GlobalResearch
Center for Research on Globalization

Profiled From Radio to Porn, British Spies Track Web Users' Online Identities

By Ryan Gallagher
Global Research, September 26, 2015
The Intercept 25 September 2015

Region: Europe
Theme: Intelligence, Police State & Civil Rights

There was a simple aim at the heart of the top-secret program: Record the website browsing habits of "every visible user on the Internet."

Before long, billions of digital records about ordinary people's online activities were being stored every day. Among them were details cataloging visits to porn, social media and news websites, search engines, chat forums, and blogs.

The mass surveillance operation code-named KARMA POLICE — was launched by British spies about seven years ago without any public debate or scrutiny. It was just one part of a giant global Internet spying apparatus built by the United Kingdom's electronic eavesdropping agency, Government Communications Headquarters, or GCHQ.

The revelations about the scope of the British agency's surveillance are contained in documents obtained by *The Intercept* from National Security Agency whistleblower Edward Snowden. Previous reports based on the leaked files have exposed how GCHQ taps into Internet cables to monitor communications on a vast scale, but many details about what happens to the data after it has been vacuumed up have remained unclear.

Amid a renewed push from the U.K. government for more surveillance powers, more than two dozen documents being disclosed today by *The Intercept* reveal for the first time several major strands of GCHQ's existing electronic eavesdropping capabilities.

One system builds profiles showing people's web browsing histories. Another analyzes instant messenger communications, emails, Skype calls, text messages, cell phone locations, and social media interactions. Separate programs were built to keep tabs on "suspicious" Google searches and usage of Google Maps.

The surveillance is underpinned by an opaque legal regime that has authorized GCHQ to sift through huge archives of metadata about the private phone calls, emails and Internet browsing logs of Brits, Americans, and any other citizens all without a court order or judicial warrant.

Metadata reveals information about a communication such as the sender and recipient of an email, or the phone numbers someone called and at what time but not the written content of the message or the audio of the call.

As of 2012, GCHQ was storing about 50 billion metadata records about online communications and Web browsing activity every day, with plans in place to boost capacity to 100 billion daily by the end of that year. The agency, under cover of secrecy, was working

to create what it said would soon be the biggest government surveillance system anywhere in the world.

Radio radicalization

The power of KARMA POLICE was illustrated in 2009, when GCHQ launched a top-secret operation to collect intelligence about people using the Internet to listen to radio shows.

The agency used a sample of nearly 7 million metadata records, gathered over a period of three months, to observe the listening habits of more than 200,000 people across 185 countries, including the U.S., the U.K., Ireland, Canada, Mexico, Spain, the Netherlands, France, and Germany.

A GCHQ graphic illustrating how KARMA POLICE works

A summary report detailing the operation shows that one aim of the project was to research "potential misuse" of Internet radio stations to spread radical Islamic ideas.

GCHQ spies from a unit known as the Network Analysis Center compiled a list of the most popular stations that they had identified, most of which had no association with Islam, like France-based Hotmix Radio, which plays pop, rock, funk and hip-hop music.

They zeroed in on any stations found broadcasting recitations from the Quran, such as a popular Iraqi radio station and a station playing sermons from a prominent Egyptian imam named Sheikh Muhammad Jebril. They then used KARMA POLICE to find out more about these stations' listeners, identifying them as users on Skype, Yahoo, and Facebook.

The summary report says the spies selected one Egypt-based listener for "profiling" and investigated which other websites he had been visiting. Surveillance records revealed the listener had viewed the porn site Redtube, as well as Facebook, Yahoo, YouTube, Google's blogging platform Blogspot, the photo-sharing site Flickr, a website about Islam, and an Arab advertising site.

GCHQ's documents indicate that the plans for KARMA POLICE were drawn up between 2007 and 2008. The system was designed to provide the agency with "either (a) a web browsing profile for every visible user on the Internet, or (b) a user profile for every visible website on the Internet."

The origin of the surveillance system's name is not discussed in the documents. But KARMA POLICE is also the name of a popular song released in 1997 by the Grammy Award-winning British band Radiohead, suggesting the spies may have been fans.

A verse repeated throughout the hit song includes the lyric, "This is what you'll get, when you mess with us."

The Black Hole

GCHQ vacuums up the website browsing histories using "probes" that tap into the international fiber-optic cables that transport Internet traffic across the world.

A huge volume of the Internet data GCHQ collects flows directly into a massive repository named Black Hole, which is at the core of the agency's online spying operations, storing raw logs of intercepted material before it has been subject to analysis.

