

# THE // INTERCEPT

## **Snowden Documents Reveal Covert Surveillance and Pressure Tactics Aimed at WikiLeaks and Its Supporters**

By [Glenn Greenwald](#) and [Ryan Gallagher](#)

February 18<sup>th</sup>, 2014

Top-secret documents from the National Security Agency and its British counterpart reveal for the first time how the governments of the United States and the United Kingdom targeted WikiLeaks and other activist groups with tactics ranging from covert surveillance to prosecution.

The efforts – detailed in documents provided previously by NSA whistleblower Edward Snowden – included a broad campaign of international pressure aimed not only at WikiLeaks founder Julian Assange, but at what the U.S. government calls “the human network that supports WikiLeaks.” The documents also contain internal discussions about targeting the file-sharing site Pirate Bay and hacktivist collectives such as Anonymous.

One [classified document](#) from Government Communications Headquarters, Britain’s top spy agency, shows that GCHQ used its surveillance system to secretly monitor visitors to a WikiLeaks site. By exploiting its ability to tap into the fiber-optic cables that make up the backbone of the Internet, the agency confided to allies in 2012, it was able to collect the IP addresses of visitors in real time, as well as the search terms that visitors used to reach the site from search engines like Google.

Another classified document from the U.S. intelligence community, dated August 2010, recounts how the Obama administration urged foreign allies to file criminal charges against Assange over the group’s publication of the Afghanistan war logs.

[A third document](#), from July 2011, contains a summary of an internal discussion in which officials from two NSA offices – including the agency’s general counsel and an arm of its Threat Operations Center – considered designating WikiLeaks as “a ‘malicious foreign actor’ for the purpose of targeting.” Such a designation would have allowed the group to be targeted with extensive electronic surveillance – without the need to exclude U.S. persons from the surveillance searches.

In 2008, not long after WikiLeaks was formed, the U.S. Army prepared a report that identified the organization as an enemy, and [plotted how it could be destroyed](#). The new documents

provide a window into how the U.S. and British governments appear to have shared the view that WikiLeaks represented a serious threat, and reveal the controversial measures they were willing to take to combat it.

In a statement to *The Intercept*, Assange condemned what he called “the reckless and unlawful behavior of the National Security Agency” and GCHQ’s “extensive hostile monitoring of a popular publisher’s website and its readers.”

“News that the NSA planned these operations at the level of its Office of the General Counsel is especially troubling,” Assange said. “Today, we call on the White House to appoint a special prosecutor to investigate the extent of the NSA’s criminal activity against the media, including WikiLeaks, its staff, its associates and its supporters.”

Illustrating how far afield the NSA deviates from [its self-proclaimed focus](#) on terrorism and national security, the documents reveal that the agency considered using its sweeping surveillance system against Pirate Bay, which has been accused of facilitating copyright violations. The agency also approved surveillance of the foreign “branches” of hacktivist groups, mentioning Anonymous by name.

The documents call into question the Obama administration’s repeated insistence that U.S. citizens are not being caught up in the sweeping surveillance dragnet being cast by the NSA. Under the broad rationale considered by the agency, for example, any communication with a group designated as a “malicious foreign actor,” such as WikiLeaks and Anonymous, would be considered fair game for surveillance.

Julian Sanchez, a research fellow at the Cato Institute who specializes in surveillance issues, says the revelations shed a disturbing light on the NSA’s willingness to sweep up American citizens in its surveillance net.

“All the reassurances Americans heard that the broad authorities of the FISA Amendments Act could only be used to ‘target’ foreigners seem a bit more hollow,” Sanchez says, “when you realize that the ‘foreign target’ can be an entire Web site or online forum used by thousands if not millions of Americans.”

### **GCHQ Spies on WikiLeaks Visitors**

The system used by GCHQ to monitor the WikiLeaks website – codenamed ANTICRISIS GIRL – is described in a classified PowerPoint presentation prepared by the British agency and distributed at the 2012 “SIGDEV Conference.” At the annual gathering, each member of the “Five Eyes” alliance – the United States, United Kingdom, Canada, Australia and New Zealand – describes the prior year’s surveillance successes and challenges.

