WHAT DOES THE DARK NET MEAN FOR THE FUTURE OF INTELLIGENCE WORK?

The 2014 Annual Vincent Briscoe Security Lecture
Imperial College, London

Jamie Bartlett, Demos

29th October, 2014

DEMOS

FULL TEXT

It's a great honour to be able to speak to you about my new book, The Dark Net at the annual Vincent Briscoe lecture.

I'm going to take you back to 1844. 'No man's correspondence is safe. No man's confidence can be deemed secret; the secrets of no family or no individual can be guaranteed from reaching the ear of a cabinet Minister'. So wrote The Times. Britain was in the middle of a scandal. The Home Secretary had decided to secretly monitor the letters of an exiled Italian called Guiseppe Mazzini, the leader of *Le Giovine Italia*. When Mazzini petitioned parliament, the Home Secretary replied that 'it was not for the public good to pry or inquire into the particular causes which called for the exercise thereof'. He therefore would not 'consent to enter into any further explanations'.

We are faced with a very similar set of challenges: new technology and ways of communicating disrupting the methods and law we have built for a different era. Today I'm going to talk about where I think it might be heading.

Some clues are found in my book the Dark Net. It's series of portraits of some of the net's least explored subcultures: some of the extremities of what people do under the conditions of anon- or pseudon- ymity online. It covers the anonymizing network Tor (which often mistakenly called the dark net) but also many of the parts of the internet that most of us know and use every day: internet trolls on 4chan, radical nationalists on Facebook, pro-anorexia communities on blogs and forums. It's called the Dark Net not because it's necessarily all bad, but rather that it's underexplored and obscure.

Over the course of one year, I immersed myself in these underexplored subcultures, and met the people who are part of them. I don't have time to go into what I found: although suffice to say it is all far more interesting and morally ambiguous than I'd expected.

Today I am going to focus on just one part of the book: the changing ways in which people can and do stay secret and hidden online; and what I think this might mean for security and intelligence work. My argument is simple, really. The world is changing: and the security services work needs to change with it.

Cast your mind back to the early 1990s. Although it started as a small academic project, networked computing quickly drew in all sorts of people, who saw the prospect of communicating via a screen as an opportunity for both good and ill. The US government was increasingly worried about this new, ungovernable public space. Although still tiny, "cyberspace" was becoming a nuisance to the law: untraceable paedophile networks were sharing illegal images of children, anonymous hackers were stealing intellectual property, and internet trolling was rife.

In response to these trends, in 1990 the FBI launched Operation Sun Devil, a nationwide, over-the-top crackdown on hackers and upped their monitoring of the online world; and tried to prevent the spread of powerful cryptography software.

The response was precisely the opposite of what the US government hoped. A group called the 'cypherpunks', a small collection of Californian libertarians determined to build or share cryptography – tools and techniques to keep secret, to avoid detection. It became an email list, which predicted, developed or invented almost every technique now employed by computer users to avoid government surveillance. (Assange became was a member of that list in 1995). Phil Zimmerman decided to work on and then release his open source Pretty Good Privacy encryption system, which is still the industry standard today. The Electronics Frontier Foundation was set up and remains an influential and fierce defender of online privacy. Every reaction has a counter-reaction. And this counter reaction was called the 'crypto-wars'.

Any of this sound familiar? It should of course. In response to another perceived overreach of governments into private digital spaces, we're entering a second crypto-war. This is going to challenge how the security services work.

A good example of why are the dark net markets. Let me explain to you how they work.

You can't access the dark net markets using a normal browser like Chrome or Internet Explorer. They are websites that sit on an encrypted part of internet called 'Tor Hidden Services' where URLs are a string of meaningless numbers and letters that end in .onion, and are accessed using a special browser called 'Tor'. Tor, which was originally built by the US Navy but is now an open source project, allows people to browse the net without giving away their true location – and using Tor also allows you to connect to these Hidden Services. Although it used to be a little tricky to set up, Tor now looks and feels like any other web browser. True, it's a little slower on account of how it cloaks your identity (which entails bouncing your URL request around the world via several other 'nodes' that use the same software) but that's a price many are willing to pay for online anonymity. This little known parallel internet is a natural home for an uncensored drugs marketplace, as it is for whistleblower websites and political dissidents who also rely on its powers of obfuscation (one reason why Tor is widely considered vital for freedom of speech around the world).

