**Terrorism DA**

**1NC**

**UQ**

**Surveillance now**

**Effective surveillance now – regardless of sunset on PATRIOT Act wiretapping program**

**Savage et al 6/4/15** (Charlie Savage is a Washington correspondent for The New York Times. He is known for his work on presidential power and national security legal policy matter, “Hunting for Hackers, N.S.A. Secretly Expands Internet Spying at U.S. Border”, <http://www.nytimes.com/2015/06/05/us/hunting-for-hackers-nsa-secretly-expands-internet-spying-at-us-border.html?ref=topics>, 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, the measure 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 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.

**ISIS is in the US, surveillance is key now**

Evan **Perez and** Shimon **Prokupecz**, CNN Updated 4:56 PM ET, Sat **May 30**, 2015 (CNN, FBI struggling with surge in homegrown terror cases, available online at <http://www.cnn.com/2015/05/28/politics/fbi-isis-local-law-enforcement/>)

New York (CNN) **The New York Police Department and other law enforcement agencies around the nation are increasing their surveillance of ISIS supporters in the U.S., in part to aid the FBI which is struggling to keep up with a surge in the number of possible terror suspects,** according to law enforcement officials. The change is part of the fallout from the terrorist attack in Garland, Texas earlier this month. The FBI says two ISIS supporters attempted a gun attack on a Prophet Mohammad cartoon contest but were killed by police. One of the attackers, Elton Simpson, was already under investigation by the FBI but managed to elude surveillance to attempt the foiled attack. Texas man charged with providing support to ISIS Texas man charged with providing support to ISIS. **FBI Director James Comey told a group of police officials around the country** in a secure conference call this month **that the FBI needs help to keep tabs on hundreds of suspects.** As a result, some police agencies are adding surveillance teams to help the FBI monitor suspects. Teams of NYPD officers trained in surveillance are now helping the FBI's surveillance teams to better keep track of suspects, law enforcement officials say. NYPD Commissioner William Bratton has said he wants to add 450 officers to the force's counterterrorism unit, partly to counter the increasing domestic threat posed by ISIS sympathizers**. The same is happening with other police departments around the country.** The Los Angeles Police Department's counterterrorism unit is also beefing up its surveillance squads at the request of the FBI, law enforcement officials say. **Comey said at an unrelated news conference Wednesday that he has less confidence now that the FBI can keep up with the task.** Hayden: Attacks like TX shooting will be "new **normal" "It's an extraordinarily difficult challenge task to find** -- that's the first challenge -- **and then assess those who may be on a journey from talking to doing and to find and assess in an environment where increasingly, as the attorney general said, their communications are unavailable to us even with court orders,"** Comey said. **"They're on encrypted platforms, so it is an incredibly difficult task** that we are enlisting all of our state, local and federal partners in and we're working on it every single day, **but I can't stand here with any high confidence when I confront the world that is increasingly dark to me and tell you that I've got it all covered,**" he said. "We are working very, very hard on it but it is an enormous task."

**Links**

**Generic**

**Surveillance key to stop terrorism**

**Bolton 15** (John Bolton is a lawyer and researcher at the American Enterprise Institute for US Foreign policy and national security, “NSA activities key to terrorism fight”, <https://www.aei.org/publication/nsa-activities-key-to-terrorism-fight/>, April 28, 2015)

Congress is poised to decide whether to re-authorize programs run by the National Security Agency that assess patterns of domestic and international telephone calls and emails to uncover linkages with known terrorists. These NSA activities, initiated after al-Qaeda’s deadly 9/11 attacks, have played a vital role in protecting America and our citizens around the world from the still-metastasizing terrorist threat. The NSA programs do not involve listening to or reading conversations, but rather seek to detect communications networks. If patterns are found, and more detailed investigation seems warranted, then NSA or other federal authorities, consistent with the Fourth Amendment’s prohibition against unreasonable searches and seizures, must obtain judicial approval for  more specific investigations. Indeed, even the collection of the so-called metadata is surrounded by procedural protections to prevent spying on U.S. citizens. Nonetheless, critics from the right and left have attacked the NSA for infringing on the legitimate expectations of privacy Americans enjoy under our Constitution. Unfortunately, many of these critics have absolutely no idea what they are talking about; they are engaging in classic McCarthyite tactics, hoping to score political points with a public justifiably worried about the abuses of power characteristic of the Obama administration. Other critics, following Vietnam-era antipathies to America’s intelligence community, have never reconciled themselves to the need for robust clandestine capabilities. Still others yearn for simpler times, embodying Secretary of State Henry Stimson’s famous comment that “gentlemen don’t read each others’ mail.” The ill-informed nature of the debate has facilitated scare-mongering, with one wild accusation about NSA’s activities after another being launched before the mundane reality catches up. And there is an important asymmetry at work here as well. The critics can say whatever their imaginations conjure up, but NSA and its defenders are significantly limited in how they can respond. By definition, the programs’ success rests on the secrecy fundamental to all intelligence activities. Frequently, therefore, explaining what is not happening could well reveal information about NSA’s methods and capabilities that terrorists and others, in turn, could use to stymie future detection efforts. After six years of President Obama, however, trust in government is in short supply. It is more than a little ironic that Obama finds himself defending the NSA (albeit with obvious hesitancy and discomfort), since his approach to foreign and defense issues has consistently reflected near-total indifference, except when he has no alternative to confronting challenges to our security. Yet if harsh international realities can penetrate even Obama’s White House, that alone is evidence of the seriousness of the threats America faces. In fact, just in the year since Congress last considered the NSA programs, the global terrorist threat has dramatically increased. ISIS is carving out an entirely new state from what used to be Syria and Iraq, which no longer exist within the borders created from the former Ottoman Empire after World War I. In already-chaotic Libya, ISIS has grown rapidly, eclipsing al-Qaeda there and across the region as the largest terrorist threat. Boko Haram is expanding beyond Nigeria, declaring its own caliphate, even while pledging allegiance to ISIS. Yemen has descended into chaos, following Libya’s pattern, and Iran has expanded support for the terrorist Houthi coalition. Afghanistan is likely to fall back under Taliban control if, as Obama continually reaffirms, he withdraws all American troops before the end of 2016. **This is not the time to cripple our intelligence-gathering capabilities against the rising terrorist threat. Congress should unquestionably reauthorize the NSA programs**, but only for three years. That would take us into a new presidency, hopefully one that inspires more confidence, where a calmer, more sensible debate can take place.

**Surveillance Key to Stopping ISIS in the US**

**Rory Carroll** Wednesday **4-22**-2015 (The Guardian, NSA surveillance needed to prevent Isis attack, claims former intelligence chair Mike Rogers, former chairman of the House intelligence committee, says the NSA needs to preserve its wide powers in case of an attack on US homeland, found online at http://www.theguardian.com/us-news/2015/apr/22/mass-surveillance-needed-isis-attack-mike-rogers)

**Mass surveillance should be retained because of the prospect of Islamic State attacks within the United States,** a key Republican ally of the National Security Agency has claimed. **Mike Rogers, the former chairman of the House intelligence committee, said the NSA needed to preserve its wide powers in case Isis used its bases in Syria and Iraq to unleash atrocities on the US homeland. “Now you have a very real face on what the threat is,”** Rogers told the Guardian on Tuesday. “**Somebody calling back from Syria to Minnesota, either recruiting somebody or giving the operational OK to do something. That’s real and it’s serious. Before it seemed all hypothetical. Now you can see it.” He added: “Think about how many people are in Syria with western passports or even American passports. I want to know if they pick up the phone. If they’re calling back to the States, I don’t know about you, but I want to know who they’re talking to and what they’re talking about.”** Rogers gave the warning as negotiators in the House of Representatives wrangled over a revamp of the USA Freedom Act, a bill that aimed to stop the NSA from its daily collection of US phone records in bulk which failed in the Senate in 2014, and is now returning to Congress.

