online anonymity islamic state and surveillance

Jamie Bartlett
Alex Krasodomski-Jones

March 2015

DEMOS

Published by Demos March 2015

Third Floor
Magdalen House
136 Tooley Street
London
SE1 2TU

hello@demos.co.uk
www.demos.co.uk

INTRODUCTION

This is a very short discussion paper about the way in which terrorist groups, and specifically Islamic State, use modern encryption systems to evade surveillance. It examines how the risks of online anonymity are weighed against its many social, personal and economic benefits. It sets out a small number of recommendations about how the intelligence and security services might respond to the growing availability and use of encryption services.

BACKGROUND

Islamist terrorists have long used a variety of types of encryption software in their communications. Back in 2007, al-Qaeda's Global Islamic Media Front (GIMF) released their own encryption software: Asrar al-Mujahedeen. This was the first purpose-made Islamist encryption software, primarily used for email communications. It is routinely updated and promoted in Jihadist magazines. More recently, the al-Qaeda associated al-Fajr Technical Committee has released Amn al-Mujahid for Windows, which encrypts emails, instant messages and SMS.

Ways of evading surveillance and detection are – predictably enough – frequently discussed on forums and websites, by terrorists and serious and organized criminals of all types. For example, Anders Breivik, the Norwegian terrorist who murdered seventy-seven people in 2011, wrote a manual that set out best practice recommendations regarding the use of Tor and Virtual Private Network services. Terrorists are, by and large, early adopters of any technology that can help them achieve their objectives.

None more so than Islamic State – currently the main concern for our security services. The 'frontier' of holy war is shifting to the virtual front: increasingly, professional media teams are embedded with Islamic State fighting units, and they draw on a global network of media supporters. Since 2011, members of jihadist forums have issued media strategies that encourage the development of this 'media mujahidin'.

Social media is especially valuable to Islamic State since it allows anyone to join this media mujahideen. A large quantity of propaganda from Islamic State sympathisers or active supporters is posted daily on social media platforms each day from all over the world. Because Islamic State considers the media mujahideen significant, they work hard to evade censorship as well as surveillance. When YouTube deletes a propaganda video, Islamic State sympathisers typically post it on text-based sharing boards like justepaste.it or elsewhere, and alert followers to its new location – from where it is very quickly downloaded and re-posted across multiple sites. This makes censorship of their material very difficult. By the time YouTube's content manager has seen the video and taken steps to block it, it's already distributed to thousands of users' computers all over the world, from where it can be re-uploaded again. Similarly, whenever their social media accounts are shut down, they immediately start another one – or, more often, have multiple accounts ready to hand.

THE SNOWDEN EFFECT

One of the major concerns following the revelations of government internet surveillance by Edward Snowden is the possibility that terrorist groups learn from those revelations and take evasive measures in response: thereby making the already difficult task of monitoring or censoring terrorist activity even more difficult. (Note: this is not a comment on the rights or wrongs of Snowden's activity, rather the more specific question of how it affects the way intelligence and security services work).

The effect of the Snowden revelations has indeed been significant. Already it has sparked something of a privacy backlash, one which will have far reaching consequences for how the intelligence agencies operate. We call it 'The Snowden Effect'.

First, public concern about internet privacy has been increasing, and not only in relation to governments: polls suggest that members of the public are also worried about the way private companies collect, process and use their personal data. There's been a flurry of 'crypto-parties' around the world, where internet users can learn about the latest techniques to protect their privacy online for free. Anonymous browsers like 'Tor', which are used to browse the net without revealing a user's IP address, are becoming more popular: there are now an estimated 2.5 million daily users. Tor can also be used to access 'Hidden Services' (usually referred to as the 'dark net') which are an encrypted network of sites that use the Tor protocol, making it very difficult for websites or the people who use them to be located. Facebook users, who used to be happy sharing everything with anyone, are inching towards more private settings. Phil Zimmermann's PGP ('Pretty Good Privacy') text and file encryption software is being downloaded by a growing number of people.

Second, many of the large technology companies have become more hesitant to work with the intelligence and security services. One of the authors recently spoke to an official from a large social media platform provider who explained her company was very disappointed to learn of the extent of surveillance: 'Our trust in the spies has been severely damaged. It will take years to rebuild it.' For these companies, users' trust in the security of their platform is vital. Many of the large companies have added extra layers of encryption to their systems – making it harder for the third parties to spy on them. New social media companies have even popped up – like the 'anti- Facebook', ad-free social network site Ello. 'Collecting and selling your personal data, reading your posts to your friends, and mapping your social connections for profit is both creepy and unethical,' Ello declares. 'Under the guise of offering a "free" service, users pay a high price in intrusive advertising and lack of privacy … Ello doesn't sell ads. Nor do we sell data about you to third parties.' Many of these companies are based overseas, making it still more difficult to access information, even under legal warrant. Since so much of modern intelligence work now relies on internet-based companies handing over information to the authorities, this is a significant move.