In a top-secret presentation at the conference, two GCHQ spies outlined how ANTICRISIS GIRL was used to enable “targeted website monitoring” of WikiLeaks ([See slides 33 and 34](#)). The agency logged data showing hundreds of users from around the world, including the United

States, as they were visiting a WikiLeaks site –contradicting [claims](#) by American officials that a deal between the U.K. and the U.S. prevents each country from spying on the other’s citizens.

The IP addresses collected by GCHQ are used to identify individual computers that connect to the Internet, and can be traced back to specific people if the IP address has not been masked using an anonymity service. If WikiLeaks or other news organizations were receiving submissions from sources through a public dropbox on their website, a system like ANTICRISIS GIRL could potentially be used to help track them down. (WikiLeaks has not operated a public dropbox since 2010, when it shut down its system in part due to security concerns over surveillance.)

In its PowerPoint presentation, GCHQ identifies its target only as “wikileaks.” One slide, displaying analytics derived from the surveillance, suggests that the site monitored was the official wikileaks.org domain. It shows that users reached the targeted site by searching for “wikileaks.org” and for “maysan uxo,” a term associated with a series of leaked Iraq war logs that are hosted on wikileaks.org.

The ANTICRISIS GIRL initiative was operated by a GCHQ unit called Global Telecoms Exploitation (GTE), which was [previously reported by The Guardian](#) to be linked to the large-scale, clandestine Internet surveillance operation run by GCHQ, codenamed TEMPORA.

Operating in the United Kingdom and from secret British eavesdropping bases in Cyprus and other countries, GCHQ conducts what it refers to as “passive” surveillance – indiscriminately intercepting massive amounts of data from Internet cables, phone networks and satellites. The GTE unit focuses on developing “pioneering collection capabilities” to exploit the stream of data gathered from the Internet.

As part of the ANTICRISIS GIRL system, the documents show, GCHQ used publicly available analytics software called [Piwik](#) to extract information from its surveillance stream, not only monitoring visits to targeted websites like WikiLeaks, but tracking the country of origin of each visitor.

It is unclear from the PowerPoint presentation whether GCHQ monitored the WikiLeaks site as part of a pilot program designed to demonstrate its capability, using only a small set of covertly collected data, or whether the agency continues to actively deploy its surveillance system to monitor visitors to WikiLeaks. It was [previously reported in The Guardian](#) that X-KEYSCORE, a comprehensive surveillance weapon used by both NSA and GCHQ, allows “an analyst to learn the IP addresses of every person who visits any website the analyst specifies.”

GCHQ refused to comment on whether ANTICRISIS GIRL is still operational. In an email citing the agency’s boilerplate response to inquiries, a spokeswoman insisted that “all of GCHQ’s work is carried out in accordance with a strict legal and policy framework which ensures that our activities are authorized, necessary and proportionate, and that there is rigorous oversight.”

But privacy advocates question such assurances. “How could targeting an entire website’s user base be necessary or proportionate?” says Gus Hosein, executive director of the London-based human rights group Privacy International. “These are innocent people who are turned into suspects based on their reading habits. Surely becoming a target of a state’s intelligence and security apparatus should require more than a mere click on a link.”

The agency’s covert targeting of WikiLeaks, Hosein adds, call into question the entire legal rationale underpinning the state’s system of surveillance. “We may be tempted to see GCHQ as a rogue agency, ungoverned in its use of unprecedented powers generated by new technologies,” he says. “But GCHQ’s actions are authorized by [government] ministers. The fact that ministers are ordering the monitoring of political interests of Internet users shows a systemic failure in the rule of law.”

### **Going After Assange and His Supporters**

The U.S. attempt to pressure other nations to prosecute Assange is recounted in a file that the intelligence community calls its “Manhunting Timeline.” The document details, on a country-by-country basis, efforts by the U.S. government and its allies to locate, prosecute, capture or kill alleged terrorists, drug traffickers, Palestinian leaders and others. There is a timeline for each year from 2008 to 2012.

An entry from August 2010 – headlined “United States, Australia, Great Britain, Germany, Iceland” – states: “The United States on August 10 urged other nations with forces in Afghanistan, including Australia, United Kingdom, and Germany, to consider filing criminal charges against Julian Assange.” It describes Assange as the “founder of the rogue Wikileaks Internet website and responsible for the unauthorized publication of over 70,000 classified documents covering the war in Afghanistan.”

