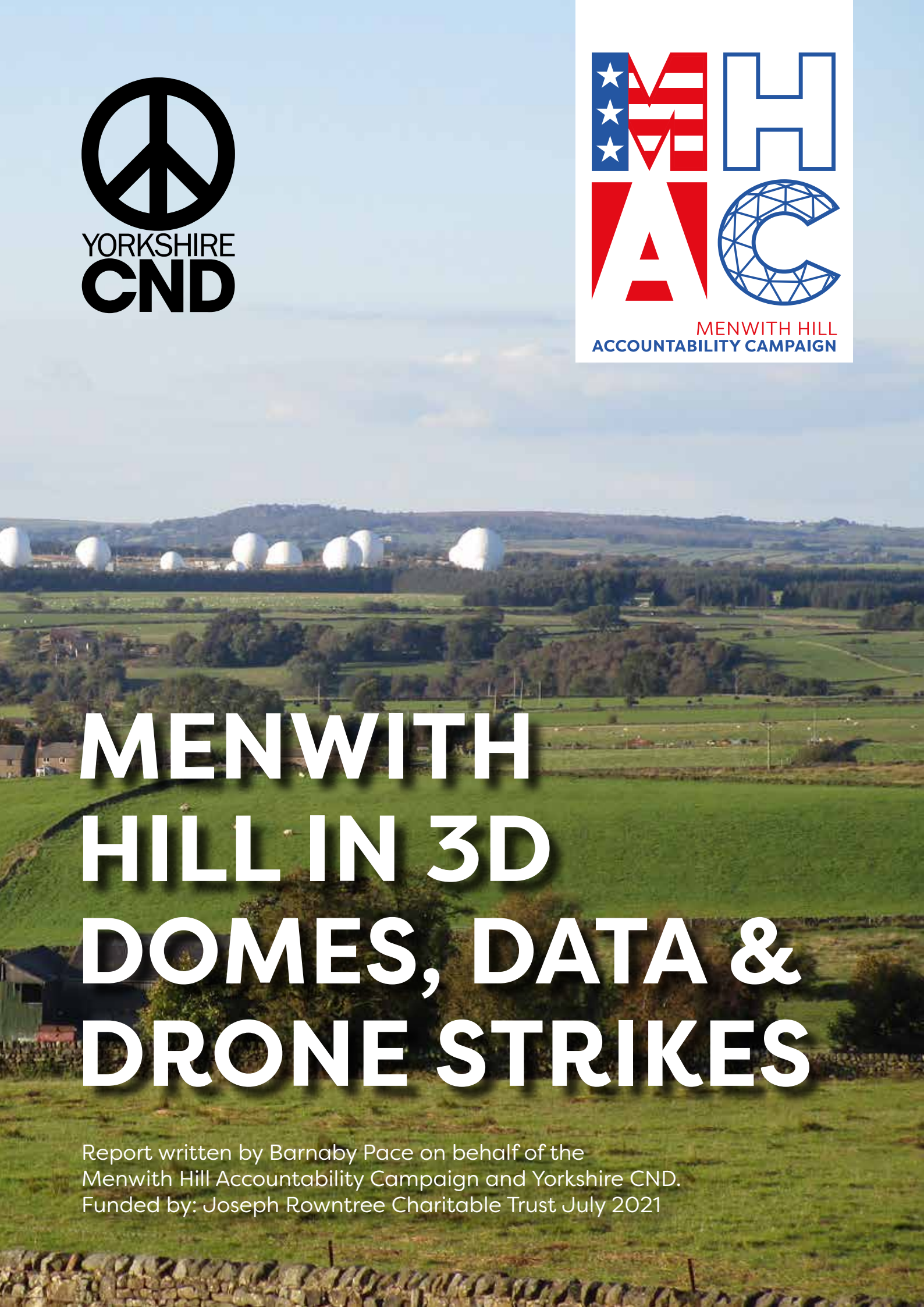
YORKSHIRE CND

MENWITH HILL ACCOUNTABILITY CAMPAIGN



MENWITH HILL IN 3D DOMES, DATA & DRONE STRIKES

Report written by Barnaby Pace on behalf of the
Menwith Hill Accountability Campaign and Yorkshire CND.
Funded by: Joseph Rowntree Charitable Trust July 2021

The Menwith Hill Accountability Campaign thanks Barnaby Pace for all his work on this report

CONTENTS

ABOUT THE AUTHOR

Barnaby Pace is a journalist and campaigner. His writing has been included in ***Offensive Insecurity: The role of science and technology in UK security strategies, African Muckraking: 75 Years of Investigative Journalism from Africa, How To Pay a Bribe: Thinking Like a Criminal to Thwart Bribery Schemes*** and the ***SIPRI Yearbook*** and he was a primary researcher ***for Shadow World: Inside the Global Arms Trade.***

He holds a Master's degree in Mechanical Engineering from the University of Warwick.

MENWITH HILL IN 3D: DOMES, DATA AND DRONE STRIKES

FOREWORD BY THE MENWITH HILL ACCOUNTABILITY CAMPAIGN

The Menwith Hill Accountability Campaign (MHAC) is a peace organisation formed and run by volunteers. It was launched in 2017 to continue some of the work of The Campaign for the Accountability of American Bases (CAAB) and other peace groups. The organisation now concentrates on monitoring activities at the US Communications Intelligence (COMINT) base at Menwith Hill, near Harrogate, North Yorkshire, and making them more widely known.

Our proposal was to conduct a short research project to update, as far as possible, our understanding of the role of Menwith Hill and the military-related activities carried out there, which have significant implications for the peace and security of the local area, Britain, Europe and the whole world.

In particular we wanted to explore the issues around the legality of these activities and the extent to which those responsible for them are accountable to the UK Parliament.

It is important that the information presented in a 2012 research report produced by Yorkshire Campaign for Nuclear Disarmament (CND) ("Lifting the Lid on Menwith Hill... The Strategic Roles and Economic Impact of the US Spy Base in Yorkshire"[1]) be updated to include recent developments and disclosures, for example from Edward Snowden, that have captured public attention and aroused concern. MHAC supporters are aware that they lack up-to-date credible information to present to the public and that the technology and awareness of intelligence gathering have changed since 2012.

THE RESEARCH OBJECTIVES

- To investigate and produce a factual, unbiased document on the current state of knowledge of the activities at Menwith Hill;
- To identify the current political, legal and moral issues that present a challenge to these activities.

WHY NOW?

Two recent incidents have highlighted the importance of Menwith Hill as part of the global US intelligence collection network. They have made the possible consequences of Menwith Hill's role extremely important as issues for a much wider political and public understanding and discussion.

On Friday 3 January 2020 Iranian General Qasem Soleimani was killed by an armed US drone. It is probable that the facilities at Menwith Hill were used to target that drone strike[2].

The second event concerns the death of 19-year-old Harry Dunn, killed on 27 August 2019 while riding his motorcycle near the exit from RAF Croughton, a US communications and intelligence base in Oxfordshire. This issue is of importance to MHAC since on 11 August 2015 one of our supporters, Barbara Penny, a Quaker from Harrogate, was struck by a car while taking part in our regular peaceful protest at the Nessfield Gate of Menwith Hill and suffered serious injuries.

The driver was charged with grievous bodily harm and admitted that his car had hit Barbara, but he was found not guilty by a jury at Leeds Crown Court. However Barbara Penny was able to obtain an out-of-court settlement for damages.

Important questions of accountability and the right to protest arise from the above events:

- Are UK personnel involved in supplying targeting data for US drone strikes acting illegally?
- Should Americans working on US bases in the UK be effectively exempt from UK legal processes?
- To what extent are the activities of individuals and groups who take part in protests and demonstrations monitored by national and other security organisations?
- How do we ensure that the right to protest is protected?

MHAC was pleased that the research work would be undertaken by an experienced researcher, Barnaby Pace, who has an impressive track record of research on politics and security issues.

The work was overseen by a working group of MHAC and CND campaigners, who acted as the project managers.

MHAC hopes this research will be shared widely as a document and as a short film. MHAC will continue to make the research available on the Menwith Hill Accountability Campaign website (**https://themhac.uk**).

1. "Lifting the Lid on Menwith Hill", a 2012 Yorkshire CND report, available from: **https://cnduk.org/wp-content/uploads/2018/02/liftingthelid.pdf**
2. In response to a parliamentary question asking whether Menwith Hill had a role in the drone programme that assassinated Qasem Soleimani Anne-Marie Trevelyan, on behalf of the Government, said "In accordance with long-standing policy we do not comment on the details of the operations carried out at RAF Menwith Hill in providing intelligence support." HC Deb, 10 February 2020, cW **https://www.theyworkforyou.com/wrans/?id=2020-02-04.12409.h**

INTRODUCTION

Menwith Hill Station in Yorkshire has the appearance of an RAF base. However it is in fact the United States' National Security Agency's (NSA) largest-known overseas surveillance facility where UK and US intelligence personnel collaborate to operate a vast global surveillance network which, among other roles, plays a key part in targeting US drone strikes.

Leaks of secret intelligence agency documents in recent years have exposed how eavesdropping technology at Menwith Hill is capable of collecting data from hundreds of millions of emails and phone calls a day and of pinpointing communication devices on the ground[3].

The UK and US intelligence agencies have been exposed as using these capabilities to spy on leaders of allied nations, aid agencies and vast swathes of the population.

According to documents from whistle-blowers, programmes developed at Menwith Hill have been used to support British and American troops in ongoing conflicts in Iraq and Afghanistan but have been also used outside of war zones as part of covert missions in Yemen, Somalia, Pakistan and Lebanon[4].

Leaked documents also identify Menwith Hill as providing the intelligence used in "a significant number of capture-kill operations", including targeting information for US covert drone strikes as part of a wider assassination programme that has been criticised as amounting to extrajudicial executions[5].

Between 2010 and 2020 more than 14,000 drone strikes were carried out by US forces, killing somewhere between 8,858 and 16,901 people according to a database created by the Bureau for Investigative Journalism. However the role of intelligence agencies' extraordinary spying capabilities should not mislead the public into believing that drone strikes are accurate. A 2014 study by Reprieve found that US attempts to kill 41 men as part of its "targeted killing" campaign resulted in the deaths of an estimated 1,147 people[6], a ratio of 28 people killed for every person specifically targeted.

The Bureau of Investigative Journalism estimates that in the last ten years between 910 and 2,200 of the victims of US drone strikes have been civilians, with between 283 and 454 of them being children[7].

The UK Government has publicly stated that all activities at the base are carried out with the "full knowledge and consent" of British officials[8]. However, as explored later in this report, legal rulings in the UK and abroad in recent years have raised questions around the legality of surveillance operations at Menwith Hill and the lethal drone strikes they support. Ministerial and parliamentary oversight similarly appears to be very limited.

Menwith Hill also forms part of US missile defense system. A Government minister confirmed in 2019 that "There are three radomes at RAF Menwith Hill that form part of the US Space Based Infra-Red System, and these radomes are a fully operational part of the US Defence Support Programme Missile Warning facilities."[9] Missile defence systems have been criticised as being responsible for fuelling nuclear-arms races and encouraging leaders to act more aggressively. Menwith Hill's role in the US system also makes it a potential target in the event of a conflict.

Please note that the US spelling of 'defense' is used in this report to signify specific reference to US missile defense systems. In addition, although bases such as Menwith Hill in the UK are described as RAF, the majority of staff at them are US military or intelligence. Those in command are usually from the US.

US and UK forces' activities at Menwith Hill and their role in missile defense[10], unprecedented state surveillance, conflict and assassination campaigns should be of serious concern to the local community in Yorkshire and local and national Government.

3. The Intercept, 30/11/2017, Ryan Gallagher, "U.K. Government Pressured Over Secret Base's Role In Trump's Drone Strikes", **https://theintercept.com/2017/11/30/drone-strikes-gchq-trump-menwith-hill-uk/**

4. The Intercept, 30/11/2017, Ryan Gallagher, "U.K. Government Pressured Over Secret Base's Role In Trump's Drone Strikes", **https://theintercept.com/2017/11/30/drone-strikes-gchq-trump-menwith-hill-uk/**

5. Bureau of Investigative Journalism, Drone Warfare database, **https://www.thebureauinvestigates.com/projects/drone-war** ; The Intercept, 6/9/2016, "Inside Menwith Hill", **https://theintercept.com/2016/09/06/nsa-menwith-hill-targeted-killing-surveillance/**

6. The Guardian, 24/11/2014, "41 men targeted but 1,147 people killed: US drone strikes – the facts on the ground", **https://www.theguardian.com/us-news/2014/nov/24/-sp-us-drone-strikes-kill-1147**

7. Bureau for Investigative Journalism, "Drone Warfare", Accessed on 31/1/2020, **https://www.thebureauinvestigates.com/projects/drone-war**

8. Parliamentary answer from Mark Francois (Minister of State, Ministry of Defence), 3/7/2014, **https://questions-statements.parliament.uk/written-questions/detail/2014-06-25/202447**

9. Parliamentary answer from Mark Lancaster The Minister of State, Ministry of Defence, 18/3/2019, HC Deb, 18 March 2019, cW, **https://www.theyworkforyou.com/wrans/?id=2019-03-11.230899.h&s=menwith**

10. House of Commons Library, 27/11/2008, Claire Taylor, "UK Participation in US Missile Defence", **https://researchbriefings.files.parliament.uk/documents/SN04664/SN04664.pdf**

MENWITH HILL AND THE STATUS OF FORCES AGREEMENT

The base, just a few miles west of Harrogate, is designated as RAF Menwith Hill but according to the UK Government in 2020 only ten British military personnel were stationed there. Instead the base was revealed to be staffed by more than 600 American contractors, civilians and military personnel alongside nearly 500 British non-military personnel, including an unspecified number of employees from the UK intelligence agency GCHQ[11].