Third, and most significant, are the long-term effects. Motivated by an honourable desire to protect online freedom and privacy for everyone, hundreds of computer scientists and internet specialists are working on ingenious ways of keeping online secrets, preventing censorship, and fighting against centralised control. We anticipate that soon there will be a new generation of easy-to-use, auto-encryption internet services. Services such as MailPile, and Dark Mail – email services where everything is automatically encrypted. Then there's the Blackphone – a smart phone that encrypts and hides everything you're doing. There are dozens – hundreds, perhaps – of new bits of software and hardware like this that cover your tracks, being developed as you read this – and mainly by activists motivated not by profit, but by privacy. Within a few short years, we think a far greater proportion of internet communications and activity will be encrypted, and harder for the intelligence and security services to access.

And there are even more revolutionary plans in the pipeline. Back in 2009, in an obscure cryptography chat forum, a mysterious man called Satoshi Nakamoto invented the crypto-currency Bitcoin. It turns out the real genius of Bitcoin was not the currency at all, but the way that it works. Bitcoin creates an immutable, unchangeable public copy of every transaction ever made by its users, which is hosted and verified by every computer that downloads the software. This public copy is called the 'blockchain'. Pretty soon, enthusiasts figured out that the blockchain system could be used for anything. Armed with 30,000 Bitcoins (around $12 million) of crowdfunded support, the Ethereum project is dedicated to creating a new, blockchain-operated internet. Ethereum's developers hope the system will herald a revolution in the way we use the net – allowing us to do everything online directly with each other, with no centralised servers capturing and controlling the content. This is what's called a 'distributed trust' network: a decentralised system where no one person or authority controls or runs the network. Since it runs in this decentralised way and is backed by strong encryption, its designers think it will create a network that's almost impossible to censor.

Already others have applied this principle to all sorts of areas. One man built a permanent domain name system called Namecoin; another an untraceable email system call Bitmessage. Perhaps the most interesting of all is a social media platform called Twister, a sort of anonymous version of Twitter. Miguel Freitas, the Brazilian who spent three months building it, tells me he was sparked into action when he read that David Cameron had considered shutting down Twitter after the 2011 riots. 'The internet alone won't help information flow,' Freitas explained to one of the authors, 'if all the power is in the hands of a few people.'

Taken together, this amounts to a second 'Crypto-War' – a struggle between citizens and governments over the right and ability to stay hidden online. (Interestingly, the first Crypto-War began in the early 1990s, when internet users were also concerned about internet privacy being eroded by state surveillance. Then, as now, the result was an enormous growth in software and hardware available for citizens to evade surveillance).

These new developments augur well for freedom and privacy on the net: and the very many benefits this will bring for most of us. This powerful combination of public appetite and new technology means staying hidden online is becoming easier and more sophisticated. It might feel unlikely at a time when every click and swipe is being collected by someone somewhere, but in the years ahead, it will be harder for external agencies to monitor or collect what we share and see; and censorship will become far more difficult.

Although this software is typically being built for whistleblowers, journalists and ordinary internet users who have legitimate concerns about internet privacy, the unfortunate truth is that serious criminals will be among the earliest adopters. These developments will therefore create new and very significant challenges for the intelligence and security services.

EVIDENCE

There is significant evidence about the way in which serious and organised criminal activity makes use of modern encryption. A recent study from the University of Portsmouth found that child pornography sites accounted for nearly 83 per cent of traffic in the 'dark net'. (This data is disputed: these illegal pornography sites themselves only account for 2 per cent of the 45,000 sites available through Tor, and "traffic" also refers not only to individuals but to automated 'bots', DDOS attacks, and law enforcement officers who monitor the sites.) Dark net market places where all and any narcotics can be bought and sold are significant and growing, and have been documented at length by Jamie Bartlett in his book *The Dark Net*. It is well established that criminals of all shades tend to be what's called 'early adopters' of technology: and are usually, as one might expect, looking for ways to make the job of catching them more difficult.

In our own research into the subject, we have found some limited evidence of Twitter users sympathetic to Islamic State sharing occasional information about the importance of using encryption when on the net; and in one case complaining that the website ask.fm (sometimes used by Islamic State sympathisers to ask questions about their faith) was blocking access by users of Tor.

We have recently discovered a new piece of evidence that demonstrates the extent to which Islamic State sympathisers are up to speed with the latest counter-surveillance software. It is a blog post that was uploaded on the text sharing board justpaste.it (a legal website that allows people to upload text and image documents anonymously).

