Yet we suggest that whatever the economic context, the digital terrain will be full of opportunities for digital disrupters: and, in many ways, the numbers of 'digital disrupters' might not be as important as they might have been in previous times: we live in an age where smaller numbers of people have the capacity to orchestrate events that would be impossible for previous generations.

# Speed, Security and Radical Social Change

There are two narratives that often dominate discussions about the future of security/ crime, technology and young people. The first position is that governments will be able to use techniques of risk-assessment and data mining in order to identify children/young people who may grow up to problems for society; pre-emptive strategies coupled with new technologies of surveillance and control will enable societies to manage future disrupters (The Cabinet Office, 2007). The second position is that societies are increasingly fractured: contemporary Europe, for example, is seen to confront a future where unemployment - and more 'precarious' forms of employment – create a social landscape that lacks cohesion or a sense of a shared purpose or set of values. The diversity of contemporary society can exacerbate the sense of no longer living in a shared space. In this context, the 'digital divide' is no longer geopolitical (or divided on North/South lines); the divide between the networked, information elite and those left behind is acute at the domestic level of 'developed states'. The divisions in society will intensify between the highly educated 'globals' and those who live on the edges of the global economy, the 'locals' who are confused (and angered) by the rapidly changing worlds around them (Bauman 1999).

These narratives lead to conclusions that continue the preoccupations of policing and security in the modern age: develop policing strategies that are able to prevent the dangerous 'multitudes' from reaching 'tipping points' where behaviour becomes a threat to economy and society. The threat is viewed primarily of the damage that young people can inflict on property (burning down buildings, looting private property, preventing the normal activities of the city) – but underneath this is a fear of more revolutionary organization (radical political movements that see the creation of a new society and economy). The logic of policing and security in the modern age has been focused on ensuring that potentially disruptive activities can be contained (through urban planning, welfare and education schemes and surveillance). The anxiety has been driven primarily by the fear of gangs and riots, the activities of 'packs' and 'networks' (in the context of radicalisation and terror), and the possibility of revolution or revolt (Virilio, 2006).

Police in France or England in the 18th or 19th centuries would understand the problems confronted by police in England during the riots of 2011 (although the 'tools' of communication might shock them). They would understand the problems of managing the 'feral' under-classes, those outside of 'civilized' society: the production of order and security in public space.

We begin from the assumption that the acceleration in digital culture is not simply an acceleration exploited by the affluent and educated 'globals': we have already seen how technology can be used as tools in the context of a riot – but what will digital natives be able to do in 5 or 10 or 15 years? What type of technology will a young person in a low income household have access to? And what level of education would they need to do things that we would currently think are very clever? How would they be able to undermine the technologies increasingly used to manage and control them? What would they be able to do a critical digital infrastructure out of *boredom*?

Of course, we have no way of knowing whether the security solutions of the future will eradicate the glitches and flaws in new technologies that can be exploited by digital disrupters. Will growing complexity and sophistication in our digitalization of society proceed with better digital security and protection? Or will the intensifying digitalizing of society lead to increasing vulnerability? In economic terms, will Europe overcome financial crisis to develop industries that will offer decent prospects for young people in a time where other regions are moving ahead? Will the digitalization of society intensify inequality, centralising the economic 'good life' in an elite and leaving the rest in increasingly underpaid and dull jobs? We do not know how the economic situation in Europe will play out – but what interests us is the issue of young people and technology: are we failing to grasp the implications of Moore's Law for the future use of technology by young people? What types of problem could be on the horizon? And what could we start doing now to prepare for a future where the individual – even the poorest and most marginalized – could be 'tooled up' with technology that is far more advanced than even our most powerful contemporary technologies? What will the digital gangs of the future look like?

# Case Studies

Here we present a number of key examples that we believe capture the attributes that need to be considered in order to define a digital disrupter.

### UK Riots

The riots in the UK in 2011 saw young people using their mobile phones, social media sites and other technologies to organise fast, swarm-like behaviour. These technologies enabled the rioters to coordinate themselves in ways not previously seen by the responding public services and enabled them to stay ahead of law enforcement.

*"The police were dealing with a different situation from that which they had seen before. One comment that a number of chief constables and officers have made to me is that they were surprised by the speed with which gangs were able to mobilise through the use of social media…"*

Theresa May 2011 (Houses of Parliament, Daily Hansard - Debate, 2011)

What also became an issue was the intelligence that could or could not be gained by government agencies in order to respond to the riots. Public sources of information - such as some social media site and mapping information - could be easily accessed,; encrypted services such as the Blackberry Messenger (BBM) service (Research In Motion, 2013) or sites governed by laws protecting civilian rights to data privacy (DPA) (Her Majesty's Government, 1998) required the use of legal approaches such as the Regulator Investigatory Powers Act (RIPA) (Her Majesty's Government, 2000) in order to access the data they contained. This legal response, with its rightly provisioned set of checks and balances could not keep up with the rapidly evolving nature of the events on the ground, with the speed of the riots driven by the participant's *augmentation* through technology. The immediate response from the government was an attempt to curtail the use of social media and provide new legislative powers.

*"Social networking sites such as Twitter and Facebook and messaging services such as BlackBerry Messenger have been used to co-ordinate criminality and stay one step ahead of the police. I will therefore convene a meeting with ACPO, the police and representatives from the social media industry to work out how we can improve the technological and related legal capabilities of the police."*

Theresa May 2011 (Houses of Parliament, Daily Hansard - Debate, 2011)

However, as will be seen later in our discussion on the definition of a digital disrupter, it was realized that such actions would have a significant impact on the possible benefits that could be realized. The riots were disruptive in the way that the rioters utilised new technologies. What is important is the positive disruptive response that this provoked. The police and communities took to using social media and other technologies in new and interesting ways in order to support the prevention of the riots and the clean-up operations that followed, as mentioned in the Riots Communities and Victims Panel (The Riots Communities and Victims Panel, 2012). Examples of this type of response can also be seen in the way that micro blogging and social media were used in response to hurricane Katrina (Torrey, Burke, Lee, Dey, Fussell, & Keisler, 2007)

### Anonymous and the Occupy Movement

While the rioting in the UK in 2011 evolved from an offline act into a physical and virtual social organism with its activities accelerated through the use of technology, the emergence of groups such as Anonymous and the various Occupy movements demonstrate the reverse path. The now iconic hacktivist group Anonymous has

been described by some media commentators as the ultimate form of democracy as it is without a given leader or organisational structure and their "operations" are solicited and supported through crowdsourced consensus. Arguable the Loki of the Internet, Anonymous assists and causes mischief in equal measure in the virtual communities it calls home and that we all interact with on a daily basis. The group is well known for its support for causes such as open data, government transparency, copyright freedom, support for the Arab Spring and vigilante activities such as project chanology and the naming of the alleged bully of Amanda Todd (Sieczkowski, 2012). However, there is a dark side to their activities as can be seen by their attack on McKay Hatch who ran the only "No Cussing Club" which was targeted by Anonymous with Hatch's personal details leaked on the Internet resulting in abusive communications to him and his family (Rogers, 2009).

Anonymous have evolved from a grass roots movement of digitally skilled individuals orchestrating attacks for the "lulz", to an online globally political, media savvy movement that is able to galvanise support for their actions beyond their immediate membership, resulting in real world disruption as evidenced by the occupy movement. This type of mobilization from below is increasingly felt in mainstream politics across Europe (for example, the success of Beppe Grillo in the Italian general elections) (Bartlett, 2013 ). Anonymous act with a single identity embodied by the character V from the V for Vendetta graphic novel, which depicts a totalitarian regime and a popular uprising. It is interesting to note the concept of a group represented by a single voice and visualisation and plays into the very question of identity in an online world. The recent report by the Department of Business Innovation and Skills (BIS) (The Government Office for Science, 2013) concluded that identifies in the UK over the next ten years will be increasingly dynamic and volatile and that the traditional notation of identity becomes less meaningful in a hyper-connected world where the virtual identity, or identities, are just as important societally, psychologically and commercially as those physical ones. The identity of Anonymous is possibly the first example of this manifestation of disruptive breakdown in the traditional notion of identity.

What is interesting is the physical manifestation of Anonymous in the real world through the Occupy and similar movements. Here the multitude-as-one identity translated into many people donning the iconic "V" masks during their protests. However, this was not the only aspect of Anonymous that spilled out onto the streets: their ingenuity and propensity for disruption followed. Live streaming blogger Tim Pool developed cheap drone technology to cover the Occupy Wall Street movement with his footage and image library being used by mainstream media companies (Captain, 2012); the occupy movement also saw ad hoc networks set up in the camps - and in nearby facilities - in order to continue the dissemination of information regarding the protests and the actions of law enforcement officers. This arguably was the first real dramatic, mass disruptive use of "sousveillance" (surveillance *from below*) (Mann, Nolan, & Wellman, 2003) to monitor and publicise the actions of those given power and authority.

## High Profile Disrupters

There have been a series of high profile digital disrupters in the news for various and significant reasons. We shall present the cases of Aaron Swartz and Bradley Manning.

***Aaron Swartz*** was born in 1986 and was quickly recognised as a leading light in the development of Internet technologies. He contributed to the development of the Rich Site Summary (RSS) feed format used throughout the Internet and was heavily involved in the development of political movements to combat copyright, helping to establish Creative Commons, organising online protests against US political bills such as SOPA. In the latter part of his life he moved away from issues surrounding copyright and started to focus his attention on what he believed to be systemic corruption in the US political system working with activists groups such as Rootstrikers. By any stretch of the imagination Aaron was a digital disrupter: he generated disruptive technologies and was responsible for significant social change and - at the age of 24 - he was made a research fellow at Harvard University. However, on Jan 6 2011 he was arrested in connection with the systematic downloading of academic journal articles from JSTOR. He was pursued on counts of wire fraud, computer fraud and obtaining information from a protected computer. It is worth noting that JSTOR refused to press charges against Swartz and - as a member of Harvard - he was entitled to unlimited access to JSTOR through the university agreement

with the company. Several commentators, including Lawrence Lessig, a personal friend and mentor, have stated that while they did not necessarily agree with Aaron's actions they felt that the government's approach was heavy handed with the potential for a maximum penalty of 35 years in prison, a $1M fine, and supervised release. After two years from the initial arrest Aaron still had not had his day in court and unfortunately on 11/1/13 he was found dead in his apartment.