**Internal Links**

**ISIS in the US**

**WND 04/25/15** (WND is an independent news source, “2 U.S. agencies warn on imminent ISIS attack”, <http://www.wnd.com/2015/04/2-u-s-agencies-warn-on-imminent-isis-attack/>, 04/25/15)

WASHINGTON – While the FBI investigates a possible ISIS terror attack on the basis of intercepted chatter and intelligence information, the TSA issued a classified warning that ISIS is planning an attack on U.S. soil. Little is known about the nature of the attack other than its imminence, which has prompted the TSA to deploy its new Visible Intermodal Prevention and Response teams, or VIPR, to various undisclosed locations. The VIPR teams include airports, train stations and other busy transportation hubs. One law enforcement source suggested parts of California were of special concern.As a result of the FBI warning, some cities have increased security as a precaution, but those cities have not been disclosed. The TSA classified warning was issued Friday. The FBI investigation was confirmed Saturday. **While ISIS has warned repeatedly it planned to target the U.S., this is the first time the U.S. intelligence community has acted on what it perceives as a viable, if general, threat. So far, ISIS has only attacked U.S. targets abroad.**

**Terrorism will be nuclear – ISIS has the means and the money to acquire nukes, at the least dirty bombs with nuclear materials**

**Lalbiakchhunga 15** (K. Lalbiakchhunga is a research scholar at the Jawaharlal Nehru University in the school of international studies, “NUCLEAR TERRORISM AND THE THREAT OF DIRTY BOMB”, Global Journal of Multidisciplinary Studies, 4(3), February 2015)

Allegations or indications that various terrorist/non-state groups have tried in the past to acquire nuclear and other radioactive material have been widely reported and indictments in criminal prosecutions of alleged members of terrorist groups have, in several cases, included such charges (IAEA: 2014). According to Lee (2003), accounts of varying credibility also point to efforts by terrorists to purchase finished nuclear weapons from inside the former USSR and apparently, the Aum Shinrikyo cult apparently harbored such intentions which is evident in the documents seized from the cult‟s “construction minister,” who had visited Russia extensively in the early 1990s, contained the ominous notation, “How much is a nuclear warhead?” and listed several prices, though whether these references reflected actual negotiations was not clear (Lee, 2003). Osama bin Laden's assertion in 1998 that it was his Islamic duty to acquire weapons of mass destruction ensured that the fulfillment of this intent would become a top priority for his lieutenants in the ensuing years (Mowatt-Larssen, 2010). The Tehreek-e-Taliban Pakistan‟s (TTP‟s) is another potential group that might have intention to acquire nuclear or radiological capability. Operating in Pakistan which is the hotspot of nuclear insecurity, this group may have been want to use nuclear or radiological weapon to fulfill their avowed objective of establishing an Islamic state. Finally, **the most potent terrorist group ISIS pose the gravest danger to proliferation of nuclear and fissile material**. In June 2014, the ISIS capture Mosul city in Iraq and took possession of about 40 kilograms radiological materials from Mosul University. Since then they started threatening countries like Israel and Britain with nuclear attack (Cefaratti, 2014; Su, 2014). For example, in 1995, Chechen extremists threatened to bundle radioactive material with explosives to use against Russia in order to force the Russian military to withdraw from Chechnya. While no explosives were used, officials later retrieved a package of cesium-137 the rebels had buried in a Moscow park (USNRC: 2014). **The matter becomes more worst if we look at the level of nuclear insecurity in different parts of the world**. The former Soviet states like Russia, Ukraine, Kazakhstan, Belarus and Georgia has large stockpile of fissile materials and nuclear insecurity in Pakistan is well known. Beside, several radiological materials have been available in open market as they are use in peaceful purposes like industry, hospital and university. These materials like caecium-137 or cobalt-60 has capability of unleashing enormous destruction if detonated in densely populated areas. Cases of Nuclear and Radioactive material Trafficking Nuclear terrorism requires the acquisition of nuclear materials by terrorist groups. But processing radioactive materials to be use either for nuclear weapon or other peaceful uses require sophiscated technology and human resources which terrorist usually lacking. But this shortcoming can be overcome through illicit trafficking and theft of nuclear material. This shortcut method can lead to nuclear proliferation and the possible construction of improvised nuclear devices or radiological dispersal and exposure devices. The continued reports of illicit trafficking in nuclear and other radioactive material from different parts of the world especially after the end of Cold war makes nuclear terrorism all the more plausible. The IAEA Incident and Trafficking Database (ITDB) reported that from January 1993 to December, 2013, a total of 2477 incidents were reported to the ITDB by participating States and some nonparticipating States. Of the 2477 confirmed incidents, 424 involved unauthorized possession and related criminal activities. Incidents included in this category involved illegal possession, movement or attempts to illegally trade in or use nuclear material or radioactive sources. Sixteen incidents in this category involved high enriched uranium (HEU) or plutonium. There were 664 incidents reported that involved the theft or loss of nuclear or other radioactive material and a total of 1337 cases involving other unauthorized activities, including the unauthorized disposal of radioactive materials or discovery of uncontrolled sources (IAEA: 2014a). Result From the above analysis, the following inferences can be drawn 1**. Nuclear terrorism is a clear and present danger and especially the threat of dirty bomb is very real due to availability of radiological substance in an open market.** 2. There are terrorist groups who have intention to acquire weapons of mass destruction and will not hesitate to use it. 3. From the record of IAEA, there is a vibrant nuclear black market in different parts of the world. Conclusion Looking at the intention of terrorist groups and their increase capability in terms of human resources and financial prowess, they are in a position to buy nuclear materials from black market. Groups like ISIS are estimated to have asset worth $ 2 billion. Beside, the unabated report of illicit trafficking of nuclear materials from various parts of the world is a matter of serious concern. What more worrisome is that majority of illegal trafficking and theft originated from unstable areas and terrorist hotspot like Eastern Europe and Central Asia.

**Impact**

**Retaliation would escalate**

**Speice 06** (Patrick Speice, JD Candidate, 47 Wm and Mary L. Rev. 1427, February 2006, Lexis)

Terrorist groups could acquire a nuclear weapon by a number of methods, including "steal[ing] one intact from the stockpile of a country possessing such weapons, or ... [being] sold or given one by [\*1438] such a country, or [buying or stealing] one from another subnational group that had obtained it in one of these ways." 40 Equally threatening, however, is the risk that terrorists will steal or purchase fissile material and construct a nuclear device on their own. Very little material is necessary to construct a highly destructive nuclear weapon. 41 Although nuclear devices are extraordinarily complex, the technical barriers to constructing a workable weapon are not significant. 42 Moreover, the sheer number of methods that could be used to deliver a nuclear device into the United States makes it incredibly likely that terrorists could successfully employ a nuclear weapon once it was built. 43 Accordingly, supply-side controls that are aimed at preventing terrorists from acquiring nuclear material in the first place are the most effective means of countering the risk of nuclear terrorism. 44 Moreover, the end of the Cold War eliminated the rationale for maintaining a large military-industrial complex in Russia, and the nuclear cities were closed. 45 This resulted in at least 35,000 nuclear scientists becoming unemployed in an economy that was collapsing. 46 Although the economy has stabilized somewhat, there [\*1439] are still at least 20,000 former scientists who are unemployed or underpaid and who are too young to retire, 47 raising the chilling prospect that these llkjkjklnm would be devastating in terms of immediate human and economic losses. n49 Moreover, there would be immense political pressure in the United States to discover the perpetrators and retaliate with nuclear weapons, massively increasing the number of casualties and potentially triggering a full-scale nuclear conflict. N50 In addition to the threat posed by terrorists, leakage of nuclear knowledge and material from Russia will reduce the barriers that states with nuclear ambitions face and may trigger widespread proliferation of nuclear weapons. n51 This proliferation will increase the risk of nuclear attacks against the United States [\*1440] or its allies by hostile states, n52 as well as increase the likelihood that regional conflicts will draw in the United States and escalate to the use of nuclear weapons.

**Terror attack goes nuclear, ends in extinction**

**Ayson 10** (Robert Ayson, Professor of Strategic Studies and Director of the Centre for Strategic Studies: New Zealand at the Victoria University of Wellington, 2010 “After a Terrorist Nuclear Attack: Envisaging Catalytic Effects,” Studies in Conflict & Terrorism, Volume 33, Issue 7, July, Available Online to Subscribing Institutions via InformaWorld)

