Briefing Paper

Mass surveillance: security by 'remote control' - consequences and effectiveness

Esther Kersley
August 2015

Summary:

- The Edward Snowden leaks in 2013 revealed details of extensive internet and phone surveillance by US intelligence services and their partners, including the UK. The discovery has raised serious concerns about the indiscriminate collection and analysis of data from citizens by states in the name of counter terrorism, in particular regarding the right to privacy as well as concerns around the transparency, accountability and oversight of these programmes.

- Unforeseen consequences, including the proliferation of mass surveillance technologies and a decrease in public trust in government, as well as doubts over the effectiveness of mass surveillance as a method of counter-terrorism have been found. The use of private contractors working on surveillance programmes is a further concern.

- Mass surveillance techniques are an example of security by 'remote control' - the move towards countering threats at a distance without the need to deploy large military force. As technological advances have increased government intelligence gathering capabilities, mass surveillance techniques demonstrate the increasing interconnectedness between intelligence, technology and modern day warfare and the central role communications surveillance is in playing in modern conflict.

- Research that will produce quantitative evidence of the effectiveness of mass surveillance to thwart terror plots in the UK, as well as an analysis of the cost effectiveness of mass surveillance programmes in comparison to other forms of surveillance (e.g. targeted) is needed to facilitate an informed and comprehensive debate on the subject. The establishment of a robust regulatory framework for private security companies who are trading surveillance technologies, as well as publicly available information on the scale and regulation of private contractors working on "bulk collection" programmes in the UK is also needed, as well as the development of a long-term security strategy that doesn't look to remote control as an end in itself but instead focuses on addressing the root causes of conflict.

Introduction

In June 2013 Edward Snowden, a former employee of Booz Allen Hamilton, a contractor for the NSA, leaked details of extensive internet and phone surveillance by US intelligence services and their partners (including the UK) to the media. The discovery has raised serious concerns about the indiscriminate collection and analysis of data from citizens who are not suspected of having links to terrorism or other forms of crime. The leaks revealed (amongst other things) the existence of the PRISM programme, a surveillance programme, launched in 2007, through which the United States National Security Agency (NSA) obtains internet communications from Internet Service Providers (ISPs). The PRISM programme has "front door" access to data from at least nine major US internet companies including Google, Microsoft and Yahoo. The UK has access to PRISM as it is part of the 'Five Eyes' intelligence alliance comprising Australia, Canada, New Zealand, the United States and the United Kingdom. The leaked NSA documents also revealed the existence of numerous surveillance programmes jointly operated by the Five Eyes, including two (Tempora and MUSCULAR) operated by GCHQ.[1] The Tempora surveillance programme (operated by GCHQ) taps into and stores data drawn from fibre-optic cables carrying global communications (through which the majority of digital communications travel) so that it can be sifted and analysed. This includes the recordings of phone calls, content of email messages, entries on Facebook and the history of any internet user's access to websites.

Unlike targeted surveillance ("surveillance of a specific individual - or individuals - on a case-by-case basis, based on reasonable suspicion - or probable cause")[2] - which depends upon the existence of prior suspicion of the targeted individual or organisation, mass surveillance ("the subjection of a population or significant component of a group to indiscriminate monitoring")[3] involves no prior suspicion. Whilst forms of mass surveillance have always existed in the modern state, from national databases to closed-circuit television cameras (CCTV), they are increasingly becoming more advanced due in large to rapid technological developments. Today's mass surveillance techniques are no longer restricted to "public-facing activities".[4] Although many forms of mass surveillance exist today (such as the proliferation of CCTV or biometrics), this paper will focus on one type – mass communications surveillance.

It is claimed that the mass collection of communications data is vital for counter-terrorism today in order to detect and foil terror plots. This is premised on the idea that the threat we face today is different and thus requires adjustments to our approach to intelligence collection and analysis. Unlike Cold War adversaries, terrorists today are loosely organised in diffuse, non-hierarchical structures. For counter terrorism then we must be able to find "a few small dots of data in a sea of information and make a picture out of them".[5] In the UK, the recent Intelligence and Security Committee report found that mass surveillance was used to either "investigate the communications of individuals already known to pose a threat or to generate new intelligence leads".[6]

As well as this, technological advancements and changes in the way we communicate and interact today (the majority of communications now takes place over the internet and the number of communications we undertake has grown massively), have provided more opportunity for security agencies to intercept communication.[7] The cost of storing this data has also plunged dramatically (in 1980 it cost around $100, 000 to store 1GB, as of last year it cost around 10 cents),[8] meaning it has become both technologically and financially feasible for governments to record and store our communications data.[9] Mass surveillance is also part of a growing trend, by an increasing number of states, of using communications surveillance as a method of counter-terrorism - from identifying targets for drone attacks to monitoring the activities of entire populations - it is part of the move towards security by 'remote control'.

However, mass surveillance programmes[10] are deeply controversial due to the questions they raise surrounding our right to privacy, as well as concerns around the legality, transparency and oversight of these programmes. Unforeseen consequences and concerns over the effectiveness of mass surveillance as a counter-terrorism strategy are further worries. After outlining briefly the main debates surrounding ethics, legality and transparency, this paper will focus on the longer-term implications and effectiveness of mass surveillance as a counter-terrorism strategy, before locating mass surveillance within the broader 'remote control' context.

---

1 Ewen MacAskill, Julian Borger, Nick Hopkins, Nick Davies and James Ball, 'GCHQ taps fibre-optic cables for secret access to world's communications', The Guardian, 21st June 2013 http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa, http://www.theguardian.com/world/interactive/2013/jun/06/verizon-telephone-data-court-order, http://www.theguardian.com/world/interactive/2013/nov/01/prism-slides-nsa-document

2 Marie-Helen Maras, "The social consequences of a mass surveillance measure: What happens when we become the 'others'?", International Journal of Law, Crime and Justice, Volume 40, Issue 2, p65

3 https://www.privacyinternational.org/?q=node/52

4 https://www.privacyinternational.org/?q=node/52

5 Mary DeRosa, "Data Mining and Data Analysis for Counterterrorism", Center for Strategic and International Studies (CSIS), March 2004, p5

6 ISC Privacy and Security Report, March 2015, p28

7 ISC Privacy and Security Report, , March 2015, p28

8 Ben Wizner, SECILE conference, October 2014, watch from 04:51 https://www.youtube.com/watch?v=Up5aXaHqkhE

9 Ben Wizner, SECILE conference, October 2014 https://www.youtube.com/watch?v=Up5aXaHqkhE

10 Although mass surveillance programmes have been referred to by government agencies as "bulk collection" this paper will use the term "mass surveillance", commonly used by most civil society groups and the media.