We believe that it demonstrates very clearly both how significant Islamic State sympathisers considered the internet to be as part of their struggle; and the extent to which they are aware of tools that allow them to mask their identity and circumnavigate censorship.

According to justpaste.it, this blog was created on 20th August 2014. At the time of writing (March 2015) it has had 7053 page views. As far we can best establish, the same blog was originally posted on a Wordpress blog in the same month (it's common to post the same content on multiple platforms). Its association with Islamic State comes from the name of the Wordpress blog, which is 'al khalifah aridat' which means 'the caliphate has returned'.

The title of the blog is 'Remaining Anonymous Online', and we have copied it in full, without correction, below:

> *I seek refuge in Allah from Shaytan, the accursed,*
> *"And prepare against them whatever you are able of power and of steeds of war by which you may terrify the enemy of Allah and your enemy and others besides them whom you do not know [but] whom Allah knows. And whatever you spend in the cause of Allah will be fully repaid to you, and you will not be wronged."*
> *[8:60]*
>
> *In the name of Allah, the indiscriminately merciful, the acutely merciful,*
> *All glory and thanks is to Allah, the cherisher of all of existence,*
> *And, verily, may peace and blessings be upon our leader Muhammad, his family, his companions, and all those that follow upon their path a great peace until the day of judgement.*
>
> *As for what follows,*
>
> ### ***Remaining Anonymous Online***
>
> *The question of online anonymity is an important one in this day and age. The advent of technology has made the internet ubiquitous and necessary to daily life. However, we see that the tyrants have invested in methods by which they can monitor every single particle of data that goes across the web. Every picture, phone call, text message, or any other form of anything uploaded or downloaded is monitored by these agencies. This prompts several questions, why do they monitor? Do we need to avoid their monitoring? How?*
>
> *Since this is intended to be a rather brief paper, I won't discuss these questions in depth besides the final one. Short answers will suffice the two former questions. The intelligence agencies specifically monitor the internet with the intention of dismantling anti-colonial*

narratives and attacking those who postulate them. Whether Muslim, radical socialist, anarchist, or anti-government activist, they want you. They want to know what you send, when you send it, to whom you send it to, why, and how to use it against you. They monitor your social media. Even if you never use your real name, post a picture, or leave any hints, they can track your IP address, know your identity, and jail you for a few online posts. They search for keywords such as "kafir" in order to find specific individuals. These agencies are notorious for even harassing youth around the ages of fourteen to sixteen for their beliefs and rather reckless online posting.

Do we really need to avoid this? How much danger is there? For one living in South Africa or in Sham, there may not be much danger directly. You do not need to conceal your identity from any immediate threat that would be able to reach you through your internet usage. The need to avoid these agencies is exaggerated in those living in Western countries, from Finland to the West coast of the United States. Here, kafir intelligence agencies are particularly interested in entrapping young Muslims. Sometimes, they will pretend to be sincere brothers or sisters and invite Muslims to marriage or hijrah, sometimes both, and when they coerce them, they jail them for trying to join terrorist organizations. It is clear these are amongst the foulest of Allah's creation. They want to find ikhwan who discuss these things because they know the true Islamic narrative is dangerous to their flamboyant way of life, wherein they hoard wealth from the poor and slaughter the weak. The United States government, the government of the United Kingdom, France, and elsewhere, want to jail you. They want you to suffer. And they aren't playing games.

Before I delve into how exactly this is done, I will dismiss a minor issue. Is it lying to trick the kufar into thinking we live in different locations than we actually do, through words or otherwise, even if other Muslims may hear or see this?

The ennobled messenger of Allah, sal'Allah'u alaiyhu wa' ala alaiyhi wa sahbihi salam tasleeman katheera ila yawm al din, said, in a rigorously authenticated narration,

"War is deceit."
[al-Bukhari: 3029]

The people we are fooling are ones who have an open war with Allah, his messenger, our khilafah, and just about every sincere Muslim on this planet. You are engaging in war tactics so that you can spread the true dawah and discuss matters of jihad, to uncover news about your mujahid brothers, to dismiss lies. You are entering into a sort of psychological warfare with them, they do not take it lightly, and we do not take it lightly. Therefore, we can trick them and it is totally permissible.

Ghost VPN

VPN stands for Virtual Private Network. Essentially, when one accesses a website through normal means, on their computer, they give that website their IP address. From this, the persons' address may be deduced. You may have wondered how Google knows what language to present to you without you ever having chosen it. That's how. Google knows your country, but the government agencies of the world know your home address and your entire name. That's where VPNs come in. If you use a VPN, instead of your IP telling them your real location, it will pick another location. Whether Italy, France, the Czech Republic, or in a remote location in the wilderness. If the agencies attempt to track you, their search will lead them to a dead end.