 But these two nuclear worlds—**a non-state actor nuclear attack and a catastrophic interstate nuclear exchange—are not necessarily separable**. It is just possible that **some sort of terrorist attack, and especially an act of nuclear terrorism, could precipitate a chain of events leading to a massive exchange of nuclear weapons between two or more of the states that possess them.** In this context, today’s and tomorrow’s terrorist groups might assume the place allotted during the early Cold War years to new state possessors of small nuclear arsenals who were seen as raising the risks of a catalytic nuclear war between the superpowers started by third parties. These risks were considered in the late 1950s and early 1960s as concerns grew about nuclear proliferation, the so-called n+1 problem. It may require a considerable amount of imagination to depict an especially plausible situation where an act of nuclear terrorism could lea to such a massive inter-state nuclear war. For example, in the event of a terrorist nuclear attack on the United States, it might well be wondered just how Russia and/or China could plausibly be brought into the picture, not least because they seem unlikely to be fingered as the most obvious state sponsors or encouragers of terrorist groups. They would seem far too responsible to be involved in supporting that sort of terrorist behavior that could just as easily threaten them as well. Some possibilities, however remote, do suggest themselves. For example, how might the United States react if it was thought or discovered that the fissile material used in the act of nuclear terrorism had come from Russian stocks,40 and if for some reason Moscow denied any responsibility for nuclear laxity? The correct attribution of that nuclear material to a particular country might not be a case of science fiction given the observation by Michael May et al. that while the debris resulting from a nuclear explosion would be “spread over a wide area in tiny fragments, its radioactivity makes it detectable, identifiable and collectable, and a wealth of information can be obtained from its analysis: the efficiency of the explosion, the materials used and, most important … some indication of where the nuclear material came from.”41 Alternatively, **if the act of nuclear terrorism came as a complete surprise, and American officials refused to believe that a terrorist group was fully responsible (or responsible at all) suspicion would shift immediately to state possessors.** Ruling out Western ally countries like the United Kingdom and France, and probably Israel and India as well, authorities in Washington would be left with a very short list consisting of North Korea, perhaps Iran if its program continues, and possibly Pakistan. But at what stage would Russia and China be definitely ruled out in this high stakes game of nuclear Cluedo? In particular**, if the act of nuclear terrorism occurred against a backdrop of existing tension in Washington’s relations with Russia and/or China, and at a time when threats had already been traded between these major powers, would officials and political leaders not be tempted to assume the worst? Of course, the chances of this occurring would only seem to increase if the United States was already involved in some sort of limited armed conflict with Russia and/or China, or if they were confronting each other from a distance in a proxy war**, as unlikely as these developments may seem at the present time. The reverse might well apply too: should a nuclear terrorist attack occur in Russia or China during a period of heightened tension or even limited conflict with the United States, could Moscow and Beijing resist the pressures that might rise domestically to consider the United States as a possible perpetrator or encourager of the attack? **Washington’s early response to a terrorist nuclear attack on its own soil might also raise the possibility of an unwanted (and nuclear aided) confrontation with Russia and/or China. For example, in the noise and confusion during the immediate aftermath of the terrorist nuclear attack, the U.S. president might be expected to place the country’s armed forces, including its nuclear arsenal, on a higher stage of alert. In such a tense environment, when careful planning runs up against the friction of reality, it is just possible that Moscow and/or China might mistakenly read this as a sign of U.S. intentions to use force (and possibly nuclear force) against them**

**2NC Cards**

**Uniqueness**

**Federal surveillance programs are preventing terror attacks now**

**Bash and Cohen 13** (Officials cite thwarted plots, oversight in defending surveillance By Dana Bash and Tom Cohen, CNN Updated 6:38 AM ET, Wed June 19, 2013: <http://www.cnn.com/2013/06/18/politics/nsa-leaks/>)

**Bomb plots targeting the New York Stock Exchange and the city's subway were** among more than 50 terrorist acts worldwide **thwarted by top-secret surveillance programs since the 2001 al Qaeda attacks on the United States,** security officials said Tuesday. **The** startling **details disclosed** at a House intelligence committee hearing **reflected a unified effort by the Obama administration and legislators to defend the telephone and e-mail surveillance made public** this month by classified leaks to newspapers. Testimony by Gen. Keith Alexander, **the National Security Agency director, as well as officials from the FBI, Department of Justice and the Director of National Intelligence office called the programs created under the Patriot Act in the aftermath of the 9/11 attacks a vital tool against terrorist plots. J**oined by panel Chairman Rep. Mike Rogers and other legislators, they condemned the document leaks by former government contractor Edward Snowden as harmful to the United States and its allies. The leaks also led to what officials called widespread public misinformation about the surveillance programs that necessitated the relatively rare open hearing by the intelligence panel, where they detailed previously classified information in order to set the record straight. It was the most comprehensive and specific defense of the surveillance methods that have come under ferocious criticism from civil liberties groups, some members of Congress and others concerned about the reach of government into the private lives of citizens**. National security and law enforcement officials repeated that the programs are tightly run with significant regulation and oversight by federal judges and Congress.** Addressing the most basic questions that have emerged, Rogers asked Alexander if intelligence workers have the ability to simply "flip a switch" in order to listen to phone calls or read the emails of Americans. When Alexander replied "no," Rogers asked again to reinforce the message for anyone listening. "So the technology does not exist for any individual or group of individuals at the NSA to flip a switch to listen to Americans' phone calls or read their e-mails?" he repeated. "That is correct," Alexander answered. He and others also asserted that the leaks were egregious and carry huge consequences for national security. "I think it was irreversible and significant damage to this nation," Alexander said when questioned by Rep. Michele Bachmann. "Has this helped America's enemies?" the conservative Minnesota Republican asked. "I believe it has and I believe it will hurt us and our allies," Alexander said. President Barack Obama has defended the programs as necessary in an era of terror. In an interview with PBS' Charlie Rose broadcast on Monday night, Obama said the situation requires a national debate on the balance between security and privacy. Obama bristles at suggestion he's shifted on snooping Alexander told a Senate committee last week that the surveillance programs helped stop dozens of terror plots, but he was unable then to provide classified details. Under pressure from Rogers and other legislators, Alexander joined law enforcement officials Tuesday in making public some declassified details of the Patriot Act provisions**. In recent years, Alexander said, information "gathered from these programs provided government with critical leads to prevent over 50 potential terrorist events in more than 20 countries around the world."**

**Surveillance programs stopping terror attacks now**

**Gross 13** (U.S. officials: Surveillance programs helped stop 50 terrorist plots Grant Gross covers technology and telecom policy in the U.S. government for the IDG News Service, and is based in Washington, D.C. <http://www.pcworld.com/article/2042340/us-officials-surveillance-programs-helped-stop-50-terrorist-plots.html>)

 **U.S. law enforcement agencies have disrupted more than 50 terrorist plots in the United States and other countries with the help of controversial surveillance efforts at the U.S. National Security Agency,** government officials said Tuesday. **NSA surveillance programs** recently exposed by NSA contractor Edward **Snowden have played a key role in disrupting terrorist activity in more than 20 countries, including 10 terrorist plots in the U.S., since the September 11, 2001**, terrorist attacks on the U.S., NSA director General Keith Alexander told U.S. lawmakers. **“In the 12 years since the attacks on Sept. 11, we have lived in relative safety and security as a nation,” Alexander told the U.S. House of Representatives Intelligence Committee. “That security is a direct result of the intelligence community’s quiet efforts to better connect the dots and learn from the mistakes that permitted those attacks to occur on 9/11.” NSA surveillance authorized by Congress through the Patriot Act and the FISA Amendments Act helped disrupt plots to attack the New York Stock Exchange and the New York subway system,** as well as a plot to bomb a Danish newspaper that published a cartoon of the Prophet Muhammad, officials said. Intelligence officials said they will detail classified information about other thwarted attacks lawmakers soon, they said.

**Links**

**Generic**

**Surveillance is effective at combating terrorism and is the only preventative security method against extremism**

**Inserra and Stimson 15** (David Inserra is a Research Associate for Homeland Security and Cyber Security in the Douglas and Sarah Allison Center for Foreign and National Security Policy, of the Kathryn and Shelby Cullom Davis Institute for National Security and Foreign Policy, at The Heritage Foundation. Charles D. Stimson is Manager of the National Security Law Program and Senior Legal Fellow in the Davis Institute at The Heritage Foundation, “Three Terrorist Plots Disrupted in Three Weeks: 66th Islamist Plot Reconfirms Scope of Threat”, <http://www.heritage.org/research/reports/2015/04/three-terrorist-plots-disrupted-in-three-weeks-66th-islamist-plot-reconfirms-scope-of-threat>, 2015)

This plot is the 55th homegrown plot or attack, meaning that the terrorist was radicalized here in the U.S. It is also the 18th attack or plot aimed at U.S. military targets, the most common target of Islamist terrorists. Despite suggestions to the contrary in the media and in politics, the threat of ISIS, al-Qaeda, and other Islamist terrorists striking the U.S. has not diminished. On June 1, a subsection of the Patriot Act—section 215 of the Foreign Intelligence Surveillance Action, the telephone metadata collection program—is set to expire if not reauthorized. There is no way of knowing whether section 215 was used in this case. Congress is now set to debate section 215 before it expires. A healthy discussion of U.S. security and privacy is an important one that the U.S. should have. In this debate, it is important that Congress understand that intelligence programs are critical to preventing terrorists before they strike. Security alone is not enough since the U.S. cannot make every school, military base, mall, government building, or subway secure and hardened against every type of terrorist attack. **Lawful intelligence, collected under proper warrants and court orders, is the best tool that the U.S. has in this battle against terrorists, who have increased the number of plots in recent months.** The U.S. government has a responsibility to protect Americans from danger and respect their liberties—and it must do both well. Stopping Terrorists Before They Strike As the U.S. faces an apparently growing wave of terrorism, Congress should: Maintain essential counterterrorism tools. Support for important investigative tools is essential to maintaining the security of the U.S. and combating terrorist threats. Legitimate government surveillance programs are also a vital component of U.S. national security and should be allowed to continue. The need for effective counterterrorism operations, however, does not relieve the government of its obligation to follow the law and respect individual privacy and liberty. In the American system, the government must do both equally well. Emphasize community outreach. Federal grant funds should be used to create robust community outreach capabilities in higher-risk urban areas. These funds must not be used for political pork or so broadly that they no longer target those communities at greatest risk. Such capabilities are key to building trust within these communities, and if the United States is to be successful in thwarting lone-wolf terrorist attacks, it must place effective community outreach operations at the tip of the spear. Prioritize local cyber capabilities. Building cyber-investigation capabilities in the higher-risk urban areas must become a primary focus of Department of Homeland Security grants. With so much terrorism-related activity occurring on the Internet, local law enforcement must have the constitutional ability to monitor and track violent extremist activity on the Web when reasonable suspicion exists to do so. Keeping the Homeland Safe Vigilance is necessary to combat terrorism. With three terror plots disrupted in 17 days, the idea of vigilance should take on new meaning for Americans. **The U.S. must have the strategies and tools it needs to stop terrorists before they attack again.**