Main debates

Right to privacy

Much debate to date has focused on the ethics of mass surveillance and the tension between the individual right to privacy and the collective right to security. Reports from United Nations human rights expert Ben Emmerson and the Council of Europe's Parliamentary Committee on Legal Affairs and Human Rights warn mass surveillance violates our right to privacy and thus poses a direct challenge to an established norm of international law. Ben Emmerson in his UN General Assembly report found that "Bulk access technology is indiscriminately corrosive of online privacy and impinges on the very essence of the right guaranteed by article 17".[11] The Council of Europe's report found that mass surveillance practices "endanger fundamental human rights, including the rights to privacy (Article 8 European Convention on Human Rights (ECHR)), freedom of information and expression (Article 10, ECHR), and the rights to a fair trial (Article 6, ECHR) and freedom of religion (Article 9)".[12]

In the UK, two recent major reports disagreed that mass surveillance was a breach of our human rights. The Anderson report ('A Question of Trust') found that "the capability of the security and intelligence agencies to collect and analyse intercepted material in bulk should be maintained"[13] and the Intelligence and Security Committee (ISC) report ('Privacy and Security') concluded that privacy is not an absolute right and that when it comes to terror attacks, security trumps privacy:

> "While we recognise privacy concerns about bulk interception, we do not subscribe to the point of view that it is acceptable to let some terrorist attacks happen in order to uphold the individual right to privacy – nor do we believe that the vast majority of the British public would. In principle it is right that the intelligence Agencies have this capability".[14]

The ISC report also dismissed the view that "bulk collection" constituted mass surveillance, arguing that as it is only a tiny fraction of bulk data acquired that will ever reach a human analyst, most will be filtered down automatically and thus does not amount to mass surveillance. This view has been highly challenged as many human rights campaigners argue intrusion arises at the point of collection of data rather than at the point of interrogation or analysis of that data. Dr Eric Metcalfe from JUSTICE compared mass collection programmes to "putting a CCTV camera into everyone's bedroom in the country but saying we won't turn it on until we have an authorization from a judge". The idea that collection itself is not an interference is "absurd" he argued. He also compared the programmes to collecting DNA of individuals who had not been charged or convicted of any criminal offence, which was found to be a fundamental breach to the right of privacy by the European Court of Human Rights. Similarly, supporters of mass surveillance have argued that the collection of metadata (information about who sent a communication to whom, from where to where and when, as opposed to the content) is less intrusive than content.[15] This again has been widely criticized as metadata has been found to be as – if not more – revealing and intrusive than content.[16]

Other ethical debates have focused on the threat to democracy (if intelligence agencies bypass democratic political and legal channels to implement programmes that intercept a large amount of private communications) and the effect on the freedoms of speech, information and association.[17] For example, a report by PEN International in November 2013 on the effects of mass surveillance, found that writers living in liberal democratic countries have begun to engage in self-censorship at levels approaching those seen in non-democratic countries due to the worry of government surveillance.[18] Self-censorship included avoiding writing or speaking on a particular topic, curtailing or avoiding activities on social media, deliberately steering clear of certain topics in personal phone conversations or email messages and refraining from conducting internet searches or visiting websites on topics that may be considered controversial or suspicious.[19] Another report by Human Rights Watch,

---

11 UN Special Rapporteur Ben Emerson report, "Promotion and protection of human rights and fundamental freedoms while countering terrorism", September 2014, p21

12 Council of Europe Committee on Legal Affairs and Human Rights, "Mass Surveillance" report, January 2015, p1

13 David Anderson QC, "A Question of Trust" report, June 2015, p288

14 ISC Privacy and Security Report, March 2015, p36

15 Senator Diane Feinstein said "This is just metadata. There is no content involved" in Ed O'Keefe, 'Transcript: Dianne Feinstein, Saxby Chambliss explain, defend NSA phone records program', Washington Post, June 6th 2013 http://www.washingtonpost.com/blogs/post-politics/wp/2013/06/06/transcript-dianne-feinstein-saxby-chambliss-explain-defend-nsa-phone-records-program/

16 Jane Mayer, 'What's the matter with metadata?', The New Yorker, June 6th 2013 http://www.newyorker.com/news/news-desk/whats-the-matter-with-metadata. For more information on this see: 'Me and my metadata' by Ethan Zuckerman http://www.ethanzuckerman.com/blog/2013/07/03/me-and-my-metadata-thoughts-on-online-surveillance/, Immersion https://www.aclu.org/blog/graphs-mit-students-show-enormously-intrusive-nature-metadata?redirect=blog/technology-and-liberty-national-security/graphs-mit-students-show-enormously-intrusive-nature and The Guardian guide to your metadata http://www.theguardian.com/technology/interactive/2013/jun/12/what-is-metadata-nsa-surveillance#meta=0000000

17 Council of Europe Committee on Legal Affairs and Human Rights, "Mass Surveillance" report, January 2015, p28-29

18 The report was based on a survey of 772 writers from 50 countries. PEN International, 'Global Chilling: The Impact of Mass Surveillance on International Writers', 5th January 2015 http://www.pen-international.org/wp-content/uploads/2015/01/Global-Chilling_01-05-15_FINAL.pdf

19 PEN International, 'Global Chilling: The Impact of Mass Surveillance on International Writers', 5th January 2015, p10-11 http://www.pen-international.org/wp-content/uploads/2015/01/Global-Chilling_01-05-15_FINAL.pdf

which demonstrates the effects of mass surveillance on the practice of journalism and law, found that as a result of electronic surveillance, journalists and their sources, as well as lawyers and their clients, are changing their behaviour in ways that "undermine basic rights and corrode democratic processes"[20] as a result of mass government surveillance.

Transparency, accountability and oversight

Concerns over transparency, accountability and effective oversight have been a central concern with regards to surveillance. A number of campaign and advocacy groups, including Human Rights Watch, Liberty, Privacy International, JUSTICE, Big Brother Watch and others, have raised concern over the lack of transparency and effective oversight of these programmes. They stress, in particular, the need for checks and balances so that "public trust and confidence can be enhanced" to know that "institutionally oversight is taking place as it should".[21] As well as this, judicial authorization (which will be independent from government) is vital,[22] as well as better resourcing to ensure the correct level of oversight can be maintained.[23] Increased transparency is also essential to ensure the public are informed about what is going on.