The most infamous of these dark net markets was called the Silk Road, named after the ancient trading route. Following a lengthy investigation by the FBI, the Silk Road was closed down in October 2013, after over two years of uninterrupted trade (The trial of 29-year-old Ross Ulbricht, who the FBI allege ran the site, is ongoing -- Ulbricht denies all charges). At the time, prosecutors proclaimed the beginning of the end of this illicit trade. But as soon as it was knocked offline, dozens of copycat sites were launched by anonymous operators. In 2013 there were a small handful of these marketplaces. There are now around 30 heads of Hydra: Pandora, Outlaw Market, Agora, Silk Road 2.0, 1776 Market Place, and most of them are doing a decent trade.

The first thing that strikes you on signing up to Silk Road 2.0 – which was set up within a month of the original being busted – is

how eerily familiar it all feels to anyone who's used eBay or Amazon. Every one of the thousands of products on offer has a detailed description, photograph and price. All products and vendors are rated out of five by buyers, who also provide detailed written feedback. There are customer service buttons and shopping trolley carts and free-package-and-delivery and one-off specials. You place an order; pay with Bitcoin; and wait for your product to arrive in the post.

And, of course, an unbelievable choice of products on offer. Technically speaking, Silk Road 2.0 is an anonymous market for anything (with some exceptions, such as child pornography – even radical libertarians tend to draw the line here) which means wares stretch from the mundane to the bizarre: listings include a complete box-set of *The Sopranos*; and a hundred-dollar Marine Depot Aquarium Supplies voucher. In April this year, the most popular selling item on the entire site was a fake £20 Tesco voucher. But most people are here for the drugs. There are hundreds of vendors to choose from, selling every conceivable narcotic.

It's the customer reviews, not clever encryption, that's is the key to understanding how and why these markets operate. All the vendors use pseudonyms, but they keep the same fake name to build up their reputation. Because it's so easy for buyers to switch allegiance to any one of 900 competitors at any moment, the vendors are forced to compete for custom. The only way to get it is by having a good history of positive feedback from other users. As I browsed through the marijuana offers, I found 3,000 offers advertised by over 200 different dealers. So I began to scour user reviews, trying to spot those that others had found reliable and trustworthy: "First Order was Lost...i got a reship and now im very happy...He is One of the best vendors on the road!! Very friendly and very good Communication too. i will be back Soon ;) please Check this vendor... 5 Stars'.

A few reviews like this will make a dealer's reputation. As a result, dealers here are polite, attentive, and consumer centric – offering free package and delivery on big purchases, refunds, special offers and even loyalty systems. Some even offer freebies to anyone willing

to write lengthy and careful feedback. I got in touch with 'DrugsHeaven' on the site's internal email system. He or she was based overseas, but the vendor page advertised "excellent and consistent top quality weed& hash for a fair price". There was a refund policy, estimated shipping times, detailed terms and conditions and close to 2,000 pieces of feedback over the last four months, averaging around 4.8 out of 5. (And, importantly, the occasional negative review). "I'm new here", I said. "Do you think I could just buy a tiny amount of marijuana?" DrugsHeaven quickly responded: "Hi there! Thanks for the mail. My advice is that starting small is the smart thing to do, so no problem if you want to start with 1 gram. I would too if I were you. I hope we can do some business! Kind regards. DrugsHeaven."

It's that most powerful driver – market demand – mixed with new technology that makes these markets such a formidable place. It's little surprise the dark net markets are growing so quickly: happy customers. According to a report released this month by the Digital Citizens Alliance, there are now 45 thousand drugs products for sale on these sites. In January, it was around 30 thousand. And because they live on the fringes, dark net markets are remarkably adaptive, and learn from each mistake: always innovating ways to be more secure, more decentralised, harder to combat.

Every month the sites get smarter. In April 2014 "Grams", a search engine for drugs, was launched and included "trending" searches and advertising space. Some vendors are even branding their opium or cocaine as 'fair trade', 'organic' or sourced from conflict free zones. 'We are a team of libertarian cocaine dealers' writes one dealer, targeting the ethically conscious user: 'we never buy coke from cartels! We never buy coke from police! We help farmers from Peru, Bolivia and some chemistry students in Brazil, Paraguay and Argentina. We do fair trade!'