US intelligence agencies at the site include the NSA and the National Reconnaissance Office (NRO)[12].

The Government has declined to give a detailed breakdown of personnel from the various UK and US intelligence agencies, saying that "the US authorities do not release a detailed breakdown of US civilian personnel." [13]

The United States has had troops permanently stationed in the UK since the Second World War, leasing several bases from the UK. According to the Ministry of Defence "RAF Menwith Hill is made available for use by the United States Visiting Forces (USVF) under the terms of the NATO Status of Forces Agreement (SOFA) of 1951. The presence of USVF military and civilian personnel and equipment at the base are covered by the NATO SOFA and also the Visiting Forces Act of 1952."

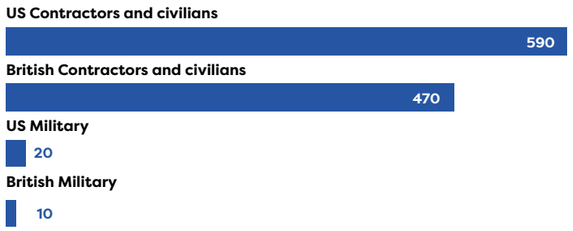
The legal arrangements regulate how US forces operate in the UK. The law establishes legal jurisdiction over military personnel and related civilians outside

of their bases, defines exemptions from passport and visa regulations and customs and excise duties, sets out the legal right for military personnel to patrol bases, move around the country, wear uniform and bear arms in the UK and lays down procedures if US military or civilian personnel break the law. The law also lays out how costs are split between the UK and visiting forces. The arrangements apply for UK military personnel in other allied NATO countries[14]. The costs to the UK taxpayer are confidential under the cost-sharing agreements[15].

Under the law British authorities are responsible for security outside the bases of visiting forces but inside US forces have authority to police their bases in the UK and take all appropriate measures to enhance security on base[16].

Menwith Hill has continued to expand over recent years, reflecting the increasingly wide-ranging and technologically sophisticated surveillance apparatus built up at the base. Between 2009 and 2012 a $40m investment in a 95,000-square-foot operations building included a new 10,000-square-foot data centre[17]. In recent years Harrogate Borough Council has granted permission for additional radar shelters to be constructed at the site, likely expanding its capabilities further[18].

Personnel based at Menwith Hill
Accurate as of August 2020



Source: Parliamentary Answer, HC Deb, 19 January 2021, cW

Menwith Hill Aerial View (2020) Source: Google Earth

11. Parliamentary answer from James Heappey, the Parliamentary Under-Secretary of State for Defence, 11/1/2021, HC Deb, 19 January 2021, cW **https://www.theyworkforyou.com/wrans/?id=2021-01-14.138040.h&s=menwith**

12. National Reconnaissance Office, "Who We Are", **https://www.nro.gov/About-NRO/The-National-Reconnaissance-Office/Who-We-Are/** ; The Intercept, Ryan Gallagher, 6/9/2016, "Inside Menwith Hill", **https://theintercept.com/2016/09/06/nsa-menwith-hill-targeted-killing-surveillance/**

13. Parliamentary answer from James Heappey, the Parliamentary Under-Secretary of State for Defence, 11/1/2021, HC Deb, 19 January 2021, cW **https://www.theyworkforyou.com/wrans/?id=2021-01-14.138040.h&s=menwith**

14. House of Commons Library, 8/1/2015, "US Forces in the UK: legal agreements", **https://researchbriefings.files.parliament.uk/documents/SN06808/SN06808.pdf**

15. The Guardian, 1/3/2012, "Menwith Hill eavesdropping base undergoes massive expansion", **https://www.theguardian.com/world/2012/mar/01/menwith-hill-eavesdropping-base-expansion**

16. House of Commons Library, 8/1/2015, "US Forces in the UK: legal agreements", **https://researchbriefings.files.parliament.uk/documents/SN06808/SN06808.pdf**

17. Data Center Dynamics, 7/10/2016, "Revealed: NSA built a 10,000 sq ft Tier III UK data center in 2011", **https://www.datacenterdynamics.com/en/news/revealed-nsa-built-a-10000-sq-ft-tier-iii-uk-data-center-in-2011/**

18. Harrogate Advertiser, 14/8/2019, "RAF Menwith Hill: Permission granted for more radar shelters at base", **https://www.harrogateadvertiser.co.uk/news/politics/council/raf-menwith-hill-permission-granted-more-radar-shelters-base-681785**

THE ROLE OF MENWITH HILL IN US MISSILE DEFENSE

In 2007 the UK formally agreed that Menwith Hill be used as part of the United States Ballistic Missile Defense System. Campaigners raised alarms that the move had been agreed without any consultation with the public or Parliament.

According to a Government minister at the time, RAF Menwith Hill would enable satellite data on missile trajectories to be passed into the new US missile defense system. The radar system at RAF Fylingdales on the North York Moors also forms part of the early-warning and tracking system designed to detect and monitor the approach of missiles to the continental US[19].

Missile defence systems work by detecting the launch of a missile attack, tracking and targeting incoming missiles and launching another missile or other projectile to intercept and destroy the first missile while in flight. Different systems attempt to intercept a missile at different stages in its flight using land-, sea- or even space-based interceptors.

In 2011 Menwith Hill's satellite downlink from the Space Based Infrared System (SBIRS), a missile-tracking satellite system, was announced. The SBIRS satellites detect and track missile launches[20]. In 2019 a Government minister confirmed that three of the radomes on the base are an active part of the SBIRS[21].

Menwith Hill is linked to Buckley, a US air base in Colorado, home to almost 100,000 military personnel and the 460th Space Wing of the US Air Force Space Command. The 460th provided "missile warning, missile defence, technical intelligence, satellite command and control, and robust aerospace communications"[22]. The unit has recently been replaced with a field unit dubbed Space Delta 4 since it has been incorporated into the new US Space Force[23].

Ronald Reagan's 1983 speech popularised the "Star Wars" concept of space-based weapons as part of a missile defense system, but like most other missile defence systems the concept has proven highly controversial, wildly expensive and technically extremely difficult.

For example, since the late 1990s the US Pentagon has spent $67 billion on just one missile defense system, the Ground-based Midcourse Defense (GMD). Despite massive spending and hype by US officials and arms company executives the system has never been proven to work in a realistic test[24]. GMD's main manufacturer is Boeing.

According to an analysis by the Union of Concerned Scientists the GMD destroyed its target in only four of 10 tests after it was fielded in 2004, even though all of the tests were held under improbably ideal conditions where operators often

had scripted knowledge of what they were facing. A report by internal US Government watchdog the Government Accountability Office similarly found in 2016 that "GMD flight testing, to date, was insufficient to demonstrate that an operationally useful defense capability exists"[25].

Missile defence systems can also be deceived by decoys or other countermeasures that any country capable of launching ballistic missiles would probably also have access to[26]. Nuclear strategists believe that any determined major power would simply overwhelm missile defence systems[27].

Backers of missile defence systems claim they are purely defensive[28]. However missile defence has been highly controversial since it was introduced.

Critics argue that missile defence systems make conflict more likely, with decision-makers believing, rightly or wrongly, that they could neutralise incoming missiles, leading them to act more aggressively.

In the early days of the Trump presidency in the US tensions escalated with North Korea. President Trump told the public not to worry about possible North Korean nuclear missiles following a missile test, saying that "We will take care of it," and "It is a situation that we will handle." Trump told Fox News that the US has "missiles that can knock out a missile in the air 97 percent of the time."[29] The former president was prone to exaggeration but, if he believed what he was saying, his statement illustrates how the hype around missile defense capabilities may have given him, as US President, a false sense of security in his dealings with the North Korean crisis[30].

Critics also argue that the deployment of missile defence systems undermines arms-control agreements, including the Nuclear Non-Proliferation Treaty, and can spur new nuclear-arms races. Russia has made clear that carrying out the agreed reductions in their arsenal of nuclear weapons depends on limiting the deployment of US missile defenses. Russia has also claimed that its newest nuclear weapons under development, including undersea torpedoes, hypersonic glide vehicles and nuclear-powered cruise missiles, are designed to overcome US missile defenses. Similarly, China has increased the number of its missiles with multiple nuclear warheads designed to avoid missile defences[31].

Ever since Reagan's "Star Wars" speech missile defence has been linked with the militarisation of space. Some space-based weapons are banned under the Outer Space Treaty (OST), which prohibits states from stationing weapons of mass destruction in space, and the 1972 Anti-Ballistic Missile (ABM) Treaty[32]. The latter was agreed between the United States and the Soviet Union (later Russia) in recognition of how the development of missile defence systems would destabilise the nuclear balance between the two countries.

The treaties have not prevented the pursuit of satellite programmes such as the SBIRS system linked to Menwith Hill, and the US unilaterally withdrew from the ABM treaty in 2002 in order to implement their missile defense programme. The reliance on military satellites arguably incentivises the development of anti-satellite weapons that could cripple both military satellites and civilian satellites that play a crucial, sometimes dual, role in our society. Several nations have already developed these dangerous weapons[33].

Menwith Hill's role in the US Missile Defense System poses grave risks. The role of the base in the system makes it a potential target in the event of a conflict, whilst the deployment of missile defense systems heightens the risk of conflict, which could rapidly become nuclear.

The lack of parliamentary debate before the deployment of the system, operated from UK territory, adds to concerns over accountability at Menwith Hill.

19. BBC News, 25/7/2007, "UK agrees missile defence request", **http://news.bbc.co.uk/1/hi/uk_politics/6916262.stm**

20. Center for Defense Information, 16/10/2007, "Fact Sheet on Space Based Infrared System", **https://web.archive.org/web/20071113202652/http://www.cdi.org/friendlyversion/printversion.cfm?documentID=4122**

21. Parliamentary answer from Mark Lancaster The Minister of State, Ministry of Defence, 18/3/2019, HC Deb, 18 March 2019, cW, **https://www.theyworkforyou.com/wrans/?id=2019-03-11.230899.h&s=menwith**

22. The Guardian, 18/6/2011, "'Son of star wars' base in Yorkshire finally ready to open", **https://www.theguardian.com/science/2011/jun/18/son-star-wars-base-yorkshire**

23. Buckley Air Force Base, "Space Delta 4 – Missile Warning", **https://www.buckley.spaceforce.mil/About-Us/Fact-Sheets/Article/322395/space-delta-4-missile-warning/**

24. Union of Concerned Scientists, 29/11/2017, "Hyping US Missile Defense Capabilities Could Have Grave Consequences", **https://blog.ucsusa.org/elliott-negin/missile-defense-risks**

25. Washington Post, 13/10/2017, "Fact Checker: Trump's claim that a US interceptor can knock out ICBMs '97 percent of the time'", **https://www.washingtonpost.com/news/fact-checker/wp/2017/10/13/trumps-claim-that-u-s-interceptors-can-knock-out-icmbs-97-percent-of-the-time/**

26. Scientific American, 14/12/2020, "It's Time to Rein in Inflated Military Budgets", **https://www.scientificamerican.com/article/its-time-to-rein-in-inflated-military-budgets/**

27. Arms Control Association, 12/2020, "Missile Defense and the Arms Race", **https://www.armscontrol.org/act/2020-12/focus/missile-defense-arms-race**

28. For example see NATO, 9/10/2019, "Ballistic missile defence", **https://www.nato.int/cps/en/natolive/topics_49635.htm**

29. Washington Post, 13/10/2017, "Fact Checker: Trump's claim that a US interceptor can knock out ICBMs '97 percent of the time'", **https://www.washingtonpost.com/news/fact-checker/wp/2017/10/13/trumps-claim-that-u-s-interceptors-can-knock-out-icmbs-97-percent-of-the-time/**

30. Union of Concerned Scientists, 29/11/2017, "Hyping US Missile Defense Capabilities Could Have Grave Consequences", **https://blog.ucsusa.org/elliott-negin/missile-defense-risks**

31. Arms Control Association, 12/2020, "Missile Defense and the Arms Race", **https://www.armscontrol.org/act/2020-12/focus/missile-defense-arms-race**

32. IISS, 20/12/2018, "Will space-based missile interceptors weaponise space?", **https://www.iiss.org/blogs/analysis/2018/12/missile-interceptors-weaponise-space**

33. Financial Times, 2/9/2020, "US military officials eye new generation of space weapons", **https://www.ft.com/content/d44aa332-f564-4b4a-89b7-1685e4579e72**

THE ROLE OF MENWITH HILL IN STATE SURVEILLANCE

The Menwith Hill base has been operating since 1954, was expanded throughout the course of the Cold War and is often said to be the largest overseas US spy base in the world[34].

The UK's state surveillance capabilities have been a closely guarded secret, with only rare exposés coming from whistle-blowers and investigative reporting.