***Bradley Manning*** was a United States Army soldier serving in Iraq with access to classified databases containing diplomatic communiques and other information (such as videos of airstrikes). Starting in November 2009 Manning is alleged to have started to feed classified information to Wikileaks. Then between April and November 2010 Wikileaks started to publish this information publically directly, with help from its media partners. Manning was arrest in May 2010 after disclosing what he had done to former hacker Adrian Lamo, who subsequently informed the FBI. Reaction by the authorities has been severe with claims form senior politicians and military personnel claiming his actions put people's lives at risk. Manning has so far been charged with 22 offenses including communicating national defence information to an unauthorised source and aiding the enemy, the last of which is a capital offence and carries with it the potential for life in prison or the death penalty. Public reaction to Manning's actions has been largely positive with him drawing significant support. He was nominated for a Nobel peace prize in 2011 and 2012, and voted the Guardian 2012 person of the year. Manning and Wikileaks are also widely credited with igniting the Arab Spring due to the fact that the exposed information detailed government corruption and decadence in the region.

What is important to note from the impact that these two individuals had was the governmental response to them. It can be strongly argued that both individuals were fighting for the openness and transparency of information yet with differing motives. Both have been architects of substantial social change, forcing society to take a hard look at how it and its elected representatives handle technologically augmented individuals who generate significant social disruption. What becomes increasingly interesting is when these types of individual become the norm, rather than the exception, and when individuals from all economic levels have access to powerful technology.

## The Digital Disruption Project

Digital Disruption is an initiative that aims is to improve the learning practices, personal development and social wellbeing of young people in the UK by developing their 'digital judgement': that is, the ability to engage critically with the content they consume, create and share online. Digital judgement combines 'traditional' critical thinking skills, such as source verification, with 'new' knowledge about how the digital world works, such as understanding search engines and Wikipedia.

The project kicked off in 2008, working with a group of young people to investigate the ways online video is affecting them and their peers. Key questions that were explored examined whether young people are more vulnerable online manipulation and what they need to do to protect themselves. These questions formed the basis of four propaganda educational films we produced in conjunction with young people. They sparked fascinating debate online, the project won a government innovation award and we were repeatedly asked to share our approach and resources. Following the success of the pilot project we partnered with Nominet Trust and think tank Demos to research digital literacy in the UK and bring Digital Disruption to a national audience. We developed resources and training programmes for both young people and educators that address the key issues identified in Demos' 'Truth, Lies and the Internet' report (Jamie Bartlett, 2011). In 2012 a website and teaching tools were launched and Digital Disruption was founded as an independent non-profit company, whose mission is to 'realise the Internet's potential to benefit individuals and society – as something that informs, empowers, liberates and enlightens'.

### Insights from Working with Young People

Misinformation is a significant problem as technology, and the public understanding of it develops, and more people are creating content and their own websites to host it. The volume of information online is only going to increase. This creates problems with searching for, and access to, reliable sources of information. The

Internet has removed the economic barrier to information dissemination which would have been previously seen as a mark of quality, it takes a considerable amount of money to publish and print a book and so the information it contains should, in theory, be of significant quality to warrant that expenditure. In a digital world it still costs a considerable amount of money to produce high quality information, but the cost of information publishing falls to zero (Varian, 1999). In this situation the only way to determine good information from bad is via the reputation of the publisher, there are no other mechanisms to determine quality. This is similar to the physical world where the reputation of a newspaper is an indication of quality for example. The issue online is that anyone can publish their own newspaper and publish whatever they want to.

Arguably information available online is subject to the concept of Asymmetric Information, presented by George Ackerlof as a Market for Lemons (Ackerlof, 1970). In this model information regarding the quality of a good, in this case information itself, is not made available to the consumer. This results in poor quality goods driving high quality goods out of the market place resulting in a market dominated by poor quality goods being sold at a higher price than you would expect. In this context 'price' is not the same as the cost of purchase, but rather an alternate value that a consumer puts on the information they consume. This can be seen across the freely available information on the Internet much of which is typically low quality with only a few trusted sources. An example of this is people who try and self-diagnose online - if you have symptoms some people are taking advice from YouTube videos and forums rather than the appropriate websites (Syed-Abdul S, 2013).

The quality of the information is one aspect but another aspect is the differentiation between factual reporting and opinion. This presents a big grey area in the digital world with the problem further compounded by the 24hour news service largely being composed of opinion discussions rather than factual reporting in order to produce content. In a youth group in Dover 14 - 18 year olds struggled to distinguish between fact and opinion which asks big questions about their competencies to conduct research and studies in the digital age. Given that young students these days are encouraged to discover information online from an early age. The ability to determine fact from fiction from opinion will be fundamental for generations to be able to educate themselves appropriately in a global information ecosystem where age is rarely an inhibitor to access. Will we therefore see the development of elites in online groups? People who can educate themselves effectively and consume information appropriately? Will they form niche elite subjects groups as we see with geek digital fraternities such as the Chaos Computer Club (Chaos Computer Club)? How can we create a sustainable solution in which the right critical thinking skills are taught to in order for the next generation to have the right set of skills to be able to handle a world that could be purely driven by electronic media?

The use of propaganda online is rife and presents a very real problem. The ability to collect data on every aspect of an individual's online activities enables the creation of very detailed profiles that can be used to target very specific messages to individuals. This is currently being used primarily for marketing purposes and very successfully too. The recent Interactive Advertising Bureau report by Price Waterhouse Coopers (Price Waterhouse Coppers LLP, 2012)showed that the Internet advertising has grown from a $7B industry in 2001 to a $32B dollar industry in 2011 with this trend set to continue. This adds a further dimension which needs to be considered, the information that is being consumed is being tailored on the fly to target individuals based on their behaviours and habits. Whether marketing, or anything else, should be considered to be propaganda or not is entirely subjective. However we are seeing this type of tailored message being used to target swing voters based on their behavioural profiles in the US (Wilson, 2012). Adults indoctrinate young people with their own ideals. Young people manipulate other young people to feel and do certain things. Therefore, we can accept the inevitability of propagandas existence but action is needed to highlight to young people (as the most impressionable) that they can be easily influenced and they need to realise that they are responsible for making decisions about what to believe.

It is clear we are living in a digital society and that it has a great impact on the way that our children are developing and exploring their environment. In what some have described as a "cyborg childhood" (May-Chahal, Mason, Rashid, Greenwood, Walkerdine, & Rayson, 2012) where children exist in a digitally augmented world which is neither online nor offline, but both, there are cultural differences that policy

makers struggle to grasp with regard to the impact this context has. Children are growing up in a world where their whole lives are being captured as digital information with the ability for that information to me replicated in high definition, without a loss of fidelity for the rest of their lives. While this has positive benefits in being able to recall events from the past of friendship and family a downside is that children can no longer make mistakes while learning about their world as those mistakes can be played back ad infinitum for the rest of the world – The Internet Never Forgets! This has potentially significant issues for dynamic social mobility and immigration using digital technology it is possible to migrate without losing contact with your original culture and community. Further, this original culture can be constantly reinforced from remote locations in real time, as a result the migrant is not required to integrate into their new society in the same way in order to remain functional and not be socially isolated. The can potentially result in echo chambers in the real world further reinforcing and ghettoization of cities and similar locations. This leads onto issues around collective responsibility in the on and offline world. In an online world there is no need for a community to manage antisocial behaviour in the same way as the real world as individuals can easily join and leave groups at will, whereas in the real-world it is much hard to constantly change your community as it often requires significant physical and financial cost. Further the notion of identity is wildly different. It is trivial to change identity online; an individual can constantly renew themselves at no physical or financial cost. Children are also growing up in a physical world heavily augmented with digital technology from the heavy use of CCTV to provide a means of protection and monitoring of communities to the augmentation of the visible reality from augmented reality systems such as Google goggles. How is this current and future technology given that the current youth is facing serious issues with technology and anti-social behaviour already, such as:

- Sexting - act of sending sexually explicit messages, photographs, videos between mobile devices
- Screen munching - A BBM screen capture service. Can be used maliciously to implicate others.
- Cyber bulling / Trolling - Posting inflammatory, extraneous, or off-topic messages in an online community
- Daggering -Daggering is a form of dance originating from the Caribbean. The dance incorporates sexual and other forms of frantic movement (If filmed and shared can be used to embarrass / intimidate)

The above themes and issues are all very live in schools. Despite some initiatives tackling these problems using drama and theatre (highlighting consequence) as well as digital (film and animated stories) problems are still at large, far from being solved and as the use of smart phones increases the problems are likely to get worse. It becomes of further interest due to psychological / sociological factors. Why would someone want to humiliate a peer by sending themselves pictured in intimate/compromising situations with another person? Why would someone create a Facebook group filled with hateful comments about a specific person and encourage others to join? Why would someone lead someone on via SMS with intentions of relations to then screen grab and send the discussion to peers breaking all trust? Why are most of the above perpetrators male? Could part of this be an innate compulsion to be the alpha male or part of a new wave of initiation into a digital tribe? Or does it come down to the age old issue of youth exploration and questioning authority?

# The Start of a New Path

As we shall demonstrate, our position is not that all examples of digital disruption are negative. There might be events when we want young people to be digital disrupters; disruption can be an important part of democracy and politics, ways to challenge and disrupt democratic processes at moments when politics is locked into ways of thinking and acting that need to be shaken up. Yet it can also lead to behaviour and activities that are socially and individually destructive. What interested us was this: in a world of rapid, exponential acceleration in the power of the technologies that we consume and use in everyday life, what types of problem (or opportunity) are on the horizon? What are the emerging social and technological trends on the horizon? What would a digital disrupter look like in the UK of the future? What would they be doing and what would they be

using? The subsequent section sets out our approach to seek some answers and identify further questions based on the background presented so far.