Ghost VPN is a popular program along these veins, but it is certainly not the only one. Many are available, and you can use whatever you feel most comfortable with. It is a program that you start, then you would begin to browse websites you don't want the government seeing you use, such as Twitter.

What are the adab of using a VPN? Never. Ever. Login with your real name or any such identifiers. Do not check your private Facebook with your full name. Do not check your private email. Or your bank account. Why not? This will show them that the person who is in Ireland is also logging into a Facebook account used by Salma Ahmad al-Sudaniyyah. And now they know your name, can find your address, and when you login to that Facebook off of a VPN, they know your home address. Turn on the VPN when no other internet browsers are open. Do what you need to do. Turn it off once done. Simple. One can download and install this off of Google search. https://www.cyberghostvpn.com/en_us

TOR

Whereas Ghost VPN was a program, TOR is an internet browser similar to Google Chrome, Firefox, and Internet Explorer. TOR uses the same line of thinking, however, instead of simply placing you in one location, it sends you internet signal through nodes, or servers, across dozens of countries. That way, any searches will come up inconclusive. TOR is a world ahead of Ghost VPN in terms of security and is the fundamental basic I recommend everyone to have. The same adab follow, no personal information on TOR whatsoever. One can choose to use Ghost VPN and TOR at the same time for additional security. This can be found and downloaded in the TOR Browser Bundle, available online. https://www.torproject.org/projects/torbrowser.html.en

Encrypted Email

Now that one has a VPN, and TOR, he needs a new email. You can't use that same email that reveals your home address. I personally recommend to turn on Ghost VPN whilst all other browsers are closed, turn on TOR, and go to bitmessage.ch. Follow the instructions there. Bitmessage is a peer-to-peer email service, meaning they don't save any of your emails *anywhere, unlike GMail which saves every email. The only person who gets your email is that other person. Emails are also sent to random peoples' inboxes, but they are not given the keys to see or decode them. This is done to confuse any spies who wish to uncover who sent what email to who. The contents of the email, the sender, and receiver are all hidden. Your email address will look something like, DA94RDGBH0SFDSG0484802@bitmessage.ch, when first making it. Simply go to the alias page, bitmessage alias, and create a nickname. You cannot login with this nickname, so it is important to save the original address, but it will end up looking like AmreekiWitness@bitmessage.ch instead of letters and numbers. This can be used to access social media. Login to your encrypted email at, bitmessage.ch/webmail .*

TAILS OS

We have discuss a program, Ghost VPN, a web browser, TOR, and now we will discuss an operating system, TAILS. The same way some people use Windows 7, Windows XP, Apple OS, or Linux, TAILS is an operating system. It is built from the ground up for the utmost privacy and security, in person, and online. It runs on a flash drive, and is a bit difficult to set up, but worth it. One boots their computer from a flashdrive, instead of when it normally boots from a hard-drive, and this allows one to access TAILS once installed. It has multiple desktops, can turn off instantly, TOR pre-installed, amongst a plethora of security features. To use a VPN and TAILS is one of the most bleeding edge forms of internet security. The same adab as before apply.
Download here: https://tails.boum.org/

Social Media

One might be asking themselves if they can continue using their old social media on these. The answer is yes, but I do not recommend it whatsoever. If one feels they post things in which they would need this security, which is most Muslims upon haqq who are active online, then they should make a disclaimer saying something similar to,
"I recant all opinions deemed dangerous or violent expressed on this page. This page was run for educational and analytic purposes only, to study the radical Muslim community for recreational purposes. I invite all those who follow this page to leave such corrupt ideology. I am not affiliated with any groups or organizations deemed terrorist or dangerous otherwise by any Western government or union of governments. I am a law abiding citizen in every regard."

And then proceed to delete all other tweets/posts on the page and after leaving this up for a few minutes, simply delete the page. Make no indication that you have done this based on instructions. You are in a war with these people, we have discussed this earlier. Now, once you are on either TOR with a VPN, TOR, and/or TAILS OS, make a new bitmessage email. Make an alias. Sign-up for Twitter on TOR. Do not post pictures or any indication of who you are explicitly. If you feel the need to alter your writing style a bit, if you were a popular page, do so. You can make subtle indications that this is so and so, however, nothing *that can be proven in a court of law. Allah'u must'a'n, may we never see inside one of those rooms for such a purpose.*

Instant Messaging

There are two forms of instant messaging that can be used. One is on Google chrome, known as Cryptocat. Simply turn off all other tabs, enter into Ghost VPN, and then use Cryptocat. The other exists on PC, Linux, and Android devices, and is known as ChatSecure. It is run through TOR and messages are encrypted. Searching online will give one all the information they need.