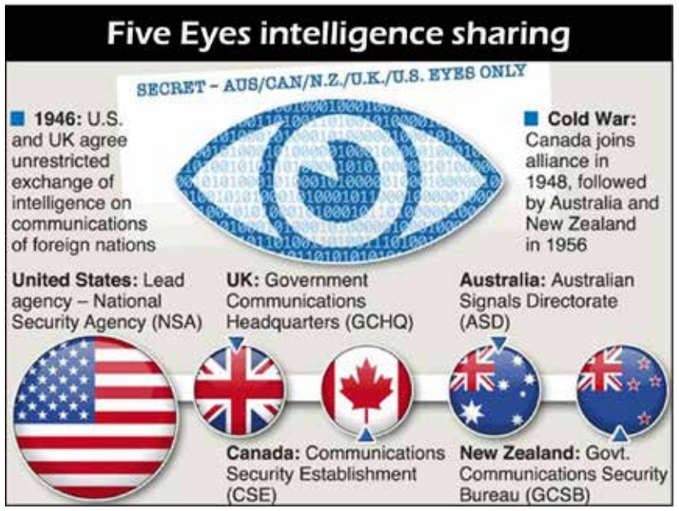
The UK and US Governments have actively misled the public about the activities at Menwith Hill. A leaked 2005 US Government document described the base's "cover story" as a facility to provide "rapid radio relay and conduct communications research". The document noted that the association of NSA or CIA personnel with the base must be kept secret as well as making clear it was "strictly prohibited" to make "any reference to satellites being operated or any connection to intelligence gathering"[35].

In 1988 investigative journalist Duncan Campbell revealed details of the ECHELON mass-surveillance programme, which was capable of intercepting satellite communications including phone calls, fax messages and emails. Campbell exposed the role of the UK's GCHQ spy agency and its collaboration with the NSA and identified Menwith Hill as a key cog in the system, with the base's characteristic golf-balled-shaped radomes concealing satellite dishes used to receive information from satellites intercepting radio signals[36].

Whistle-blowers told Campbell that the UK spied not just on perceived adversaries but also on its allies and its own citizens. Campbell continued reporting despite arrests, prosecution and censorship by UK authorities[37].

Concerns were also raised in later years that the surveillance programme was used not only for intelligence purposes but also for helping US firms win contracts, effectively industrial espionage, which if proven would have been illegal[38].

The UK is part of an international alliance known as Five Eyes together with the United States, Australia, Canada and New Zealand. The agreement began between the UK and US during the Second World War and was expanded to include the other states during the Cold War. The allies agree not to spy on one another's Governments and to share intelligence. The treaty was kept secret for many years, with Australia's Prime Minister even being unaware of the agreement until 1973[39]. It has been reported that Gough Whitlam was sacked in 1975 by the UK Government because he started to question the presence of the NSA at the US spy base at the equivalent to Menwith Hill – Pine Gap in central Australia[40]. No Government official publicly acknowledged the Five Eyes arrangement until 1999[41]. On 25 June 2010 the full text of the agreement was made public and it is available online[42].



Five Eyes Intelligence Sharing Source: https://diligentias.com/the-u-s-has-threatened-to-cut-off-intelligence-sharing-between-five-eyes/

In 2013 a leak from the US National Security Agency contractor Edward Snowden revealed for the first time the vast scale and scope of the global surveillance apparatus created by the NSA, the UK's GCHQ and other allied intelligence agencies. The Snowden revelations showed that, as the way we communicate has changed with technological developments, state surveillance has expanded to allow the collection, storage and analysis of the private information of a vast swathe of the population.

Documents leaked by Snowden showed that the NSA was capable of tracking the emails, online chats and browsing histories of millions of individuals, including monitoring activity in real time[43].

One system, codenamed PRISM, gave the NSA access to the systems of nine of the world's biggest Internet companies including Google, Facebook, Microsoft, Apple, Yahoo and Skype. The UK's GCHQ was found to have had access to the system for its own snooping since at least 2010[44]. NSA documents describe how "special programmes for GCHQ exist for focused Prism processing", suggesting that the UK agency was able to receive material from a bespoke part of the programme made to suit British interests[45].

NSA documents also showed that the agency and GCHQ jointly worked to circumvent security measures that tech giants had promised consumers would protect their Internet activity, personal data, online transactions and emails, including medical and banking data. GCHQ was revealed to have worked to break into encrypted traffic at Hotmail, Google, Yahoo and Facebook[46].

Other revelations included an NSA operation, codenamed DISHFIRE, that collected two hundred million text messages a day. The information was used to extract information on people's travel plans, contact books and financial transactions without any specific warrant and with no suspicion of illegal activity. GCHQ was able to search the database "untargeted and unwarranted"[47].

Menwith Hill and GCHQ were revealed as playing an integral part in a programme to hack into computers and networks covertly on a massive scale using automated systems. A leaked top-secret NSA document described the process as allowing "industrial-scale exploitation"[48].

Menwith Hill and GCHQ were revealed as playing an integral part in a programme to hack into computers and networks covertly on a massive scale using automated systems. A leaked top-secret NSA document described the process as allowing "industrial-scale exploitation".

Software has also been developed to control computers, take over a targeted computer's microphone and record conversations, covertly take over a computer's webcam and snap photographs or record Internet browsing and collect login details and passwords used to access websites and email accounts[49].

In addition to participating in other digital-intelligence-gathering programmes, Menwith Hill was confirmed as operating two main spying systems:

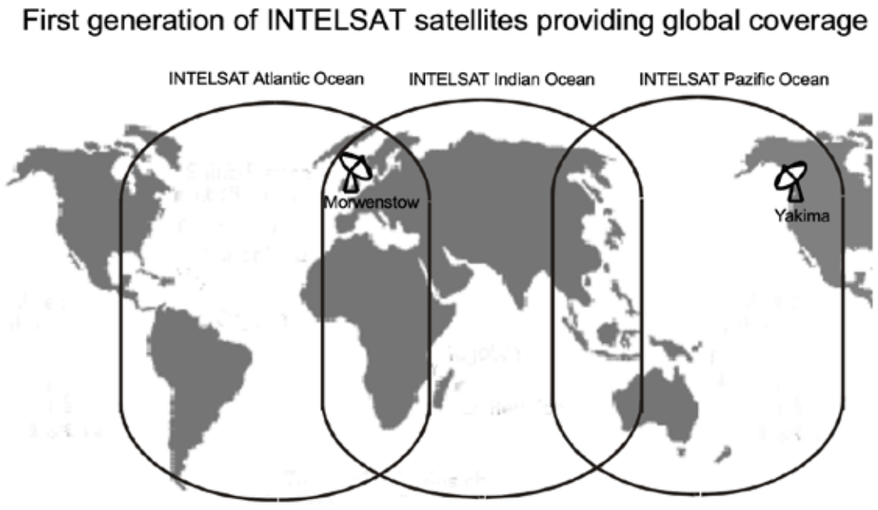
FORNSAT, an evolution of the **ECHELON** programme exposed by Campbell in the 1980s, which uses the powerful antennae contained within the golf-ball-like radomes to eavesdrop on communications as they are being beamed between foreign satellites. In 2009 Menwith Hill's foreign satellite surveillance mission, codenamed **MOONPENNY**, was monitoring 163 different satellite data links[50].

OVERHEAD, which uses US satellites to locate and monitor wireless communications such as mobile-phone calls and WiFi traffic[51].

Menwith Hill was revealed to be capable of logging hundreds of millions of communications records a day, recording information such as the sender and recipients of emails and what phone calls someone made and when, information referred to as metadata. In one twelve-hour period Menwith Hill logged 335 million metadata records[52].

GCHQ's TEMPORA programme taps into the fibre-optic cables that carry vast quantities of data. The GCHQ station at Bude in Cornwall had attached probes to more than 200 fibre-optic cables by the end of 2011 and then shared the data within GCHQ and with international partners including the NSA. An estimated 25% of all global Internet traffic runs through Cornwall, where transatlantic underwater cables that pass data from Europe to the US and back again make landfall[53]. The agency's documents described the system as "Mastering The Internet"[54].

Menwith Hill's distinctive radomes, which link to satellites in orbit, give the intelligence agencies the capacity to eavesdrop on satellite-based communications relied on in more remote parts of the world. This capability has given the base a pivotal role in conflicts in the last two decades[55].



Coverage of the US INTELSAT satellite: Menwith Hill is involved in the Atlantic and Indian Ocean systems.
Source: European Parliament, Report on the existence of a global system for the interception of private and commercial communications (ECHELON interception system) (2001/2098(INI)), p. 52/194

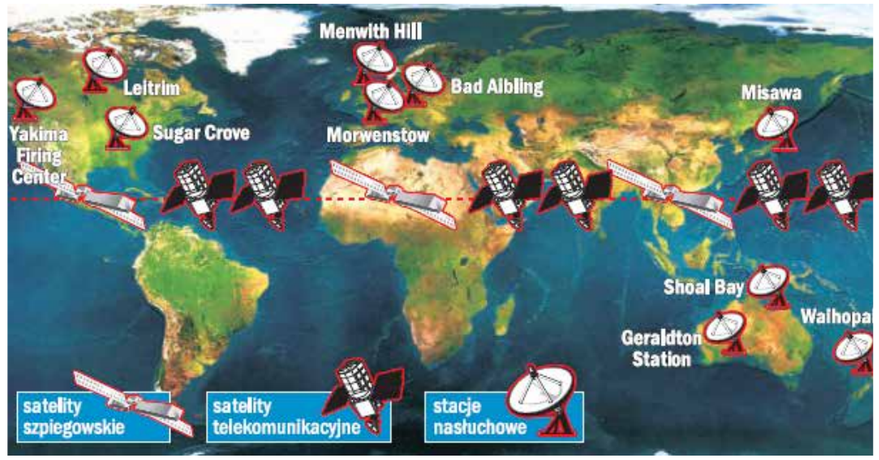
https://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A5-2001-0264+0+DOC+PDF+V0//EN&language=EN

Menwith Hill has the ability to target communications in China, Latin America, the Middle East and North Africa and also provide "continuous coverage of the majority of the Eurasian landmass," where they intercept "tactical military, scientific, political, and economic communications signals."[56]

The ramping up of surveillance did not come about by accident. According to NSA documents one crucial moment came in 2008, when the NSA Director at the time, Keith Alexander, introduced a radical shift in policy. Visiting Menwith Hill he challenged employees at the base: "Why can't we collect all the signals, all the time?" Alexander asked. "Sounds like a good summer homework project for Menwith."[57]

> *"Why can't we collect all the signals, all the time?" Alexander asked. "Sounds like a good summer homework project for Menwith."*

As surveillance ramped up to a vast scale the majority of people spied upon were never intentionally targeted. An analysis



ECHELON – The Start of Britain's Modern Day Spying Operations Source: https://tapnewswire.com/2017/01/echelon-the-start-of-britains-modern-day-spying-operations/

4.4 (S//TK) Mission 7500 (MERCURY/MC) Program Overview

(S//TK) Mission 7500 is a geosynchronous satellite system designed to provide concentrated coverage of the Eurasian landmass. The geosynchronous (GEO) orbit provides the capability to focus on target areas of interest for up to 24 hours a day. This means the satellite appears to loiter around a particular point above the equator. The primary target is strategic level communications, although operational characteristics make it useful in a wide variety of operational and tactical roles as well.

(S//TK) Potential coverage areas can be modified through satellite repositioning (lateral movement of the satellites central loiter point, east or west along the equator). This capability provides System 7500 the flexibility to focus coverage as necessary in response to crisis/contingency requirements. The amount of time it takes to reposition a satellite depends on how far the satellite is to be moved and other technological factors.

(S//TK) Mission 7500 has the capability to geolocate a stationary emitter if its signal is collected by two of the system's satellites simultaneously. Geolocation accuracy ranges [redacted] and depends on the technical characteristics of the signal being collected and spacecraft geometry (look angle, etc.) Emitter Location Data (ELD) reports can be disseminated via the Integrated Broadcast System (IBS) [redacted].

(S//TK) Data collected by Mission 7500 satellites is digitized and encrypted on the satellite and downloaded to the MGS (RAF Menwith Hill Station, Harrogate, UK). Exploitation of the intercepted data can be performed at the MGS if appropriate linguistic personnel, or appropriate technical capabilities are present. The data is relayed to National Security Agency (NSA) and the Regional SIGINT Operations Centers, in either real-time or via recording, for initial or follow-on exploitation.

Source: https://www.documentcloud.org/documents/3089521-Menwith-satellite-classification-guide.html

of NSA documents by the Washington Post found that 90% of the people caught in intercepted conversations were not the intended surveillance targets but were caught in a net the agency had cast for somebody else[58].

The Snowden leaks further revealed that the British and American intelligence agencies also surveilled friendly world leaders, including those attending diplomatic summits hosted by the UK[59]. The NSA was embarrassingly exposed as having tapped the mobile phone of the German Chancellor, Angela Merkel, and GCHQ was found to have targeted the email address of the Israeli Prime Minister, Ehud Olmert.

Another US spy/communications base, RAF Croughton in Northamptonshire, was revealed to have acted as a relay station for the data-tapping of Chancellor Merkel's phone. The base was reportedly used for "tech support activity" by the Special Collection Service (SCS), a joint CIA / NSA unit that runs some 100 listening posts around the world in parallel with a scheme overseen by GCHQ[60].

GCHQ and the NSA also targeted the EU's competition commissioner, German Government buildings in Berlin and overseas and international institutions, including the United Nations development programme, the UN's children's charity Unicef and Médecins du Monde, a French organisation that provides doctors and medical volunteers for conflict zones[61].