# Defining the Digital Disrupter

*At the heart of this report is the definition of what defines a digital disrupter. Our fundamental stance is that a digital disrupter is not inherently a digital criminal or that their acts are intentionally criminal in nature. The reverse is also true; not all digital criminals are digital disrupters. The interpretation of a disruptive act as a criminal act is one made by the government and legislative bodies of the day.*

What we can propose is that a key aspect of a digitally disruptive act is that it often does not fit within the boundaries and confines of current legislation, regulation and societal norms. This presents a problem government and the judiciary in how to handle these disrupters. Consider the response to the 2011 UK riots at the time by the UK Prime Minister and Home Secretary stating that they would be looking at new ways, including possible legislation on how to mitigate the impact of social media use for criminal activity:

*"What method we use is less important than the intent of looking at ways to ensure that, if social media are used for violent purposes, we are able to intervene."*

David Cameron (Parilament, 2011)

In the wake of the riots and the commitment for action by the government the Parliamentary Internet Communications and Technology Forum (PICTFOR) requested input from key stakeholders, regarding what if any legislative or regulatory changes needed to be put in place in order to handle similarly disruptive, and in this case criminal, activities using technology such as social media and mobile communications. Despite the negative coverage that technology was given in regards to its role in supporting the rioters and the demands at the time by senior politicians of all parties, the official recommendations made by the Home Affairs Select Committee (Committee, 2011) and the Riots Communities and Victims Panel (The Riots Communities and Victims Panel, 2012) both argued that social media should not be shut down in times of crisis and that communities and police forces should engage more with social media in order to communicate with the communities more effectively, organise positive opposition and gain intelligence on the evolving situation.

Given this definition of a digitally disruptive act, it is therefore natural to question what are the attributes associated with an individual that would lead them to undertake a digitally disruptive act. We propose that there are three key attributes that should be considered when attempting to think about a digital disrupter:

- Non-conformist attitude to society
- Non-conformist attitude to digital
- The speed of change of their environment

In order to fully understand the interplay between these attributes we developed a methodology and a framework which has a rigorous and repeatable approach to exploring digital disrupter profiles. Further, this approach enables developed profiles to be easily classified in a simple taxonomy enabling other researchers to extend the body of knowledge around the attributes and how they relate to each other. This methodology and framework is intended to assist in thought exercises exploring the role of a digital disrupter. Therefore, it should not be considered as an approach to profile real individuals.

The methodology consists of two primary phases. The first is to build the conformity profile based on digital and social conformity. This is used to build a profile back story typically up to the point before they become digitally disruptive. The second phase is to examine the speed of change of their environment in order to explore what the triggers would be for the profile to become digitally disruptive. Here we present our arguments for the use of these attributes in the framework along with a series of the profiles that were developed and discussed during the workshop. Two of these profiles are further developed and taken forward in the development of a timeline to provide a demonstration as to why the speed of change in the disrupter's environment is important to consider.

# Phase 1: Conformity to the Norm

An important attribute that surfaced early on in the discussion was the concept that a disrupter would be someone who would not conform. This non-conformist attitude comes in two distinct areas non-conformity to societal norms and to digital norms. This primarily can be modelled as leading of lagging the normal progression, or speed of change, in each of these domains. The impact of the speed of change, and importantly the impact of the rate of change in speed, will be discussed in a further section. However, we recognise that what defines "the norm" is completely subjective, related to the society which is being studied and largely beyond the scope of this paper. What is presented here is the first phase of the frameworks methodology to explore the profiles conformity in society which has a digital dimension.

## Digital Conformity

We have chosen to model digital conformity by borrowing concepts from the Law of the Diffusion of Innovation as defined by Everett Rogers in 1962 (Rodgers, 2003). The law provides a model for how ideas spread through the communities *and importantly defines categories in which parts of society fall and their rough size.* I think this could be clearer A fundamental component of the law is there is a section called the chasm between 10% and 16% adoption where innovations fail to reach wide spread acceptance. We leverage the classifications associated with the groups and the concept of the Chasm to underpin the model of digital conformity. The following classes of individual are therefore used:

- **Innovators – 2.5%:** These are the first to adopt new digital technologies, but due to their inquisitive nature are willing to take risks and ask questions as to the use and purpose of the technology. They are also likely to develop new uses for the digital technology, beyond the intended purpose.
- **Early Adopters – 13.5%:** This class follow the innovators but have a high degree of opinion leadership and therefore carry more influence than the innovators. This class is crucial in the mass leveraging mass conformity of new digital technologies. They are still likely to ask questions and investigate new uses, but they would more often than not follow the innovators lead.
- **Early Majority - 34%:** This group are the followers and more conservative than the first two groups. Once typical digital use has been demonstrated, they are likely to converge on the intended use and be much less questioning or inquisitive.
- **Late Majority – 34%:** These individuals are cynical of digital technologies and will only conform once it is clear that the majority of society do so as well. It would be very rare for this group to question the use function and potential utility of the digital technology, but they may be more concerned with whether the change should be accepted.
- **Laggards – 16%:** Individuals in the class are the last to conform, typically very change adverse and will only conform when forced to do so when their original approaches are no longer achieve the desired outcome. Even in these cases, some individuals are still unlikely to conform. Rather than question what the digital tech can do, or do differently, as with the innovators, they are more likely to question whether there is any need to change at all.

The classes as originally presented by Everett include elements of financial liquidity and social status. For our purpose the financial liquidity aspect is not relevant as individuals can transform technology at very low cost in order to drive innovation. As we have argued previously Moore's Law reduces the entry barrier for this type of digital innovation. We have also chosen to separate out the societal aspects in order to model separate classes of individual in social conformity. It is important to note that this is being used to model digital conformity and not digital innovation or the diffusion of digital innovation despite the apparent similarities. It is about the individuals association with the digital not the innovative idea that is the focus of this model. The Chasm is still an important aspect as it identifies a highly turbulent time where digital conformity is on the edge of being mainstream. The concepts and ideas that are generated by the early adopters and innovators change the intended purpose and use of the digital technology, this changes how the early majority will conform to its use. The Chasm defines the point at which there will ever be mainstream digital conformity.

Given this model and these classifications, we can see that the "norm" would be defined by the Early and Late Majority; these groups would use the technology for the intended purpose and not question its suitability or role. Those that exist outside this central group will more inquisitive (innovators) or rejecting (Laggards) but in both cases much more questioning and will therefore be much more disruptive. Individuals may hold different digital conformity roles at different times in their lives or simultaneously regarding different digital technologies.

## Social Conformity

We recognise that the concept of social conformity is a large complex field of research and is a multi-faceted issue. Here we sought to develop a simple model for classification similar to that which we have presented for digital conformity. As such we propose the following classifications:

- **Visionaries:** These individuals are ahead of the societal normal and are considered trend setters. Not all of their trends are adopted, but they are largely disruptive in nature.
- **Pragmatists:** These individuals select and adopt the dominant trends that emerge from the visionaries and co-opt them into their own social norms.
- **Conservatives:** Through the acceptance of trends by the pragmatists, conservatives will find the changes more palatable. Conservatives are risk minimisers by nature and tend not to adopt all dominant trends
- **Sceptics:** This group will continue to doubt the trends and the evidence of their acceptance

Our social conformity model is very similar to that of the digital conformity; however, it considers a much wider set of issues. Digital conformity is concerned with how and when an individual is likely to adopt new digital technologies and what they are expected to do with it. Social conformity considers the influence an individual has on society. There are natural combinations such as the visionary innovator or the sceptic laggard, yet the two attributes serve to distinctive aspects that need to be considered.

## The Map

These two aspects of conformity can be mapped in two dimensions in order to start the formulation of profiles that can be used to provoke discussion on specific conversations. What does a pragmatic innovator look like? Given this background what type of disruptive acts would they undertake? An interesting component of this map, seen in , is the inclusion of "The Chasm" from the law of diffusion of innovation. The chasm represents a time of extreme uncertainty regardless of an individual's social conformity class as it represents the tipping point on whether a digital innovation will reach the early majority and therefore become main stream.

The Map also enables the review of profiles at multiple points in time in order to explore what might happen to an individual if at first they are a visionary early adopter but become a visionary laggard. What happens when someone used to accessing the cutting edge, now no longer has that same level of access? What might they do?

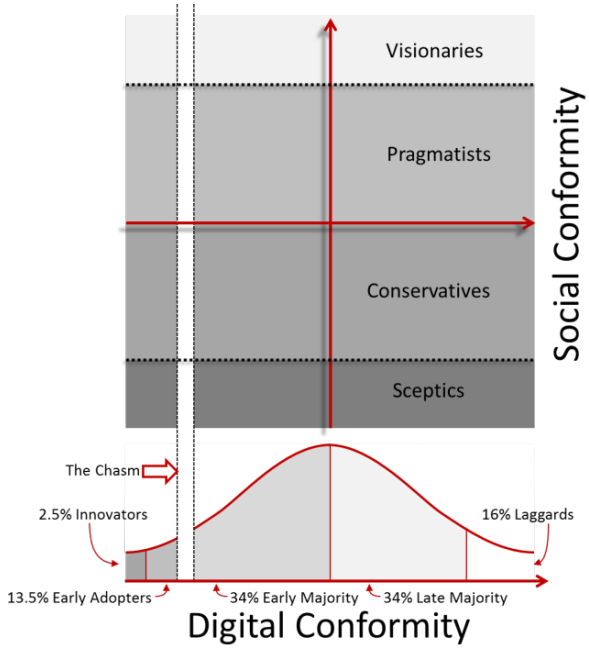
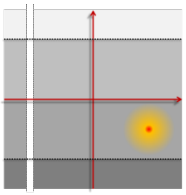


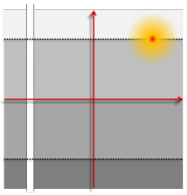

**Figure 1 Map of Conformity**

## Emergent Profiles

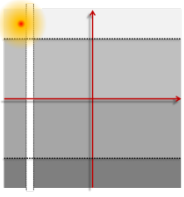
By utilising the two dimensions of conformity and the understanding driven from the discussions around the trends typified by case studies and the experiences of the Digital Disruption team, a series of profiles were created that would encapsulate extreme forms of these attributes. However, these profiles do not present a consideration of the implications of their place in the speed of change. Here is a brief summary of some that were developed and in the later sections two key profiles were expanded and taken forward.