I hope I have not written too much and that this does not bore anyone, but this is an introduction to the matter of online security. There is much I did not discuss, and perhaps some omitted that I should have. I ask Allah to accept this from me for his sake, and not for the sake of anyone else, I ask Allah to give us barakah, I ask Him, the one who hears the call of the caller, to hear our call. I ask Allah to never allow us to comitt haram online. I ask him to hasten our venturing to the lands of jihad and hijrah, the lands in which there is no worry about people spying on private matters, in which the justice of Allah is supreme over the paranoia of men.

Ameen, Ameen, Ameen.
BarakAllah feekum, ash-hadul la ilaha il Allah, wa ash hadu anna Muhammadar Rasul'Allah. And the last of our call is al-hamdulilahi rahb al-alamin.

It is not possible for us to trace the exact details of the individual who posted this blog, nor is it possible to tie it directly to Islamic State, beyond the language used and the title of the blog. Given the way the media mujahideen – that network of sympathisers who assist Islamic State from all over the world via the net, this is perhaps less important than it once was. It appears to us to be clearly directed at members of the media mujahideen sympathetic to Islamic State and their message.

Our judgement is that this blog demonstrates a reasonably good level of technical know-how associated with these tools and techniques, which are among the current best ways to protect online privacy (or, when used by Islamist extremists, evade surveillance). It also demonstrates the significance which supporters of the media mujahideen attach to internet anonymity and software in the war against the West.

On a technical point, there are frequent suggestions that terrorist groups are also using the so-called 'dark net' to communicate. The dark net (correctly known as

‘Tor Hidden Services’) is a network of around 45-60,000 sites that use the Tor protocol to mask the location of a site server, making censorship or removal very difficult. Because users access the dark net using the Tor browser – which masks a user’s IP address – this makes surveillance on the dark net very difficult. However, we have not found significant evidence to suggest the dark net is being used by terrorist groups in a major way. Because of its modest size, the dark net does not serve a valuable propaganda purpose: and there are other more convenient ways to communicate beyond setting up a Tor Hidden Service site. We stress, however, that this is a subject that is extremely difficult to research, for obvious reasons.

DISCUSSION

The issue of online anonymity – as a moral good, as a legal right, and as a technical challenge – has become one of the most pressing debates of the day. In our judgement, terrorist groups – and indeed other serious criminals – are likely to be already using these tools and techniques to make monitoring and censoring of their activity more difficult.

However, this discussion needs to be set against the considerable benefits that online anonymity brings. Syrian democrats use the same tools listed above to create secret and untraceable chat rooms to co-ordinate activity. Russian dissidents use the tools listed above to circumnavigate state censorship of the net. Gay people in the Middle East use the same tools listed above to evade the brutal enforcers of state morality. Whistleblowers rely on the same tools listed above to ensure their safety (the dark net, for example, also hosts a secure dropbox run by the New Yorker magazine). Indeed, most of the software listed in the blog above is designed for, and is being used every day by, people who employ it for social good: whether individual internet users worried about privacy for legitimate reasons, or journalists trying to keep their sources safe from dictators. The frustrating fact is that these groups and causes *depend on precisely the same software and technology as the terrorists will exploit for their own purposes*. There is no way of getting around that.

Nevertheless, this clearly creates some new challenges for the intelligence agencies, and demonstrates how difficult their job is becoming. Since the July 2005 attacks in London, it is believed that the British security services have prevented at least one or two serious terrorist attacks on the UK every year. According to a January 2015 speech by the head of MI5, Andrew Parker, in the last fourteen months the agency has stopped twenty terrorist attacks against the UK. Internet surveillance is an increasingly important part of their work.

The Snowden Effect – in particular the growing availability and use of new software which is more difficult to monitor or access – creates a broad challenge to the intelligence and security services (and indeed to policing more generally, which we don't discuss here in detail). The Snowden revelations have created a false impression that the intelligence agencies are monitoring every single thing we do online, our every click, swipe and movement. The resulting public opinion shift against internet surveillance (or, more accurately, 'bulk data access' which is then monitored with legal warrant) limits the space within which the intelligence and security services can operate. For the reasons set out above, it will be increasingly easy for criminals and terrorists to avoid internet surveillance, or at the very least, make it more difficult, time-consuming and expensive for the intelligence and security services to find and access the information they need to investigate, disrupt and hopefully prevent and prosecute terrorists.