The collaboration between the US and UK as well as the wider Five Eyes group has also raised concerns that the countries may use the exchange of intelligence as a way to circumvent legal restrictions on spying on their own citizens. Academics and campaigners have alleged that NSA spying at Menwith Hill may have included targeted surveillance of UK citizens by US personnel at the request of UK intelligence agencies, circumventing UK laws on eavesdropping[62].

In 2000 a retired Canadian intelligence agent, Mike Frost, claimed that Margaret Thatcher had requested surveillance on two of her ministers she had disagreed with. Thatcher declined to comment on the allegation at the time[63].

The breath-taking scale of the US, UK and Menwith Hill's surveillance was exposed as going far beyond the expected intelligence targets of hostile states or suspected terrorists and criminals[64].

34. The Intercept, Ryan Gallagher, 6/9/2016, "Inside Menwith Hill", **https://theintercept.com/2016/09/06/nsa-menwith-hill-targeted-killing-surveillance/**

35. The Intercept, Ryan Gallagher, 6/9/2016, "Inside Menwith Hill", **https://theintercept.com/2016/09/06/nsa-menwith-hill-targeted-killing-surveillance/; https://www.documentcloud.org/documents/3089521-Menwith-satellite-classification-guide.html**

36. The Intercept, Duncan Campbell, 3/8/2015 "My Life Unmasking British Eavesdroppers", **https://theintercept.com/2015/08/03/life-unmasking-british-eavesdroppers/**

37. OpenDemocracy, 26/8/2015, "Investigative journalist Duncan Campbell recounts his experiences unmasking British eavesdroppers", **https://www.opendemocracy.net/en/opendemocracyuk/gchq-and-me/**

38. European Parliament, 11/7/2001, "Report on the existence of a global system for the interception of private and commercial communications (ECHELON interception system) (2001/2098(INI))", **https://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A5-2001-0264+0+DOC+PDF+V0//EN&language=EN**

39. ABC News, 19/11/2013, "Explained: Australia's involvement with the NSA, the US spy agency at heart of global scandal", **https://www.abc.net.au/news/2013-11-08/australian-nsa-involvement-explained/5079786?nw=0**

40. The Guardian. John Pilger, 23/10/2014, "The British-American coup that ended Australian independence", **https://www.theguardian.com/commentisfree/2014/oct/23/gough-whitlam-1975-coup-ended-australian-independence**

41. OpenDemocracy, 31/7/2014, "The UN privacy report: Five Eyes remains", **https://www.opendemocracy.net/en/opensecurity/un-privacy-report-five-eyes-remains/**

42. National Archives, "Newly released GCHQ files: UKUSA Agreement", **http://www.nationalarchives.gov.uk/ukusa/**

43. The Guardian, 31/7/2013, "XKeyscore: NSA tool collects 'nearly everything a user does on the internet'", **https://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data** ; XKeyscore presentation from 2008 **https://www.theguardian.com/world/interactive/2013/jul/31/nsa-xkeyscore-program-full-presentation**

44. The Guardian, 7/5/2013, "UK gathering secret intelligence via covert NSA operation", **https://www.theguardian.com/technology/2013/jun/07/uk-gathering-secret-intelligence-nsa-prism**

45. The Guardian, 7/6/2013, "UK gathering secret intelligence via covert NSA operation", **https://www.theguardian.com/technology/2013/jun/07/uk-gathering-secret-intelligence-nsa-prism**

46. The Guardian, 6/9/2013, "Revealed: how US and UK spy agencies defeat internet privacy and security", **https://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security**

47. The Guardian, 16/1/2014, "NSA collects millions of text messages daily in 'untargeted' global sweep", **https://www.theguardian.com/world/2014/jan/16/nsa-collects-millions-text-messages-daily-untargeted-global-sweep**

48. The Intercept, 12/3/2014, document available at **https://theintercept.com/document/2014/03/12/industrial-scale-exploitation/**

49. The Intercept, 12/3/2014, "How The NSA Plans To Infect 'Millions' Of Computers With Malware", **https://theintercept.com/2014/03/12/nsa-plans-infect-millions-computers-malware/**

50. The Intercept, 6/9/2016, "Inside Menwith Hill", **https://theintercept.com/2016/09/06/nsa-menwith-hill-targeted-killing-surveillance/**

51. The Intercept, 6/9/2016, "Inside Menwith Hill", **https://theintercept.com/2016/09/06/nsa-menwith-hill-targeted-killing-surveillance/**

52. The Intercept, 30/11/2017, "U.K. Government Pressured Over Secret Base's Role In Trump's Drone Strikes", **https://theintercept.com/2017/11/30/drone-strikes-gchq-trump-menwith-hill-uk/**

53. BBC Horizon, 24/9/2014, "Inside the Dark Web", **https://www.bbc.co.uk/programmes/b04grp09**

54. The Guardian, 21/6/2013, "GCHQ taps fibre-optic cables for secret access to world's communications", **https://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa**

55. The Intercept, 6/9/2016, "Inside Menwith Hill", **https://theintercept.com/2016/09/06/nsa-menwith-hill-targeted-killing-surveillance/**

56. The Intercept, 6/9/2016, "Inside Menwith Hill", **https://theintercept.com/2016/09/06/nsa-menwith-hill-targeted-killing-surveillance/**

57. **https://www.documentcloud.org/documents/3089503-MHS-initiatives-maximizing-our-access.html**

58. Washington Post, 5/7/2014, "In NSA-intercepted data, those not targeted far outnumber the foreigners who are", **https://www.washingtonpost.com/world/national-security/in-nsa-intercepted-data-those-not-targeted-far-outnumber-the-foreigners-who-are/2014/07/05/8139adf8-045a-11e4-8572-4b1b969b6322_story.html**

59. New York Times, 16/6/2013, "New Leak Indicates Britain and US Tracked Diplomats", **https://www.nytimes.com/2013/06/17/world/europe/new-leak-indicates-us-and-britain-eavesdropped-at-09-world-conferences.html**

60. The Guardian, 18/6/2014, "Call to open RAF base for investigation into NSA tapping of Merkel's phone", **https://www.theguardian.com/world/2014/jun/18/labour-merkel-nsa-phone-tapping-raf-croughton**

61. The Guardian, 20/12/2013, "GCHQ and NSA targeted charities, Germans, Israeli PM and EU chief", **https://www.theguardian.com/uk-news/2013/dec/20/gchq-targeted-aid-agencies-german-government-eu-commissioner**

62. The Independent, 23/10/2011, "US spy base `taps UK phones for MI5'", **https://www.independent.co.uk/news/uk/home-news/us-spy-base-taps-uk-phones-mi5-1364399.html**

63. BBC News, 25/2/2000, "Thatcher 'spied on ministers'", **http://news.bbc.co.uk/1/hi/uk_politics/655996.stm**

64. The Guardian, 20/12/2013, "GCHQ and NSA targeted charities, Germans, Israeli PM and EU chief", **https://www.theguardian.com/uk-news/2013/dec/20/gchq-targeted-aid-agencies-german-government-eu-commissioner**

THE QUESTIONABLE LEGALITY OF UK AND US SURVEILLANCE

Old Bailey: The need for legality.
Source: Creative Commons. Wikimedia.

Both the UK and US surveillance programmes have been found to have been running illegally for many years after campaign groups mounted legal challenges made possible by the Snowden leaks.

A 2020 ruling on a lawsuit supported by the American Civil Liberties Union (ACLU) at the US Federal Appeals Court found that the NSA's warrantless telephone records database, which had collected millions of Americans' information, was illegal. Before being exposed, top US intelligence officials had insisted that the NSA never knowingly collected information on Americans at all. Following the Snowden revelations officials claimed that the spying programme had played a crucial role in the prosecution of individuals financing Somali extremists, something the court cast doubt upon[65].

Following the Snowden leaks the UK campaign group Privacy International and nine other human-rights and civil-liberties organisations challenged the legality of the UK's role in US-UK intelligence-sharing, an issue especially pertinent to Menwith Hill.

In 2015 the Investigatory Powers Tribunal (IPT), the UK's tribunal that rules on complaints against the intelligence agencies, ruled that this sharing had been illegal since the rules governing the arrangement had been kept secret[66].

This was the first time in the IPT's then 15-year history that it had ruled against an intelligence agency.

Shockingly though, the UK Government then argued successfully that, following the publicity around the sharing of surveillance data between the UK and US, the practice was now lawful because there was enough public 'signposting' about what was going on 'below the waterline'.

IPT hearings can take place in private and without the complaining party, which is justified as striking a balance between fairness to complainants and the need to safeguard national security by preventing the consideration of sensitive material in open court[67].

As Amnesty International's analysis put it, until the spying programme was exposed by whistleblowing and legal challenges it was breaking the law – but because the authorities were forced to reveal the vaguest details of how they gather and store information it is now legal for them to continue doing so[68].

"until the spying programme was exposed by whistleblowing and legal challenges it was breaking the law – but because the authorities were forced to reveal the vaguest details of how they gather and store information it is now legal for them to continue doing so."

The disclosure of the rules in the IPT case did render future use of the arrangement legal[69]. However there has been an appeal against the ruling to the European Court of Human Rights. Ten human-rights groups are arguing that the bulk-surveillance programme violates the European Convention on Human Rights, which protects the right to privacy and the right to freedom of expression[70]. This appeal was successful in May 2021.

Privacy International brought another case, which the IPT ruled on in 2018, finding in addition that the human-rights law had been broken by GCHQ's behaviour before 2015. In this case the agency had unlawfully been given unfettered authority to collect personal customer information from telecommunications companies.

Whilst celebrating the ruling Privacy International highlighted the dangers of secrecy at both GCHQ and the tribunal, noting "the error-ridden and inconsistent evidence provided by GCHQ throughout the case" and that they were not able to see the legal orders authorizing GCHQ's surveillance operations until well into legal proceedings. The group had even been forced to take the "extraordinary" step of cross-examining a GCHQ witness about "contradictory and incomplete evidence."

The group's action exposed the "willingness of telecommunications companies to secretly hand over customer data on the basis of mere verbal requests from GCHQ" while the programme was operating unlawfully for more than a decade[71].

A further challenge brought by human-rights groups, including Privacy International and Liberty, led to the European Court of Human Rights ruling in 2018 that the UK's use of bulk-interception powers was unlawful. However it was not the use of mass-surveillance systems that was deemed unlawful but rather the lack of controls in place to regulate the use of the systems. In its judgement the court deemed the regime to have a "lack of oversight of the entire selection process, including the selection of bearers for interception, the selectors and search criteria for filtering intercepted communications, and the selection of material for examination by an analyst."[72]

Together with several Internet and telecommunications companies Privacy International have also challenged the legality of GCHQ's hacking operations inside and outside the UK. The IPT ruled in 2016 that the hacking was legal under "thematic warrants", which can cover an entire class of property, persons or conduct, such as "all mobile phones in London".

However Privacy International argued that they should be able to challenge this power, winning the right to bring a case with a Supreme Court decision in 2019. They argued that thematic warrants undermine 250 years of English common law, which makes it clear that a warrant must target an identified individual or individuals, and that Parliament had not given clear permission for overriding such fundamental rights[73]. In January 2021 the UK High Court upheld Privacy's challenge and ruled that the security and intelligence services could no longer rely on 'general warrants' to interfere with property, including the hacking of computers[74].

Campaigners have also sought to test specifically whether the US forces at

Menwith Hill may be acting illegally under UK data-protection law. In 2018 Reprieve called on the UK's Information Commissioner to investigate US activities at Menwith Hill, alleging that they are collecting and processing personal data without registering with the information watchdog. However the Information Commissioner told the group that they hadn't the capacity to investigate every complaint[75].

A slew of courts have found that the NSA and GCHQ surveillance programmes unveiled by the Snowden leaks were operating illegally. However the response by the UK and US Governments has not been to shut these programmes down but instead to attempt to rebuild a legal foundation for the mass-surveillance system in order that they should continue.

The 2016 Investigatory Powers Act (IPA) was passed largely in response to the scandal around the UK's unveiled mass-surveillance system. The law adds some oversight provisions but it has been criticised by campaign groups as a "snoopers' charter"[76].

The law explicitly legalises hacking by the security services, including collecting "bulk personal datasets" where the "majority of individuals" aren't suspected of any wrongdoing but have been swept-up in the data-collection process[77].
Under the Act a total of 48 public authorities, including the Metropolitan Police, GCHQ, the Ministry of Defence and the Department for Work and Pensions, all have access to Internet connection records and Internet Service Providers have to store their users' metadata, the websites they visit and what time they do it as well as what device they use.

The IPA was heavily criticised by the public, with a petition calling for the law to be repealed gathering more than 200,000 signatures[78].

The UN's privacy chief criticised the law while it was under consideration in Parliament in 2016, saying that the intelligence provisions in the bill – particularly those of bulk hacking and bulk interception of data – "run counter to the most recent judgements of the European Court of Justice and the European Court of Human Rights, and undermine the spirit of the very right to privacy."[79]

"Intelligence provisions in the IPA – particularly those of bulk hacking and bulk interception of data – "run counter to the most recent judgements of the European Court of Justice and the European Court of Human Rights, and undermine the spirit of the very right to privacy."

Lord Strasburger, a Liberal Democrat peer who sat on the Joint Select Committee scrutinising the Government's bill, publicly called for it "to be fundamentally rethought and rebuilt", commenting that "Basically, the Home Office doesn't do privacy. It does security and ever more intrusive powers they claim will make us safer, but not privacy."[80]

GCHQ, Cheltenham Source: UK Govt MoD

The law has been challenged by civil-liberties campaigners at Liberty, who argued successfully before the High Court in 2018 that the Act was incompatible with EU law in the way that it allowed state agencies to access data held by telecommunications operators. The ruling forced the Act to be amended. Liberty is currently appealing against a 2019 ruling from the High Court that the 'bulk powers' do not breach the right to privacy and the right to freedom of expression and that the Act does contain sufficient safeguards for journalistic and legal communications[81].