Black Hole contains data collected by GCHQ as part of bulk "unselected" surveillance, meaning it is not focused on particular "selected" targets and instead includes troves of data indiscriminately swept up about ordinary people's online activities. Between August 2007 and March 2009, GCHQ documents say that Black Hole was used to store more than 1.1 trillion "events" a term the agency uses to refer to metadata records with about 10 billion new entries added every day.

As of March 2009, the largest slice of data Black Hole held 41 percent was about people's Internet browsing histories. The rest included a combination of email and instant messenger records, details about search engine queries, information about social media activity, logs related to hacking operations, and data on people's use of tools to browse the Internet anonymously.

Throughout this period, as smartphone sales started to boom, the frequency of people's Internet use was steadily increasing. In tandem, British spies were working frantically to bolster their spying capabilities, with plans afoot to expand the size of Black Hole and other repositories to handle an avalanche of new data.

By 2010, according to the documents, GCHQ was logging 30 billion metadata records per day. By 2012, collection had increased to 50 billion per day, and work was underway to double capacity to 100 billion. The agency was developing "unprecedented" techniques to perform what it called "population-scale" data mining, monitoring all communications across entire countries in an effort to detect patterns or behaviors deemed suspicious. It was creating what it saidwould be, by 2013, "the world's biggest" surveillance engine "to run cyber operations and to access better, more valued data for customers to make a real world difference."

HERE WAS A SIMPLE AIM at the heart of the top-secret program: Record the website browsing habits of "every visible user on the Internet."

Before long, billions of digital records about ordinary people's online activities were being stored every day. Among them were details cataloging visits to porn, social media and news websites, search engines, chat forums, and blogs.

The mass surveillance operation — code-named KARMA POLICE — was launched by British spies about seven years ago without any public debate or scrutiny. It was just one part of a giant global Internet spying apparatus built by the United Kingdom's electronic eavesdropping agency, Government Communications Headquarters, or GCHQ.

The revelations about the scope of the British agency's surveillance are contained in documents obtained by *The Intercept* from National Security Agency whistleblower Edward Snowden. Previous reports based on the leaked files have exposed how GCHQ taps into Internet cables to monitor communications on a vast scale, but many details about what happens to the data after it has been vacuumed up have remained unclear.

Amid a renewed push from the U.K. government for more surveillance powers, more than two dozen documents being disclosed today by *The Intercept* reveal for the first time

several major strands of GCHQ's existing electronic eavesdropping capabilities.

One system builds profiles showing people's web browsing histories. Another analyzes instant messenger communications, emails, Skype calls, text messages, cell phone locations, and social media interactions. Separate programs were built to keep tabs on "suspicious" Google searches and usage of Google Maps.

The surveillance is underpinned by an opaque legal regime that has authorized GCHQ to sift through huge archives of metadata about the private phone calls, emails and Internet browsing logs of Brits, Americans, and any other citizens — all without a court order or judicial warrant.

Metadata reveals information about a communication — such as the sender and recipient of an email, or the phone numbers someone called and at what time — but not the written content of the message or the audio of the call.

As of 2012, GCHQ was storing about 50 billion metadata records about online communications and Web browsing activity every day, with plans in place to boost capacity to 100 billion daily by the end of that year. The agency, under cover of secrecy, was working to create what it said would soon be the biggest government surveillance system anywhere in the world.

Radio radicalization

The power of KARMA POLICE was illustrated in 2009, when GCHQ launched a top-secret operation to collect intelligence about people using the Internet to listen to radio shows.

The agency used a sample of nearly 7 million metadata records, gathered over a period of three months, to observe the listening habits of more than 200,000 people across 185 countries, including the U.S., the U.K., Ireland, Canada, Mexico, Spain, the Netherlands, France, and Germany.

A GCHQ graphic illustrating how KARMA POLICE works

A summary report detailing the operation shows that one aim of the project was to research "potential misuse" of Internet radio stations to spread radical Islamic ideas.

GCHQ spies from a unit known as the Network Analysis Center compiled a list of the most popular stations that they had identified, most of which had no association with Islam, like France-based Hotmix Radio, which plays pop, rock, funk and hip-hop music.

They zeroed in on any stations found broadcasting recitations from the Quran, such as a popular Iraqi radio station and a station playing sermons from a prominent Egyptian imam named Sheikh Muhammad Jebril. They then used KARMA POLICE to find out more about these stations' listeners, identifying them as users on Skype, Yahoo, and Facebook.