In the UK, the Anderson report and the Intelligence and Security Committee (ISC) report, as well as the Independent Surveillance Review report from RUSI ('A Democratic Licence to Operate') all stressed the need for greater transparency and oversight. The ISC report found that "the legal framework has developed piecemeal, and is unnecessarily complicated" resulting in "serious concerns about the resulting lack of transparency, which is not in the public interest". They called for a "new, transparent legal framework" to replace the current one which would be a new Act of Parliament governing the intelligence and security Agencies which will clearly set out the intrusive powers available to them. The report also contains recommendations about each of the Agencies' intrusive capabilities, essential to "improve transparency, strengthen privacy protections and increase oversight".[24]

Similarly, the Anderson report found the current state of affairs to be "undemocratic, unnecessary and – in the long run – intolerable". 'A Question of Trust' recommended that the three current Commissioners offices (described as "oversight theatres") be replaced by an Independent Surveillance and Intelligence Commission (ISIC) which should be "public-facing, transparent, accessible to media and willing to draw on expertise from different disciplines" to ensure accountability. The Anderson report also found that although intelligence operations must remain secret, "public authorities, ISIC and the IPT should all be as open as possible in their work" and that "public authorities should consider how they can better inform Parliament and the public about why they need their powers, how they interpret those powers, the broad way in which those powers are used and why additional capabilities may be required".[25] As well as a new oversight body, the report also recommended that existing laws should be replaced by a single piece of legislation and that the current system of ministerial warrants be replaced by warrants issued by judges.

In a similar vein, The Royal United Services Institute (RUSI) report, commissioned by then Deputy Prime Minister Nick Clegg, found that inadequacies in law and oversight, as well as complexities around the current arrangements which makes them hard for citizens to understand, has caused a 'credibility gap' that had undermined public confidence. The report recommends a new comprehensive and legal framework, including an enhanced role for the judiciary in authorizing warrants, a reorganization and better resourcing of the oversight regime, as well as a set of tests, or 'enduring principles', that any new legislation must pass.[26]

Unintended consequences

Proliferation

A major concern with the development of mass surveillance tools is that they can be used by authoritarian regimes to suppress freedom of information and expression and track down opponents.[27] There is evidence that this is already happening: Privacy International's Surveillance Industry Index (a publicly available database on the private surveillance sector) has found that surveillance companies are selling powerful and invasive surveillance technologies that are keeping pace with the capabilities of the NSA and GCHQ, including the

20 Human Rights Watch, 'With Liberty to Monitor All: How Large-Scale US Surveillance is Harming Journalism, Law, and American Democracy', July 2014. The report interviewed 46 journalists and 42 lawyers in the US http://www.hrw.org/sites/default/files/reports/usnsa0714_ForUPload_0.pdf

21 Isabella Sankey, Liberty, transcript of oral evidence to the Privacy and Security Inquiry, Intelligence and Security Committee, 15th October 2015, p18

22 Big Brother Watch, 'Investigatory Powers Reports Briefing', p22 https://www.bigbrotherwatch.org.uk/wp-content/uploads/2015/06/Investigatory-Powers-Reports-Briefing.pdf and Privacy International https://www.privacyinternational.org/sites/default/files/PI%20submission%20UK.pdf

23 Dr Metcalfe, JUSTICE, transcript of oral evidence to the Privacy and Security Inquiry, Intelligence and Security Committee, 15th October 2015,P p16

24 ISC Privacy and Security Report, March 2015, p2

25 David Anderson QC, 'A Question of Trust' report, June 2015, p7-8, 299, 306

26 Report of the Independent Surveillance Review, RUSI, 'A Democratic Licence to Operate', July 2015

27 Council of Europe Committee on Legal Affairs and Human Rights, "Mass Surveillance" report, January 2015, p2 http://www.scribd.com/doc/253848295/Mass-Surveillance-Report

potential for the mass interception of communications. These products have been sold to Bahrain, Ethiopia and Libya, amongst others, and have been used to target pro-democracy activists, journalists and political opposition in these countries.[28]

An investigation by Privacy International and a report by Human Rights Watch on communications surveillance in Ethiopia raised worrying concerns about the extent of government surveillance and its implications. The Privacy International and netzpolitik.org investigation found that a German surveillance technology company Trovicor was playing a central role in expanding the Ethiopian government's communications surveillance capacities. The company provided equipment to Ethiopia's National Intelligence and Security Service (NISS) in 2011 and offered to massively expand the government's ability to intercept and store internet protocol (IP) traffic across the national telecommunications backbone. Trovicor' s proposal (which subsequently went through) was to double the government's internet surveillance capacity whereby two years' worth of data intercepted from Ethiopian networks would be stored,[29] essentially meaning the "entire communications backbone of the country is being surveilled".[30]

A report by Human Rights Watch raised concern about the impact of Ethiopia's government surveillance. The report found surveillance is being used as a tool to silence dissenting voices, with authorities frequently targeting the ethnic Oromo population, with intercepted phone records regularly used to arrest and detain Oromos. Although phone records are rarely used in trials, arbitrary detention without formal charges is common in Ethiopia and they are used frequently by officials during interrogations to try and extract a confession.[31] This is made worse by the widespread use of torture and other ill-treatment against political detainees in Ethiopian detention centres. As well as this, the government routinely blocks websites and jams radio and television stations and bloggers and Facebook users face harassment and the threat of arrest should they refuse to tone down their online writings.[32]

The government's monopoly over all mobile and Internet services through Ethio Telecom, its sole, state-owned telecom operator, is a further concern as it facilitates the abuse of surveillance powers. Ethiopian security officials have virtually unlimited access to the call records of all telephone users in Ethiopia and they regularly and easily record phone calls without any legal process or oversight. A further implication of government surveillance is self-censorship as the perception amongst many, especially rural Ethiopians is that government surveillance is omnipresent, causing many to refrain from openly communicating on a variety of topics across telecom networks, violating the rights to freedom of expression, association, and access to information.[33]

In Pakistan, worrying developments concerning mass surveillance have also been found. A report by Privacy International in July this year found that mass network surveillance has been in place in Pakistan since at least 2005 and that the Pakistani government obtained this technology from both domestic and foreign surveillance companies.[34] The report also revealed that in June 2013, Pakistan's intelligence agency the Inter-Services Intelligence (ISI), sought to develop a mass surveillance system by directly tapping the main fibre optic cables entering Pakistan that carried most of the nation's network communication data. This, Privacy International warns, would "make available virtually all of the nation's domestic and international communications data for scrutiny" which would be "the most significant expansion of the government's capacity to conduct mass surveillance to date".[35]

When considering the implications of mass surveillance programmes in the UK, consideration of the protocol the UK has set and the consequences of this, is essential. Privacy International's Surveillance Industry Index has found that private surveillance companies play a major role in the trade of surveillance technology, exporting to willing buyers in the form of other national governments.[36] The lack of regulation that exists in the industry means the risk of authoritarian regimes or non-state actors accessing mass communications surveillance technology is already happening and the UK's own use of these tools puts them in a weak position to curtail their spread.