This is compounded by the general explosion in online data. Because there is now so much publicly available information online about everyone, there will always be some clue, some digital breadcrumb that they will miss: which gives the impression that they are ineffective. Following the murder of Lee Rigby, it was revealed that Michael Adebowale, one of the two killers, had communicated his desire to murder a soldier via a social network platform (later revealed to be Facebook) some six months before the attack. Why, asked the Intelligence and Security Committee, who conducted an investigation into the affair, hadn't this been picked up? Because of the processing power of modern computing and the explosion of data, people have come to expect that every bit of information and data can be collected and analysed, and things can be spotted in advance. This sort of techno-utopianism is questionable in principle and unworkable in practice. There are thirteen billion direct messages sent on Facebook alone every single day (and thirty-billion on Facebook's WhatsApp messenger). Trying to spot the one message out of the half a million sent every second that clearly hints at criminal intent is not an easy task – less like spotting the terrorist needle in the haystack, and more like finding a specific piece of hay. There will always be an expert after the event retroactively predicting what happened and pointing the finger at the people who missed it. The same sort of response occurred in the recent cases of Mohammed Emwazi and the three teenage girls from East London who went to Syria in early 2015.

Taken together, these three trends – an impression of omnipotence, an increasingly difficult job, and the inevitable existence of 'missed clues' – risk undermining public confidence in the intelligence and security services. When they don't succeed (and they can't all the time) we consider them useless. And when they do succeed, we don't see or hear of it. The danger, we think, is a creeping belief that the intelligence agencies are both omnipresent and incompetent, a body that lacks broad public support and can't do its job. Given the challenges we face (and not only, perhaps not even chiefly) from groups like Islamic State, this is the precise opposite of what we want.

WAYS FORWARD

So what are the options? In early March 2015, the UK Parliamentary Office for Science and Technology released a briefing note about online anonymity, which argued that although the Tor browser and the dark net is being misused by criminals, there are significant benefits for freedom and privacy. It argued that even if technically possible – which it probably isn't – the UK government would be very unwise to seek to ban Tor or other forms of encryption. We agree with this position. Banning encryption or Tor browsers is not an acceptable or plausible option. The software itself is a huge boon for freedom and democracy around the world. A great deal of 'low level' cybercrime – such as phishing, bank fraud, hacking – is taking place online all the time (this is often called 'volume' crime). Network security, better internet privacy or use of encryption for the individual can significantly assist in the prevention of crime and protection.

Similarly, trying to weaken key encryption standards, or creating 'back door' access into secure services, unfortunately, would fundamentally undermine confidence in the entire internet, would lead to similar 'back doors' being installed by undemocratic regimes, and would significantly reduce damage the social, economic and personal benefits it brings.

But it is important to ensure the intelligence agencies have the powers to keep society safe. We do not want, and do not believe the public want, terrorists to be able to operate in certain spaces that are, and are known to be, entirely beyond the reach of the law. Therefore, we make three broad suggestions about the future of surveillance to help the intelligence and security services keep up on top of these changes.

First, we need more James Bonds and fewer Edward Snowdens. Because of the explosive growth of online data, much modern intelligence work is now based on ‘big data’ traffic or network level investigation – the sort of data collection and pattern spotting revealed by Snowden. For the reasons set out above, such methods will prove both less popular and less effective. As recently suggested by the Intelligence and Security Committee 2015 report into the Edward Snowden revelations, there will still be a need for bulk data interception at times, as this can often be extremely important in identifying areas for more targeted surveillance. (This is sometimes called ‘target delivery’ as and can be important to the discovery of serious and organized crime). Inevitably this will sometimes mean that some innocent citizens’ communications will also be collected[1]. But as a general focus, we need a return to more ‘old-fashioned’ intelligence work, but in this new environment. Fewer dragnet programmes like Tempora and Prism - in favour of more targeted and ‘human’ intelligence (often referred to as ‘HUMINT’). This doesn’t mean de-fanging our intelligence agencies, rather providing the authorities with more powers to identify and monitor suspected individuals, including online. That will require greater investment in new people, new skills, new capabilities; for example, more power and personnel to hack into targets’ computers or phones, or to place malware or tracking tools on their hardware; more digital spies that specialise in undercover work online.

Second, we need to transform how we oversee spy work. Spying is by definition secretive, but we rightly want to know that these dangerous powers are used proportionately and within strictly defined legal limits. We don’t want there to be online places which are beyond the reach of the law, but we don't want that power misused and abused. This requires the intelligence and security services to seriously examine how and how far they can open up more of their work to public scrutiny, to become more transparent without undermining national security. One way this can be achieved is through the oversight and scrutiny system. As it stands, the Intelligence and Security Committee is typically staffed by people drawn from the same establishment they are supposed to oversee. The previous chair, Sir Malcolm Rifkind, is a former Secretary of State for Defence. This is not to denigrate their work, but they are hardly representative of society. We need to bring more ordinary people into the scrutiny apparatus, to make it more like the jury system (naturally with all the vetting and care that this would require) and more reflective of the broader diversity of legitimate opinions about proportionality of measures taken.