The summary report says the spies selected one Egypt-based listener for "profiling" and investigated which other websites he had been visiting. Surveillance records revealed the listener had viewed the porn site Redtube, as well as Facebook, Yahoo, YouTube, Google's blogging platform Blogspot, the photo-sharing site Flickr, a website about Islam, and an Arab

advertising site.

GCHQ's documents indicate that the plans for KARMA POLICE were drawn up between 2007 and 2008. The system was designed to provide the agency with "either (a) a web browsing profile for every visible user on the Internet, or (b) a user profile for every visible website on the Internet."

The origin of the surveillance system's name is not discussed in the documents. But KARMA POLICE is also the name of a popular song released in 1997 by the Grammy Award-winning British band Radiohead, suggesting the spies may have been fans.

A verse repeated throughout the hit song includes the lyric, "This is what you'll get, when you mess with us."

The Black Hole

GCHQ vacuums up the website browsing histories using "probes" that tap into the international fiber-optic cables that transport Internet traffic across the world.

A huge volume of the Internet data GCHQ collects flows directly into a massive repository named Black Hole, which is at the core of the agency's online spying operations, storing raw logs of intercepted material before it has been subject to analysis.

Black Hole contains data collected by GCHQ as part of bulk "unselected" surveillance, meaning it is not focused on particular "selected" targets and instead includes troves of data indiscriminately swept up about ordinary people's online activities. Between August 2007 and March 2009, GCHQdocuments say that Black Hole was used to store more than 1.1 trillion "events" — a term the agency uses to refer to metadata records — with about 10 billion new entries added every day.

As of March 2009, the largest slice of data Black Hole held — 41 percent —was about people's Internet browsing histories. The rest included a combination of email and instant messenger records, details about search engine queries, information about social media activity, logs related to hacking operations, and data on people's use of tools to browse the Internet anonymously.

Throughout this period, as smartphone sales started to boom, the frequency of people's Internet use was steadily increasing. In tandem, British spies were working frantically to bolster their spying capabilities, with plans afoot to expand the size of Black Hole and other repositories to handle an avalanche of new data.

By 2010, according to the documents, GCHQ was logging 30 billion metadata records per day. By 2012, collection had increased to 50 billion per day, and work was underway to double capacity to 100 billion. The agency was developing "unprecedented" techniques to perform what it called "population-scale" data mining, monitoring all communications across entire countries in an effort to detect patterns or behaviors deemed suspicious. It was creating what it said would be, by 2013, "the world's biggest" surveillance engine "to run cyber operations and to access better, more valued data for customers to make a real world difference."

A document from the GCHQ target analysis center (GTAC) shows the Black Hole repository's structure.

GCHQ is able to identify a particular person's website browsing habits by pulling out the raw data stored in repositories like Black Hole and then analyzing it with a variety of systems that complement each other.

KARMA POLICE, for instance, works by showing the IP addresses of people visiting websites. IP addresses are unique identifiers that are allocated to computers when they connect to the Internet.

In isolation, IPs would not be of much value to GCHQ, because they are just a series of numbers — like 195.92.47.101 — and are not attached to a name. But when paired with other data they become a rich source of personal information.

To find out the identity of a person or persons behind an IP address, GCHQ analysts can enter the series of numbers into a separate system named MUTANT BROTH, which is used to sift through data contained in the Black Hole repository about vast amounts of tiny intercepted files known as cookies.

Cookies are automatically placed on computers to identify and sometimes track people browsing the Internet, often for advertising purposes. When you visit or log into a website, a cookie is usually stored on your computer so that the site recognizes you. It can contain your username or email address, your IP address, and even details about your login password and the kind of Internet browser you are using — like Google Chrome or Mozilla Firefox.

For GCHQ, this information is incredibly valuable. The agency refers to cookies internally as "target detection identifiers" or "presence events" because of how they help it monitor people's Internet use and uncover online identities.

If the agency wants to track down a person's IP address, it can enter the person's email address or username into MUTANT BROTH to attempt to find it, scanning through the cookies that come up linking those identifiers to an IP address. Likewise, if the agency already has the IP address and wants to track down the person behind it, it can use MUTANT BROTH to find email addresses, usernames, and even passwords associated with the IP.

Once the agency has corroborated a targeted person's IP address with an email address or username, it can then use the tiny cookie files associated with these identifiers to perform a so-called "pattern of life" analysis showing the times of day and locations at which the person is most active online.