Connected to this is the "technology arms race" states are currently engaged in whereby the growth of encryption and the diversification of the communications market means that states are constantly competing to

---

28 Mathew Rice, ' The Surveillance Industry', Privacy International, 18th November 2013 https://www.privacyinternational.org/?q=node/403

29 Claire Lauterbach, 'Ethiopia Expands Surveillance Capacity With German Tech Via Lebanon', Privacy International, 23rd March 2015 https://www.privacyinternational.org/?q=node/546

30 Email exchange with Claire Lauterbach, Privacy International, 27th May 2015

31 Human Rights Watch, "They Know Everything We Do: Telecom and Internet Surveillance in Ethiopia", March 2014, p40-45 http://www.hrw.org/sites/default/files/reports/ethiopia0314_ForUpload_1.pdf

32 Human Rights Watch, "They Know Everything We Do: Telecom and Internet Surveillance in Ethiopia", March 2014, p2 p40-45 http://www.hrw.org/sites/default/files/reports/ethiopia0314_ForUpload_1.pdf

33 Human Rights Watch, "They Know Everything We Do: Telecom and Internet Surveillance in Ethiopia", March 2014 http://www.hrw.org/sites/default/files/reports/ethiopia0314_ForUpload_1.pdf

34 Mathew Rice, "Tipping The Scales: Security And Surveillance In Pakistan", Privacy International, July 2015, p1

35 Mathew Rice, "Tipping The Scales: Security And Surveillance In Pakistan", Privacy International, July 2015, p15

36 Mathew Rice, ' The Surveillance Industry', Privacy International, 18th November 2013 https://www.privacyinternational.org/?q=node/403

have a technological edge over their targets.[37] Similar to the 'Cool War' dynamic currently taking place with regards to cyber warfare, this continuous attrition and escalation could have potentially destabilizing effects.[38]

Public trust

The public's trust in their own country's government risks being seriously eroded due to mass surveillance programmes. A report from The President's Review Group on Intelligence and Communications Technologies, a panel appointed by President Obama to review the government's surveillance activities, as well as a report from the Council of Europe parliamentary committee, both found that public trust in government has eroded as a result of the mass surveillance revelations.[39]

Research suggests that the use of mass surveillance essentially means everyone is considered a 'risk' from the state, thus sending a message to citizens that they can't be trusted. As trust is reciprocal, citizen's trust in their government will rely on the extent to which they believe their government trusts them. Mass surveillance not only fosters suspicion as to why information was retained in the first place but also in terms of how this information will inevitably be used and will thus result in a loss of citizens' trust in governments.[40]

A number of surveys that came out following the Snowden leaks - when citizens first became aware of the mass interception of their communications by governments - seem to support this. The first, a YouGov survey conducted by Amnesty International of 15,000 people across 13 countries in 2015 was designed to gauge the public's view of mass surveillance and concluded that it was deeply unpopular. The poll found that across all 13 countries, there was no majority support for surveillance – only 26% of people, overall, agreed that the government should monitor the communications and Internet activity of its own citizens and nearly two thirds said they wanted tech companies – like Google, Microsoft and Yahoo – to secure their communications to prevent government access.[41]

Another major survey, the CIGI-Ipsos Global Survey on Internet Security and Trust, undertaken by the Centre for International Governance Innovation (CIGI) and conducted by global research company Ipsos, surveyed 23,376 Internet users in 24 countries in 2014 to look specifically at the issue of trust around internet security. The survey found that just under half (47%) would trust their own government to run the internet when given a choice of various governance sources, the majority (57%) choosing the multi-stakeholder option —a "combined body of technology companies, engineers, non-governmental organizations and institutions that represent the interests and will of ordinary citizens, and governments." Furthermore, 61% of those surveyed were concerned with the police or other government agencies from their own country secretly monitoring their online activities.

The survey also revealed the extent to which the public are changing their online behaviour. Of the 60% of those surveyed that had heard of Edward Snowden, 39% have taken steps to protect their online privacy and security as a result of his revelations, a quarter of all those surveyed.[42] Two US surveys conducted in 2014 and 2015 by the Pew Research Center also found that the Snowden leaks had an impact on the public's relationship with their government in relation to online privacy. The first survey, conducted in 2014, found that most adults did not agree that it was a good thing for government to "keep an eye" on internet activity. It also found that overall, 80% of American adults agreed or strongly agreed that Americans should be concerned about the government's monitoring of phone calls and internet communications. In 2015, the study found that over a third of those who had heard of surveillance programmes had taken at least one step to hide or shield their information from the US government (however, in contrast to the earlier study it found that only 52% of those polled were "somewhat" or "very" concerned about US government surveillance of data communications).[43]

This is supported by a steep increase in the use of Tor (an open source network that allows users to obscure their online activity) which went from 500,000 daily users worldwide to more than 4 million following the Snowden leaks.[44] Other internet privacy platforms have also seen an increase in use since the Snowden leaks. The search engine, DuckDuckGo for example, which doesn't track or store data about its users, received 50% more traffic within days of the leaks.[45]

In the UK, although the Anderson report found that a

37 David Anderson QC, "A Question of Trust" report, June 2015, p195

38 Alberto Muti and Katherine Tajer with Larry MacFaul, VERTIC, "Cyberspace: An Assessment of Current Threats, Real Consequences and Potential Solutions", Remote Control Project, October 2014, p12

39 The President's Review Group on Intelligence and Communications Technologies, "Liberty and Security in a Changing World", December 2013, p117 and Council of Europe Committee on Legal Affairs and Human Rights, "Mass Surveillance" report, January 2015, p31

40 Marie-Helen Maras, "The social consequences of a mass surveillance measure: What happens when we become the 'others'?", International Journal of Law, Crime and Justice, Volume 40, Issue 2, p69-72

41 Amnesty International, https://www.amnesty.org/en/articles/news/2015/03/global-opposition-to-usa-big-brother-mass-surveillance/

42 CIGI-IPSOS Global Survey On Internet Security And Trust, https://www.cigionline.org/sites/default/files/survey/slides.pdf

43 Pew Research Center, "Public Perceptions of Privacy and Security in the Post-Snowden Era", (2014) and Pew Research Center, "Americans' privacy strategies post-Snowden" (2015)

44 http://www.theguardian.com/technology/2013/nov/05/tor-beginners-guide-nsa-browser

45 http://www.theguardian.com/world/2013/jul/10/nsa-duckduckgo-gabriel-weinberg-prism

change in attitude amongst citizens in the UK is less apparent than in other countries, the Snowden leaks have damaged people's belief in the safety of their data, with most believing that neither government nor private companies can now keep their data completely secure.[46] Although public opinion surveys should be treated with caution, there seems to be strong indication that the Snowden revelations have had a detrimental impact on citizen's trust in their government with regards to their online privacy.