**Strong surveillance programs key to combat terrorism**

**Inserra 15** (David Inserra is a Research Associate on Homeland Security and Cybersecurity at the Douglas and Sarah Allison Center for Foreign and National Security Policy, “69th Islamist Terrorist Plot: Ongoing Spike in Terrorism Should Force Congress to Finally Confront the Terrorist Threat”, http://www.heritage.org/research/reports/2015/06/69th-islamist-terrorist-plot-ongoing-spike-in-terrorism-should-force-congress-to-finally-confront-the-terrorist-threat)

Terrorism Not Going Away This 69th Islamist plot is also the seventh in this calendar year. Details on how exactly Rahim was radicalized are still forthcoming, but according to anonymous officials, online propaganda from ISIS and other radical Islamist groups are the source.[5] That would make this attack the 58th homegrown terrorist plot and continue the recent trend of ISIS playing an important role in radicalizing individuals in the United States. It is also the sixth plot or attack targeting law enforcement in the U.S., with a recent uptick in plots aimed at police. While the debate over the PATRIOT Act and the USA FREEDOM Act is taking a break, the terrorists are not. **The result of the debate has been the reduction of U.S. intelligence and counterterrorism capabilities, meaning that the U.S. has to do even more with less when it comes to connecting the dots on terrorist plots**.[6] Other legitimate intelligence tools and capabilities must be leaned on now even more. Protecting the Homeland To keep the U.S. safe, Congress must take a hard look at the U.S. counterterrorism enterprise and determine other measures that are needed to improve it. Congress should: Emphasize community outreach. Federal grant funds should be used to create robust community-outreach capabilities in higher-risk urban areas. These funds must not be used for political pork, or so broadly that they no longer target those communities at greatest risk. Such capabilities are key to building trust within these communities, and if the United States is to thwart lone-wolf terrorist attacks, it must place effective community outreach operations at the tip of the spear. Prioritize local cyber capabilities. **Building cyber-investigation capabilities in the higher-risk urban areas must become a primary focus of Department of Homeland Security grants. With so much terrorism-related activity occurring on the Internet, local law enforcement must have the constitutional ability to monitor and track violent extremist activity on the Web when reasonable suspicion exists to do so.** Push the FBI toward being more effectively driven by intelligence. While the FBI has made high-level changes to its mission and organizational structure, the bureau is still working on integrating intelligence and law enforcement activities. Full integration will require overcoming inter-agency cultural barriers and providing FBI intelligence personnel with resources, opportunities, and the stature they need to become a more effective and integral part of the FBI. Maintain essential counterterrorism tools. **Support for important investigative tools is essential to maintaining the security of the U.S. and combating terrorist threats. Legitimate government surveillance programs are also a vital component of U.S. national security and should be allowed to continue.** The need for effective counterterrorism operations does not relieve the government of its obligation to follow the law and respect individual privacy and liberty. In the American system, the government must do both equally well. Clear-Eyed Vigilance The recent spike in terrorist plots and attacks should finally awaken policymakers—all Americans, for that matter—to the seriousness of the terrorist threat. Neither fearmongering nor willful blindness serves the United States. Congress must recognize and acknowledge the nature and the scope of the Islamist terrorist threat, and take the appropriate action to confront it.

**Surveillance key – need proactive counterterrorism surveillance networks to prevent attacks**

**Zuckerman et al 13** (Jessica Zuckerman is a policy analyst at the Heritage Foundation, Steven Bucci is the director at the Douglas and Sarah Allison Center for Foreign and National Security Policy, James Carafano is the vice president at the Kathryn and Shelby Cullom Davis Institute for National Security and Foreign Policy, and the E. W. Richardson Fellow, “60 Terrorist Plots Since 9/11: Continued Lessons in Domestic Counterterrorism,” <http://www.heritage.org/research/reports/2013/07/60-terrorist-plots-since-911-continued-lessons-in-domestic-counterterrorism>, 2013)

Three months after the attack at the Boston Marathon, the pendulum of awareness of the terrorist threat has already begun to swing back, just as it did after 9/11. Due to the resilience of the nation and its people, for most, life has returned to business as usual. The threat of terrorism against the United States, however, remains. Expecting to stop each and every threat that reaches a country’s borders is unreasonable, particularly in a free society committed to individual liberty. Nevertheless, there are important steps that America’s leaders can take to strengthen the U.S. domestic counterterrorism enterprise and continue to make the U.S. a harder target. Congress and the Administration should: Ensure a proactive approach to preventing terrorist attacks. Despite the persistent threat of terrorism, the Obama Administration continues to focus on reactive policies and prosecuting terrorists rather than on proactive efforts to enhance intelligence tools and thwart terrorist attempts. This strategy fails to recognize the pervasive nature of the threat posed by terrorist groups such as al-Qaeda and homegrown extremism. The Administration, and the nation as a whole, should continue to keep in place a robust, enduring, and proactive counterterrorism framework in order to identify and thwart terrorist threats long before the public is in danger. Maintain essential counterterrorism tools. **Support for important investigative tools** such as the PATRIOT Act **is essential to maintaining the security of the U.S. and combating terrorist threats. Key provisions** within the act, **such as the** roving **surveillance authority** and business records provision, **have proved essential for thwarting terror plots**, yet they require frequent reauthorization. In order to ensure that law enforcement and intelligence authorities have the essential counterterrorism tools they need, Congress should seek permanent authorization of the three sun setting provisions within the PATRIOT Act.[208] Furthermore, legitimate government surveillance programs are also a vital component of U.S. national security, and should be allowed to continue. Indeed, in testimony before the house, General Keith Alexander, the director of the National Security Agency (NSA), revealed that more than 50 incidents of potential terrorism at home and abroad were stopped by the set of NSA surveillance programs that have recently come under scrutiny. That said, the need for effective counterterrorism operations does not relieve the government of its obligation to follow the law and respect individual privacy and liberty. In the American system, the government must do both equally well. Break down the silos of information. Washington should emphasize continued cooperation and information sharing among federal, state, and local law enforcement agencies to prevent terrorists from slipping through the cracks between the various jurisdictions. In particular, the FBI should make a more concerted effort to share information more broadly with state and local law enforcement. State and local law enforcement agencies are the front lines of the U.S. national security strategy. As a result, local authorities are able to recognize potential danger and identify patterns that the federal authorities may miss. They also take the lead in community outreach, which is crucial to identifying and stopping “lone wolf” actors and other homegrown extremists. Federal law enforcement, on the other hand, is not designed to fight against this kind of threat; it is built to battle cells, groups, and organizations, not individuals. Streamline the domestic counterterrorism system. The domestic counterterrorism enterprise should base future improvements on the reality that governments at all levels are fiscally in crisis. Rather than add additional components to the system, law enforcement officials should streamline the domestic counterterrorism enterprise by improving current capabilities, leveraging state and local law enforcement resources and authorities, and, in some cases, reducing components where the terrorist threat is not high and the financial support is too thin or could be allocated more effectively. For example, the Department of Homeland Security should dramatically reduce the number of fusion centers, many of which exist in low-risk areas or areas where similar capabilities exist. An easy way to reduce the number of fusion centers is to eliminate funding to those that are located outside the 31 urban areas designated as the highest risk. Fully implement a strategy to counter violent extremism. Countering violent extremism is an important complementary effort to an effective counterterrorism strategy. In August 2011, the U.S. government released a strategic plan called “Empowering Local Partners to Prevent Violent Extremism in the United States.”[209] The plan focuses on outlining how federal agencies can assist local officials, groups, and private organizations in preventing violent extremism. It includes strengthening law enforcement cooperation and helping communities understand how to counter extremist propaganda (particularly online). Sadly, this plan is not a true strategy. It fails to assign responsibilities and does not direct action or resource investments. More direction and leadership must be applied to transform a laundry list of good ideas into an effective program to support communities in protecting and strengthening civil society. Vigilance Is Not Optional In a political environment of sequestration on the one hand and privacy concerns on the other, there are those on both sides of the aisle who argue that counterterrorism spending should be cut and U.S. intelligence agencies reigned in. As the above list indicates however, the long war on terrorism is far from over. Most disturbingly, an increasing number of Islamist-inspired terrorist attacks are originating within America’s borders. The rise of homegrown extremism is the next front in the fight against terrorism and should be taken seriously by the Administration. While there has not been another successful attack on the homeland on the scale of 9/11, the bombings in Boston reminded the country that the threat of terrorism is real and that continued vigilance is critical to keeping America safe. Congress and the Administration must continue to upgrade and improve the counterterrorism capabilities of law enforcement and intelligence agencies as well exercise proper oversight of these capabilities. The American people are resilient, but the lesson of Boston is that the government can and should do more to prevent future terror attacks.