> the agency was extracting data containing information about people's visits to the adult website YouPorn

In turn, the usernames and email and IP addresses can be entered into other systems that enable the agency to spy on the target's emails, instant messenger conversations, and web

browsing history. All GCHQ needs is a single identifier — a "selector," in agency jargon — to follow a digital trail that can reveal a vast amount about a person's online activities.

A top-secret GCHQ document from March 2009 reveals the agency has targeted a range of popular websites as part of an effort to covertly collect cookies on a massive scale. It shows a sample search in which the agency was extracting data from cookies containing information about people's visits to the adult website YouPorn, search engines Yahoo and Google, and the Reuters news website.

Other websites listed as "sources" of cookies in the 2009 document (see below) are Hotmail, YouTube, Facebook, Reddit, WordPress, Amazon, and sites operated by the broadcasters CNN, BBC, and the U.K.'s Channel 4.

In one six-month period between December 2007 and June 2008, the document says, more than 18 billion records from cookies and other similar identifiers were accessible through MUTANT BROTH.

The data is searched by GCHQ analysts in a hunt for behavior online that could be connected to terrorism or other criminal activity. But it has also served a broader and more controversial purpose — helping the agency hack into European companies' computer networks.

In the lead up to its secret mission targeting Netherlands-based Gemalto, the largest SIM card manufacturer in the world, GCHQ used MUTANT BROTH in an effort to identify the company's employees so it could hack into their computers.

The system helped the agency analyze intercepted Facebook cookies it believed were associated with Gemalto staff located at offices in France and Poland. GCHQ later successfully infiltrated Gemalto's internal networks, stealing encryption keys produced by the company that protect the privacy of cell phone communications.

Similarly, MUTANT BROTH proved integral to GCHQ's hack of Belgian telecommunications provider Belgacom. The agency entered IP addresses associated with Belgacom into MUTANT BROTH to uncover information about the company's employees. Cookies associated with the IPs revealed the Google, Yahoo, and LinkedIn accounts of three Belgacom engineers, whose computers were then targeted by the agency and infected with malware.

The hacking operation resulted in GCHQ gaining deep access into the most sensitive parts of Belgacom's internal systems, granting British spies the ability to intercept communications passing through the company's networks.

Cryptome surveillance

In March, a U.K. parliamentary committee published the findings of an 18-month review of GCHQ's operations and called for an overhaul of the laws that regulate the spying. The committee raised concerns about the agency gathering what it described as "bulk personal datasets" being held about "a wide range of people." However, it censored the section of the report describing what these "datasets" contained, despite acknowledging that they "may be highly intrusive."

The Snowden documents shine light on some of the core GCHQ bulk data-gathering programs that the committee was likely referring to — pulling back the veil of secrecy that has shielded some of the agency's most controversial surveillance operations from public scrutiny.

KARMA POLICE and MUTANT BROTH are among the key bulk collection systems. But they do not operate in isolation — and the scope of GCHQ's spying extends far beyond them.

GCHQ's logo for the SOCIAL ANTHROPOID system

The agency operates a bewildering array of other eavesdropping systems, each serving its own specific purpose and designated a unique code name, such as:SOCIAL ANTHROPOID, which is used to analyze metadata on emails, instant messenger chats, social media connections and conversations, plus "telephony" metadata about phone calls, cell phone locations, text and multimedia messages; MEMORY HOLE, which logs queries entered into search engines and associates each search with an IP address;MARBLED GECKO, which sifts through details about searches people have entered into Google Maps and Google Earth; andINFINITE MONKEYS, which analyzes data about the usage of online bulletin boards and forums.

GCHQ has other programs that it uses to analyze the content of intercepted communications, such as the full written body of emails and the audio of phone calls. One of the most important content collection capabilities isTEMPORA, which mines vast amounts of emails, instant messages, voice calls and other communications and makes them accessible through a Google-style search tool named XKEYSCORE.

As of September 2012, TEMPORA was collecting "more than 40 billion pieces of content a day" and it was being used to spy on people across Europe, the Middle East, and North Africa, according to a top-secret memo outlining the scope of the program. The existence of TEMPORA was first revealed by *The Guardian* in June 2013.

To analyze all of the communications it intercepts and to build a profile of the individuals it is monitoring, GCHQ uses a variety of different tools that can pull together all of the relevant information and make it accessible through a single interface.