PARLIAMENTARY OVERSIGHT

There also appears to be a lack of ongoing scrutiny of GCHQ's programmes in Parliament's processes. In 2013, following the publication of the Snowden leaks, the former cabinet minister Chris Huhne, who while in Government sat on the National Security Council, revealed that he had been unaware of several GCHQ programmes and capabilities. Huhne said that his fellow ministers were also in "utter ignorance" of GCHQ's TEMPORA and PRISM programmes[82]. Huhne noted that at the time the Home Office had argued for the need for a communications data bill to enable surveillance to be carried out without revealing that GCHQ already had remarkably extensive capabilities. Huhne explained, "Throughout my time in parliament, the Home Office was trying to persuade politicians to invest in 'upgrading' Britain's capability to recover data showing who is emailing and phoning whom. Yet this seems to be exactly what GCHQ was already doing. Was the Home Office trying to mislead?" and "This lack of information, and therefore accountability, is a warning that the supervision of our intelligence services needs as much updating as their bugging techniques."[83]

Also in 2013 Charles Farr, then Director General of the Office for Security and Counter-Terrorism, told a parliamentary committee that he too was unaware of some of the GCHQ and NSA operations exposed by Snowden[84].

In fact a leaked GCHQ memo revealed that the agency feared a "damaging public debate" on the scale of its activities because it could lead to legal challenges against its mass-surveillance programmes. The document recorded GCHQ's position as part of a political debate in 2009 over making telephone-intercept evidence admissible in criminal trials, which the agency opposed[85]. According to the documents GCHQ feared possible legal challenges on whether their programmes violated the right to privacy if evidence of its surveillance methods became admissible in court.

GCHQ also worked to assist the Government with "press handling" by lining up advocates including the Liberal Democrat peer and former intelligence services commissioner Lord Carlile[86].

Part of Parliament's role is to control and provide oversight of all Government services and state operations, either direct or indirectly via ministers, through public and Parliamentary accountability. The legitimate need for some secrecy around security matters means that there is inevitably some need to balance accountability with confidentiality concerning the security services. However the UK's oversight mechanism is notably

secretive and limited.

Parliamentary oversight of GCHQ and other UK intelligence services is carried out through the Intelligence and Security Committee (ISC) but this committee works in a radically different way from other parliamentary committees that oversee other parts of Government.

Unlike other parliamentary committees, members are nominated by the Prime Minister in consultation with opposition party leaders before being approved by Parliament. Members are security-vetted and are often selected on the basis of former ministerial or other roles that interacted with the security services. The Committee's hearings are usually private, unlike most other committees' public sessions, and nearly all security and intelligence personnel giving evidence to the Committee are heard in private. The Committee's reports are usually heavily vetted to avoid revealing any secret information[87].

A 2014 report of the Commons' Home Affairs Committee found that the Committee's set-up risked "the potential for political deference" [to ministers and the intelligence services] and "the over-identification of the members with the security and intelligence services"[88].

An ISC report in the wake of the Snowden leaks did acknowledge that intelligence agencies needed to "step out of the shadows" – a contrast with the politicians and spy chiefs who had previously condemned Snowden as a traitor and questioned the patriotism of reporters for publishing his disclosures. The Committee did recommend some safeguards but also recommended limiting any transparency. The report was criticised as hollow, especially as it came on the heels of legal rulings finding the intelligence agencies had been operating illegally[89].

The risks for politicisation of the ISC came to the fore in 2019 and 2020 when the Committee prepared a report on Russian interference with UK politics and public life. The report was sent to the Government for clearance in October 2019, two months before a General Election, but was not released until July 2020.

After the 2019 election the Government delayed the reinstatement of the ISC for nine months, months in which no parliamentary oversight of the intelligence services was possible.

The Government attempted to impose former minister Chris Grayling as chairperson of the Committee by nominating him and other Conservative members who vowed to vote for Grayling despite his questionable record in Government and his lack of experience in security matters[90]. The Justice and Security Act 2013 sets specific rules for the Committee, specifying that the Committee elects its own chair from among its members[91].

In July 2020 Julian Lewis, a Conservative former chair of the Defence Committee, stood against Grayling in the election for the chair and was elected with the support of the opposition members of the Committee. In response the Conservative Party punished Lewis, expelling him from the Parliamentary Conservative Party[92]. The ISC published the report into Russian interference shortly afterwards.

Whether the episode was down to fear of the contents of the report becoming public or part of a wider attempt to impose control on parliamentary committees by the Government, the current Government clearly attempted to curtail further what limited independent oversight there is over the security services. On the other hand the drama demonstrates that there are MPs who will fight for their independence in oversight roles and that they are a crucial part of holding the Government and its agencies accountable.

MPs and ministers being kept in the dark over crucial security matters raises serious questions about whether any truly effective oversight exists over the types of activity GCHQ carries out at Menwith Hill and other similar installations. The recent attempt by the current Government to manipulate the ISC, the main parliamentary oversight over the security services, shows how limited the oversight functions are and how perilously close they came to being seriously interfered with.

65. Reuters, 2/9/2020, "US court: Mass surveillance program exposed by Snowden was illegal", **https://www.reuters.com/article/us-usa-nsa-spying/us-court-mass-surveillance-program-exposed-by-snowden-was-illegal-idUSKBN25T3CK**

66. Privacy International, 6/2/2015, "GCHQ-NSA intelligence sharing unlawful, says UK surveillance tribunal", **https://privacyinternational.org/press-release/1544/gchq-nsa-intelligence-sharing-unlawful-says-uk-surveillance-tribunal**

67. House of Commons Library, 28/5/2019, "What does the Supreme Court's ruling on the Investigatory Powers Tribunal mean for parliamentary sovereignty?", **https://commonslibrary.parliament.uk/what-does-the-supreme-courts-ruling-on-the-investigatory-powers-tribunal-mean-for-parliamentary-sovereignty/**

68. Amnesty International, 12/1/2018, "UK government's mass spying ruled unlawful", **https://www.amnesty.org.uk/uk-government-gchq-ipt-mass-spying-surveillance**

69. Privacy International, 4/2018, "Policy Briefing – UK Intelligence Sharing Arrangements"

70. Privacy International, "10 Human Rights Organisations v. United Kingdom", **https://privacyinternational.org/legal-action/10-human-rights-organisations-v-united-kingdom**

71. Investigatory Powers Tribunal, 23/7/2018, Case Number IPT/15/110/CH, "Final Judgment - Privacy International and (1) Secretary of State for Foreign and Commonwealth Affairs and others", **https://www.ipt-uk.com/judgments.asp?id=45** ; Privacy International, 23/7/2018, "Legal judgment finds successive foreign secretaries unlawfully gave GCHQ free rein to collect our data", **https://privacyinternational.org/press-release/2206/press-release-legal-judgment-finds-successive-foreign-secretaries-unlawfully**

72. European Court of Human Rights, 13/9/2018, Big Brother Watch and Others v. the United Kingdom - complaints about surveillance regimes, **http://hudoc.echr.coe.int/eng-press?i=003-6187848-8026299** Wired, 13/9/2018 **,** "The UK's mass surveillance regime has broken the law (again)", **https://www.wired.co.uk/article/uk-mass-surveillance-echr-ruling**

73. Privacy International, "The Queen on the application of Privacy International v. Investigatory Powers Tribunal (UK General Hacking Warrants)", January 2021, **https://privacyinternational.org/legal-action/queen-application-privacy-international-v-investigatory-powers-tribunal-uk-general**

74. Privacy International, 8/01/2021, "Victory at the High Court against the government's use of 'general warrants'", **https://privacyinternational.org/news-analysis/4359/victory-high-court-against-governments-use-general-warrants**

75. The Guardian, 29/5/2018, "US eavesdropping base in Yorkshire flouting UK law, claims group", **https://www.theguardian.com/world/2018/may/29/us-eavesdropping-base-in-yorkshire-flouting-uk-law-menwith-hill**

76. ComputerWorld, 31/7/2019,"The Snoopers' Charter: Everything you need to know about the Investigatory Powers Act", **https://www.computerworld.com/article/3427019/the-snoopers-charter-everything-you-need-to-know-about-the-investigatory-powers-act.html**

77. UK Parliament, Investigatory Powers Act, https://www.legislation.gov.uk/ukpga/2016/25/contents/enacted; Wired, 8/5/2017, "What is the IP Act and how will it affect you?", **https://www.wired.co.uk/article/ip-bill-law-details-passed**

78. UK Parliament, "Repeal the new Surveillance laws (Investigatory Powers Act)", **https://petition.parliament.uk/archived/petitions/173199**

79. Wired, 9/3/2016, "UN warns UK's IP Bill 'undermines' the right to privacy", **https://www.wired.co.uk/article/un-privacy-ip-bill-not-compliant-international-law**

80. Wired, 11/2/2016, "Snooping law must be 'fundamentally rethought and rebuilt,' Lord Strasburger says", **https://www.wired.co.uk/article/strasburger-ip-bill-rewritten**

81. Liberty, "Legal Challenge: Investigatory Powers Act", **https://www.libertyhumanrights.org.uk/issue/legal-challenge-investigatory-powers-act/**

82. The Guardian, 6/10/2013, "Cabinet was told nothing about GCHQ spying programmes, says Chris Huhne", **https://www.theguardian.com/uk-news/2013/oct/06/cabinet-gchq-surveillance-spying-huhne**

83. The Guardian, 6/10/2013, "Cabinet was told

nothing about GCHQ spying programmes, says Chris Huhne", **https://www.theguardian.com/uk-news/2013/oct/06/cabinet-gchq-surveillance-spying-huhne**

84. Evening Standard, 13/11/2013, "Terror boss 'unaware of GCHQ ops'", **https://www.standard.co.uk/panewsfeeds/terror-boss-unaware-of-gchq-ops-8933663.html**

85. The Guardian, 25/10/2013, "Leaked memos reveal GCHQ efforts to keep mass surveillance secret", **https://www.theguardian.com/uk-news/2013/oct/25/leaked-memos-gchq-mass-surveillance-secret-snowden**

86. The Guardian, 25/10/2013, "Leaked memos reveal GCHQ efforts to keep mass surveillance secret", **https://www.theguardian.com/uk-news/2013/oct/25/leaked-memos-gchq-mass-surveillance-secret-snowden**

87. Democratic Audit, 3/10/2018, "How accountable are the UK's security and intelligence services to Parliament?", **https://www.democraticaudit.com/2018/10/03/audit2018-how-accountable-are-the-uks-security-and-intelligence-services-to-parliament/**

88. Home Affairs Committee, 2014, Seventeenth Report Counter-terrorism", **https://publications.parliament.uk/pa/cm201314/cmselect/cmhaff/231/23102.htm**

89. The Guardian, 12/3/2015, "ISC report acknowledges failings but paves way for snoopers' charter", **https://www.theguardian.com/us-news/2015/mar/12/intelligence-agencies-finally-understand-need-to-step-out-of-the-shadows**

90. The Guardian, 16/7/2020, "Julian Lewis: attempt to impose Grayling was 'improper request'", **https://www.theguardian.com/politics/2020/jul/16/julian-lewis-attempt-to-impose-grayling-was-improper-request**

91. Prospect, 16/7/2020, "Julian Lewis strikes a blow for parliamentary integrity", **https://www.prospectmagazine.co.uk/politics/julian-lewis-strikes-a-blow-for-parliamentary-integrity-chris-grayling-isc-intelligence-security-committee**

92. BBC News Online, 16/7/2020."Russia report: New intelligence committee chair loses Tory whip",. **https://www.bbc.co.uk/news/uk-politics-53422010**

DRONE WARFARE

A Reaper MQ-9 Remotely Piloted Air System (RPAS) prepares for take-off in Afghanistan
Source: https://www.defenceimagery.mod.uk/fotoweb/archives/5042-Downloadable%20Stock%20Images/Archive/MOD/45152/45152585.jpg (Used under the Open Government Licence)

Between 2010 and 2020 more than 14,000 drone strikes were carried out by US forces, killing somewhere between 8,858 and 16,901 people according to a database created by the Bureau for Investigative Journalism, which estimates that between 910 and 2,200 of the victims were civilians, including between 283 and 454 children[93].

In recent years the UK has joined the US in using drone strikes both in recognised warzones and as part of a "targeted killing" strategy – a term that has been criticised as euphemistically describing an assassination or extrajudicial execution programme[94].

The UK's assassination strategy emerged in 2015 when David Cameron announced "a new departure" for Britain, where a British citizen could be intentionally killed outside of any warzone[95]. The first victim of this policy was Reyaad Khan, a British member of Islamic State, who was killed by an RAF drone in Syria[96].

The UK Government has been criticised, including by the Intelligence and Security Committee (ISC), for its secrecy around the programme and the killing of Khan. The Committee chair expressed "profound" disappointment after the Government blocked access to key evidence and ministerial decision-making material, evading oversight[97].