**The Labourer:** Is defined as someone who is a Conservative Late Majority/Laggard. The Labourer is a real-world worker that isn't trying to create a job through the Internet as opposed to the others who are making money through online advertising and creating their own digital campaigns. They don't need to leave the house to make money. They launch their personalities online and know how to 'play' the Internet. The 'labourer' goes out to earn money without the use of the digital. He doesn't realise that his career path will discontinue when he will be replaced with machines/robots in the future.

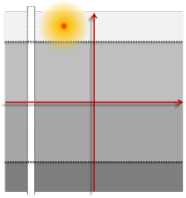


**One Face:** Is an individual defined by the attributes of being a Visionary/Pragmatist and Late Majority/Laggard. One Face only maintains a single identity shunning the ability for multiple identities that new technologies provide in a world where multiple identities are the norm, for example One Face's friends have multiple social identities online- One for work, one for socialising, and one for dating. One face has rejected this reality that digital can leverage your success in offline situations. One face doesn't have an online presence, or has exactly the same personality / image online as offline.



**Education Disrupter:** This individual is defined as being in the Visionary Early Adopter. The Education Disrupter has media savvy parents who have encouraged them to question the given wisdom on education to such a degree that they eventually remove themselves from mainstream education to pursue a path off self-directed learning. With strong guidance from their parents the Education Disrupter will take their parents super liberal point of view and mix it with more anarchic politics found online as they begin to seek acceptance and experiment in the digital space for freedom of expression.

**Digital Activist:** This has the properties of being a Visionary Early Majority. A Digital Activist is able to make use of commonly available but yet advanced technology in interesting ways to put across their radical viewpoint on the injustices that they perceive to be around them. The Digital Activist shuns more conventional approaches to communication and action against individuals and organisations adopting a more technological approach and able to build grass root support for actions quickly through the speed and power of modern communication systems.



# Phase 2: The Speed of Change

The last phase of the methodology is to examine the speed of change in the profiles environment. In professions such as cyber security where risk management and assessment is undertaken considerable effort is put into the concept of Threat Agent Modelling (Jones & Ashenden, 2005). A threat agent in our context can be considered a digital disrupter who poses a threat to the status quo. Basic threat agent modelling considers elements such as education, capability, access to the target and so on to assess the threat that the actor may pose to the target. However, this basic modelling excludes concepts around motivation and triggers, just because someone has access and capability, does not mean they are a threat, but they may become a threat if they are fired from their job for example. In a similar way we can model an individual as a visionary innovator, but they may not become disruptive until a trigger causes them to take action. In this way it is the transition from one speed to another and importantly the rate of that change, i.e. the acceleration or deceleration, of that transition that may trigger action. It is for this reason that we have chosen to model a digital disrupter with a third dimension which is the speed of change of their circumstance or environment.

A range of different tempo changes should be considered such as slow policy lead or soci-economic changes. However an important aspect of the speed of change here is the rapid nature that the interconnected digital world can change an environment. Information can be propagated near instantaneously and so it is possible for someone to be caught up in high profile phenomena overnight with only minimal input.

# Thinking in Three Attributes

We attempt to explore the combination of three attributes by first creating two profiles based on the visionary innovator but with different socio-economic backgrounds. We then map out how we expect those profiles to behave in the presence of different rates of change and the potential impact and links that speed of change has with social and digital conformity. We first present the background for each of the profiles in the social and digital conformity dimensions and then present a discussion on the impact of the rates of change.

### @GraffitiBoy

GraffitiBoy is a visionary innovator with a poor socio-economic background. His parents are working class mainly taking skilled and unskilled labouring jobs. As a bright individual he is often bored at school as he is working beyond the level that is available to him thus forcing him to look elsewhere for education and inspiration. While not directly malicious this disinterest with the mainstream education that he is put through leads to anti-social behaviour online and offline. He has a fascination with technology but with ungrounded moral guidance, due the fact that his teachers and parents don't understand what he is doing or what he is capable of doing, coupled with his only source of guidance being the Internet he quickly finds his technological talents can earn him respect and money undertaking criminal activity.

Much of the evidence that this type of individual has been taken from the information collected by the Guardian newspaper from the experience of the London riots (Guardian, Reading the Riots, 2011). From monitoring the arrests and court cases the researchers in conjunction with the London School of Economics. Their analysis of the data released by the Ministry of Justice showed that the majority of the rioters were

white, males under the age between the age of 10 to 17 and a similar number between 18 and 20. The report also shows that of the 10 to 17 year olds that were involved, the majority came from a socially deprived background as measured by metrics such as accepting free school meals, absenteeism or special educational needs.

### @SearchGirl

SearchGirl was developed as a counter point to GraffitiBoy in that they have the same attributes, but she comes from an upper middle class family with liberal views, similar in concept to the Educational Disrupter profile discussed previously. However SearchGirl does not follow, she leads the pack, constantly questioning what can be done with new technology and in turn develops new technology. She is supported heavily by her parents who encourage her exploration and due to her parental background and the high quality education she receives; she is able to access appropriate moral guidance at home and at school.

### The Context, Environment and Thinking about Speed.

In order to explore these characters we established a context grounded in current government policy. The environment was established in a low economic area of a London in which a large search engine company establishes a free school to focus on STEM subjects particularly IT. The establishment of the school causes significant “Educational Migration” of families, such as SearchGirl’s, into the area where GraffitiBoy’s family lives and has grown up for generations. In this setting SearchGirl and GrafitiBoy grow up together on the same street; however, while SearchGirl is able to attend the new free school, GrafitiBoy is forced to enter the local comprehensive. This use of the free school policy is coupled with the Governments approach to big data, cloud computing and smart cities, with the move to establish wide scale data collection and the use of Smart City technology to increase the commercial prospect of businesses in a digital age.

In order to understand how this might play out a timeline of events was developed covering the time that both SearchGirl and GrafitiBoy enter secondary school until 18. The timeline developed two separate profiles for the speed of change of context for each profile. For GrafitiBoy, the speed change profile was deliberately variable, that is he constantly goes through accelerations and decelerations in his environment. These changes are mainly due to traditional socio-economic issues such as parental unemployment. In contrast SearchGirl has a rapid and unexpected change which is largely due to the imagined future network environment and the speed with which this might cause changes in an individual’s life. This aspect was inspired by the rapid changes seen in the financial markets dues to the interconnectedness of the digital systems that are used to drive and realise profits in that sector. What follows is a mapping of that timeline.

## The Timeline

| "@SearchGirl" | Date | "@GraffitiBoy" | Age |
|---|---|---|---|
| | **Dec-12** | | |
| **A large search engine company announces that it is going to create a free school in a deprived London borough. The school will offer substantial access to new technology and an advanced science, secular curriculum with a trade-off that all pupils and staff will be extensively data mined for behaviour data and activity data. The search company seeks to drive the STEM subjects forward in the country specifically computer science education.** | | | **7** |
| | **Jan-13** | | |
| **Government announces that all government data services for all departments will be moved to the G-Cloud by 2016. It is the most ambitious government IT project and has a considerable number of doubters after recent large scale government IT failures** | | | |
| | **Jun-13** | | |
| **Large middle class migration to the borough driving house prices up significantly in order to take advantage of the new school which will be opening in October. This forces out much of the original local community and displaces a large number of the lower paid jobs.** | | | **8** |
| | **Aug-13** | | |
| SearchGirl's family moves to area. She is oldest in the class becomes friends with GraffitiBoy | | | |
| | **Sep-13** | | |
| **Search School has its first intake of students to much fanfare** | | | |

| "@SearchGirl" | Date | "@GraffitiBoy" | Age |
|---|---|---|---|
| | **Feb-15** | | |
| **Search school announces significant over subscription and established a STEM based assessed entry exam.** | | | |
| | **Mar-15** | | |
| Starts to receive private tuition in order prep for entrance exam. | | Wins science prize in school for an innovative iPhone app. | |
| | **Apr-15** | | **10** |
| **Using data mining techniques the school identifies a series of bullying activities and uses intervention techniques to manage the behaviour. Politicians cite this as an example of the power of data mining.** | | | |
| | **Nov-15** | | |
| **UK government announce setbacks in the G-Cloud project.** | | | |
| **Search school announces the opening of a primary school in the region and another secondary school in Manchester** | | | |
| | **Feb-16** | | |
| Passes Entrance exam in the top 5% of the class | | Passes entrance exam but is two places below the cut off line due to number of places available in school | |
| | **Apr-16** | | **11** |
| **Using data mining techniques of the search school identifies a data set that indicates a number of the children from other secondary schools in the area who friends of pupils at the school are suffering from significant sexual abuse. This leads to the breakup of one of the largest UK child abuse and pornography rings ever seen in the UK and identifies suspects in over 30 other countries. Worldwide there are 350 convictions. Politicians seize this incident to expound the virtues of data mining and argue for more funding for the G-Could project. Public support drives the impetus and more funding is granted.** | | | |
| | **Sep-16** | | |
| **UK government and search company announce partnership to provide the G-Cloud services.** | | | |
| Starts at search school and immediately shows significant talent | | Starts at local comprehensive Streamed into to set | |