Other issues

Other consequences of mass surveillance programmes have also been found. These include the weakening of internet security as mass surveillance relies on creating and maintaining vulnerabilities in communications networks which undermine the communications infrastructures that we rely on. The creation of "back doors" and other weaknesses in security standards and implementation could easily be exploited by non-state groups.[47] In May this year, a group of tech companies, including Facebook, Google and Yahoo (as well as civil society groups and academics) signed a letter to President Obama urging him to oppose efforts that would force companies to build in ways for law enforcement to access products and services protected by encryption. The letter warned that "introducing intentional vulnerabilities into secure products for the government's use will make those products less secure against other attackers". The potential attackers they listed included street and computer criminals, repressive governments and foreign intelligence agencies.[48] Prior to this, Facebook CEO and founder Mark Zuckerberg publically called the US government a "threat" to the internet as it was making it less secure.[49]

The damaging of state to state relations has also been found to be another consequence of mass surveillance, the Council of Europe report found that Brazil-US relations and US-German relations had been damaged by the Snowden leaks.[50] There is also a risk of 'mission creep' whereby there is a temptation to expand the use of new tools once they have been implanted for one purpose. With mass surveillance there is the risk that if this new, intrusive technology is deemed acceptable for counter terrorism, its use will gradually be expanded and used in other areas of law enforcement.[51]

46 David Anderson QC, "A Question of Trust" report, June 2015, p36
47 Council of Europe Committee on Legal Affairs and Human Rights, "Mass Surveillance" report, January 2015, p20 Council of Europe Committee on Legal Affairs and Human Rights, "Mass Surveillance" report, January 2015, p20
48 Letter from tech companies, civil society groups and academics to President Obama, 19th May 2015 https://static.newamerica.org/attachments/3138--113/Encryption_Letter_to_Obama_final_051915.pdf
49 Mark Zuckerberg Facebook post, 13th March 2014 https://www.facebook.com/zuck/posts/10101301165605491
50 Council of Europe Committee on Legal Affairs and Human Rights, "Mass Surveillance" report, January 2015, p30
51 Mary DeRosa, "Data Mining and Data Analysis for Counterterrorism", Center for Strategic and International Studies (CSIS), March 2004, p16 and The President's Review Group on Intelligence and Communications Technologies, "Liberty and Security in a Changing World", December 2013, p114

Effectiveness

False positives, data overload and a waste of resources

There are two main types of data mining techniques used for counterterrorism: the first, "subject-based" or "link analysis" data-mining uses aggregated public records or other large collections of data to find links between a subject and other people, places or things.[52] For example, subject-based data mining can include people who own cars with licence plates that are discovered at the scene of a terrorist act or whose fingerprints match those of people known to be involved in terrorist activities.[53] The second is "pattern-based" data mining techniques that attempt to find patterns that can predict terrorist planning or attacks.[54] For example, a pattern of a "sleeper" terrorist might be a person in the country on a student visa who purchases a bomb-making book and 50 medium sized loads of fertilizer. Or, if the concern is that terrorists will use large trucks for attacks, automated data analysis might be conducted regularly to identify people who have rented large trucks, used hotels or drop boxes as addresses, and fall within certain age ranges or have other features that are part of a known terrorist pattern.[55] Pattern-based techniques will require either a feedback mechanism to generate learning over time or are more assumption dependent than subject-based techniques.[56] In practice many of the approaches used will be a combination of these two types.

The use of data-mining and automated data-analysis techniques used to filter down the vast amounts of data acquired in mass surveillance programmes comes with a high risk of false positives. 'False positives' are bad data or imperfect search models that incorrectly identify people as matches or links, for example someone being placed in a "worthy of further investigation" category who has no terrorist connection. In contrast, a 'false

52 Mary DeRosa, "Data Mining and Data Analysis for Counterterrorism", Center for Strategic and International Studies (CSIS), March 2004, p6
53 Committee on Technical and Privacy Dimensions of Information for Terrorism Prevention and Other National Goals, National Research Council, "Protecting Individual Privacy in the Struggle Against Terrorists: A framework for program assessment", p21
54 Mary DeRosa, "Data Mining and Data Analysis for Counterterrorism", Center for Strategic and International Studies (CSIS), March 2004, p8
55 Mary DeRosa, "Data Mining and Data Analysis for Counterterrorism", Center for Strategic and International Studies (CSIS), March 2004, p8
56 Committee on Technical and Privacy Dimensions of Information for Terrorism Prevention and Other National Goals, National Research Council, "Protecting Individual Privacy in the Struggle Against Terrorists: A framework for program assessment", p22

negative' would be when someone is not identified as a match, when in fact he/she is.

False positive can arise in two main ways. The first source of false positives is in the validity of the model used to distinguish between a terrorist and other innocent people (i.e. being able to separate the "noise" of innocent behaviour from the "signal" of terrorist activities). A perfect model would be one in which a set of measurable characteristics would correctly identify an individual with 100 percent accuracy and others would be identified as innocent. In the real world no model is perfect and so false positives and false negatives are inevitable. The second source of false positives is imperfect data. Data quality can be hampered by a range of reasons from keyboarding errors and faulty intelligence to incorrect or obsolete information from bad data sets.

It has been suggested that data mining for terrorism comes with a higher risk of false positives than when used in other settings (such as credit card fraud detection) due to the quality of data available[57] and the rarity of terror attacks (data mining is most useful when there are broad patterns and regular and frequent occurrences, as opposed to terror attacks which are unpredictable and erratic).[58] As well as this, the high cost of false alarms in the context of terrorism could render data mining an unsuitable tool as a false positive could result in the detention or arrest of an innocent person and long-term damage to his or her reputation and a false negative could result in a terrorist attack taking place, resulting in a loss of life.[59]

A recent report from the Committee on Technical and Privacy Dimension of Information for Terrorism Prevention and Other National Goals at the National Research Council found that communications surveillance that use data collection and analysis techniques cannot easily be applied to detecting and pre-empting a terrorist attack and that success in using these tools "may not be possible at all". "Automated identification of terrorists through data mining (or any other known methodology)" they argue, "is neither feasible as an objective nor desirable as a goal of technology development efforts". The report advises policy makers and government officials responsible for developing, purchasing, deploying, and using information-based programmes to "systematically evaluate the effectiveness of those programs and assess whether they are warranted in light of their likely effectiveness".[60]

Another concern with data mining is that the false positives and 'noise' it generates will cause a sea of data that will swamp analysts, taking investigative and analytical resources and attention away from more appropriate counter-terrorism methods.[61] NSA whistle blower William Binney, Security technologist Bruce Schneier and mathematics, computing and technology lecturer Ray Corrigan all agree that mass surveillance is making analysts less effective[62] as "each alert requires a lengthy investigation to determine whether it's real or not" which "takes time and money, and prevents intelligence officers from doing other productive work".[63] "What they are doing is making themselves dysfunctional by taking all this data"[64] Binney argues. The Council of Europe Parliamentary Committee suggests that focusing more resources on targeted surveillance instead would likely prove more effective.[65]

---

57 Data tracks of terrorists in commercial and government administrative databases are co-mingled with enormously larger volumes of similar data associated with innocent individuals and links found among records in databases of varying accuracy will tend to reflect the most inaccurate of the databases involved, Committee on Technical and Privacy Dimensions of Information for Terrorism Prevention and Other National Goals, National Research Council, "Protecting Individual Privacy in the Struggle Against Terrorists: A framework for program assessment", p78. Also see Bruce Schneier, "Why Mass Surveillance Can't, Won't, And Never Has Stopped A Terrorist", digg, March 2015 http://digg.com/2015/why-mass-surveillance-cant-wont-and-never-has-stopped-a-terrorist who argues in commercial settings, applications will generally have access to substantial amounts of relatively complete and structured data. In contrast, data associated with terrorists are sparse and mostly collected in unstructured form (free text, video, audio recordings).