Finally, we need to worry less about censoring online content – such as the pointless and unwinnable whack-a-mole war against Islamic State propaganda – which has left us chasing uncomfortable propaganda around the net to little avail. Instead we must focus our limited resources on enabling people to develop their own critical faculties to reject these ideologies, and on preventing actual murders and actual attacks. That will also mean striking up new tactical alliances with groups like Anonymous – who have showed recently that they can be a vital ally in disrupting Islamic State's online activity.

The traditional model of counter-terrorism and intelligence is one of secrets and whispers. It's based on top-down control: stemming the flow of information and disrupting and restricting the way terrorists and serious criminals communicate and operate. But groups like Islamic State – like all of us – now live online, and the internet runs to a very different logic: it allows for the production, distribution and access of information, without limits or control. It is open to all and hard to repress. On balance, this is a positive thing for individual freedom, opportunity and equality. It will always be used for ill purpose too, which is why we will increasingly depend on strong intelligence services that people can trust.

NOTES

[1] In a sense, this is the significant difference of opinion between the privacy campaigners and security services: whether you agree that government should create the capabilities to be able to access everything, even if rarely used? The meaningful fault line is between those who generally say 'yes, as long as it's not misused: and the risks can be managed by good oversight and scrutiny' and those who say 'no, because it will always be misused, now or in future, and even building the capability – such as bulk access – is a form of intrusion'. Some tend to the first (social/liberal democrat) others to the second (liberal/libertarian). Both are legitimate positions to take, both are not stupid, and shouldn't be treated with the sort of derision that tends to characterise the discussion about internet surveillance.

Demos – Licence to Publish

The work (as defined below) is provided under the terms of this licence ('licence'). The work is protected by copyright and/or other applicable law. Any use of the work other than as authorized under this licence is prohibited. By exercising any rights to the work provided here, you accept and agree to be bound by the terms of this licence. Demos grants you the rights contained here in consideration of your acceptance of such terms and conditions.

1 Definitions

a 'Collective Work' means a work, such as a periodical issue, anthology or encyclopedia, in which the Work in its entirety in unmodified form, along with a number of other contributions, constituting separate and independent works in themselves, are assembled into a collective whole. A work that constitutes a Collective Work will not be considered a Derivative Work (as defined below) for the purposes of this Licence.

b 'Derivative Work' means a work based upon the Work or upon the Work and other pre-existing works, such as a musical arrangement, dramatization, fictionalization, motion picture version, sound recording, art reproduction, abridgment, condensation, or any other form in which the Work may be recast, transformed, or adapted, except that a work that constitutes a Collective Work or a translation from English into another language will not be considered a Derivative Work for the purpose of this Licence.

c 'Licensor' means the individual or entity that offers the Work under the terms of this Licence.

d 'Original Author' means the individual or entity who created the Work.

e 'Work' means the copyrightable work of authorship offered under the terms of this Licence.

f 'You' means an individual or entity exercising rights under this Licence who has not previously violated the terms of this Licence with respect to the Work,or who has received express permission from Demos to exercise rights under this Licence despite a previous violation.

2 Fair Use Rights

Nothing in this licence is intended to reduce, limit, or restrict any rights arising from fair use, first sale or other limitations on the exclusive rights of the copyright owner under copyright law or other applicable laws.

3 Licence Grant

Subject to the terms and conditions of this Licence, Licensor hereby grants You a worldwide, royalty-free, non-exclusive,perpetual (for the duration of the applicable copyright) licence to exercise the rights in the Work as stated below:

a to reproduce the Work, to incorporate the Work into one or more Collective Works, and to reproduce the Work as incorporated in the Collective Works;

b to distribute copies or phonorecords of, display publicly,perform publicly, and perform publicly by means of a digital audio transmission the Work including as incorporated in Collective Works; The above rights may be exercised in all media and formats whether now known or hereafter devised.The above rights include the right to make such modifications as are technically necessary to exercise the rights in other media and formats. All rights not expressly granted by Licensor are hereby reserved.

