The New York Times | http://nyti.ms/1dP5ida

POLITICS

Hunting for Hackers, N.S.A. Secretly Expands Internet Spying at U.S. Border

By **CHARLIE SAVAGE, JULIA ANGWIN, JEFF LARSON and HENRIK MOLTKE** JUNE 4, 2015

WASHINGTON — Without public notice or debate, the Obama administration has expanded the National Security Agency's warrantless surveillance of Americans' international Internet traffic to search for evidence of malicious computer hacking, according to classified N.S.A. documents.

In mid-2012, Justice Department lawyers wrote two secret memos permitting the spy agency to begin hunting on Internet cables, without a warrant and on American soil, for data linked to computer intrusions originating abroad — including traffic that flows to suspicious Internet addresses or contains malware, the documents show.

The Justice Department allowed the agency to monitor only addresses and "cybersignatures" — patterns associated with computer intrusions — that it could tie to foreign governments. But the documents also note that the N.S.A. sought permission to target hackers even when it could not establish any links to foreign powers.

The disclosures, based on documents provided by Edward J. Snowden, the former N.S.A. contractor, and shared with The New York Times and ProPublica, come at a time of unprecedented cyberattacks on American financial institutions, businesses and government agencies, but also of greater scrutiny of secret legal justifications for broader government surveillance.

While the Senate passed legislation this week limiting some of the N.S.A.'s authority, it involved provisions in the U.S.A. Patriot Act and did not apply to the warrantless wiretapping program.

Government officials defended the N.S.A.'s monitoring of suspected hackers as necessary to shield Americans from the increasingly aggressive activities of foreign governments. But critics say it raises difficult trade-offs that should be subject to public debate.

The N.S.A.'s activities run "smack into law enforcement land," said Jonathan Mayer, a cybersecurity scholar at Stanford Law School who has researched privacy issues and who reviewed several of the documents. "That's a major policy decision about how to structure cybersecurity in the U.S. and not a conversation that has been had in public."

It is not clear what standards the agency is using to select targets. It can be hard to know for sure who is behind a particular intrusion — a foreign government or a criminal gang — and the N.S.A. is supposed to focus on foreign intelligence, not law enforcement.

The government can also gather significant volumes of Americans' information — anything from private emails to trade secrets and business dealings — through Internet surveillance because monitoring the data flowing to a hacker involves copying that information as the hacker steals it.

One internal N.S.A. document notes that agency surveillance activities through "hacker signatures pull in a lot."

Brian Hale, the spokesman for the Office of the Director of National Intelligence, said, "It should come as no surprise that the U.S. government gathers intelligence on foreign powers that attempt to penetrate U.S.

networks and steal the private information of U.S. citizens and companies." He added that "targeting overseas individuals engaging in hostile cyberactivities on behalf of a foreign power is a lawful foreign intelligence purpose."

The effort is the latest known expansion of the N.S.A.'s warrantless surveillance program, which allows the government to intercept Americans' cross-border communications if the target is a foreigner abroad. While the N.S.A. has long searched for specific email addresses and phone numbers of foreign intelligence targets, the Obama administration three years ago started allowing the agency to search its communications streams for less-identifying Internet protocol addresses or strings of harmful computer code.

The surveillance activity traces to changes that began after the Sept. 11 terrorist attacks. The government tore down a so-called wall that prevented intelligence and criminal investigators from sharing information about suspected spies and terrorists. The barrier had been erected to protect Americans' rights because intelligence investigations use lower legal standards than criminal inquiries, but policy makers decided it was too much of an obstacle to terrorism investigations.

The N.S.A. also started the warrantless wiretapping program, which caused an outcry when it was disclosed in 2005. In 2008, under the FISA Amendments Act, Congress legalized the surveillance program so long as the agency targeted only noncitizens abroad. A year later, the new Obama administration began crafting a new cybersecurity policy — including weighing whether the Internet had made the distinction between a spy and a criminal obsolete.

"Reliance on legal authorities that make theoretical distinctions between armed attacks, terrorism and criminal activity may prove impractical," the White House National Security Council wrote in a classified annex to a policy report in May 2009, which was included in the N.S.A.'s internal files.

About that time, the documents show, the N.S.A. — whose mission includes protecting military and intelligence networks against intruders — proposed using the warrantless surveillance program for

cybersecurity purposes. The agency received “guidance on targeting using the signatures” from the Foreign Intelligence Surveillance Court, according to an internal newsletter.

In May and July 2012, according to an internal timeline, the Justice Department granted its secret approval for the searches of cybersignatures and Internet addresses. The Justice Department tied that authority to a pre-existing approval by the secret surveillance court permitting the government to use the program to monitor foreign governments.

That limit meant the N.S.A. had to have some evidence for believing that the hackers were working for a specific foreign power. That rule, the N.S.A. soon complained, left a “huge collection gap against cyberthreats to the nation” because it is often hard to know exactly who is behind an intrusion, according to an agency newsletter. Different computer intruders can use the same piece of malware, take steps to hide their location or pretend to be someone else.

So the N.S.A., in 2012, began pressing to go back to the surveillance court and seek permission to use the program explicitly for cybersecurity purposes. That way, it could monitor international communications for any “malicious cyberactivity,” even if it did not yet know who was behind the attack.

The newsletter described the further expansion as one of “highest priorities” of the N.S.A. director, Gen. Keith B. Alexander. However, a former senior intelligence official said that the government never asked the court to grant that authority.

Meanwhile, the F.B.I. in 2011 had obtained a new kind of wiretap order from the secret surveillance court for cybersecurity investigations, permitting it to target Internet data flowing to or from specific Internet addresses linked to certain governments.

To carry out the orders, the F.B.I. negotiated in 2012 to use the N.S.A.’s system for monitoring Internet traffic crossing “chokepoints operated by U.S. providers through which international communications enter and leave the United States,” according to a 2012 N.S.A. document. The N.S.A. would send the intercepted

traffic to the bureau's "cyberdata repository" in Quantico, Virginia.

The disclosure that the N.S.A. and the F.B.I. have expanded their cybersurveillance adds a dimension to a recurring debate over the post-Sept. 11 expansion of government spying powers: Information about Americans sometimes gets swept up incidentally when foreigners are targeted, and prosecutors can use that information in criminal cases.

Citing the potential for a copy of data "exfiltrated" by a hacker to contain "so much" information about Americans, one N.S.A. lawyer suggested keeping the stolen data out of the agency's regular repository for information collected by surveillance so that analysts working on unrelated issues could not query it, a 2010 training document showed. But it is not clear whether the agency or the F.B.I. has imposed any additional limits on the data of hacking victims.

In a response to questions for this article, the F.B.I. pointed to its existing procedures for protecting victims' data acquired during investigations, but also said it continually reviewed its policies "to adapt to these changing threats while protecting civil liberties and the interests of victims of cybercrimes."

None of these actions or proposals had been disclosed to the public. As recently as February, when President Obama spoke about cybersecurity at an event at Stanford University, he lauded the importance of transparency but did not mention this change.

"The technology so often outstrips whatever rules and structures and standards have been put in place, which means that government has to be constantly self-critical and we have to be able to have an open debate about it," Mr. Obama said.

Julia Angwin and Jeff Larson report for ProPublica.

Laura Poitras contributed reporting.