In 2016 Parliament's Joint Committee on Human Rights investigated the UK's policy on lethal drone strikes. The report found that UK personnel would be in "considerable doubt about whether what they are being asked to do is lawful" and that it "may therefore expose them, and Ministers, to the risk of criminal prosecution for murder or complicity in murder." [98]

Jeremy Wright, the UK Attorney General, claimed in 2017 that no "specific" advance evidence of a terror plot threatening UK interests was legally necessary before launching pre-emptive drone strikes against suspects overseas. Wright argued in a public speech that "where the evidence supports an assessment that an attack is imminent it cannot be right that a state is prevented from meeting its first duty of protecting its citizens without nailing down the specific target and timing of an attack. Apart from anything else, our enemies will not always have fixed plans. They are often opportunists." [99]

In a 2018 article for the Spectator Boris Johnson suggested the UK took drone strikes not only in self-defence against an imminent threat to the UK but also as "payback" or revenge[100].

The prospect of UK Government officials deciding behind closed doors on whether or not to kill a British citizen extra-judicially at all, let alone on the basis of a secretive and vague process, should alarm the public.

DATA-DRIVEN DRONE STRIKES

US drone strikes are not limited to the regular US military: hundreds of strikes have been carried out in Yemen, Pakistan and Somalia by the secretive Central Intelligence Agency and Joint Special Operations Command at the Pentagon[101].

Although many US drone strikes have taken place as part of actual armed conflicts, the US also asserts the right to target and deliberately kill individuals, members of particular groups whom they deem to be a threat to the USA or those believed to have an association with certain of those groups, wherever they are – and often they are far from any recognised battlefield.

These types of strike have been justified either on the basis of a right of self-defence against individuals and groups of people who, it is claimed, pose a real and imminent threat to the USA, or as part of the doctrine that treats the whole world as a battlefield – as part of the "global war on terror"[102].

The number of US drone strikes increased significantly during the Obama administration, which oversaw more drone strikes in Obama's first term than over the whole of the George W. Bush presidency. Donald Trump reportedly rolled back previous restrictions, including the removal of the requirement that drone strikes outside of recognised conflict zones target only high-level members of enemy armed forces and permitting the targeting of a much larger number of individuals – even if they had not been clearly identified [103]. Joe Biden has been criticised for his silence on the issue of US drone wars, leading many to

expect that the programmes will likely continue in a similar vein[104].
During Barack Obama's presidency weekly meetings on drone killings were dubbed "Terror Tuesdays". A grisly slideshow of potential targets was presented, with the US President and his advisers deciding their fate[105]. The state surveillance apparatus, exposed by the Snowden leaks, was key to the logic of targeting individuals for assassination. A former US drone operator, quoted by investigative news outlet 'The Intercept', explained that the NSA helped target people for drone strikes by analysing the location of phones. "It's really like we're targeting a cellphone," said the former drone operator. "We're not going after people — we're going after their phones, in the hopes that the person on the other end of that missile is the bad guy." [106]

"It's really like we're targeting a cellphone," said the former drone operator. "We're not going after people — we're going after their phones, in the hopes that the person on the other end of that missile is the bad guy."

Michael Hayden confirmed this method for identifying targets at a debate at Johns Hopkins University: "We kill people based on metadata." [107]

Intelligence programmes at Menwith Hill have reportedly played a key role in operations to "eliminate" people in Yemen, as part of a deadly drone bombing campaign that has resulted in dozens of civilian deaths in a country that neither the UK nor US has declared war with.

According to documents leaked by Edward Snowden and reported by 'The Intercept', in 2016 Menwith Hill was used to aid "a significant number of capture-kill operations". The NSA developed programmes at Menwith Hill to locate Internet users in remote parts of the world. One programme, created in 2006 and codenamed GHOSTHUNTER, aimed at locating targets when they logged onto the Internet[108]. A 2008 NSA document described the "success of the **GHOSTHUNTER** prototype developed at Menwith Hill Station, a tool that enabled a significant number of capture-kill operations against terrorists." [109]

(U) **Going Global**

(S//SI//REL) The GHOSTHUNTER prototype (see background) capitalized on the co-location of Overhead SIGINT and FORNSAT* at Menwith Hill Station to combine collection from both apertures to perform precise geolocations of VSATs. With APPARITION, this capability will not be limited to collocated sites; it will now be possible for collection from sites ***worldwide*** to be combined with Overhead collection. Plans call for APPARITION to be deployed to a number of FORNSAT and Special Collection Service (SCS) sites in the coming years.

(S//SI//REL) This first APPARITION system builds on lessons learned from the initial GHOSTHUNTER implementation, and represents a more generic concept of operations (CONOP) for use worldwide. Rather than "chasing" the targets when they come on-line in a reactive approach, APPARITION uses an "industrial survey" concept that proactively targets and geolocates VSATs and populates the MASTERSHAKE (see background) database with the results. This approach reduces response time: by interrogating the database, a geolocation of the VSAT can be provided within seconds of the target appearing on-line.

Source: https://www.documentcloud.org/documents/3089509-APPARITION-becomes-a-reality-new-corporate-VSAT.html

GHOSTHUNTER was described in NSA documents being used in 2007 to track a suspected al Qaeda "facilitator" in Lebanon, who was described as "highly actionable," suggesting he had been judged to be a legitimate target to kill or capture[110]. In another 2007 operation **GHOSTHUNTER** was used by Menwith Hill operatives to identify an alleged Al Qaeda weapons-procurer in Iraq after he logged into an email account at an Iraqi Internet café. Spy satellites operated from Menwith Hill took aerial photos of the area and the information was reportedly passed to nearby military commanders for a "targeting plan"[111].

Menwith Hill analysts also tracked members of the Taliban, leading to "approximately 30 enemy killed" – according to a 2011 top-secret report[112].

In 2012 Menwith Hill analysts tracked another target in Helmand Province and within an hour a Predator drone had been called in, presumably to launch an airstrike[113].

Menwith Hill's role was not limited to conventional war zones. The aim of one specific operation, codenamed GHOSTWOLF, was to identify targets at Internet cafes in Yemen's Shabwah province and in the capital, Sana'a. NSA documents linked the method to operations to "capture or eliminate" suspected terrorists in the country, suggesting it was used to provide targets for US drone strikes there[114]. The leaked top-secret documents confirmed for the first time the role of Menwith Hill in targeting US drone strikes in Yemen[115].

(TS//SI//REL) Analysts: The technique described below is currently being used only in Yemen, but it could potentially be applied to internet cafes in other geographic regions, under certain conditions. If you have questions about whether this might work on your target, please contact the author.

(TS//SI//REL) In late 2009, analysts at Menwith Hill Station envisioned a new way to geolocate targets who are active at internet cafés in Yemen: combine HUMINT information with networking protocols and passive SIGINT collection to obtain target geolocations. MHS has collaborated with offices across the enterprise[1] to turn this concept into a new mission capability. Currently, the technique enables the identification of tasked and hot-listed targets active at almost 40 different geolocated internet cafés in Sana'a and Shabwah, Yemen.

(TS//SI//REL) In the short time that results from this technique have been available, many targets have been located to these cafés, including targets tasked by several target offices at NSA[2] and GCHQ. Perhaps most significantly, the technique provides some insight into the movements and activities of terrorist targets in Yemen (Al Qaeda in the Arabian Peninsula and Al Qaeda in East Africa -- both high priorities for the Intelligence Community).

(TS//SI//REL) Most internet users in Yemen access the internet via YemenNet, a telecommunications company and ISP (internet service provider) owned and operated by a subdivision of Yemen's Ministry of Telecommunications and Information technology. YemenNet provides services to subscribers primarily via ADSL, DSL, and dial-up connections by dynamically allocating IPs from a pool of 10000-20000 IP addresses. The use of dynamic IPs and landlines for internet connections means that many traditional geolocation techniques (like GHOSTHUNTER[3]) cannot be applied. Instead, MHS analysts determined they could combine HUMINT information from physical surveys of cafés (MORK data) with Tailored Access Operation (TAO - S32) collection of RADIUS[4] logs (WINDCHASER) and passive collection of target activity (MARINA, XKEYSCORE) to provide target geolocations. The basic steps of the process are:

Source: https://www.documentcloud.org/documents/3089514-New-technique-geolocates-targets-active-at.html

The casualty-tracking group Airwars found that US drone strikes in Yemen during the Trump administration killed at least 86 civilians, including 28 children[116].

In 2020 a US drone strike was used to assassinate top Iranian military official Qasem Soleimani in Baghdad[117]. The strike, approved by President Trump, provoked retaliatory Iranian missile strikes on US forces in Iraq that threatened to spill into outright war[118]. The killing of an Iranian official in Iraq without any congressional approval nor evidence of any imminent threat posed by Soleimani appeared likely to be illegal under US, Iraqi and international law. The killing was not approved by the US Congress nor Iraqi Government. The Trump administration claimed it was authorized under both the Constitution and a 2002 'Authorization of Use of Military Force Against Iraq'. However, as Chairman of the House Committee on Foreign Affairs Engel pointed out, "The 2002 authorization was passed to deal with Saddam Hussein. This law had nothing to do with Iran or Iranian Government officials in Iraq. To suggest that 18 years later this authorization could justify killing an Iranian official stretches the law far beyond anything Congress ever intended."

The United Nations special rapporteur investigating extrajudicial and summary executions reported that the killing was unlawful under international law given the lack of evidence that Soleimani posed any imminent threat[119]. An Iraqi court issued an arrest warrant for Trump on a charge of premeditated murder[120].

Activists and a British MP have raised concerns that Menwith Hill may have played a part in the killing given the base's role in other targeted killings in the Middle East by US forces. In response to a parliamentary question by Alex Sobel, MP for Leeds North-West, asking whether Menwith Hill had a role in the killing, a Government minister would only state: "In accordance with long-standing policy we do not comment on the details of the operations carried out at RAF Menwith Hill in providing intelligence support."

The involvement of the UK and Menwith Hill in an assassination that threatened to spark a war should be of great concern. The UK Government's failure to assure the public that the base was not involved raises deep questions about the accountability for actions at the base.

According to Amnesty International, in addition to Menwith Hill, other UK RAF bases – RAF Croughton in Northamptonshire, RAF Molesworth in Cambridgeshire and RAF Digby in Lincolnshire – all allegedly contribute support to the US lethal-drone programme through logistics, communications or support for surveillance and intelligence operations.

THE ROLE OF OTHER US BASES IN THE UK[121]

A total of 11 bases in the UK, including Menwith Hill, are designated for use by US forces:

- RAF Alconbury
- RAF Barford St John
- RAF Croughton
- RAF Fairford
- RAF Feltwell
- RAF Lakenheath
- RAF Menwith Hill
- RAF Mildenhall
- RAF Molesworth
- RAF Welford
- Blenheim Crescent

The majority of staff at these bases and the Commanding Officer will be from the US.

For example RAF Croughton reportedly has a direct fibre-optic communications link with Camp Lemonnier, a US military base in Djibouti from which most US drone strikes on Yemen and Somalia are carried out[122].

Other bases act as airfields for US air squadrons. RAF Lakenheath in Suffolk is the base for two squadrons of US F-35 multi-role aircraft[123]. The supersonic stealth aircraft are capable of dropping nuclear bombs[124]. RAF Lakenheath has also been the base for US F-15 fighter jets[125], which are also capable of dropping nuclear bombs[126]. In 2008 the 110 nuclear weapons US forces stored at Lakenheath were reportedly withdrawn. The move followed consistent anti-nuclear protest[127].

As previously mentioned, RAF Fylingdales in Yorkshire provides intelligence and communications support, including the hosting of a powerful radar that forms part of the US/UK Ballistic Missile Early-Warning System (BMEWS). Flight Lieutenant Rich Weeks, quoted in a 2019 article for the armed forces broadcaster 'Forces.net', explained that the role of the base makes it a likely target for a missile strike in the event of conflict. "If we were a target, we would've already completed our mission, so our mission would've already been done," he said. "That's the mindset of the people that work here." [128]

93. Bureau for Investigative Journalism, "Drone Warfare", accessed on 31/1/2020, **https://www.thebureauinvestigates.com/projects/drone-war**

94. New York Times, 7/3/2018, "Learning From Israel's Political Assassination Program", **https://www.nytimes.com/2018/03/07/books/review/ronen-bergman-rise-and-kill-first.html**

95. Hansard, 9/9/2015, Column -399, **https://publications.parliament.uk/pa/cm201516/cmhansrd/cm150909/debtext/150909-0001.htm#150909-0001.htm_spnew19**

96. The Guardian, 26/4/2017, "Briton killed in drone strike on Isis 'posed serious threat to UK'", **https://www.theguardian.com/uk-news/2017/apr/26/briton-killed-in-drone-strike-on-isis-posed-serious-threat-to-uk-reyaad-khan**

97. The Guardian, 26/4/2017, "Briton killed in drone strike on Isis 'posed serious threat to UK'", **https://www.theguardian.com/uk-news/2017/apr/26/briton-killed-in-drone-strike-on-isis-posed-serious-threat-to-uk-reyaad-khan**

98. UK Parliament, Joint Committee on Human Rights, 27/4/2016, "The Government's policy on the use of drones for targeted killing", **https://publications.parliament.uk/pa/jt201516/jtselect/jtrights/574/574.pdf**

99. The Guardian, 11/1/2017, "'Specific' terror evidence not necessary for RAF drone strikes", **https://www.theguardian.com/world/2017/jan/11/raf-drone-strikes-terror-attorney-general**

100. The Spectator, 28/7/2018, "Boris Johnson – Diary 26 July 2018", **https://www.spectator.co.uk/article/diary---26-july-2018**