| "@SearchGirl" | Date | "@GraffitiBoy" | Age |
|---|---|---|---|
| | **Jan-17** | | |
| | | Starts skipping class as he finds the classes too easy and not challenging | |
| | **Feb-17** | | |
| | | Finds online technology and science group and starts to self-educate | |
| **SearchGirl starts providing GraffitiBoy with material from her school and provides some tuition** | | | |
| | **May-17** | | |
| | | Achieves top marks in his school for STEM, but is failing English and other humanities | |
| | **Jun-17** | | |
| Gets internship at the search company in America | | Is very disenfranchised when SG leaves as there is no one else he can talk to about what he is doing | **12** |
| | **Jul-17** | | |
| | | Hangs around with the local kids at the park. Low level physical nuisance, such as graffiti as bored. | |
| | **Sep-17** | | |
| Streamed into the acceleration programme and made year head student | | | |
| | **Nov-17** | | |
| | | Parents unable to afford a system needed to carry on his own self education with SearchGirll materials | |
| | | Turns to web and social networks to be self-taught | |
| | **Dec-17** | | |
| **The government announces a major new initiative with the search company to improve policing services through data mining.** | | | |

| "@SearchGirl" | Date | "@GraffitiBoy" | Age |
|---|---|---|---|
| | **Jan-18** | | |
| | | Shows up a teacher at school as he knows more about technology than they do. He gets into trouble for the embarrassment caused, despite only trying to help. | |
| | **Feb-18** | | |
| | | Starts a series of low level attacks against the school which are embarrassing. Lewd images on public displays, the printing of embarrassing emails. In retribution for the apparent injustice. | |
| | **Apr-18** | | |
| | **Government announces the national smart cities project. All major UK cities will be augmented with smart technology to provide total high-speed free data coverage as an infrastructure. This provides a range of basic level services that are free to be developed upon, such as geo-location.** | | |
| | | Suspended due to the attacks. Has nothing to do but hang round on line or at the park with the other kids. | |
| | **May-18** | | **13** |
| | **The crime data mining initiative starts to see considerable success in targeting key criminals and successfully prosecuting them.** | | |
| | **Jun-18** | | |
| Summer internship in Switzerland | | Father gets job as driver and level 1 installation engineer to help create smart city project | |
| | **Jul-18** | | |
| | | Mother gets job on the smart city project, Father takes him along to some of the jobs when mum is at work. | |
| | **Aug-18** | | |
| | **Based on the success of the data mining crime analysis programme the governments creates a new programme which uses big data sets to identify the best ways to rehabilitate criminals. This is due in part to the overcrowding of prisons as a result of the success of the crime analysis project.** | | |
| | **Dec-18** | | |
| | | Goes into work with mum and dad. | |
| | **Jun-19** | | |
| Decides not to go to internship in the states | | Spends much of the summer going to work with mum or dad, or spending time with SG | |
| | **Aug-19** | | **14** |
| | **After a year the rehabilitation programme shows great success with high numbers of criminals not re-offending and become proactive members of society.** | | |
| | **Oct-19** | | |
| | | Finds a carders forum and learns how to skim Proximity based card transactions. | |

| "@SearchGirl" | Date | "@GraffitiBoy" | Age |
|---|---|---|---|
| | **Feb-20** | | |
| | | Becomes well known for fixing a big issue with cracking cards on the forum and has may discussions with regard to the security issues of the proximity payment system. However, does not steal much, but just enough to buy new gadgets and systems to aid his experiments and learning. | |
| | **Mar-20** | | |
| **The success of the rehabilitation project causes a significant impact on the welfare state as there are increasing numbers of people who are fit for work but cannot obtain jobs.** | | | |
| | | Notices strange things happening and weird behaviour on carders forum indicating that there may be police on there. Resolves to leave and covers his tracks. | |
| | **May-20** | | |
| | | Police call at his home to ask questions about the forum, which he denies anything to do with. Police find no strong evidence of a link. | **15** |
| | **Jul-20** | | |
| **New Female Prime minister, who was the minister in charge of the crime and rehabilitation projects, is elected on the promise of an improved welfare system and a return to a more manufacturing based industry for the country and driving jobs and recruitment.** | | | |
| | **Aug-20** | | |
| | | Mother let go from smart city job. Get job in local petrol station and has to work shifts. | |
| | **Oct-20** | | |
| | | Father let go, but gets job as janitor at the search school | |
| | **Nov-20** | | |
| Is the first non-search company employee to get code into production by developing and proving a revolutionary new data mining algorithm for incomplete data sets | | | |

| "@SearchGirl" | Date | "@GraffitiBoy" | Age |
|---|---|---|---|
| | **Jan-21** | | |
| **London is completely augmented.** | | | |
| | | Meets with a group of other disenfranchised teens from the online hacker groups many of whom attend his school. They form the UrbanCyTex gang. | |
| | **Feb-21** | | |
| **Major piece of government legislation goes through the commons which reforms the employment and welfare state. At its heart is the concept of using data mining to find the right jobs for out of work people which maximises their prospects.** | | | |
| | **Mar-21** | | |
| Her new data algorithm finds a malicious set of trading behaviour and averts a near fatal financial collapse. Hailed as the ideal output of the search school. Visits the Prime Minister at No. 10 etc. | | | |
| | **Apr-21** | | |
| | | The UrbanCyTex start to attack the smart city infrastructure using basic attack like replacing QR codes and performing traditional graffiti | |
| | **May-21** | | |
| | | Thrill seeking behaviour increases for UrbanCyTex and start to perform more sophisticated technological attacks, for example changing historical augmented reality and VR city dioramas into hard-core pornography. These types of attacks require proximity thus increasing the thrill level due to the potential of being captured. | **16** |
| | **Jul-21** | | |
| | | Group is caught when the smart tourist area around No. 10 is subverted to show the current and previous Prime Minister in various lewd activities | |
| | **Aug-21** | | |
| | | After investigation the UrbanCyTex group is caught and given a caution and a fine which is a significant amount for his family. He is also required to attend school regularly. | |
| | **Sep-21** | | |
| **Open source, anonymous data sets which are produced from data mining are made available from the government for companies to use to drive innovation.** | | | |
| **A large supermarket chain utilise the government data sets to enhance their supply chain in order to deliver more efficiencies in the delivery of services to town populations. It also uses the data to drive recruitment and financial services provision.** | | | |
| | **Dec-21** | | |
| | | Father laid off from job as janitor at the searchschool for repeatedly being late as he had to make sure his son went to his school. | |

| "@SearchGirl" | Date | "@GraffitiBoy" | Age |
|---|---|---|---|
| | **Jan-22** | | |
| | | Starts to truant as the lessons are boring and he can learn more at home from the internet again. | |
| | **May-22** | | |
| | **First school leavers all 95% hold 5 A-level equivalent A-B grade** | | |
| Top of her class in the GCSEs. All A's at 90% or above. | | Leaves school having achieved high grades in STEM but failing pretty much everything else. | |
| | **Jun-22** | | |
| | **The government announces a new scheme to just in time fund and deliver services for local councils using data mining as the trigger set.** | | |
| | **Jul-22** | | |
| | | Reunites with members from UrbanCyTex and starts a more proactive series of attacks against the smart city designed to disrupt its operation as a protest of the lack of jobs available to them. Group calls themselves: The Nameless. Using financial ecrime to fund some of these activities. | |
| | **Aug-22** | | **17** |
| | | The Nameless rapidly get a cult following online due to their digital savviness and high profile targets. | |
| | **Oct-22** | | |
| After submitting an essay on feminist sexual literacy of the 2010's her parents are identified by her algorithm as sexually abusing her, due to the nature and style of her writing. She returns home to see her parents being arrested. | | The Nameless launches an attack on the financial sector slowing trading systems, causing millions of losses to traders. | |
| | **Nov-22** | | |
| | **Financial sector recovers in part due to insurance and more resilience in the sector due to the legislation introduced after the last financial collapse.** | | |
| Seeks comfort from GB, as parents still remain under arrest and she is in local care. Very isolated at school due to the rumours etc. to do with her parents | | | |
| | **Dec-22** | | |
| Discovers flaw in the data mining algorithms that led to the identification of her parents abusers, but before she can inform anyone GB is arrested. Parents are released but she can only see them under supervision. | | GB is identified as a member of The Nameless by SG's algorithm, and he and the other ring leaders are arrested. | |

| "@SearchGirl" | Date | "@GraffitiBoy" | Age |
|---|---|---|---|
| | **Jan-23** | | |
| SG is again held up by the prime minister as a shining light of the search school system. Still socially isolated but in media spotlight causes significant withdraw1. Visits GB in prison. | | Released under bail to appear in court at a later time for the full case. | |
| | **Feb-23** | | |
| Her visits to the prison cause her to be identified via data mining as a potential member of the Nameless. She is interviewed by the police. | | | |
| She seeks comfort in GB and have discussions on how unfair the world and authorities are. They discuss the flaw in the data mining algorithm. | | | |
| | **Mar-23** | | |
| | | Develops an exploit for the flaw in the data mining algorithm which means that he can cause anybody to be suspected of a crime and possibly arrested with the injection of specific, false data sets. He demonstrates this to SG by getting the police that arrested her parents arrested as part of a credit card fraud investigation. | |
| After seeing the exploits in action, she realises that she can bring down the whole system by polluting the governments who data set. | | | |
| **National news story regarding the arrest and release of the two police officers. Civil liberties groups point to the issues of the g-cloud and data mining as the technology is blamed for the mistake.** | | | |
| | **Apr-23** | | **18** |
| | | Cultivates a very big botnet for use by SG | |
| SG deploys the exploit onto the bot net to slowly corrupt the datasets of millions. | | | |
| | **May-23** | | |
| **Crime rates and arrests start to massively rise** | | | |
| **Just in time systems for government service fund distribution is disrupted as the data sets become corrupted.** | | | |
| | **Jun-23** | | |
| **Secondary consumers of government data starts to suffer as they end up incorrectly provisioning the capacity in their supply chains etc. This costs companies significant amounts of money** | | | |
| **The criminal justice system starts to struggle under the strain of the number of arrests and then the release of people associated with crimes they did not take part in.** | | | |
| **The losses in the commercial sector, manufacturing, food supply cause disruption in the financial markets and share prices start to collapse.** | | | |
| **Data corruption impacts the financial markets directly, coupled with the financial issues other industry sectors are suffering causes the banking sector to tighten and slow down the amount of credit it is offering.** | | | |
| **Wage payments are starting to be affected coupled with the banks inability to lend causes much civil unrest which further increases the strain on the policing and justice system.** | | | |
| **The government issues a state of emergency and shuts down the g-cloud and data mining services, issuing statements that they are working with the search provider to resolve the technical issues and that the disruption is caused by a large scale attack from forces unknown.** | | | |
| **Mass civil unrest as essential items becomes difficult to obtain such as foodstuffs and fuel. Further money is not available from the high streets banks.** | | | |

# Conclusion

*The idea of a 'digital divide' is undoubtedly a concept that raises important questions about inequality domestically and internationally. But we suggest that the acceleration of digital life might have important implications for a 'digital divide': the different categories of users and consumers might be transformed by the proliferation of cheaper and more powerful technologies.*

The time between an introduction of cutting edge technology used by the elite of early adopters and innovators – and the widespread use of the new technology – might shorten. The potential for disruptive and radical use of the new technology is not something we should necessarily be afraid of – or be the cause of panic on the part of politicians and policymakers: the acceleration of digital culture can provide a range of benefits across society.