In response to questions from *The Intercept*, the NSA suggested that the entry is “a summary derived from a 2010 article” in the *Daily Beast*. [That article](#), which cited an anonymous U.S. official, reported that “the Obama administration is pressing Britain, Germany, Australia, and other allied Western governments to consider opening criminal investigations of WikiLeaks founder Julian Assange and to severely limit his nomadic travels across international borders.”

The government entry in the “Manhunting Timeline” adds Iceland to the list of Western nations that were pressured, and suggests that the push to prosecute Assange is part of a broader campaign. The effort, it explains, “exemplifies the start of an international effort to focus the legal element of national power upon non-state actor Assange, and the human network that supports WikiLeaks.” The entry does not specify how broadly the government defines that “human network,” which could potentially include thousands of volunteers, donors and journalists, as well as people who simply spoke out in defense of WikiLeaks.

In a statement, the NSA declined to comment on the documents or its targeting of activist groups, noting only that the agency “provides numerous opportunities and forums for their analysts to explore hypothetical or actual circumstances to gain appropriate advice on the

exercise of their authorities within the Constitution and the law, and to share that advice appropriately.”

But the entry aimed at WikiLeaks comes from credentialed officials within the intelligence community. In an interview in Hong Kong last June, Edward Snowden made clear that the only NSA officials empowered to write such entries are those “with top-secret clearance and public key infrastructure certificates” – a kind of digital ID card enabling unique access to certain parts of the agency’s system. What’s more, Snowden added, the entries are “peer reviewed” – and every edit made is recorded by the system.

The U.S. launched its pressure campaign against WikiLeaks less than a week after the group began publishing the Afghanistan war logs on July 25, 2010. At the time, top U.S. national security officials accused WikiLeaks of having [“blood” on its hands](#). But several months later, [McClatchy reported](#) that “U.S. officials concede that they have no evidence to date that the documents led to anyone’s death.”

The government targeting of WikiLeaks nonetheless continued. In April 2011, [Salon reported](#) that a grand jury in Virginia was actively investigating both the group and Assange on possible criminal charges under espionage statutes relating to the publication of classified documents. And in August of 2012, the *Sydney Morning Herald*, citing secret Australian diplomatic cables, [reported](#) that “Australian diplomats have no doubt the United States is still gunning for Julian Assange” and that “Australia’s diplomatic service takes seriously the likelihood that Assange will eventually be extradited to the US on charges arising from WikiLeaks obtaining leaked US military and diplomatic documents.”

Bringing criminal charges against WikiLeaks or Assange for publishing classified documents would be highly controversial – especially since the group partnered with newspapers like *The Guardian* and *The New York Times* to make the war logs public. “The biggest challenge to the press today is the threatened prosecution of WikiLeaks, and it’s absolutely frightening,” James Goodale, who served as chief counsel of the *Times* during its battle to publish The Pentagon Papers, [told the Columbia Journalism Review](#) last March. “If you go after the WikiLeaks criminally, you go after the *Times*. That’s the criminalization of the whole process.”

In November 2013, *The Washington Post*, citing anonymous officials, [reported](#) that the Justice Department strongly considered prosecuting Assange, but concluded it “could not do so without also prosecuting U.S. news organizations and journalists” who had partnered with WikiLeaks to publish the documents. According to the *Post*, officials “realized that they have what they described as a ‘*New York Times* problem’” – namely, that any theory used to bring charges against Assange would also result in criminal liability for the *Times*, *The Guardian*, and other papers which also published secret documents provided to WikiLeaks.

### **NSA proposals to target WikiLeaks**

As the new NSA documents make clear, however, the U.S. government did more than attempt to engineer the prosecution of Assange. NSA analysts also considered designating WikiLeaks as a “malicious foreign actor” for surveillance purposes – a move that would have significantly

expanded the agency's ability to subject the group's officials and supporters to extensive surveillance.

Such a designation would allow WikiLeaks to be targeted with surveillance without the use of "defeats" – an agency term for technical mechanisms to shield the communications of U.S. persons from getting caught in the dragnet.