SAMUEL PEPYS is one such tool, built by the British spies to analyze both the content and metadata of emails, browsing sessions, and instant messages as they are being intercepted in real time.

One screenshot of SAMUEL PEPYS in action shows the agency using it to monitor an individual in Sweden who visited a page about GCHQ on the U.S.-based anti-secrecy website Cryptome.

Domestic spying

Partly due to the U.K.'s geographic location — situated between the United States and the western edge of continental Europe — a large amount of the world's Internet traffic passes through its territory across international data cables.

In 2010, GCHQ noted that what amounted to "25 percent of all Internet traffic" was

transiting the U.K. through some 1,600 different cables. The agency said that it could "survey the majority of the 1,600" and "select the most valuable to switch into our processing systems."

Many of the cables flow deep under the Atlantic Ocean from the U.S. East Coast, landing on the white-sand beaches of Cornwall in the southwest of England. Others transport data between the U.K. and countries including France, Belgium, Germany, the Netherlands, Denmark, and Norway by crossing below the North Sea and coming aground at various locations on England's east coast.

According to Joss Wright, a research fellow at the University of Oxford's Internet Institute, tapping into the cables allows GCHQ to monitor a large portion of foreign communications. But the cables also transport masses of wholly domestic British emails and online chats, because when anyone in the U.K. sends an email or visits a website, their computer will routinely send and receive data from servers that are located overseas.

"I could send a message from my computer here [in England] to my wife's computer in the next room and on its way it could go through the U.S., France, and other countries," Wright says. "That's just the way the Internet is designed."

In other words, Wright adds, that means "a lot" of British data and communications transit across international cables daily, and are liable to be swept into GCHQ's databases.

A map from a classified GCHQ presentation about intercepting communications from undersea cables.

GCHQ is authorized to conduct dragnet surveillance of the international data cables through so-called external warrants that are signed off by a government minister.

The external warrants permit the agency to monitor communications in foreign countries as well as British citizens' international calls and emails —for example, a call from Islamabad to London. They prohibit GCHQ from reading or listening to the content of "internal" U.K. to U.K. emails and phone calls, which are supposed to be filtered out from GCHQ's systems if they are inadvertently intercepted unless additional authorization is granted to scrutinize them.

However, the same rules do not apply to metadata. A little-known loophole in the law allows GCHQ to use external warrants to collect and analyze bulk metadata about the emails, phone calls, and Internet browsing activities of British people, citizens of closely allied countries, and others, regardless of whether the data is derived from domestic U.K. to U.K. communications and browsing sessions or otherwise.

In March, the existence of this loophole was quietly acknowledged by the U.K. parliamentary committee's surveillance review, which stated in a section of its report that "special protection and additional safeguards" did not apply to metadata swept up using external warrants and that domestic British metadata could therefore be lawfully "returned as a result of searches" conducted by GCHQ.

Perhaps unsurprisingly, GCHQ appears to have readily exploited this obscure legal

technicality. Secret policy guidance papers issued to the agency's analysts instruct them that they can sift through huge troves of indiscriminately collected metadata records to spy on anyone regardless of their nationality. The guidance makes clear that there is no exemption or extra privacy protection for British people or citizens from countries that are members of the Five Eyes, a surveillance alliance that the U.K. is part of alongside the U.S., Canada, Australia, and New Zealand.

"If you are searching a purely Events only database such as MUTANT BROTH, the issue of location does not occur," states one internal GCHQ policy document, which is marked with a "last modified" date of July 2012. The document adds that analysts are free to search the databases for British metadata "without further authorization" by inputing a U.K. "selector," meaning a unique identifier such as a person's email or IP address, username, or phone number.

Authorization is "not needed for individuals in the U.K.," another GCHQdocument explains, because metadata has been judged "less intrusive than communications content." All the spies are required to do to mine the metadata troves is write a short "justification" or "reason" for each search they conduct and then click a button on their computer screen.

Intelligence GCHQ collects on British persons of interest is shared with domestic security agency MI5, which usually takes the lead on spying operations within the U.K. MI5 conducts its own extensive domestic surveillance as part of a program called DIGINT (digital intelligence).

> We think and behave differently based on the assumption that people may be watching.

GCHQ's documents suggest that it typically retains metadata for periods of between 30 days to six months. It stores the content of communications for a shorter period of time, varying between three to 30 days. The retention periods can be extended if deemed necessary for "cyber defense."