101. Bureau for Investigative Journalism, "History Of Drone Warfare", **https://www.thebureauinvestigates.com/explainers/history-of-drone-warfare**

102. Amnesty International, 2018, "Deadly Assistance: The Role Of European States In US Drone Strikes", **https://www.amnesty.org.uk/files/2018-04/Deadly%20Assistance%20Report%20WEB.pdf?nnxzvq2lenq0LiFu64kg6UtyT2I8Zs3B**

103. Amnesty International, 2018, "Deadly Assistance: The Role Of European States In US Drone Strikes", p4, **https://www.amnesty.org.uk/files/2018-04/Deadly%20Assistance%20Report%20WEB.pdf?nnxzvq2lenq0LiFu64kg6UtyT2I8Zs3B**

104. The Intercept, 22/11/2020, "Joe Biden's Silence On Ending The Drone Wars", **https://theintercept.com/2020/11/22/biden-drones-endless-wars/**

105. The Guardian, 14/7/2013, "Obama's secret kill list – the disposition matrix", **https://www.theguardian.com/world/2013/jul/14/obama-secret-kill-list-disposition-matrix**

106. The Intercept, 30/11/2017, Ryan Gallagher, "U.K. Government Pressured Over Secret Base's Role In Trump's Drone Strikes", **https://theintercept.com/2017/11/30/drone-strikes-gchq-trump-menwith-hill-uk/**

107. The Intercept, 30/11/2017, Ryan Gallagher, "U.K. Government Pressured Over Secret Base's Role In Trump's Drone Strikes", **https://theintercept.com/2017/11/30/drone-strikes-gchq-trump-menwith-hill-uk/**

108. The Intercept, 6/9/2016, "Inside Menwith Hill", **https://theintercept.com/2016/09/06/nsa-menwith-hill-targeted-killing-surveillance/**

109. **https://www.documentcloud.org/documents/3089509-APPARITION-becomes-a-reality-new-corporate-VSAT.html**

110. The Intercept, 6/9/2016, "Inside Menwith Hill", **https://theintercept.com/2016/09/06/nsa-menwith-hill-targeted-killing-surveillance/**

111. The Intercept, 6/9/2016, "Inside Menwith Hill", **https://theintercept.com/2016/09/06/nsa-menwith-hill-targeted-killing-surveillance/**

112. The Intercept, 6/9/2016, "Inside Menwith Hill", **https://theintercept.com/2016/09/06/nsa-menwith-hill-targeted-killing-surveillance/; https://www.documentcloud.org/documents/3089519-Afghanistan-30-enemy-killed-Jan-Feb-2012.html**

113. The Intercept, 6/9/2016, "Inside Menwith Hill", **https://theintercept.com/2016/09/06/nsa-menwith-hill-targeted-killing-surveillance/;**

114. The Intercept, 30/11/2017, Ryan Gallagher, "U.K. Government Pressured Over Secret Base's Role In Trump's Drone Strikes", **https://theintercept.com/2017/11/30/drone-strikes-gchq-trump-menwith-hill-uk/**

115. The role of UK intelligence and military forces in Yemen and Drone Strikes is also explored in Vice News, 7/4/2016, "Britain's Covert War in Yemen", **https://www.vice.com/en/article/8x3enb/britains-covert-war-in-yemen-a-vice-news-investigation**

116. Airwars, 28/10/2020, "Trump in Yemen: New Airwars study shines light on opaque campaign", **https://airwars.org/news-and-investigations/trump-in-yemen-new-study-shines-light-on-campaign/**

117. BBC News, 4/1/2020, "Qasem Soleimani: Thousands mourn assassinated Iranian general", **https://www.bbc.co.uk/news/world-middle-east-50991810**

118. Reuters, 10/2/2020, "More than 100 US troops diagnosed with brain injuries from Iran attack", **https://www.reuters.com/article/us-usa-pentagon-tbi-exclusive/exclusive-more-than-100-u-s-troops-diagnosed-with-brain-injuries-from-iran-attack-officials-idUSKBN2041ZK**

119. New York Times, 9/7/2020, "The Killing of Qassim Suleimani Was Unlawful, Says U.N. Expert", **https://www.nytimes.com/2020/07/09/world/middleeast/qassim-suleimani-killing-unlawful.html?referringSource=articleShare**

120. Bloomberg, 7/1/2021, "Iraq Issues Arrest Warrant for Trump Over Soleimani Killing", **https://www.bloomberg.com/news/articles/2021-01-07/iraq-court-issues-arrest-warrant-against-trump-for-murder**

121. UK Defence Journal, 22/6/2020"Which British Bases are designated for use by NATO and the US?", **https://ukdefencejournal.org.uk/which-british-bases-are-designated-for-use-by-nato-and-the-us/**

122. Amnesty International, 2018, "Deadly Assistance: The Role Of European States In US Drone Strikes", **https://www.amnesty.org.uk/files/2018-04/Deadly%20Assistance%20Report%20WEB.pdf?nnxzvq2lenq0LiFu64kg6UtyT2I8Zs3B**

123. Parliamentary written statement from Michael Fallon The Secretary of State for Defence, 8/1/2015, HC Deb, 8 January 2015, c13WS, **https://www.theyworkforyou.com/wms/?id=2015-01-08a.13WS.6&s=menwith#g13WS.7**

124. Popular Mechanics, 24/11/2020, "Declassified: Watch an F-35 Drop a Dummy Thermonuclear Bomb", **https://www.popularmechanics.com/military/weapons/a34775048/watch-f-35-drop-b-61-thermonuclear-bomb/**

125. Royal Air Force Lakenheath, "48th Fighter Wing Fact Sheet", **https://www.lakenheath.af.mil/About-Us/Fact-Sheets/48th-Fighter-Wing-Fact-sheet/**

126. DefenseNews, 8/6/2020, "F-15E becomes first aircraft compatible with new nuclear bomb design", **https://www.defensenews.com/smr/nuclear-arsenal/2020/06/08/f-15e-becomes-first-aircraft-certified-for-new-nuclear-bomb-design/**

127. Guardian, 26/6/2008, "US removes its nuclear arms from Britain", **https://www.theguardian.com/world/2008/jun/26/usforeignpolicy.nuclear; Federation of American Scientists, 26/6/2008,** "US Nuclear Weapons Withdrawn From the United Kingdom", **https://fas.org/blogs/security/2008/06/us-nuclear-weapons-withdrawn-from-the-united-kingdom/**

128. Forces.net, 15/11/2019, "RAF Fylingdales: What Does The Royal Air Force Station Do?", **https://www.forces.net/news/raf-fylingdales-what-does-royal-air-force-station-do**

LEGALITY OF ASSISTING IN DRONE STRIKES

The American Civil Liberties Union (ACLU) argues that the US targeted-killing programme is illegal under the US Constitution and international law[129].

The decision-making process behind US drone strikes is shrouded in secrecy. In October 2017 the Trump administration secretly adopted new looser rules governing lethal force in drone strikes and other killings abroad. According to media reports the new Trump rules eliminated the requirement that a person must present a "continuing, imminent" threat to the United States before being targeted for killing[130]. The new rules also reportedly removed a vetting requirement that meant that attacks required prior approval from top officials from the Departments of State, Defense, Justice, and Homeland Security as well as the Director of National Intelligence, CIA, the National Counterterrorism Center and Joint Chiefs of Staff. If the agency officials did not reach a consensus then the President personally had to approve a strike. The revised rule shifts more authority to the CIA and the Pentagon, leaving even fewer safeguards against people being killed illegally[131].

The ACLU went to court to try to force disclosure of the rules for attacks. In response the administration refused even to admit the existence of a new policy. The courts rebuked the Trump administration in September 2020, ruling that the existence of the rules could not be kept a secret, although the policy itself could remain secret[132].

It has been reported that the UK, Germany, the Netherlands and Italy have all played a significant role in providing operational and logistical support to the US lethal drone programme as well as collaborating in intelligence gathering used to support the programme[133].

In the UK a civil case brought by Abdul-Hakim Belhaj, a former opponent of the Gaddafi regime in Libya, set an important precedent, establishing that the UK Government can face legal liability for collaborating with foreign states in illegal acts.

In 2004 Belhaj and his pregnant wife, Fatima Boudchar, were detained and tortured in a CIA blacksite in Bangkok and then rendered to Libya. In the same month another opponent of Gaddafi, Sami al-Saadi, together with his wife and two young children, were abducted in Hong Kong and rendered to Libya. Once in Libya Abdul-Hakim Belhaj and Sami al-Saadi were detained, tortured and subjected to unfair trials before both being sentenced to death. They were later released in March 2010. When the Gaddafi regime fell in 2011 secret documents were found in the offices of Libyan intelligence officials that showed the apparent involvement of the British security services – MI5 and MI6 – in the rendition of Belhaj, Sami al-Saadi and others.

The families of Sami al-Saadi and Abdul-Hakim Belhaj brought a lawsuit against the British authorities for their ordeal. Sami al-Saadi and his family agreed a settlement of £2.23 million. Belhaj and Boudchar made an offer to settle their claim for £1, but only on the condition of a public apology and an admission of liability. Their offer was not accepted. In 2013 the UK Government attempted to have the claim dismissed on the grounds that it involved the alleged acts of other

states and might give rise to criticism of those states, particularly the US. In 2017 the courts ruled in favour of Belhaj and Boudchar.

The ground-breaking decision opened the UK authorities to accountability for their role in illegal operations that involve other states. On 10 May 2018 the Attorney General, Jeremy Wright QC MP, gave an unreserved apology to Belhaj and Boudchar on behalf of the Prime Minister for the UK Government's role in "their detention, rendition and suffering"[134].

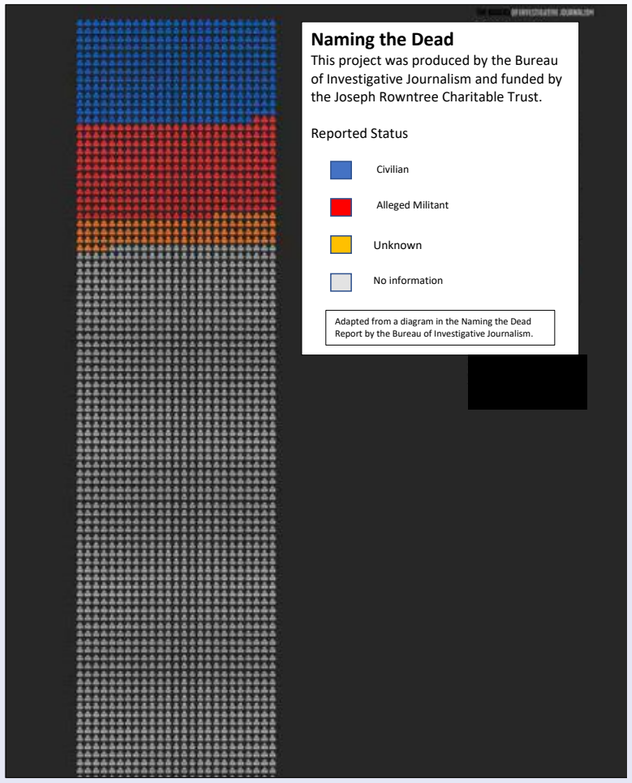
A German court ruling in 2019 has added to the possible legal peril in assisting in drone strikes.

In March 2019 an appeal court in Germany ruled in favour of Faisal Bin Ali Jaber, a Yemeni engineer, who had argued that the German Government had a responsibility to prevent US forces using Ramstein Airbase in unlawful drone strikes in Yemen. In August 2012 US drone strikes had killed Salem bin Ali Jaber, Faisal's brother-in-law (an imam who preached against Al Qaeda) and his nephew Waleed, a policeman. Faisal's relatives were offered $100,000 as compensation from Yemeni intelligence but the US has not admitted responsibility.

The appeal court found that Faisal and his family "are justified in fearing risks to life and limb from US drone strikes that use Ramstein Air base in violation of International Law". The German Government denied any knowledge of or responsibility for the drone-strikes ruling[135].

The Ramstein airbase provides essential satellite relay infrastructure for US drones and the German court found that there were "weighty indicators to suggest that at least part of the US armed drone strikes ... in Yemen are not compatible with international law and that plaintiffs' right to life is therefore unlawfully compromised." [136]

The United Nations' special rapporteur on extrajudicial executions, Agnès Callamard, called the ruling a "watershed" decision that brings the US Government's legal justification of lethal drone strikes into question. The ruling was overturned in November 2020 by Germany's highest administrative court. However the brave challenge by Faisal Bin Ali Jaber is likely to raise concerns in the corridors of power that there could be accountability for assisting in drone strikes.



Naming the Dead
Source: Bureau of Investigative Journalism Infographic
https://www.thebureauinvestigates.com/namingth-edead/visualisation/

DIPLOMATIC IMMUNITY

In 2019 Harry Dunn was riding his motorcycle near Croughton in Northamptonshire when he was struck and killed by Anne Sacoolas, who was driving in the opposite direction on the wrong side of the road. Sacoolas was reported to be a former CIA officer and is married to Jonathon Sacoolas, a CIA operative who was working at the US communications and surveillance station at Croughton[137].

Sacoolas admitted that she had been driving the car on the wrong side of the road but she fled the UK, claiming diplomatic immunity[138].

The English High Court ruled in November 2020 that Sacoolas did have diplomatic immunity. A spokesperson for Dunn's family said they would appeal against the ruling[139]. The Crown Prosecution Service has called on Sacoolas to return to the UK to face a criminal trial[140].