But this acceleration should be a cause of concern because new types of digital distribution are bound to emerge (especially in conjunction with the digitalizing of all aspects of economic and social life, the networking of critical infrastructures): our position is based on the view that technology is rarely used solely for the purposes that it was designed for; people find new ways to use and abuse technology – this is integral to the creativity of new digital technologies. And technology rarely progresses without the potential for accidents or vulnerabilities that can be exploited: it is naive to think better technical fixes and security solutions will keep ahead of accelerating technologies, enabling us to remove risk and insecurity.

This initial attempt to think about the future of digital disrupters points to a number of questions that we think need to be the basis for future research:

1. We need to examine acceleration in technology: what are the emerging 'tools' and practices on the horizon? What technology will be widely available to young people in the coming years? In order to begin to open up these questions we need dialogue that brings in perspectives from the policy world, academia, business and technologists.
2. We need to develop innovative ways to explore our technological futures, developing techniques that allow new possibilities to be presented in the public sphere to a range of different actors. In the final part of this report we include a fictional depiction of one possible scenario. We need to open our thinking to the problems of an 'accelerated' reality, a world where the future accelerates towards us – where disruptive change can occur faster than we expect.
3. We need to address the question of inequality of opportunity in contemporary society: we need to take seriously the possibility that European society will not deliver the 'good life' (the good jobs, housing, consumption) that young people see advertised all around them. In particular, we should take seriously the possibility that a: increasingly powerful technology will continue to become cheaper and b. we might be living in a technological culture where one doesn't need a degree in computer science to do what we currently think is very clever.

Digital disruption will continue be an inevitable part of life; we need to take seriously the idea that smaller numbers will be able to orchestrate large scale disruption. We might need to take seriously the possibility that those young people who are currently living on the margins of society might have an increasingly national or global reach through new technology. Controlling digital disrupters through new techniques of policing and

cyber security might be futile: there will always be a vulnerability to exploit. When considering these approaches we recommend that they following principles:

- *Principle 1: Do not plan for a uniform digital divide, Moore's Law makes it messy and fragmented,*
  The digital divide cannot be counted upon to ensure that socially disaffected groups cannot create digital disruption. It is clear that Moore's Law, driven by consumer need, bridges the divide in unpredictable ways enabling the mass adoption of technologically sophisticated devices. As a result any policy must consider that all individuals regardless of socio-economic background are capable of digital disruption.
- *Principle 2: In order to understand and benefit from digital disruption we need to adopt innovative digitally disruptive practices*
  Digital disruption thrives on the unconventional and the new and that this forms the dialogue of the digital disrupter. In order to benefit, extract the best and navigate the negative we must become conversant in this language, rapidly adopting innovative and disruptive practices.
- *Principle 3: What we consider exceptional now will become the norm tomorrow*
  As we have presented Moore's Law and consumer need is accelerating the future towards us. Wisdom becomes conventional overnight in a globalised information economy and technology rapidly catalysing or socio-cultural evolution. Our approaches must consider the reality that we cannot plan for the future to the smallest detail.

*In light of our discussion and research it is our belief that we need to consider more radical social policies in a society confronted with generations living with the consequences of Moore's Law.*

# Interpretation of the Story

***What follows is a creative interpretation of the timeline presented in this report. It was developed as if it were of a dossier compiled after the incidents described in the timeline have occurred in order to understand the causes of the actions of the key actors involved in the timeline. The reader will note that there are some deviations from the presented timeline and key points in order to serve creative purposes. The purpose of this work is to force the reader to start to think about how we would interpret the actions of a digital disrupter post event, rather than thinking about the potential activities of the disrupter pre-event. We leave it to the reader to draw their own conclusions***

**X123a Preliminary Timeline on James Young (aka 'Graffiti Boy') and the 233x1 event**

**Information Classification: Confidential**

**Abstract: This report presents a preliminary briefing to the Joint Services Intelligence Committee on the timeline of the activities of James Young and Laura Caton in relation to the 233x1 event. All sources presented in this report have been taken from verified and credible OSINT, HUMINT, SIGINT, TECHINT and FININT sources.**

Minutes from Stockton Council Education Strategy Meeting, January 13: ' We would like to note our immense pleasure in the search engine company Toku announcing that it is going to create a free school in what is a very deprived London borough. The school will offer substantial access to new technology and an advanced science (with a secular curriculum): it was agreed that pupils and staff being extensively data mined for behaviour data and activity data was a small price to pay for the creation of the school. It was agreed that the school council would have to work hard to respond to any anxieties in the local community about the data mining and privacy. But it was noted that this type of data mining goes on anyway – and the information generated by the scheme was likely to improve health, safety, wellbeing and economic vitality in the area. We are particularly excited by the desire to drive the STEM subjects (especially computer science). We hope the students make the most of this opportunity.'

BBC news Online, February 13: 'The Government announced today that government data services for all departments will be moved to the G-Cloud by 2016. The government IT project continues to draw criticism after a number of high profile government IT failures but the minister for science and technology, Dr David King, told the BBC that the G-Cloud would enable new types of Big Data analysis as well as reducing the costs of key government activities.' However, political analysis and leading academic Dr Max Lucy further criticised the development as 'The government once again attempting to create an Orwellian world akin to 1984' and cited the potential impact of such a project could have catastrophic implications for society.

Stockton Evening News, July 13: ‘House prices in the borough increased by 15 per cent since the announcement of the launch of the Toku academy school in October. Local councillors fear that the price increase will continue to force young people from the borough to leave the London, leaving gaps in key services.’

@searchGirl, September 10: “Ok this isn’t the worst place to move to. And lessons aren’t like school #andtheboysareprettycute”

@searchGirl, September 10, September 15: “Some of the boys here are just stupid. But not all of them #GraffitiBoy”

NatSec Risk Assessment Case History: Case XILX (James Young): ‘James seemed to adjust well to the new school. Many of the behavioural problems he exhibited in his previous schools seemed to disappear. Teachers seemed impressed with his understanding of coding. He was soon put into the special class on ?????. And while he didn’t get on with the other boys in the class – most of whom were the children of Professionals; he did become friends with Laura Caton, the daughter of two lawyers. Caton and Young sat together through class and worked on a number of projects together. Teachers report that James had difficulty explaining his work to the rest of the class.’

@searchGirl, October 15: “Got to stay home tonight. Because they have got me a tutor #isthisreallyncessary?”

NatSec Risk Assessment Case History: Case XILX (James Young): ‘While James made good progress on a number of projects with possible business application, the managers of the school felt that he was becoming too aggressive to other students. On October the 16th James punched another student in the face 5 times. The student was taken to the local hospital but lost a tooth. The parents threatened legal action against the school. James was expelled.’

@searchGirl, October 25: ‘This school has got really boring#theyjusthatemecosimbetterthanthem.’

Minutes from Stockton Council Education Strategy Meeting, April 15: ‘We were pleased to note the success of the first data-mining exercise to identify bullying activities in the new school. The data has been used for intervention techniques to manage the behaviour. We were

especially pleased that politicians have cited this experiment as an example of the power of data mining.'

NatSec Risk Assessment Case History: Case XILX (James Young): 'Teachers comment that James remained quiet and 'distant' in class in his new school. But James managed to win the first prize in the government's national competition for mobile phone apps. He failed to attend the prize giving ceremony at the Toku headquarters.'

BBC news Online, November 15: 'UK government announce setbacks in the G-Cloud project. The problems have not been disclosed but are thought to centre around...

Minutes from Stockton Council Education Strategy Meeting, May 16: 'Using data mining techniques the new school identified a data set that indicates a number of the children at the new school are suffering from significant sexual abuse. This leads to the breakup of one of the largest UK child abuse and pornography rings ever seen in the UK and identifies suspects in over 30 other countries. Worldwide there are 350 convictions. Politicians seize this incident to expound the virtues of data mining and argue for more funding for the G-Could project.'

BBC news Online, November 15: 'Today the UK government and Toku announced a partnership to provide the G-Cloud services.'

NatSec Risk Assessment Case History: Case XILX (James Young): 'It was noted by the school that in October James began missing classes. When he was asked about his absences James told teachers that they were all wasting their time because he found the classes boring. Research revealed that James began to self-educate using a variety of on-line forums. It also appears to be the case that Laura Caton (SearchGirl) was passing on her notes and projects. At home there appears to have been a marked increase in his parents' consumption of alcohol (bought on their weekly trips to the supermarket). But over the next month's James submits work of exceptional quality for his STEM subjects. However, he continues to have trouble with English and other humanities subjects. While his grasp of STEM subjects is exceptional, he continues to struggle to express himself both verbally and in written work. In June of that year Laura Caton leaves for America, for an internship in Google. Alcohol consumption increases at home and James appears to spend more time on the local park where a group of young people he met online to meet up to exchange memory sticks and...'

@searchGirl, September: ‘Can’t believe I am back in the UK#GETMEBACKTOAMERICA’

BBC News On-line, Jan 18: ‘Today the government announced a major new initiative with the search company Toku to improve policing services through data mining.’