58 Bruce Schneier, "Why Mass Surveillance Can't, Won't, And Never Has Stopped A Terrorist", digg, March 2015 http://digg.com/2015/why-mass-surveillance-cant-wont-and-never-has-stopped-a-terrorist and see Zeynep Tufekci, 'Terror and the limits of mass surveillance', Financial Times, 3rd February 2015

59 Mary DeRosa, "Data Mining and Data Analysis for Counterterrorism", Center for Strategic and International Studies (CSIS), March 2004

60 Committee on Technical and Privacy Dimensions of Information for Terrorism Prevention and Other National Goals, National Research Council, "Protecting Individual Privacy in the Struggle Against Terrorists: A framework for program assessment", p48

61 Committee on Technical and Privacy Dimensions of Information for Terrorism Prevention and Other National Goals, National Research Council, "Protecting Individual Privacy in the Struggle Against Terrorists: A framework for program assessment", p40 and Zeynep Tufekci, 'Terror and the limits of mass surveillance', Financial Times, 3rd February 2015

62 Ray Corrigan, "Mass surveillance not effective for finding terrorists", New Scientist, January 2015 http://www.newscientist.com/article/dn26801-mass-surveillance-not-effective-for-finding-terrorists.html#.VZ5JevlVikp, Bruce Schneier, "Why Mass Surveillance Can't, Won't, And Never Has Stopped A Terrorist", digg, March 2015 http://digg.com/2015/why-mass-surveillance-cant-wont-and-never-has-stopped-a-terrorist, William Binney in "NSA Struggles to Make Sense of Flood of Surveillance Data", Wall Street Journal, December 2015

63 Bruce Schneier, "Why Mass Surveillance Can't, Won't, And Never Has Stopped A Terrorist", digg, March 2015 http://digg.com/2015/why-mass-surveillance-cant-wont-and-never-has-stopped-a-terrorist

64 William Binney in "NSA Struggles to Make Sense of Flood of Surveillance Data", Wall Street Journal, December 2015 http://www.wsj.com/articles/SB10001424052702304202204579252022823658850

65 Council of Europe Committee on Legal Affairs and Human Rights, "Mass Surveillance" report, January 2015, p2 http://website-pace.net/documents/19838/1085720/20150126-

Ability to foil terror plots

Supporters of mass surveillance argue that you cannot find the 'needle' unless you have a 'haystack' and thus mass surveillance programmes are essential tools in order to protect national security:

> "In order to identify, understand and counter national security threats facing the UK, our Agencies need information… They must also be able to generate and quickly assess new leads that could reveal emerging threats or identify previously unknown subjects of concern… This may require the Agencies to sift through 'haystack' sources – without looking at the vast majority of material that has been collected – in order to identify and combine the 'needles' which allow them to build an intelligence picture".[66]

However, three reports have come out of the US in recent years casting doubt on the effectiveness of mass surveillance programmes to thwart terror plots. The first, is a declassified 2009 report from the US government, made available in April 2015 following a Freedom of Information Act lawsuit by The New York Times. The report was a joint project in 2009 by Inspector Generals for five intelligence and law enforcement agencies (the Department of Defence, the Department of Justice, the CIA, the NSA, and the Office of National Intelligence) about the Stellar Wind programme (codename for the N.S.A. warrantless wiretapping and bulk phone and e-mail records collection surveillance programme) approved by President George W. Bush shortly after the September 11 2001 terrorist attacks. The report is an amalgamation of over 200 interviews, conducted by the participating Inspector Generals, including interviews with former NSA, CIA and FBI employees. Thousands of electronic and hardcopy documents were also examined, including the Presidential Authorizations, terrorist threat assessments, legal memorandums, applicable regulations and policies, briefings, reports, correspondence and notes.[67]

The report sheds doubt on the value of the mass surveillance programme, Stellar Wind, to FBI counter-terrorism efforts. To quantify its value for counter-terrorism operations the report conducted two statistical studies. The first, conducted in early 2006 sampled unique telephone numbers and email addresses the NSA provided the FBI from the inception of the Stellar Wind programme in 2001 to 2005. The study sought to determine what percentage of the tippers (alert messages and other early-stage reports used to highlight anticipated events to relevant officials) resulted in "significant contribution(s) to the identification of terrorist subjects or activity on US soil". For the purpose of the study, a tipper was considered "significant if it led to any of three investigative results: the identification of a terrorist, the deportation from the United States of a suspected terrorist, or the development of an asset that can report about the activities of terrorists".

Although the report included several redacted paragraphs describing "success cases", the study found that just 1.2% of tippers had made a "significant" contribution to identifying a terrorist, deporting a terrorism suspect or development of confidential information about terrorists. A second study was conducted in 2006 which reviewed tippers from August 2004 to January 2006, applying the same methodology for assessing "significance" that was used in the first study. The second study found that none have proved useful.[68]

The report also attempted to assess Stellar Winds value by conducting interviews with various FBI officials and employees. Here a difference of opinion was found about the utility of the mass surveillance programme. Members of Team 10, for example, were strong advocates of the programme, stating that they believed it "contributed significantly to FBI international terrorism investigations". Interviews with the supervisory special agents who managed counter terrorism programmes at two FBI field offices, found very different views saying the programme was "not an effective way to identify threats". Tippers, they said, were especially frustrating compared to other counter terrorism leads as they did not provide sufficient information to prioritize the leads. One supervisory special agent said he felt the project "perverted the logical priority of tasking". The report found that none of the agents interviewed could identify an investigation in their office in which tippers played a significant role, nor could they recall how such a tipper contributed to any of their international terrorism cases.[69]

The second report on the effectiveness of mass surveillance programmes is from Washington based think tank New America Foundation. The report, 'Do NSA's Bulk Surveillance Programs Stop Terrorists?' again attempts a quantitative analysis to assess the