4 Restrictions

The licence granted in Section 3 above is expressly made subject to and limited by the following restrictions:

a You may distribute,publicly display, publicly perform, or publicly digitally perform the Work only under the terms of this Licence, and You must include a copy of, or the Uniform Resource Identifier for, this Licence with every copy or phonorecord of the Work You distribute, publicly display,publicly perform, or publicly digitally perform.You may not offer or impose any terms on the Work that alter or restrict the terms of this Licence or the recipients' exercise of the rights granted hereunder.You may not sublicence the Work.You must keep intact all notices that refer to this Licence and to the disclaimer of warranties.You may not distribute, publicly display, publicly perform, or publicly digitally perform the Work with any technological measures that control access or use of the Work in a manner inconsistent with the terms of this Licence Agreement.The above applies to the Work as incorporated in a Collective Work, but this does not require the Collective Work apart from the Work itself to be made subject to the terms of this Licence. If You create a Collective Work, upon notice from any Licencor You must, to the extent practicable, remove from the Collective Work any reference to such Licensor or the Original Author, as requested.

b You may not exercise any of the rights granted to You in Section 3 above in any manner that is primarily intended for or directed toward commercial advantage or private monetary compensation.The exchange of the Work for other copyrighted works by means of digital filesharing or otherwise shall not be considered to be intended for or directed toward commercial advantage or private monetary compensation, provided there is no payment of any monetary compensation in connection with the exchange of copyrighted works.

C If you distribute, publicly display, publicly perform, or publicly digitally perform the Work or any Collective Works,You must keep intact all copyright notices for the Work and give the Original Author credit reasonable to the medium or means You are utilizing by conveying the name (or pseudonym if applicable) of the Original Author if supplied; the title of the Work if supplied. Such credit may be implemented in any reasonable manner; provided, however, that in the case of a Collective Work, at a minimum such credit will appear where any other comparable authorship credit appears and in a manner at least as prominent as such other comparable authorship credit.

5 Representations, Warranties and Disclaimer

A By offering the Work for public release under this Licence, Licensor represents and warrants that, to the best of Licensor's knowledge after reasonable inquiry:
i Licensor has secured all rights in the Work necessary to grant the licence rights hereunder and to permit the lawful exercise of the rights granted hereunder without You having any obligation to pay any royalties, compulsory licence fees, residuals or any other payments;
ii The Work does not infringe the copyright, trademark, publicity rights, common law rights or any other right of any third party or constitute defamation, invasion of privacy or other tortious injury to any third party.
B except as expressly stated in this licence or otherwise agreed in writing or required by applicable law,the work is licenced on an 'as is'basis,without warranties of any kind, either express or implied including,without limitation,any warranties regarding the contents or accuracy of the work.

6 Limitation on Liability

Except to the extent required by applicable law, and except for damages arising from liability to a third party resulting from breach of the warranties in section 5, in no event will licensor be liable to you on any legal theory for any special, incidental,consequential, punitive or exemplary damages arising out of this licence or the use of the work, even if licensor has been advised of the possibility of such damages.

7 Termination

A This Licence and the rights granted hereunder will terminate automatically upon any breach by You of the terms of this Licence. Individuals or entities who have received Collective Works from You under this Licence,however, will not have their licences terminated provided such individuals or entities remain in full compliance with those licences. Sections 1, 2, 5, 6, 7, and 8 will survive any termination of this Licence.
B Subject to the above terms and conditions, the licence granted here is perpetual (for the duration of the applicable copyright in the Work). Notwithstanding the above, Licensor reserves the right to release the Work under different licence terms or to stop distributing the Work at any time; provided, however that any such election will not serve to withdraw this Licence (or any other licence that has been, or is required to be, granted under the terms of this Licence), and this Licence will continue in full force and effect unless terminated as stated above.

8 Miscellaneous

A Each time You distribute or publicly digitally perform the Work or a Collective Work, Demos offers to the recipient a licence to the Work on the same terms and conditions as the licence granted to You under this Licence.
B If any provision of this Licence is invalid or unenforceable under applicable law, it shall not affect the validity or enforceability of the remainder of the terms of this Licence, and without further action by the parties to this agreement, such provision shall be reformed to the minimum extent necessary to make such provision valid and enforceable.
C No term or provision of this Licence shall be deemed waived and no breach consented to unless such waiver or consent shall be in writing and signed by the party to be charged with such waiver or consent.
D This Licence constitutes the entire agreement between the parties with respect to the Work licensed here.There are no understandings, agreements or representations with respect to the Work not specified here. Licensor shall not be bound by any additional provisions that may appear in any communication from You.This Licence may not be modified without the mutual written agreement of Demos and You.

This is a very short discussion paper about the way in which terrorist groups, and specifically Islamic State, use modern encryption systems to evade surveillance. It examines how the risks of online anonymity are weighed against its many social, personal and economic benefits. It sets out a small number of recommendations about how the intelligence and security services might respond to the growing availability and use of encryption services.

Jamie Bartlett is Director of the Centre for the Analysis of Social Media at Demos and Author of *The Dark Net*.
Alex Krasodomski-Jones is a Research Associate at Demos.