NatSec Risk Assessment Case History: Case XILX (James Young): ‘Laura Caton is made head girl of the school. Her experience as an intern at Google has given her added maturity. But she continues to talk with James. It saddens her to see what has happened to him so she continues to pass on teaching material (copywrited by Toku). The hardware that James has at home is unable to cope with the type of projects she sends him. This frustrates James and he turns more to the self-educating groups on-line. It is believed that it is at this point that he begins to orchestrate minor exploits directed at the school (lewd pictures of digital notice boards, the circulation of confidential emails). He would later tell us that he respected the school but was frustrated by the lack of opportunity to develop his skills further.

BBC News Online, April 1: ‘The crime data mining initiative has seen considerable success in targeting key criminals and successfully prosecuting them, the Prime minister told parliament today.’

BBC News Online, April 18: ‘The government announced the next stage in the national smart cities project. All UK cities will be augmented with smart technology to provide total high speed free data coverage. The initiative will provide a range of basic level services that will free to be develop on. The government hopes that the tourist economy will benefit from innovative geo-location projects, as well as improving the already high levels of security and safety in UK cities.’

NatSec Risk Assessment Case History: Case XILX (James Young): ‘In May James is suspended from his secondary school after his involvement in the various cyber-attacks is proved beyond reasonable doubt. James spends more time in the local park where he becomes a dealer in various low level cybercrimes. His father gets a new job as an installation engineer on the borough smart city project; his mother also works as an administrator. This raises the level of income in the household but alcohol consumption continues to increase. Laura Caton becomes an intern for the summer in Geneva at an international organization dealing with cyber-crime and civil liberties. Laura sends James lengthy emails about her life in Geneva. He reads the emails repeatedly.’

BBC News Online, July 20: ‘Following the success of the datamining crime analysis programme the governments has created a new programme which uses big data sets to identify the best ways to rehabilitate criminals. This move is seen as critical in light of the overcrowding of prisons as a result of the success of the crime analysis project.’

NatSec Risk Assessment Case History: Case XILX (James Young): From August to April James works with his mother in the office of the borough smart cities project, doing mainly basic clerical work. Co-workers say that he became much friendlier and more talkative during his time on the project: he was very polite and considerate to all his co-workers. As Laura Caton waits for her A Level results, she spends more time with James, taking him to the Tate, encouraging him to read books. James takes a particular interest in Orwell’s 1984. He goes on to read about the life of Karl Marx and the science fiction stories of Philip K Dick. He also spends time on-line looking for recipes to cook. He cooks meals for both Caton and his parents. Caton turns down an internship with Toku in California so she can stay in London. In August she wins her place at Oxford to study computer science.’

BBC News Online, September 1st: ‘Today the government announced the digital rehabilitation programme shows great success with high numbers of criminals not re-offending and becoming proactive members of society.’

NatSec Risk Assessment Case History: Case XILX (James Young): ‘Laura Caton begins her life as a student at Oxford University in September. She appears to thrive in this new environment, joining a number of societies and developing a number of data mining projects. James continues to do clerical work in the offices of the smart city project. He joins a carders forum and learns how to skim Proximity based card transactions. Over time, he becomes well known for fixing a big issue with cracking cards on the forum; he appears to have had many discussions about the security issues of the proximity payment system. The police find the discussions fascinating. James doesn’t appear to steal much at this stage, just enough to buy new gadgets and systems to aid his experiments and learning.’

BBC News Online, March 20th: ‘Government figures released today showed unemployment reaching 17 per cent. Economists believe that this rebalancing of the economy due to the impact of new technology will only be temporary. Opposition leaders called for a radical rethink of economic policy.’

NatSec Risk Assessment Case History: Case XILX (James Young): ‘In August the first stage of the smart cities project comes to an end. James and his parents all lose their jobs. James’ father finds a job

with the council managing cleaning robots. But the loss of income in the family makes life difficult. James begins to attend meetings of a radical movement composed of unemployed graduates. He finds the discussions too intellectual and abstract. He emails Laura for a reading list of radical political thinkers. She replies two weeks later telling him to start courses at the local higher education college. He doesn't reply to her. He decides to contact other local hackers in order to plan exploits that will generate an income. The group operates better than James intended. He soon has enough money to move out of home into his own flat. The flat becomes the base for what James calls the UrbanCyTex collective. Soon over ten young people are living and working from the flat. James teaches the younger members how to perform the necessary exploits. He seems to have enjoyed his new role as teacher and leader of the 'gang.' As part of the initiation ceremony new recruits have to find ways to tamper with the infrastructure of the smart city. Exploits include: tampering with tourist augmented reality systems to create unsettling and confusing experiences for tourists to London; changing QR codes and covering the city with obscene graffiti. Over time the gang performs more daring exploits, targeting banks with anti-capitalist graffiti and infecting Sainsbury's apps for children with pornographic material. Police are unable to detect the culprits.

In November, Laura Caton sells her data mining algorithm for incomplete data sets to Toku. The Financial Times heralds her work as revolutionary. The Prime Minister tells a parliamentary committee that her success illustrates the importance of the new academies. The Sunday Times profiles Miss Caton in their magazine, suggesting she is a star in a new generation that will revolutionise life in the UK. James emails Laura in a rather sarcastic email. She doesn't reply to the email. She achieves exceptional results in her end of year exams.'

BBC News Online, April 5th: 'The government announced a new scheme today that will enable data mining to be used to find jobs for the unemployed. Jack Skelly, leader of Unemployed UK, told the BBC that this was merely part of the governments' PR campaign to mask the increasingly serious situation that the unemployed find themselves in.'

NatSec Risk Assessment Case History: Case XILX (James Young): 'Laura Caton's data algorithm uncovers malicious trading behaviour at Barclays. The discovery helps the Bank avoid major losses. After being interviewed on the evening news, a picture of her face is inserted into augmented reality sites across London. Police are confused by the exploit. Caton emails James, asking: 'Grow up.'

BBC News Online, September 21st: ‘The government has announced a new scheme to release anonymized data sets that are created by data mining for use by business. It is hoped that the data sets will help drive innovation. A number of supermarkets have expressed an interest in the data sets in order to improve the delivery of services across the country.’

NatSec Risk Assessment Case History: Case XILX (James Young): The UrbanCyTex collective begins to fragment into two factions: one that seeks to continue to make money; and one that wants to attack the state out of a sense of grievance. James attempts to keep the peace but a new group emerges, The Nameless. The leader of The Nameless is a 20 year old – Mark Bell - who James had trained over the previous 18 months. The Nameless proceed to orchestrate large scale attacks on the infrastructure of the smart city: they are able to confuse the police about the emergence of smart mobs in a manner that causes a considerable cost for the MET. It becomes increasingly difficult for any Apple products to operate in London; Facebook becomes too risky to use.

In early October Laura Caton’s father dies of a heart attack. She leaves Oxford for London: in the days after the funeral she meets James. James confides in her that he has made mistakes and UrbanCyTex and The Nameless are all out of his control. He wants to leave London but doesn’t know where to go. She suggests that he comes to Oxford where she has recently bought a beautiful apartment with a number of rooms. She tells him that he could work for her. He apologises for posting her picture around London. He decides to leave for Oxford.

The next morning (October 10th) the MET – using Miss Caton’s algorithm – arrest James for his association with The Nameless. He is taken out of London to a high security prison in Suffolk. He is placed in an isolation wing with no access to phone, television or computer.

Caton employs a top London lawyer to defend James. She is unable to visit him. James is released from the isolation wing but is beaten severely by other inmates. On October 10th Caton is taken in to an Oxford police station for interrogation about involvement with The Nameless after data mining placed her on a list of potential suspects. Caton realises that the algorithm she designed contains significant flaws. She tells the CEO of Toku about the flaws but he seems uninterested. We think that it is at this point she decides to create the bot-net that lead to the events of 15/11. She designs a bot-net that corrupts the data sets of millions, an intense attack on the G-Cloud. Police are unable to deal with the data about potential terrorist attacks; supermarkets have their just in time deliveries seriously affected. On the 15th of November the benefits system makes

all citizens eligible for income support. The following day the system erases all data about welfare recipients. This was a miscalculation on the part of Caton: the combination of an imploding police force and angry welfare recipients caused 6 days of severe rioting. 70 UK citizens lost their lives: the cost to the UK taxpayer was £900 million.

At this stage, we are unable to produce sufficient evidence to take any action against Miss Caton. She has now left Oxford and works in California for Toku. Her father's death affected her very badly but she seems to be a well-adjusted adult, tipped for the top position in Toku by the age of 30. Young is still in prison in Suffolk. Although his mental health deteriorates, we agree that it would be unwise to take him out of the isolation wing. The prison is just too networked.'

# Writing Team

## About the Authors

**Mark Lacy: Associate Director for Security Futures at Security Lancaster**

Mark holds a PHD in International Relations and prior to his work in Security Lancaster he was part of a team that set up an inter-disciplinary theme year on New Sciences of Protection: Designing Safe Living' which brought together designers, technologists and social scientists to collaborate in various ways on emerging security problems and their social, economic and political impacts.

**Dr Daniel Prince: Associate Director of Partnership at Security Lancaster**

Daniel is an associate director for Security Lancaster, managing business partnerships and enterprise. Prior to this he was the course director for the multi-disciplinary MSc in Cyber Security teaching penetration testing, digital forensics and information security risk management. Daniel holds a PhD in Computer Science and has worked on projects with numerous large technology companies such as Cisco and Microsoft.

## Workshop Team from Bold Creative

**Mr Martin Orton: Founder + Managing Director of Bold Creative**

Martin heads up a multi-disciplinary team of designers, youth engagement specialists and communications experts. Since founding Bold Creative in 2004, Martin has led the company to break new ground in using participatory approaches to design to solve big social issues facing young people in the UK today, from digital literacy to bullying, child poverty, crime and health issues. His expertise includes youth policy and strategic campaign development, qualitative user-led research and creative solutions. Martin has consulted and conducted research for public, private and third sector clients, and has spearheaded numerous ground breaking projects that have enabled youth voices to be heard in mainstream media. In the past five years he's won a UNICEF award, a Promax Gold, 2 BAFTA's and a Prix Jeunesse Award.