MassSurveillance-EN.pdf

66 Co-ordinated by Cabinet Office on behalf of HMG (agreed by the Security and Intelligence Agencies and the National Crime Agency, and relevant Ministers), written evidence to Intelligence and Security Committee HMG, February 2014, p4 https://b1cba9b3-a-5e6631fd-s-sites.googlegroups.com/a/independent.gov.uk/isc/public-evidence/12march2015/20150312-P%2BS-027-HMG.pdf?attachauth=ANoY7crmamQUHO3REsbKUY5hbqOe8azEu-Ru7J54qRcncntdYlX5832jLposh8azn2zFE_4CCUrEt8gnl3QFwskixwe40C6gEgj5SEJ0_tk7uJTadRTiyHlkzk4ndbpMwt7EPjLEl5iHW81-aOyz6qohAJdj0yj8DnkOE8S4WcgMywj_GnRoGUQ0UBhZVnlHtVDSeovGkLoT5a10vEePo5eWAqmG8SKCGJiLGlfhq1TA5vspicElTFGv7rPYQfXGK94Zu5BaT7arDc0ARmZ-O5Y5m_MQ-oZWcg%3D%3D&attredirects=0

67 Inspectors General report on the president's surveillance program, July 2009, P12-14 https://s3.amazonaws.com/s3.documentcloud.org/documents/2065871/savage-foia-stellarwind-ig-report.pdf

68 Inspectors General report on the president's surveillance program, July 2009, p303-305 https://s3.amazonaws.com/s3.documentcloud.org/documents/2065871/savage-foia-stellarwind-ig-report.pdf

69 Inspectors General report on the president's surveillance program, July 2009, p438-445 https://s3.amazonaws.com/s3.documentcloud.org/documents/2065871/savage-foia-stellarwind-ig-report.pdf

effectiveness of NSA mass surveillance, this time by compiling a database of all individuals in the US (as well as U.S. persons abroad) recruited by al-Qaeda or like-minded groups or inspired by al-Qaeda's ideology, and charged in the US with an act of terrorism since 9/11, in order to ascertain the initial impetus for investigation.[70]

An analysis of all these cases was conducted by reviewing court documents, wire service reports and news stories as sources to determine how the investigations into these extremists began in order to assess the relative importance of the NSA's mass surveillance programmes in this. The report found that NSA mass collection played an identifiable role in, at most, 1.8% of terrorism cases examined. Traditional investigative methods initiated the majority (60%) of terrorism cases. This includes community or family tips which made up 17.8% of total cases, as well as informants (16%), routine law enforcement (12%), militant self-disclosed by publicizing extremist activity (4%) and suspicious activity reports (8.4%). In 28% of cases the impetus for investigation is unknown as court record and public reporting do not identify which methods initiated the investigation.

The report also went into detail in a few key cases where the government had exaggerated the role of mass surveillance in thwarting these plots. David Coleman Headley's plot to attack the Danish newspaper Jyllands-Posten in 2009 was one such example. Here, the US government claimed NSA mass surveillance identified Headley as a threat and prevented the attack. A report by ProPublica, however, found that Headley had been identified before NSA played a role in the investigation and that their contributions were "more modest" than those offered by the intelligence community. A White House appointed panel that reviewed the surveillance programme's role in counterterrorism investigations, concluded the government's claim was wrong. Chair of the Privacy and Civil Liberties Oversight Board, David Medine told ProPublica, "We're aware of no indication that bulk collection of telephone records through section 215 made any signification contribution to the David Coleman Headley investigation".[71]

Finally, a report from The President's Review Group on Intelligence and Communications Technologies, a panel appointed by President Obama to review the government's surveillance activities, also questioned the effectiveness of mass collection techniques. Their report 'Liberty and Security in a Changing World', published in December 2013 found on the question of mass collection that:

> "Our review suggests that information contributed to terrorist investigations by the use of section 215 telephony meta-data was not essential to preventing attacks and could readily have been obtained in a timely manner using conventional section 215 orders".[72]

In the UK, two major reports on surveillance (the ISC and Anderson reports) defended the effectiveness of mass collection programmes. The Intelligence and Security Committee report provided three redacted case studies from GCHQ (available in the classified version)[73] and in the Anderson report, six (non redacted) case studies were provided to demonstrate the programme's effectiveness.[74] To date, no quantitative study has been attempted to gauge the effectiveness of mass surveillance in the UK for counter-terrorism. The higher number of terror cases and the closed nature of UK trials would make this task significantly harder than in the US.[75]

Contractors

The Snowden leaks also shone a light on the use of contractors by the intelligence community, as Edward Snowden was himself a former Booz Allen Hamilton employee. In 2013, the Washington Post (using figures from a report on security clearance determinations by the Office of the Director of National Intelligence from June 2013) found that approximately 1 in 4 intelligence workers was a contractor and that 70% or more of the intelligence community's secret budget had gone to private firms (over 1, 900 of them) performing everything from "information technology installation and maintenance" to "intelligence analysis and agent protection".[76] The Post's investigation also found that in 2012 roughly 500,000 private contractors had security clearance to handle "top-secret material" (the most sensitive intelligence, material that if made publicly available would cause "exceptionally grave danger" to national security).[77]

---

70 Peter Bergen, David Sterman, Emily Schneider and Bailey Cahall, "Do NSA's Bulk Surveillance Programs Stop Terrorists?", New America Foundation, January 2014, https://static.newamerica.org/attachments/1311-do-nsas-bulk-surveillance-programs-stop-terrorists/IS_NSA_surveillance.pdf

71 Sebastian Rotella, The Hidden Intelligence Breakdowns Behind the Mumbai Attacks, ProPublica, April 2015 http://www.propublica.org/article/the-hidden-intelligence-breakdowns-behind-the-mumbai-attacks

72 The President's Review Group on Intelligence and Communications Technologies, "Liberty and Security in a Changing World", December 2013, p104 https://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf

73 ISC Privacy and Security Report, March 2015, p32-33

74 David Anderson QC, "A Question of Trust" report, June 2015, p337

75 Email correspondence with Peter Bergen and David Sterman, New America Foundation, February 2015

76 Robert O'Harrow Jr., Dana Priest and Marjorie Censer, "NSA leaks put focus on intelligence apparatus's reliance on outside contractors", Washington Post, June 2013 http://www.washingtonpost.com/business/nsa-leaks-put-focus-on-intelligence-apparatuss-reliance-on-outside-contractors/2013/06/10/e940c4ba-d20e-11e2-9f1a-1a7cdee20287_story.html?hpid=z1

77 The report made clear that clearance doesn't mean all these workers get to see every classified document out

This increase in contractors reflects a wider shift towards outsourcing in the US government over the past 15 years due to cutbacks in government agencies and a commitment by the Bush administration to smaller government. The large scale use of contractors by intelligence agencies raises concerns over effective regulation as the procedure to vet intelligence workers has been called into question. A review by the Government Accountability Office in 2009 found that of 3,500 security clearance reviews, almost nine in ten lacked documentation and of those, nearly a quarter were still approved. "DOD adjudicators granted clearance eligibility without requesting missing investigative information or fully documenting unresolved issues in 22 percent of DOD's adjudicative files," the auditors said. Glenn Voelz, an Army intelligence officer previously assigned to the Joint Chiefs of Staff at the Pentagon, warned in a 2009 essay that "the rapid and largely unplanned integration of many nongovernmental employees into the workforce presents new liabilities that have been largely ignored to this point".[78]

The use of contractors in highly sensitive government operations raises a number of concerns, from the lack of effective regulation and oversight mechanisms, to moral concerns regarding the ethics of intelligence agencies (that hold highly sensitive personal information) employing contractors motivated by financial gain. In the UK, information on the use of contractors by GCHQ for sensitive operations is harder to come by as GCHQ are classified as a section 23 body and subsequently not subject to the Freedom of Information Act.