One secret policy paper dated from January 2010 lists the wide range of information the agency classes as metadata — including location data that could be used to track your movements, your email, instant messenger, and social networking "buddy lists," logs showing who you have communicated with by phone or email, the passwords you use to access "communications services" (such as an email account), and information about websites you have viewed.

GCHQ headquarters in Cheltenham, England.
www.gchq.gov.uk

Records showing the full website addresses you have visited — for instance, www.gchq.gov.uk/what_we_do — are treated as content. But the first part of an address you have visited — for instance, www.gchq.gov.uk — is treated as metadata.

In isolation, a single metadata record of a phone call, email, or website visit may not reveal much about a person's private life, according to Ethan Zuckerman, director of

Massachusetts Institute of Technology's Center for Civic Media.

But if accumulated and analyzed over a period of weeks or months, these details would be "extremely personal," he told *The Intercept*, because they could reveal a person's movements, habits, religious beliefs, political views, relationships, and even sexual preferences.

For Zuckerman, who has studied the social and political ramifications of surveillance, the most concerning aspect of large-scale government data collection is that it can be "corrosive towards democracy" — leading to a chilling effect on freedom of expression and communication.

"Once we know there's a reasonable chance that we are being watched in one fashion or another it's hard for that not to have a 'panopticon effect,'" he said, "where we think and behave differently based on the assumption that people may be watching and paying attention to what we are doing."

Light oversight

A GCHQ spokesman declined to answer any specific questions for this story, citing a "longstanding policy" not to comment on intelligence matters. The spokesman insisted in an emailed statement that GCHQ's work is "carried out in accordance with a strict legal and policy framework, which ensures that our activities are authorised, necessary and proportionate, and that there is rigorous oversight."

It is unclear, however, whether there are sufficient internal checks in place in practice to ensure GCHQ's spies don't abuse their access to the troves of personal information.

According to agency's documents, just 10 percent of its "targeting" of individuals for surveillance is audited annually and a random selection of metadata searches are audited every six months.

When compared to surveillance rules in place in the U.S., GCHQ notes in one document that the U.K. has "a light oversight regime."

The more lax British spying regulations are reflected in secret internal rules that highlight greater restrictions on how NSA databases can be accessed. The NSA's troves can be searched for data on British citizens, one document states, but they cannot be mined for information about Americans or other citizens from countries in the Five Eyes alliance.

No such constraints are placed on GCHQ's own databases, which can be sifted for records on the phone calls, emails, and Internet usage of Brits, Americans, and citizens from any other country.

The scope of GCHQ's surveillance powers explain in part why Snowden told*The Guardian* in June 2013 that U.K. surveillance is "worse than the U.S." In an interview with *Der Spiegel* in July 2013, Snowden added that British Internet cables were "radioactive" and joked: "Even the Queen's selfies to the pool boy get logged."

In recent years, the biggest barrier to GCHQ's mass collection of data does not appear to have come in the form of legal or policy restrictions. Rather, it is the increased use of encryption technology that protects the privacy of communications that has posed the

biggest potential hindrance to the agency's activities.

"The spread of encryption … threatens our ability to do effective target discovery/development," says a top-secret report co-authored by an official from the British agency and an NSA employee in 2011.

"Pertinent metadata events will be locked within the encrypted channels and difficult, if not impossible, to prise out," the report says, adding that the agencies were working on a plan that would "(hopefully) allow our Internet Exploitation strategy to prevail."

———

Documents published with this article:

- TDI Introduction
- TINT External July 2009
- Social Anthropoid Briefing
- Sensitive Targeting Authorisation
- QFD BLACKHOLE Technology Behind INOC
- Pull Steering Group Minutes
- Access: Vision 2013
- Op Highland Fling Event Log
- Operational Engineering November 2010
- NGE BLACK HOLE ConOp
- Next Generation Events
- Events Analysis
- Legalities
- JCE UK Legalities Context
- HRA Auditing
- GCHQ Analytic Cloud Challenges
- Events
- Demystifying NGE Rock Ridge
- Data Stored in BLACK HOLE
- Cyber Defence Operations Legal Policy
- Crypt Discovery Activity
- Content-Metadata Matrix
- Cloud Developers Exchange July 2011
- Broadcast Analysis
- Blazing Saddles Tools
- Architecture Risk 2012
- ADD SD BLACK HOLE
- 200G Iris Access

Comment on Global Research Articles on our Facebook page

Become a Member of Global Research

Articles by: Ryan Gallagher