**FISA/PATRIOT Act**

**Surveillance techniques under the US PATRIOT Act are key to stop terrorism – prevents flow of information and resources between terrorist cells**

**McNeil 09** (Jena Baker McNeill is Policy Analyst for Homeland Security in the Douglas and Sarah Allison Center for Foreign Policy Studies, a division of the Kathryn and Shelby Cullom Davis Institute for International Studies, at The Heritage Foundation, “Patriot Act: A Chance to Commit to National Security”, <http://www.heritage.org/research/reports/2009/10/patriot-act-a-chance-to-commit-to-national-security>, 2009)

On September 22-23, the House and Senate Judiciary Committees held hearings to examine reauthorization of key provisions of the Patriot Act, which helps law enforcement fight terrorism through more flexible surveillance and investigation methods and easier information sharing. Key provisions of the act will expire on December 31 if Congress does not reauthorize them. The three foiled terrorist plots announced this past week are evidence that **America's counterterrorism tools are working**. And **the Patriot Act is a key element in this framework**. Not only does it **help fight terrorism by aiding authorities in their effort to stop the flow of information and resources between terrorist groups**, but it does so in a way that is consistent with the U.S. Constitution. This tool should be supported and maintained by Congress. Three Key Provisions The Patriot Act, enacted shortly after the attacks on 9/11, was intended to help law enforcement share information as well as to provide more extensive methods by which to track down terrorists at the earliest stages of terrorist plot formation. The act makes it easier for authorities to conduct surveillance on terrorists, with key provisions that account for modern technologies (such as cell phones). While there are multiple provisions that make up the Patriot Act, there are three provisions set to expire this year: 1. Section 206: **Roving Surveillance Authority**. This provision **allows** law enforcement, after approval from the court created by the Foreign Intelligence Surveillance Act (FISA), to conduct **continuous surveillance of national security suspects across modes of communications**. It is meant **to stop terrorists who often switch telecommunications devices** (like cell phones) **to evade authorities**. While roving surveillance has been available to authorities in criminal investigations prior to 2001, Section 206 would allow authorities to perform such an act in national security investigations. This gives law enforcement flexibility, but it does so with built-in procedural safeguards, such as a requirement that the requesting authority demonstrate probable cause for the surveillance. It further requires continuous monitoring by the FISA court and extensive oversight by Congress. This section, used approximately 140 times since 2001, is a gigantic step forward in terms of helping law enforcement fight terrorism in a modern, technological world. 2. Section 215: Business Record Orders under FISA. This provision allows law enforcement, with approval from the FISA court, to require disclosure of documents and other records from businesses and other institutions (third parties) without a suspect's knowledge. It is essentially a way for prosecutors to obtain evidence in national security investigations in a fashion similar to that of a grand jury subpoena. The difference is that Section 215 actually requires more procedural safeguards than a grand jury subpoena, including a requirement that the requesting authority show relevance and obtain court approval (the grand jury standard being a simple showing of relevance). It further protects civil liberties by requiring additional approval for document requests that might have the slightest relation to freedom of speech and expression, such as library records. It has been used approximately 250 times since 9/11. 3. Section 6001 of the Intelligence Reform and Terrorism Prevention Act: The Lone Wolf Provision. This provision allows law enforcement to track non-U.S. citizens acting alone to commit acts of terrorism that are not connected to an organized terrorist group or other foreign power. While the FBI has confirmed that this section has never actually been used, it needs to be available if the situation arises where a lone individual may seek to do harm to the United States. A Success Story **The U.S. has not experienced a terrorist attack on its own soil since 9/11, despite repeated attempts.** In fact, an examination of publicly available information demonstrates that at least 26 terrorist plots have been foiled since 9/11. The 2002 Lackawanna Six plot, where individuals involved in the drug trade went overseas to obtain terrorist training, was foiled partly because law enforcement was able to pursue the investigation as a single case, a luxury afforded to them only because of changes made under the Patriot Act. Under a pre-Patriot Act standard, law enforcement would have been required to pursue the drug investigation separately from the terrorism plot, unable to share information and evidence acquired. Attorney General John Ashcroft has credited the Patriot Act as a major factor in the arrest of 310 terrorism suspects. And just this week, the success of the Patriot Act was recognized by President Barack Obama when he expressed his support for its reauthorization. While the FBI has not indicated whether this week's foiled plots were the result of the Patriot Act's provisions, a spokesman stated that he could not discuss the tools used to investigate the case because these authorities were before the FISA court.[1] Time to Institutionalize Our Counterterrorism Tools Despite repeated attempts to demonstrate abuse, little evidence has ever been proffered to demonstrate any Patriot Act misuse. In fact, at times the Patriot Act offers significantly more protections than available under common criminal investigations. And more often than not, it simply modernizes already-available tools that prosecutors have used routinely in criminal investigations well before 2001. These provisions are subject to routine oversight by both the FISA court and Congress. The act has been narrowed and refined continuously, contributing to the fact that no single provision of the Patriot Act has ever been found unconstitutional. **Congress should resist initiatives that would repeal or erode key provisions of the Patriot Act and should fully institutionalize these tools into the broader counterterrorism framework**. As former White House Homeland Security Advisor Ken Weinstein, phrased it, "There is no reason to return to the days when it was easier for prosecutors to secure records in a simple assault prosecution than for national security investigators to obtain records that may help prevent the next 9/11."

**PATRIOT Act key – give investigative power to local and national law enforcement to stop terrorist plots**

**Zuckerman et al 12** (Jessica Zuckerman is a policy analyst at the Heritage Foundation, Steven Bucci is the director at the Douglas and Sarah Allison Center for Foreign and National Security Policy, James Carafano is the vice president at the Kathryn and Shelby Cullom Davis Institute for National Security and Foreign Policy, and the E. W. Richardson Fellow, “Fifty Terror Plots Foiled Since 9/11: The Homegrown Threat and the Long War on Terrorism,”http://www.heritage.org/research/reports/2012/04/fifty-terror-plots-foiled-since-9-11-the-homegrown-threat-and-the-long-war-on-terrorism, 2012)

The death of Osama bin Laden marked an important victory in the long war on terrorism. The war, however, is not won. Terrorists, including those radicalized in the United States, continue to seek to harm the U.S. and its people. As the first anniversary of the death of bin Laden approaches, Congress and the Administration should be mindful of what is needed to continue to combat the threat of terrorism at home and abroad. **In order to prevent the next terrorist attack, lawmakers should: · Preserve existing counterterrorism and intelligence tools, such as the PATRIOT Act**. Support for important investigative tools, such as the PATRIOT Act, is essential to maintaining the security of the United States and combating terrorist threats. **Key provisions in the act, such as the roving surveillance authority** and business records provisions, **have proven essential in thwarting numerous terror plots.** For instance, the PATRIOT Act’s information-sharing provisions were essential for investigating and prosecuting homegrown terrorists, such as the Lackawanna Six. This case, along with others, demonstrates that national security investigators continue to require the authorities provided by the PATRIOT Act to track leads and dismantle plots before the public is put in danger. Bearing this fact in mind, Congress should not let key provisions of the PATRIOT Act expire, and instead, should make them permanent.