Conclusion: Mass surveillance as a method of security by 'remote control'

The use of mass surveillance techniques for counter-terrorism is a product of technological advancement, but is also an example of the move towards security by 'remote control' - the global trend towards countering threats at a distance without the need to deploy large military force. It is pervasive yet largely unseen, minimising its engagement and risk while extending its reach beyond conflict zones. Drones, special forces, private military and security companies (PMSCs) and cyber activities, as well as intelligence and surveillance methods, are all part of this emerging strategy.[79]

Intelligence has always been an essential component in war, however, modern warfare is increasingly looking to infer knowledge from "phenomena", such as social media feeds, open source text and surveillance drones, rather than traditional intelligence gathering techniques (e.g. human intelligence gathering, interrogation etc.).[80] As technological advances have increased governments' digital intelligence gathering capabilities, mass surveillance techniques demonstrate the interdependence between intelligence and surveillance and the increasing interconnectedness between intelligence, technology and modern combat.

Like other remote control methods, mass surveillance of citizens' communications data is appealing as it is perceived as cost-free and plays to Western states' technological strengths. The perceived ease of remote control has, however, blinded policy makers from considering the broader and long term implications it is having. Like the use of drones, special forces and private military companies, the secretive nature of mass surveillance programmes means they operate in an accountability vacuum, with little transparency or oversight, rendering the public unable not only to hold government to account, but to assess these techniques' perceived effectiveness.

Furthermore, like other forms of remote control, mass surveillance comes with a host of unforeseen consequences and there is doubt over its ability to achieve long-term peace and security. As this paper has shown, proliferation of mass surveillance technologies by an increasing number of states, as well as a decrease in the public's trust in its own government and a weakening of trust between states, are all worrying implications of mass surveillance. As well as this, the effectiveness of these programmes at countering terrorism has been thrown into question with little evidence of their ability to thwart terror plots, as well problems associated with the suitability of these techniques for counter-terrorism (such as data overload and false positives) that could lead to resources being taken away from more effective counter-terrorism techniques. Moreover, the use of contractors in these highly sensitive operations raises concerns around effective regulation and oversight mechanisms.

Remote warfare exists in the absence of a coherent strategy, dictated by technology and what can be done, as opposed to what should be done. In the UK, a recent Remote Control project report from Dr Jon Moran found that confused thinking over security - caused by a global ambition for UK security, on the one hand,

there and various analysts have pointed out that Snowden was likely to have needed even higher clearance than "top secret" to gain access to PRISM and other surveillance programs. Washington Post, June 2013 http://www.washingtonpost.com/blogs/wonkblog/wp/2013/06/11/about-500000-private-contractors-have-access-to-top-secret-information/

78 Robert O'Harrow Jr., Dana Priest and Marjorie Censer, "NSA leaks put focus on intelligence apparatus's reliance on outside contractors", Washington Post, June 2013 http://www.washingtonpost.com/business/nsa-leaks-put-focus-on-intelligence-apparatuss-reliance-on-outside-contractors/2013/06/10/e940c4ba-d20e-11e2-9f1a-1a7cdee20287_story.html?hpid=z1

79 http://remotecontrolproject.org/a-new-way-of-war/

80 Crofton Black, "US Special Operations Command Contracting: Data-Mining the Public Record", Remote Control Project, September 2014, p41 http://remotecontrolproject.org/wp-content/uploads/2014/09/CroftonBlack_USSOCOM-Contracting-Report_NE.pdf

combined with a shrinking military capacity and a series of recently unsuccessful military deployments, on the other - has led to remote warfare becoming a 'stop gap' in the absence of any long-term strategy, at risk of becoming a 'strategy of tactics' that will become an end in itself.[81] Remote warfare does not have the ability to solve conflict on its own as it does little to address the long term embedded issues which are connected to new conflicts.[82] Instead, an effective strategy will be one that takes a long term view of security. For counter-terrorism this will focus on targeting the underlying conditions and root causes of radicalisation in order to foster long-term security.

We recommend:

- Research and analysis to evaluate the strategic effects of mass surveillance. In particular, research that will produce quantitative evidence on the effectiveness of mass surveillance to thwart terror plots in the UK, as well as an analysis of the cost effectiveness of mass surveillance programmes in comparison to other forms of surveillance (e.g. targeted).

- Research and analysis to evaluate the consequences of mass surveillance, in particular in-depth investigation into the impact of mass surveillance programmes on communities who feel particularly targeted by counter terrorism measures.

- Establishment of a robust regulatory framework for private security companies who are trading surveillance technologies.

- Publicly available information on the use of private contractors at GCHQ, including the numbers working on 'bulk interception' programmes and their level of security clearance, as well as information on the current regulatory procedures in place to vet intelligence workers.

- Development of a long-term security strategy that doesn't look to remote control as an end in itself but instead focuses on addressing the root causes of conflict.

81 Dr Jon Moran, "Remote Warfare (RW): Developing a framework for evaluating its use", Remote Control Project, March 2015, p10-12

82 B. Zala and P. Rogers, The 'Other' Global Security Challenges: Socioeconomic and Environmental Realities after the War on Terror RUSI Journal, Aug 2011, Vol. 156, No. 4; Paul Rogers A century on the edge: from Cold War to hot world, 1945–2045 International Affairs 90: 1 (2014) p.109

The Remote Control project is a project of the Network for Social Change hosted by the Oxford Research Group. Remote Control examines changes in military engagement, in particular the use of drones, special forces, private military companies and cyber and intelligence activities. The project acts as a facilitator for the exchange of information and commissions and publicises work undertaken in the area, aiming to examine the long-term effects of remote warfare.

Esther Kersley is the Research and Communications Officer for the Remote Control project. She joined the Remote Control project in 2013. Prior to joining Remote Control, Esther worked in Berlin for the anti-corruption NGO Transparency International as an editorial and online communications officer. She has also worked with the Quilliam Foundation and IPCRI (Israel/Palestine Center for Research and Information), a Jerusalem based think tank. Esther holds an MSc in Comparative Politics, Conflict Studies from the London School of Economics.

Remote Control Project
Oxford Research Group
Development House
56-64 Leonard Street
London EC2A 4LT
United Kingdom

+44 (0)207 549 0298

media@remotecontrolproject.org
http://remotecontrolproject.org

Published by the Remote Control project, August 2015

Image: Creative Commons, flickr: Shawn Harquail