In a US civil lawsuit brought by Dunn's family, Sacoolas' lawyers revealed that at the time of the crash she was employed by a US intelligence agency and that was "especially a factor" in why she chose to flee the UK. The UK Government has claimed it was unaware she was working for an intelligence agency at the time[141].

In the course of legal cases brought by Harry Dunn's family, documents were released by the UK Government that revealed that around 200 American civilian and technical staff at Croughton were given diplomatic immunity for activities linked to the war on terror in 2006. The Times reported that this bulk immunity may still be in place.

The Times said the admission by the Government raised questions over whether the immunity might be related to drone strikes or extraordinary rendition. "The only thing I can think of that makes sense is that they were involved in things which might have been in breach of British law, such as rendition," former cabinet minister David Davis told The Times.

Unnamed Whitehall sources cited by The Times said it was wrong to assume that the immunity was given for such purposes and that there was a variety of possible technical reasons[142].

In October 2020 the Government stated that the US personnel based at Menwith Hill as well as The [US] Joint Intelligence and Analysis Center at Molesworth and bases at Fairford, Lakenheath and Mildenhall do not hold diplomatic immunity[143].

The potential for a similar incident to occur at Menwith Hill is obvious. In August 2015 an MHAC campaigner, Barbara Penny from Harrogate, was seriously injured when she was hit by a car outside the Menwith Hill base.

Incident at Nessfield Gate, Menwith Hill
photo by Tim Harberd

Penny settled out of court for damages and the driver was charged with causing

grievous bodily harm but acquitted by a jury at trial[144].

The difficulty of securing justice for the killing of Harry Dunn, the discovery that Anne Sacoolas was employed by an intelligence agency without the UK's knowledge and the revelation of bulk immunity for foreign military and intelligence personnel raise grave questions over the ability to hold US forces accountable in the UK and the safety of residents near US bases.

GCHQ, NSA and the Ministry of Defence were asked for comment regarding the allegations in this report. GCHQ and NSA did not respond. A Ministry of Defence spokesperson declined to respond to specific points but stated that "RAF Menwith Hill is part of a worldwide US Defence communications network, with the base supporting a variety of communications activity. US forces maintain robust civilian and military cooperation with the United Kingdom and manage all base activities in accordance with the agreements made between the United States and Her Majesty's Government."

129. ACLU, "Targeted Killing", **https://www.aclu.org/issues/national-security/targeted-killing**

130. New York Times, 21/9/2017, "Trump Poised to Drop Some Limits on Drone Strikes and Commando Raids", **https://www.nytimes.com/2017/09/21/us/politics/trump-drone-strikes-commando-raids-rules.html**

131. Human Rights Watch, 26/ 7/2017, "How Obama's Drones Rulebook Enabled Trump", **https://www.hrw.org/news/2017/09/26/how-obamas-drones-rulebook-enabled-trump**

132. ACLU, 6/10/2020, "ACLU V. DOD - FOIA Case Seeking Trump Administration's Secret Rules For Lethal Strikes Abroad", **https://www.aclu.org/cases/aclu-v-dod-foia-case-seeking-trump-administrations-secret-rules-lethal-strikes-abroad**

133. Amnesty International, 2018, "Deadly Assistance: The Role Of European States In US Drone Strikes", **https://www.amnesty.org.uk/files/2018-04/Deadly%20Assistance%20Report%20WEB.pdf?nnxzvq2lenq0LiFu64kg6UtyT2I8Zs3B**

134. Leigh Day, "Lawyers for Libyan couple welcome Government apology over illegal rendition", **https://www.leighday.co.uk/latest-updates/news/2018-news/lawyers-for-libyan-couple-welcome-government-apology-over-illegal-rendition/**

135. **ecchr.eu/en/case/important-judgment-germany-obliged-to-scrutinize-us-drone-strikes-via-ramstein/**

136. Reprieve, 19/03/2019, "UK 'on notice' after court rules Germany failed in duty to protect innocent civilians from US drones", **https://reprieve.org/uk/2019/03/19/uk-on-notice-after-court-rules-germany-failed-in-duty-to-protect-innocent-civilians-from-us-drones/**

137. The Telegraph, 22/10/2019 , "Police chief in charge of Harry Dunn car crash case says he would not do anything differently as he admits his officers missed two opportunities to arrest diplomat's wife", **https://www.telegraph.co.uk/news/2019/10/22/anne-sacoolas-harry-dunn-british-detectives-sent-us/** ; The Guardian, 9/2/2020, "Harry Dunn's family seek answers over reports Anne Sacoolas was CIA officer", **https://www.theguardian.com/uk-news/2020/feb/09/anne-sacoolas-cia-officer-government-comment-harry-dunn**

138. The Telegraph, 22/10/2019 , "Police chief in charge of Harry Dunn car crash case says he would not do anything differently as he admits his officers missed two opportunities to arrest diplomat's wife", **https://www.telegraph.co.uk/news/2019/10/22/anne-sacoolas-harry-dunn-british-detectives-sent-us/**

139. The Guardian, 24/11/2020, "Harry Dunn's parents lose high court immunity case", **https://www.theguardian.com/uk-news/2020/nov/24/harry-dunn-parents-lose-high-court-immunity-case**

140. BBC News, 2/11/2020, "Harry Dunn death: CPS urge Anne Sacoolas to surrender", **https://www.bbc.co.uk/news/uk-england-northamptonshire-54783900 15**

141. Sky News, 4/2/2021, "Harry Dunn: UK government 'didn't know' Anne Sacoolas worked for US intelligence", **https://news.sky.com/story/harry-dunn-uk-government-didnt-know-anne-sacoolas-worked-for-us-intelligence-12208634**

142. The Times, 2/9/2020, "US airbase staff given immunity from prosecution in war on terror", **https://www.thetimes.co.uk/edition/news/us-airbase-staff-given-immunity-from-prosecution-in-war-on-terror-w86jmn7tq**

143. Parliamentary answer from Wendy Morton, Parliamentary Under-Secretary (Foreign, Commonwealth and Development Office), 8/10/2020, HC Deb, 8 October 2020, cW **https://www.theyworkforyou.com/wrans/?id=2020-10-05.99102.h&s=menwith#g99102.q0**

144. Harrogate Informer, 11/6/2019 , "Peace campaigner struck by Menwith Hill car rebuilds her life after Harrogate's Truth Legal helps her win compensation battle", **https://www.harrogate-news.co.uk/2019/06/11/peace-campaigner-struck-by-menwith-hill-car-rebuilds-her-life-after-harrogates-truth-legal-helps-her-win-compensation-battle/**

CONCLUSION

The Menwith Hill base has been shrouded in secrecy for decades and it has taken the actions of courageous whistle-blowers, dogged campaigners and investigative journalists to bring to light its role in a vast state surveillance apparatus, assassination programme and US missile defense.

Despite local opposition the US spy base at Menwith Hill has continued to expand in recent years, likely further enhancing its capabilities[145]. Its role in mass surveillance and extrajudicial killings was exposed by the Snowden leaks, which provided a snapshot of transparency. However secrecy around Menwith Hill has not lessened.

The base's US missile-defense role makes it a potential target in the event of conflict whilst the hype around missile-defence systems could make leaders more aggressive and nuclear conflict more likely.

The UK and US's intelligence capabilities, based in part at Menwith Hill, have been exposed as often being used not to tackle violent crime or terrorism but to spy on leaders of allied nations, aid agencies and vast swathes of the population. The surveillance systems have been found to have been operating illegally for years in a slew of court judgements following challenges by campaigners.

The response of the UK Government has not been to change its behaviour but to rewrite the laws underpinning its intelligence operations in an effort to legalise its actions while limiting public scrutiny and accountability.

Parliamentary accountability for the security services, already limited to the secretive Intelligence and Security Committee (unlike normal parliamentary select committees), was dramatically interfered with in 2019 and 2020, apparently to prevent the Committee's investigation into Russian interference in British public life being released. The Committee was disbanded for nine months, during which time no effective parliamentary oversight could occur. When the Conservative former Chair of the Defence Committee, Julian Lewis, nominated by the Government to the Committee, was elected Chair by his peers over the Government's preferred candidate the Conservative party expelled him.

A single, secretive committee, too cosy with the security services and too easily influenced by Government, is clearly insufficient to oversee large, powerful and secretive intelligence services. Much more rigorous and independent oversight is clearly needed.

More troubling still, Menwith Hill has been exposed as playing a direct role in drone assassination campaigns outside of war zones which, even when they kill only the intended person, amount to an extrajudicial death penalty. Moreover, drone strikes have been found to have killed hundreds of innocent civilians.

A 2014 study by Reprieve found that US attempts to kill 41 named men as part of the US "targeted killing" campaign resulted in the deaths of an estimated 1,147 people[146], a rate of 28 people killed for every person targeted.

In one case analysed by Reprieve it took

seven drone strikes before the US killed its target. In those strikes as many as 164 people died, including 11 children[147]. If anything there is a risk that the use of drones and technologically advanced intelligence-gathering techniques gives a false impression of accuracy and can lower the bar for conflict. The UK's use of drone strikes, including lethal strikes outside of war zones, raises grave concerns – especially given the UK Government's loosely defined rules for killings and their resistance to scrutiny.

Legal challenges against the UK's surveillance apparatus and its involvement in drone strikes have shown that the UK's security services were acting unlawfully for years, though many crucial cases are still being fought in the courts.

The tragic death of Harry Dunn illustrated publicly the difficulties in holding US intelligence personnel stationed in the UK to account. The incident could easily have occurred at Menwith Hill, as illustrated by the injury of campaigner Barbara Penny in 2015.

Activists, journalists, victims and their families, human-rights and civil-liberties campaigners have all been crucial to holding the powerful accountable in public and before the law.

While the US and UK forces operating at Menwith Hill continue to operate beyond public scrutiny and accountability, the Orwellian surveillance systems and extrajudicial executions exposed in recent years will likely continue.

145. BBC, 14/8/2019, "RAF Menwith Hill: Spy base radar antenna shelters approved", **https://www.bbc.co.uk/news/uk-england-york-north-yorkshire-49348848**

146. The Guardian, 24/11/2014, "41 men targeted but 1,147 people killed: US drone strikes – the facts on the ground", **https://www.theguardian.com/us-news/2014/nov/24/-sp-us-drone-strikes-kill-1147**

147. Reprieve, 31/12/2014, "You Never Die Twice: Multiple Kills in the US Drone Program", **https://reprieve.org/uk/2014/12/31/you-never-die-twice-multiple-kills-in-the-us-drone-program/**

DEMANDS

THE MENWITH HILL ACCOUNTABILITY CAMPAIGN AND YORKSHIRE CND NOTE WITH ALARM THE ACTIVITIES AT MENWITH HILL DESCRIBED ABOVE AND DEMAND:

- **That any US military activity or US security agency activity carried out at Menwith Hill be carried out in such a way as to make those responsible fully accountable to the UK;**
- **That all US military and security activity in the UK comply with UK and international law;**
- **The cessation of all illegal UK and US military and security activity in the UK.**

Approaching Menwith Hill Photo by Tim Harberd

ORGANISATIONS AND EQUIPMENT ASSOCIATED WITH MENWITH HILL

ACTIVE SIGINT	Infects computers with malware
CIA	US Central Intelligence Agency
COMINT	Communications Intelligence and Information system
DISHFIRE	Secret global surveillance collection system and database run by the NSA and GCHQ that collects hundreds of millions of text messages daily from around the world
ELINT	Electronic Intelligence
ECHELON	Surveillance programme
FORNSAT	Listens to communication between foreign satellites
GCHQ	UK surveillance organisation
GEO	Geosynchronous orbit
GHOST HUNTER	Surveillance for military operations
HUMINT	Information system
JUMPSEAT	Collects signals from satellites with elliptical orbits
LEO	Low Earth Orbit
MGS	Mission Ground Station
MOONPENNY	Menwith Hill's foreign-satellite surveillance mission, has been monitoring 163 different satellite data links since 2009
NEMESIS	Targets commercial satellites for surveillance
NRO	US National Reconnaissance Organisation
NSA	US National Security Agency
OVERHEAD	US satellites used to locate & monitor wireless communications, cell phones and Wi-Fi
PRISM	The PRISM program utilises extensive data-mining efforts to collect information and analyse it for patterns of terrorist or other potential criminal activity.
SBIRS	Space-Based Infra-Red System for US missile defence
SIGINT	Interception of signals
TEMPORA	GCHQ's programme for tapping into fibre-optic communications cables
TORUS SYSTEM	A satellite receiving system, part of Sniffit, all for global surveillance, can receive signals from up to 35 communications satellites
TRUMPET	Replacement for Jumpseat
XKEYSCORE	Searches and analyses global Internet data

This list is probably not complete: it is based only on what is in the public domain.
23 April 2021

This publication was funded by the Joseph Rowntree Charitable Trust

The views expressed are not necessarily those of the Trust.

Radome rising
Photo by Tim Harberd

Report Designed by
Katie Edwards Design
www.katieedwardsdesign.co.uk

Printed by Enid Taylor Ltd
01423 567764
info@enidtaylor.co.uk

For more information and to join the campaigns contact:

Menwith Hill Accountability Campaign
mail@themhac.uk
www.themhac.uk

Yorkshire CND
01274 730 795
info@yorkshirecnd.org.uk
www.yorkshirecnd.org.uk

Photo by Tim Harberd