**NSA**

**NSA surveillance key to stop terrorism – detects communication networks that are necessary to locating terrorist**

**Bolton 15** (John Bolton is a lawyer and researcher at the American Enterprise Institute for US Foreign policy and national security, “NSA activities key to terrorism fight”, <https://www.aei.org/publication/nsa-activities-key-to-terrorism-fight/>, April 28, 2015)

Congress is poised to decide whether to re-authorize programs run by the National Security Agency that assess patterns of domestic and international telephone calls and emails to uncover linkages with known terrorists. These NSA activities, initiated after al-Qaeda’s deadly 9/11 attacks, have played a vital role in protecting America and our citizens around the world from the still-metastasizing terrorist threat. The NSA programs do not involve listening to or reading conversations, but rather seek to detect communications networks. If patterns are found, and more detailed investigation seems warranted, then NSA or other federal authorities, consistent with the Fourth Amendment’s prohibition against unreasonable searches and seizures, must obtain judicial approval for  more specific investigations. Indeed, even the collection of the so-called metadata is surrounded by procedural protections to prevent spying on U.S. citizens. Nonetheless, critics from the right and left have attacked the NSA for infringing on the legitimate expectations of privacy Americans enjoy under our Constitution. Unfortunately, many of these critics have absolutely no idea what they are talking about; they are engaging in classic McCarthyite tactics, hoping to score political points with a public justifiably worried about the abuses of power characteristic of the Obama administration. Other critics, following Vietnam-era antipathies to America’s intelligence community, have never reconciled themselves to the need for robust clandestine capabilities. Still others yearn for simpler times, embodying Secretary of State Henry Stimson’s famous comment that “gentlemen don’t read each others’ mail.” The ill-informed nature of the debate has facilitated scare-mongering, with one wild accusation about NSA’s activities after another being launched before the mundane reality catches up. And there is an important asymmetry at work here as well. The critics can say whatever their imaginations conjure up, but NSA and its defenders are significantly limited in how they can respond. By definition, the programs’ success rests on the secrecy fundamental to all intelligence activities. Frequently, therefore, explaining what is not happening could well reveal information about NSA’s methods and capabilities that terrorists and others, in turn, could use to stymie future detection efforts. After six years of President Obama, however, trust in government is in short supply. It is more than a little ironic that Obama finds himself defending the NSA (albeit with obvious hesitancy and discomfort), since his approach to foreign and defense issues has consistently reflected near-total indifference, except when he has no alternative to confronting challenges to our security. Yet if harsh international realities can penetrate even Obama’s White House, that alone is evidence of the seriousness of the threats America faces. In fact, just in the year since Congress last considered the NSA programs, the global terrorist threat has dramatically increased. ISIS is carving out an entirely new state from what used to be Syria and Iraq, which no longer exist within the borders created from the former Ottoman Empire after World War I. In already-chaotic Libya, ISIS has grown rapidly, eclipsing al-Qaeda there and across the region as the largest terrorist threat. Boko Haram is expanding beyond Nigeria, declaring its own caliphate, even while pledging allegiance to ISIS. Yemen has descended into chaos, following Libya’s pattern, and Iran has expanded support for the terrorist Houthi coalition. Afghanistan is likely to fall back under Taliban control if, as Obama continually reaffirms, he withdraws all American troops before the end of 2016. **This is not the time to cripple our intelligence-gathering capabilities against the rising terrorist threat. Congress should unquestionably reauthorize the NSA programs**, but only for three years. That would take us into a new presidency, hopefully one that inspires more confidence, where a calmer, more sensible debate can take place.

**Drones**

**Domestic drones key to war on terror – provide information for counterterrorism**

**O’Brien 13** (Michael O’brien is a political reporter at NBC news, “FBI director tells Congress agency uses drones for surveillance on U.S. soil”, <http://nbcpolitics.nbcnews.com/_news/2013/06/19/19041488-fbi-director-tells-congress-agency-uses-drones-for-surveillance-on-us-soil?lite>, 6/19/13)

FBI director Robert Mueller said Wednesday that the nation's top law enforcement bureau uses drones to conduct surveillance on U.S. soil, though only on a "very, very minimal basis." Mueller, the FBI director since 2001 who is set to retire this year, acknowledged that his agency uses drones in its investigative and law enforcement practices, and is further working to establish better guidelines for the use of drones. "We are in the early stages of doing that, and I will tell you that our footprint is very small, we have very few, and have limited use. And we're exploring not only the use, but the necessary guidelines for that use," Mueller told senators at a hearing this morning when asked about the use of drones. The government's use of drones on U.S. soil has been well-documented. The Department of Homeland Security, for instance, employs aerial drones to help police the United States border with Mexico. Mueller said that drones are used for surveillance, though, only on a "seldom" basis. The FBI director's words come amid a simmering national debate in recent months about what limits should be placed on the government in its law enforcement and anti-terrorism activities. Sen. Rand Paul, R-Ky., for instance, waged a filibuster challenging President Barack Obama's use of drones in pursuing terrorist suspects. Paul won an affirmation from the administration that it was their thought that it would be illegal for the government to use a drone strike against a U.S. citizen on American soil. The drones that have come into practice in the United States, though, are different from the armed, militarized drones used in military operations. Still, the exchange reflects broader concerns about the scope of government power, represented most recently and most vividly by revelations about the National Security Agency's collection of phone and internet "meta-data" for analysis. Mueller, like virtually every other administration official and senior lawmaker who has spoken about the NSA practices in recent weeks, defended the NSA's activities as an invaluable tool in the government's pursuit of terrorist suspects. "If we're going to prevent terrorist attacks, we have to be on their communications," Mueller said during his appearance before the Senate Judiciary Committee. "You never know which dot will be critical. You need as many as you can get. Let there be no mistake, there would be fewer dots to connect if you don't have a data base that retains those records." As to the prosecution of Edward Snowden, the self-admitted leaker of information about NSA monitoring, Mueller said the leak had done legitimate harm to U.S. safety, and vowed to pursue Snowden. "As to the person who has admitted to making these disclosures, he is the subject of an ongoing criminal investigation," Mueller said. "These disclosures have caused significant harm to our nation and to our safety, and we are taking all necessary steps to hold accountable that person for these disclosures."

**Court approval/Oversight**

**Court approval creates too many hoops for intelligence programs to jump through – makes counter terrorism ineffective**

**Wiser 14** (Daniel Wiser is a researcher at the center for security policy, “Altering NSA Surveillance Programs Would Interfere With Vital Intelligence Operations”, <http://www.centerforsecuritypolicy.org/2014/01/14/altering-nsa-surveillance-programs-would-interfere-with-vital-intelligence-operations/>, 1/14/2014)

A national security think tank criticized on Monday recommendations by President Barack Obama’s review group to alter National Security Agency (NSA) surveillance programs and said they would interfere with vital U.S. intelligence operations. The report by the Center for Security Policy (CSP) said the group’s recommendations would “eviscerate” the NSA’s collection of phone metadata, which is used for counterterrorism purposes. The group proposed that phone companies or a private third party hold the data and only allow access to them on a case-by-case basis if the NSA obtains an order from the Foreign Intelligence Surveillance (FISA) Court. Phone “metadata” includes the numbers dialed, call times, and durations of calls, but not the content or subscriber names. President Obama is expected to embrace many of the recommendations in an address on Friday. Wholesale changes to the metadata program would likely require congressional or court involvement. CSP president and CEO Frank Gaffney said President Obama must be careful not to overreact to revelations about the program released in documents by NSA leaker Edward Snowden. “It is highly unfortunate that in response to Edward Snowden’s actions, this review group—convened by President Obama—is advocating measures that will fundamentally interfere with vital U.S. intelligence operations,” Gaffney said in a press release. “**The threats our nation continues to face demand an empowered and agile intelligence capability** with appropriate oversight by Congress, and it is our hope that President Obama’s response to his review group’s report will reflect an understanding of that need, rather than a capitulation to those whose real agenda is to weaken America’s capacity for self-defense,” he added. The CSP report takes issue with a number of the review group’s recommendations, including several related to the metadata program authorized by Section 215 of the Patriot Act**. Requiring intelligence agencies to obtain court approval for so-called 215 orders creates legal obstacles to accessing data that might be needed to address urgent national security threats such as potential terrorist attacks**, the report said. It instead suggested that President Obama defer to bipartisan legislation currently working its way through the intelligence committees that would require NSA analysts to have a “reasonable articulable suspicion” that a phone number is associated with terrorism before querying the metadata. The report also said moving the data to private companies would raise new privacy concerns because it would then be held on less secure servers in numerous locations and be managed by more people. The metadata program is currently subject to oversight by the congressional intelligence committees and the FISA court, and only 22 intelligence agents have access to the database. “While the review group would keep the 215 program in place, we oppose all of its recommendations on this program as they would place so many limitations on the metadata program that it would be rendered virtually useless,” the report said. “We also believe these recommendations address privacy concerns that lack validity and would actually increase the potential for real privacy violations.” The report also defended the metadata program’s counterterrorism credentials. “Although the review group report states that the 215 program ‘was not essential to preventing terrorist attacks,’ review group member Michael Morell contradicted this finding just after the report was issued when he said in a Dec. 27, 2013 Washington Post op-ed that if the metadata program had been in place before September 2001, ‘it would likely have prevented 9/11’ and ‘has the potential to prevent the next 9/11.’” Additionally, the report raised concerns that extending privacy rights under U.S. law to foreign persons would tie the hands of intelligence agencies and prevent them from considering political or religious motivations, such as the Islamic extremism of al Qaeda members. The Senate Judiciary Committee will hold a hearing tomorrow on the recommendations by President Obama’s review group. Two federal judges so far have issued contradictory rulings about the constitutionality of the metadata program. Judge Richard Leon said the program was “likely unconstitutional” and “Orwellian,” while Judge William Pauley said it was an important tool for apprehending terrorist conspirators and confirming ties.