This creates a moral dilemma. The offline drugs market as it stands is all local monopolies and cartels. By introducing clever payment mechanisms, feedback systems, and real competition, power is shifting to the users. The most surprising statistics about the Silk Road 2.0 is not the amount of available drugs (although

that is truly staggering); it's the satisfaction scores. When I analysed 120,000 customer reviews made on the site earlier this year, over 95 percent scored 5/5. On the streets, drug purity is wildly variable: the average purity of street cocaine is 25 per cent, but has been found as low as 2 per cent, typically cut with mixing substances such as Benzocaine. This is extremely dangerous, because overdosing is often the result of not knowing the purity, dosage, or content of the drug you take. The user-ranking system provides a safer, systematic and reliable way of determining the quality and purity of the product: trusting the feedback of people who have used the product. And think of the possible social benefits too. Half of the 7,000 organised crime gangs in the UK are involved in drugs. From what little is known of them, most of the dealers on dark net markets resemble middle managers in logistics companies who spend their days taking and shipping orders all day and working out new marketing strategies.

And yet: they also mean more and better drugs more readily available at a competitive price, and that's nothing to celebrate. I also suspect that we will soon see more people using the Silk Road for wholesale: students purchase a stash and then sell it to friends; even on the streets.

But the dark net markets are more than just a place to score. There is a bustling online community dotted all over the world comprising libertarians, bitcoin fanatics, drugs aficionados and dealers, who all constantly monitor the markets, check security vulnerabilities and performance, and update others on what they find. Each has his or her own motivations – for the libertarians it’s a way of denuding the state – but together they keep these sites functioning smoothly.

And many of the people involved see it as the digital front in a battle over individual liberty: a rejection of internet surveillance and censorship that they believe has come to dominate modern life online.

In response to the revelations by NSA whistleblower Edward Snowden – just like in 1993 – there has been a growth in the use of tools for citizens to keep their privacy online. Both Tor browsers,

Tor Hidden Services, PGP encryption – have all seen increases in use. That reflects both growing public worry about online privacy, and increased awareness of the tools out there that can help. We are about to see a new generation of easy to use auto-encryption services: 'MailPile', Dark Mail, Jitsi. And alongside this: a new generation of distributed social networks: which are built on a model of no centralized server (often based on the block chain technology that underpins bitcoin). Take 'Twister', which is a distributed social media platform using the Bitcoin blockchain. Your posts would become part of the public blockchain record, and every user of the platform would have their own copy. Everything could be done anonymously, and censorship would be close to impossible. No one can shut it down, because no one owns it.' I interviewed Miguel Freitas: Twister's chief developer. Miguel worked for several straight months – also unpaid, just as Zimmermann did when working on PGP – to convert the blockchain model into a social media platform after the British Prime Minister, David Cameron, admitted his government considered shutting down Twitter during the 2011 London riots. 'I tried searching for peer-to-peer microblogging alternatives, but I couldn't find any,' he told me. 'The internet alone won't help information flow if all the power is in the hands of Facebook and friends.'

The motivations of many of the people who design and create these tools is typically honourable and well intentioned: a desire to help make sure people can remain private and secret online, to keep communication open and not controlled by third parties. In the UK that's a good thing. In places like Russia or China, it's the difference between life and death.

Due to that same combination of demand and technology I discussed in the dark net markets, these technologies are going to become increasingly easy to use, more widespread and ever more sophisticated.

And the frustrating reality is – and it is something sometimes overlooked by civil liberties groups – it will also be the terrorists,

the serious criminals, who will be the early adopters, thereby making intelligence work significantly harder.

The evidence on this is pretty clear. Although it is vital for free expression, according to researchers at the University of Luxembourg, 44 per cent of Tor Hidden Services are given up to criminality (mainly anonymous market places and illegal pornography). Anders Breivik, in his 'Manifesto' urged others to use the Tor browser. I have already seen Islamic State Twitter accounts sharing information about how to use Tor; al-Qaeda and Islamic State have both created their own versions of Pretty Good Privacy encryption. We already have seen Islamic State use Diaspora (which is similar to Twister): given the way they tend to use various social platforms to publish and share propaganda in a way that makes it difficult to remove, the shift to distributed social networking sites impossible to censor is almost impossible. And it's not just drugs for sale on the dark net markets: some of them sell guns, bomb making instructions, zero-hour exploit hacks, botnets – which could potentially create a significant opportunity for terrorist groups.