**Mr Luke Newbold: Digital Lead at Bold Creative**

Trained in Drama, Applied Theatre & Education and with extensive experience in web development and interactive design, Luke is an expert in developing processes whereby young people and industry professional's co-design innovative projects. Luke is responsible for masterminding the delivery of all of Bold Creative's digital projects, as well as managing the internal design, production and research teams. In the past year he has produced the UCLH children and young patient's website, a campaign for the Private Equity Foundation and four storybook apps, working alongside young people to create engaging, honest and inspirational content.

**Ms Rebecca Ford: Project Director for the Digital Disruption Project**

Rebecca joined Bold Creative in 2009 and worked in communications and business development roles before being appointed as project director in 2011. Rebecca initiated founding the Digital Disruption Project as a non-profit company in 2011 and now directs this alongside other Bold Creative projects. Prior to working at Bold Creative Rebecca completed an MSc in Social Anthropology at UCL, and her early work was in interfaith youth engagement. In addition to her work at Bold Creative and the

Digital Disruption Project, Rebecca is currently involved in the development of Values-Based Education, an initiative adopted by 2,000 UK schools that is proven to enhance social values of children and young people.

# References


Acker, J. C., & Mbiti, I. M. (2010). Mobile Phones and Economic Development in Africa. *Journal of Economic Perspectives, 24*(3), 207-232.

Ackerlof, G. (1970). The Market for Lemons: Quality Uncertainty and the Market Mechanism. *The Quarterly Journal of Economics, 84*(3), 488-500.

Amazon Inc. (2013). *Amazon Elastic Compute Cloud (Amazon EC2)*. Retrieved April 24, 2013, from Amazon Web Services: 2013

Bartlett, J. (2013 ). *Why Did the Pollsters Miss Beppe Grillo?* . Retrieved 3 2013, 7, from ttp://www.huffingtonpost.co.uk/jamie-bartlett/beppe-grillo-why-did-pollsters-miss-him_b_2763790.html

Bauman, Z. (1999). Globalization: The Human Consequences. Cambridge: Polity Press.

Brodkin, J. (2012). *With 16 petaflops and 1.6M cores, DOE supercomputer is world's fastest*. Retrieved 03 07, 2013, from http://arstechnica.com/information-technology/2012/06/with-16-petaflops-and-1-6m-cores-doe-supercomputer-is-worlds-fastest/

The Cabinet Office (2007). *Building on Progress: Security, Crime and Justice*. London: Cabinet Office.

Captain, S. (2012). *Livestreaming Journalists Want to Occupy the Skies With Cheap Drones*. Retrieved 3 7, 13, from http://www.wired.com/threatlevel/2012/01/occupy-drones/

Chaos Computer Club. (n.d.). *Chaos Computer Club English Home Page*. Retrieved April 24, 2013, from The Chaos Computer Club: http://www.ccc.de/en

Committee, H. o. (2011). *Policing Large Scale Disorder: Lessons from the disturbances of August 2011.* London: Houses of Pariliament.

Guardian, T. (2011). *Reading the Riots*. Retrieved 3 7, 2013, from http://www.guardian.co.uk/uk/series/reading-the-riots

Guardian, T. (2011). *The UK Riots 2011*. Retrieved 3 7, 2013, from http://www.guardian.co.uk/uk/london-riots

Her Majesty's Government. (1998). Data Protection Act 1998. *Data Protection Act*. The Crown.

Her Majesty's Government. (2000). Regulatory Investigatory Powerss Act 2000. *Regulatory Investigatory Powerss Act 2000.* The Crown.

Houses of Parliament. (2011). *Daily Hansard - Debate*. Retrieved 3 7, 2013, from http://www.publications.parliament.uk/pa/cm201011/cmhansrd/cm110811/debtext/110811-0003.htm#11081117000001

Houses of Parliament. (2011). *Daily Hansard - Debate*. Retrieved 3 6, 2013, from http://www.publications.parliament.uk/pa/cm201011/cmhansrd/cm110811/debtext/110811-0002.htm#1108117000003

Jamie Bartlett, C. M. (2011). *Truth, lies and the internet.* Demos.

Jones, A., & Ashenden, D. (2005). *Risk Management for Computer Security.* Butterworth-Heinemann.

Lanier, J. (2013). *Who Owns the Future?* Simon & Schuster .

Mann, S., Nolan, J., & Wellman, B. (2003). Sousveillance: Inventing and Using Wearable Computing Devices for Data Collection in Surveillance Environments*. *Surveillance & Society, 1*(3), 331-355.

May-Chahal, C., Mason, C., Rashid, A., Greenwood, P., Walkerdine, J., & Rayson, P. (2012). Safeguarding Cyborg Childhoods: Incorporating the On/Offline Behaviour of Children into Everyday Social Work Practices. *British Journal of Social Work*.

Meyer, D., Zhang, L., & Fall, K. (2007). *Report from the IAB Workshop on Routing and Addressing.* Internet Engineering Task Force IETF.

Moore, G. E. (1965, april 19). Cramming More Components Onto Integrated Circuits. *Electronics Magazine, 18*(8), pp. 4-7.

Parilament, U. (2011). *Daily Hansard - Debate*. Retrieved 3 6, 2013, from http://www.publications.parliament.uk/pa/cm201011/cmhansrd/cm110811/debtext/110811-0002.htm#1108117000003

Price Waterhouse Coppers LLP. (2012). *IAB internet advertising revenue report: 2012 first six months' results.* Price Waterhouse Coppers LLP.

Research In Motion. (2013). *BlackBerry Messenger*. Retrieved April 24, 2013, from Blackberry: http://uk.blackberry.com/bbm.html

Rodgers, E. (2003). *Diffusion of Innovations* (5th ed.). New York: Simon & Schuster International.

Rogers, J. (2009, January 15). *Teenage founder of No Cussing Club under siege*. Retrieved April 24, 2013, from Ventura County Star, The Associated Press: http://www.vcstar.com/news/2009/jan/15/teenage-founder-of-no-cussing-club-under-siege/

Sieczkowski, C. (2012, October 16). *Amanda Todd's Alleged Bully Named By Anonymous After Teen's Tragic Suicide*. Retrieved April 24, 2013, from The Huffington Post: http://www.huffingtonpost.com/2012/10/16/amanda-todd-bully-anonymous-suicide_n_1969792.html

Syed-Abdul S, F.-L. L. (2013). Misleading Health-Related Information Promoted Through Video-Based Social Media: Anorexia on YouTube. *Journal of Medical Internet Research*.

Taleb, N. N. (2010). *The Black Swan: Second Edition: The Impact of the Highly Improbable: With a new section: "On Robustness and Fragility"* (2nd edition ed.). Random House Trade Paperbacks.

The Government Office for Science. (2013). *Foresight Future Identieis.* London: The Government Office for Science.

The Riots Communities and Victims Panel. (2012). *After the riots: The final report of the Riots Communities and Victims Panel.* London: The Riots Communities and Victims Panel.

Torrey, C., Burke, M., Lee, M., Dey, A., Fussell, S., & Keisler, S. (2007). Connected Giving: Ordinary People Coordinating Disaster Relief on the Internet. *Proceedings of the 40th Hawaii International Conference on System Sciences* (p. 179a). IEEE.

Varian, C. S. (1999). *Information Rules.* Harvard Business School Press.

Virilio, P (2006). Speed and Politics. Los Angeles: Semiotexte.

Wilson, B. (2012, Novemeber 1). *US presidential election 2012: targeted online video ads redefine tactics*. Retrieved April 24, 2013, from The Guardian Online: http://www.guardian.co.uk/media-network/media-network-blog/2012/nov/01/us-presidential-election-2012-barack-obama-mitt-romney

**Security Futures'** mission is to is create a space where we could develop innovative techniques to think about the future, techniques that draw together the insight and expertise of researchers working across different disciplines. In this collaborative space, researchers and other partner organisations have the freedom to explore questions about security and technology. But also to formulate the questions that we might need to start asking about the emerging trends in technology, society and security. A space where we can bring together people working on the cutting edges of technology, social, legal and political disciplines to ask questions about the world we live in. A space where we might begin to imagine new horizons and start to see the problems that

**Bold Creative** is a London-based digital agency that specialises in creating content and campaigns to engage, educate, entertain and inspire young people. They are a socially conscious organisation driven by their ability to develop new and creative ways to build real value into the way young audiences interact with important causes. Their track record in design, production, and interactive uniquely enables them to achieve very specific social and educational aims.

**The Digital Disruption Project** is an initiative that aims is to improve the learning practices, personal development and social wellbeing of young people in the UK by developing their 'digital judgement': that is, the ability to engage critically with the content they consume, create and share online. Digital judgement combines 'traditional' critical thinking skills, such as source verification, with 'new' knowledge about how the digital world works, such as understanding search engines and Wikipedia.

**Security Lancaster** is a university wide research centre on security and protection sciences. It delivers research and education that innovates and creatively challenges the way that individuals, organisations and societies secure and protect themselves. This is achieved via engagement and collaboration with organisations from a range of sectors along with governments. The centres approach delivers the very best use-inspired and pure research alongside cutting edge education that delivers real impact and social change.

This work was funded by Security Lancaster via the auspices of Lancaster University's Faculty of Science and Technology.

**Science and Technology Business Partnerships and Enterprise**

As well as working with a range of external partners, ICT and Security form part of a wider theme based team across Science and Technology at Lancaster who offer expertise in:

- Advanced Manufacturing
- Energy
- Environment
- Health & Human Development
- Quantum Technologies
- Mathematics and Statistics

**Working in Partnership**

Across the themes we form collaborative partnerships around these 5 key areas:

- Collaborative Research and Consultancy
- Training and Education
- Co-location and Secondment
- Student Placements
- Product Development and IPR

For more information regarding the event related to this report and for further details of other associated events and information please visit

**http://www.security-centre.lancs.ac.uk/digidistrupt**