**TC – Rights**

**Terrorism causes policies that hurt rights**

**Caldwell 10** (Tracey-Kay, editor at BellaOnline, “Terrorism and Freedom”, http://www.bellaonline.com/articles/art46178.asp)

Freedom, is the most important word in the War on Terrorism. On 9/11/2001, President Bush declared, “Freedom has been attacked, but freedom will not be defeated.” But it is freedom that has been most endangered since 9/11, with secretive subpoenas, secretive arrests, secretive detentions, and secretive trials. Lynch quotes author James Bovard as observing that, “For Bush, freedom seems to be whatever extends his own political power. Whatever razes any barriers to executive power—that is freedom.” Is that the freedom that Americans were concerned with after 9/11? Did we want freedom for our President from the checks and balances that our Constitution provides? Or were we more interested in Webster’s New World Dictionary’s definition of freedom as “the state or quality of being free; exemption or liberation from the control of some other person or some arbitrary power; liberty; independence.”
Protecting our freedom and winning the War on Terror can only be achieved when we focus on the real threat, the ones who perpetrated the acts that led to death of three thousand people on 9/11. When we stop allowing our political leaders to use the War on Terror to further there own goals and powers. When we hold them accountable for not capturing Bin Laden, for not thwarting the growth and popularity of Al-Queda throughout the world. We must not allow them to use Doublespeak, to redefine the vocabulary, to confuse the message of the War on Terror, to leave us less safe, while they increase their own power.

**TC – Economy**

**Terrorism is the best internal link to economy**

**International Review 02** (Jan. 29, http://www.int-review.org/terr25a.html)

Terror Attack on Global Economic Progress The repercussions trickle down through every layer of the global economy. In the era of globalization, the September 11 terrorist attacks on New York and Washington have had worldwide economic consequences, felt even in those countries that are not likely to become terrorist targets themselves. Ultimately, some of the weakest Third World economies could suffer the worst fallout from the September attacks. The necessary preoccupation with counter-terrorism measures is also diverting attention and resources away from economic development throughout the world. The Group of Seven (G-7) top industrial countries is concerned about panic in the banking sector. On September 13, the U.S. Federal Reserve made US$50 billion available to stabilize European banking systems. Many G-7 central banks have cut interest rates to boost consumer confidence and funnel more money into the ailing global economy. Macro-Economic Realities The U.S. Treasury concedes that a recession may well result from the September 11 horrors. A decline in gross domestic product is likely to continue into at least the first quarter of 2002. Before September 11, U.S. gross domestic product was expected to increase by 2 percent in the fourth quarter of 2001. In the days following the attacks in New York and Washington, U.S. employers cut more than 248,000 jobs. The transportation sector was especially hard hit, with more than 96,000 lay-offs. The attacks have also curbed consumer spending, which normally accounts for about two thirds of U.S. economic activity. European Impact Reduced consumer confidence is evident in most member states of the European Union. Even Britain, which enjoyed the strongest economic position prior to the terrorist attacks, was forced to revise downward its modest expectations of GDP growth for this year. Concerns about further terrorist designs on air travel have sent Europe's airline industry into a tailspin. The Belgian carrier Sabena filed for bankruptcy. Government bailouts were necessary for airlines in France and Switzerland. Major carriers in Britain, Italy, the Netherlands and Scandinavia cut flight capacity, scrapping certain routes and layed off tens of thousands of employees. Some European airlines are adding "crisis" or "war" surcharges -- to help defray the soaring insurance costs -- to ticket prices. Stock markets throughout Europe have wobbled, not only because of investor uncertainty. The very integrity of G-7 stock markets has been under assault, as financial investigators in Germany, Italy and Switzerland explore evidence that al-Qaida, the Afghanistan-based Middle Eastern terrorist network behind the September 11 attacks, engaged in insider trading. Aware that the attacks would devastate the airline and insurance industries in Europe, al-Qaida members reportedly profited from "put options," negotiable bids speculating that the price of certain airline and insurance stocks would decline within a short time frame. East Asian Impact Japan, already in a recession, is likely to face deeper economic challenges. The decline in U.S. consumer spending will hurt, among other things, the Japanese auto industry. Japan, Asia's sole G-7 member, has seen its economic difficulties multiply since the September terrorist attacks. Since the United States buys about 40 percent of Japanese exports, reduced U.S. consumption means declines in Japanese exports, production, employment and capital investment. Tourism has also dropped off since September 11. In Okinawa alone, 78,000 tourist trips were canceled between mid-September and mid-October. Japan Airlines and All Nippon Airways have been forced to cut flights since September 11. Similar cuts have been made by Malaysian Air and Korean Air, which is considering hundreds of layoffs. Carriers in Thailand and China have added surcharges to air ticket prices. Cambodia, which nets about US$120 million a year from tourism, reported that 30 percent of foreign tourists canceled bookings in the second half of September. Cambodia is also worried about textile exports, 75 percent of which are sold to the U.S. market. Some cash-starved Asian firms may fail because of growing concern among international investors about taking commercial risks. About US$3.5 billion worth of debt refinancing is already in question in East Asia. The most imperiled country in the region is the Philippines, where the government will probably increase deficit spending to cushion the domestic impact of the global recession. Impact on Latin America and Caribbean Latin America, as a whole, had been expected to realize modest economic growth, about 1.3 percent, in 2001. Since the September terrorist attacks, economists now believe that regional GDP may not grow at all. The post-attack economic climate is drying up the tourism industry in Latin America and the Caribbean. Aeromexico and Mexicana Airlines have already laid off thousands of workers. Hotel reservations in El Salvador were half the normal volume in late September. Export industries in Mexico and Central America are reeling from reduced consumption in the United States and from the post-attack plunge in many commodity prices. By early October 2001, Guatemalan employers had laid off 250,000 workers, mostly in the textile industry. That number could grow by another 15 percent in the coming months. Even countries whose economies are less interwoven with the U.S. market are hurting. Speculation born of economic uncertainty devalued Brazil's currency by more than 8 percent. This will translate into increased government debt. Global risk aversion in the wake of the terrorist attacks will deepen the difficulty of attracting foreign investors so badly needed in Argentina, where debt default was already a possibility before September 11. Impact on Muslim Countries Muslim countries are experiencing the same post-attack losses in their tourism and travel sectors. By early October 2001, eight foreign carriers had suspended flights into Pakistan, while freight insurance surcharges were driving up the costs of imports to that country. Masood Ali Khan, head of Pakistan's Tourism Development Corporation, predicts a decline in tourism of between 80 and 90 percent for the coming months. In Egypt, hotel occupancy rates dropped by nearly 50 percent in the second half of September. Tourism is Egypt's top hard-currency earner. During an October meeting of tourism ministers from the Organization of the Islamic Conference (OIC), representatives from Iran's Supreme Tourism Council pleaded for joint action to overcome terrorism-related obstacles to tourism development. The post-attack difficulties of the global aviation industry have also hurt the Organization of Petroleum Exporting Countries. By early October, the price of crude oil had declined to US$20.44 a barrel, well below OPEC's target range of US$22 to US$28. Demand for jet fuel is particularly depressed, because of air safety concerns General Problems for Developing Countries Increased freight insurance costs since the September attacks may put some basic imports beyond the capabilities of the world's poorest countries. Some panic buying of food staples has already been reported, in an apparent attempt to stock up before transportation costs go higher. World Bank analysts predict that the post-attack economic uncertainty will deepen poverty in Africa in particular. The World Bank believes the Third World will feel the impact of the post-attack recession through 2002. Development Focus Blurred Numerous conferences addressing economic development have been postponed or derailed since the September attacks. Concerns about further terrorist attacks delayed gatherings of the World Bank, International Monetary Fund, the U.N. Food and Agriculture Association and a summit of francophone countries. The World Trade Organization decided to relocate its November summit, originally planned for Qatar, worried about the security of the Middle Eastern venue. Beijing implemented tight security for the late October conference of the 21-nation Asia-Pacific Economic Cooperation (APEC) forum. The participants had planned to focus on new development initiatives, such as the "Human Capacity Building Promotion Program," a campaign to promote the region's information technology industry. But development concerns were given less attention than the threat of terrorism -- and the need to regain economic ground lost since the September attacks. Insurance Industry Insurers from many countries have had to cover unparalleled losses from the World Trade Center attack. Lloyd's of London expects its insurance syndicates to cover claims amounting to US$1.9 billion. Swiss Re, a major reinsurer (a business that insures regular insurance companies against an unanticipated spike in claims) expects to cover US$1.24 billion in claims resulting from the U.S. attacks. The overall cost of insurance claims resulting from the September 11 horrors could amount to US$35 billion. As a result, insurance prices are rising, while demand for insurance increases in anticipation of additional acts of terror by Osama bin Laden's network. The price hikes are passed along to other companies, to governments and ultimately to the individual taxpayer and consumer. Food and other basic consumer items could become more expensive as freight insurance costs increase. In anticipation of higher freight prices down the line, Egypt made unusually large purchases of U.S. wheat following the attacks. Pakistan is already struggling with price increases for certain imports, because of rising freight insurance costs. Air travelers are encountering new surcharges to cover higher insurance costs. On October 1, Thai Airways International began adding a US$1.25 surcharge to most of its flights. The Chinese government authorized domestic air carriers to levy surcharges of up to US$2.50 per passenger on international routes. Alitalia imposed a "crisis surcharge" of US$5.50 for each leg of an air journey. The Airline Industry More expensive airline insurance costs, heightened security expenditures and public fears about the safety of air travel translate into huge losses for airlines throughout the world. The airline industry is a major factor in the health of an industrialized economy. In the United States, for example, that industry contributes 10 percent to the gross domestic product, directly and indirectly. Following the September 11 attacks in the United States, the global civil aviation industry plunged into its worse crisis in more than 50 years, costing the sector 400,000 jobs around the world. The International Labor Organization reported in January 2002 that the attacks affected every segment in the industry - carriers, airports, aircraft manufacturers, services, parking lots and rented vehicles. In the aftermath of September 11, the Italian airline, Alitalia, considered cutting 2,500 jobs, while the Belgian carrier Sabena filed for bankruptcy. The Swiss government bailed out Swissair after the carrier grounded its planes for lack of cash in late September. KLM Royal Dutch Airlines plans to reduce capacity by 15 percent and ask its workers to take a "substantial" pay cut. Scandinavia's SAS, suffering a 20 percent drop in business-class traffic since September 11, will reduce flight capacity by 12 percent in 2002 and cut about 1,100 jobs. Malaysian Airlines System has cut 12 international flights. Korean Air has suspended flights on five international routes and reduced four others temporarily, while another Korean airline, Asiana, may slash 1,200 jobs. Japan Airlines and All Nippon Airways are also scrapping some international flights