[That top-secret document](#) – which summarizes a discussion between the NSA's Office of the General Counsel and the Oversight and Compliance Office of the agency's Threat Operations Center – spells out a rationale for including American citizens in the surveillance:

"If the foreign IP is consistently associated with malicious cyber activity against the U.S., so, tied to a foreign individual or organization known to direct malicious activity our way, then there is no need to defeat any to, from, or about U.S. Persons. This is based on the description that one end of the communication would always be this suspect foreign IP, and so therefore any U.S. Person communicant would be incidental to the foreign intelligence task."

In short, labeling WikiLeaks a "malicious foreign target" would mean that anyone communicating with the organization for any reason – including American citizens – could have their communications subjected to government surveillance.

When NSA officials are asked in the document if WikiLeaks or Pirate Bay could be designated as "malicious foreign actors," the reply is inconclusive: "Let us get back to you." There is no indication of whether either group was ever designated or targeted in such a way.

The NSA's lawyers did, however, give the green light to subject other activists to heightened surveillance. Asked if it would be permissible to "target the foreign actors of a loosely coupled group of hackers ... such as with Anonymous," the response is unequivocal: "As long as they are foreign individuals outside of the US and do not hold dual citizenship ... then you are okay."

### **NSA Lawyers: "It's Nothing to Worry About"**

Sanchez, the surveillance expert with the Cato Institute, says the document serves as "a reminder that NSA essentially has carte blanche to spy on non-Americans. In public statements, intelligence officials always talk about spying on 'terrorists,' as if those are the only targets — but Section 702 [of the 2008 FISA Amendments Act] doesn't say anything about 'terrorists.' They can authorize collection on any 'persons reasonably believed to be [located] outside the United States,' with 'persons' including pretty much any kind of group not 'substantially' composed of Americans."

Sanchez notes that while it makes sense to subject some full-scale cyber-attacks to government surveillance, "it would make no sense to lump together foreign cyberattackers with sites voluntarily visited by enormous numbers of Americans, like Pirate Bay or WikiLeaks."

Indeed, one entry in the NSA document expressly authorizes the targeting of a "malicious" foreign server – offering Pirate Bay as a specific example – "even if there is a possibility that

U.S. persons could be using it as well.” NSA officials agree that there is no need to exclude Americans from the surveillance, suggesting only that the agency’s spies “try to minimize” how many U.S. citizens are caught in the dragnet.

Another entry even raises the possibility of using X-KEYSCORE, one of the agency’s most comprehensive surveillance programs, to target communications between two U.S.-based Internet addresses if they are operating through a “proxy” being used for “malicious foreign activity.” In response, the NSA’s Threat Operations Center approves the targeting, but the agency’s general counsel requests “further clarification before signing off.”

If WikiLeaks were improperly targeted, or if a U.S. citizen were swept up in the NSA’s surveillance net without authorization, the agency’s attitude seems to be one of indifference. According to the document – which quotes a response by the NSA’s Office of General Counsel and the oversight and compliance office of its Threat Operations Center – discovering that an American has been selected for surveillance must be mentioned in a quarterly report, “but it’s nothing to worry about.”

The attempt to target WikiLeaks and its broad network of supporters drew sharp criticism from the group and its allies. “These documents demonstrate that the political persecution of WikiLeaks is very much alive,” says Baltasar Garzón, the Spanish former judge who now represents the group. “The paradox is that Julian Assange and the WikiLeaks organization are being treated as a threat instead of what they are: a journalist and a media organization that are exercising their fundamental right to receive and impart information in its original form, free from omission and censorship, free from partisan interests, free from economic or political pressure.”

For his part, Assange remains defiant. “The NSA and its U.K. accomplices show no respect for the rule of law,” he told *The Intercept*. “But there is a cost to conducting illicit actions against a media organization.” Referring to a [criminal complaint](#) that the group filed last year against “interference with our journalistic work in Europe,” Assange warned that “no entity, including the NSA, should be permitted to act against a journalist with impunity.”

Assange indicated that in light of the new documents, the group may take further legal action.

“We have instructed our general counsel, Judge Baltasar Garzón, to prepare the appropriate response,” he said. “The investigations into attempts to interfere with WikiLeaks’ work will go wherever they need to go. Make no mistake: those responsible will be held to account and brought to justice.”