Herein lies the problem then. Even though the criticism of the intelligence services is often exaggerated – that we are living in some kind of 'Orwellian nightmare' – it has become something of an accepted wisdom that the intelligence agencies are snaffling up every single thing we do online, our every click, swipe and movement.

And yet, simultaneously, I think it is going to become increasingly difficult to stop terrorist attacks – especially of the 'lone wolf' variety, and especially as there are more and better ways to stay anonymous and hidden online. To make matters worse: because there is always some clue, some digital breadcrumb out there, every attack or serious crime will be accompanied by retroactive prediction by so called experts: 'why didn't you stop this'?

This may combine to create a public image of an intelligence apparatus that is both omnipresent and incompetent: which is the precise opposite of what we want.

So what, if anything, is the solution?

First, I think this is going to presage a return to more 'old fashioned' intelligence work. Traffic or network level investigation – the sort of bulk data collection and pattern spotting I think will be increasingly unpopular, and less likely to be effective. During the Cold War, Soviet cyphers were too strong for GCHQ to break, so British intelligence switched to recruiting more Soviet agents: Oleg Gordievsky. If the state considers you to be a legitimate target for security investigation but can't track your online activity using an anonymous browser, they'll put a bug in your bedroom instead. I predict more agents, more 'human intelligence' in future. And that will require greater investment in digital policing: new people, new skills, new capabilities

But this type of intelligence work is more targeted – it focuses on the most serious crimes – but is also more morally hazardous, more intrusive to people's privacy. And that, in turn, will require a new legal settlement about how public agencies can access our private information online. The legitimacy of security work depends on public understanding, trust and confidence. This is where systems of oversight and scrutiny are vital. As it stands, oversight and scrutiny systems are not sufficiently trusted: typically staffed by people drawn from the same establishment they are supposed to oversee. We at Demos would like to see the establishment of Surveillance Juries: legally appointed, security vetted members of the public – perhaps with the inclusion of some civil liberties groups – who can take part in overseeing the work of our intelligence agencies.

The trends above might also necessitate new strategic priorities. You cannot go after everyone on the dark net. Take the case of indecent images of children, which I cover in chapter 4 in my book. Essentially what has happened is that the supply of illegal images has become distributed. Tor Hidden Service act as something of a recycling plant: people upload illegal material to a central hub – and then hundreds download onto their own servers. When it's

taken down, someone simply uploads it again. In 1997, the NSPCC thought there was 7,000 illegal images in circulation. In 2012, the Child Exploitation and Online Protection centre found an individual collector with over 2 million. Although all governments promise to rid the net of this material, I'm afraid it's not possible. We need more resources invested in digital policing to match the way crime has shifted online; but perhaps also a strategic focus on the most serious crimes. And we heard recently that the National Crime Agency accept that it simply does not have the resources to go after everyone who accesses illegal pornography online – they will put their resources into tracking and arresting the most serious offenders. This was a brave and candid statement and the right approach, provided it's combined with a smart tactical approach that ensures people don't think they can break the law without consequence.

And that, too, might require striking new alliances – driven by strategic priorities. Tor Hidden Services might be uncensored, but they are not without some community self-policing. Among the hacker community who know this area far better than I do, there is a very strong revulsion against people using these services to harm innocent citizens: whether that is Islamic State, or child abuse images, or people trafficking. It was Anonymous hacktivists (and then more recently two vigilante hackers) – who helped to identify and remove Tor Hidden Service sites which were hosting child pornography. Anonymous might be no friend to the US government: but it recently 'declared war' on ISIS. In this space, governments would be wise to work with anyone willing to help.

You will note that many of these general questions are not new. But on the fringes, on the edges, I think we are forced to see them and address them with more clarity. The Mazzini scandal, where I started this talk, put an end to the political spying on letters for 50 years – and even led to the Home Office dismantling the cryptographic know how of the department that was much missed at the outbreak of world war 1. We don't have that luxury. Our house, fridge and keys will soon be online; we'll even begin to wear the internet soon. As we struggle onwards, perhaps Mazzini himself

has one more lesson for us: ‘Slumber not in the tents of your fathers’. He later wrote. ‘The world is advancing. Advance with it!’

CHECK BY DELIVERY