**Terrorism would collapse the global economy**

**DEPARTMENT OF WASHINGTON FILE** **02** (“TERRORISM DESTROYS LIVES AND ECONOMIES.” AMBASSADOR FRANCIS TAYLOR'S REMARKS IN MANILA. [HTTP://CANBERRA.USEMBASSY.GOV/HYPER/2002/1112/EPF203.HTM](http://CANBERRA.USEMBASSY.GOV/HYPER/2002/1112/EPF203.HTM))

Terrorism not only destroys lives, but has a "tremendous economic impact" as well, says Ambassador Francis X. Taylor, the coordinator for counterterrorism at the U.S. Department of State. In remarks delivered November 8 in Manila, the Philippines, to the International Conference on Terrorism and Tourism Recovery, Taylor said the World Bank estimates that over 360,000 jobs in Indonesia were effectively lost because of a single terrorist attack in Bali. Taylor said the jobs that were lost in Indonesia "were connected to a global economy that enables tourists from Australia, Europe, the United States, Japan and many other countries around the world to go to beautiful beaches and resorts, and the resorts of Bali, and to vacation spots here in the Philippines and in many other nations around the world." The "global economy," he said, is supported by global institutions that include transportation systems and security standards, international banking and financial institutions, and information systems. "More fundamentally, political institutions, democracy, and the rule of law create the stability that allows our economies to prosper in this global environment that we operate in," Taylor said. "These global institutions are key to our prosperity, but they can also be exploited by terrorists who use them to move money, manpower, and materials, such as explosives or weapons, across borders and through our banks."

**Aff**

**Defense**

**NSA Surveillance fails**

**Bulk data collection and specific investigations by the NSA only has effected 1.8% of counterterrorism cases – traditional investigation technique solve**

**Bergen et al 14** ( Peter Bergen is the director of the National Security Program at the New America Foundation, where David Sterman and Emily Schneider are research assistants and Bailey Cahall is a research associate, “Do NSA's Bulk Surveillance Programs Stop Terrorists?”, New America Foundation, <http://pierreghz.legtux.org/streisand/autoblogs/frglobalvoicesonlineorg_0e319138ab63237c2d2ae> ff84b4cb506d936eab8/media/e1982452.Bergen\_NAF\_NSA20Surveillance\_1\_0.pdf, January 2014)

A. Traditional investigative methods initiated the majority of terrorism cases. Traditional investigative methods initiated 60 percent of the cases we identified. In 5 percent of the cases, a violent incident occurred prior to prevention, and in 28 percent of the cases – involving 62 individuals – court records and public reporting do not identify which methods initiated the investigation. The unclear cases may have been initiated by an undercover informant, a family member tip, other traditional law enforcement methods, CIA- or FBIgenerated intelligence, NSA surveillance of some kind, or any number of other methods. Additionally, some of these cases may be too recent to have developed a public record large enough to identify which investigative tools were used. In 23 of these 62 unclear cases (37 percent), an informant was involved, though we were unable to determine whether the informant initiated the investigation. **The widespread use of informants suggests that if there was an NSA role in these cases, it was limited and insufficient to generate evidence of criminal wrongdoing without the use of traditional investigative tools.** NSA surveillance of any kind, whether bulk or targeted of U.S. persons or foreigners, played an initiating role in only 7.5 percent of cases. To break that down further: **The controversial bulk collection of telephone metadata appears to have played an identifiable role in, at most, 1.8 percent of the terrorism cases** we examined. In a further 4.4 percent of the cases, NSA surveillance under Section 702 of targets reasonably believed to be outside of the country that were communicating with U.S. citizens or residents likely played a role, while NSA surveillance under an unknown authority likely played a role in 1.3 percent of the cases we examined.

**Metadata fails**

**Metadata collection is not efficient or effective – nearly zero impact on terrorist organizations**

**Bergen et al 14** ( Peter Bergen is the director of the National Security Program at the New America Foundation, where David Sterman and Emily Schneider are research assistants and Bailey Cahall is a research associate, “Do NSA's Bulk Surveillance Programs Stop Terrorists?”, New America Foundation, <http://pierreghz.legtux.org/streisand/autoblogs/frglobalvoicesonlineorg_0e319138ab63237c2d2aeff84> b4cb506d936eab8/media/e1982452.Bergen\_NAF\_NSA20Surveillance\_1\_0.pdf, January 2014)

B. Surveillance of American phone metadata has had no discernible impact on preventing acts of terrorism and only the most marginal of impacts on preventing terrorist-related activity, such as fundraising for a terrorist group. **NSA director** Gen. Alexander, under tough questioning from Sen. Patrick Leahy (D-Vt.) during a Senate Judiciary Committee hearing on October 2, 2013, **admitted that there was only one plot** – that involving Basaaly Moalin – **in which, due to the bulk collection of American telephone metadata under Section 215, terrorist activity was prevented**.\* Our findings are consistent with that admission: The Moalin case is the only plot we were able to identify in which Section 215 appeared to play a potentially key role. Basaaly Moalin, a San Diego cabdriver, provided $8,500 to al-Shabaab, al-Qaeda’s affiliate in Somalia, in 2007 and 2008.9 The U.S. government claimed that it used telephone metadata under Section 215 to identify Moalin as someone who was in contact with al-Shabaab officials. Three co-conspirators – Mohamed Mohamed Mohamud, Issa Doreh, and Ahmed Nasiri Taalil Mohamud – were charged along with Moalin. Even granting the government’s explanation of the case, the Moalin case does not provide a particularly convincing defense of the need for bulk collection of American telephone metadata. The total amount going to a foreign terrorist organization was around $8,500 and the case involved no attack plot anywhere in the world, nor was there a threat to the United States or American targets.10 The four individuals involved in the plot make up only 1.8 percent of the 225 cases we identified. **The case highlights a disconnect between government officials’ statements defending the NSA’s bulk phone metadata program as critical to American national security and how it has been actually used.** One reason offered by officials as to why the bulk collection of Americans’ phone records is necessary is that it saves valuable time in investigations.11 But this supposed efficiency cited by the government is not supported by the facts in the Moalin case. Before the House Judiciary Committee in July 2013, Stephanie Douglas, executive assistant director of the FBI’s National Security Branch, said that in October 2007, the NSA provided a phone number to the FBI with an area code consistent with San Diego, saying the phone number had been in contact with someone affiliated with an al-Qaeda branch.12 But the FBI did not begin monitoring Moalin’s phone calls immediately after receiving the tip. Instead, it did not start investigating Moalin and wiretapping his calls until two months later, in December 2007, according to the affidavit submitted by the government in support of a search warrant.13 This two-month delay is inconsistent with the justification the government has been using to defend the bulk collection of citizens’ metadata. Similarly, U.S. District Judge Richard Leon, who presided over a federal court case challenging the constitutionality of the bulk collection program, and who read the government’s affidavits regarding the necessity of the program for national security, ruled in favor of an injunction against the NSA programs on December 16, 2013. He noted that the plaintiffs have a “substantial likelihood” of showing their privacy interests outweigh the Government’s interest in the NSA’s bulk collection of American telephone metadata, and therefore the NSA’s bulk collection program constitutes an unreasonable search under the Fourth Amendment. **14 He said in his opinion that given the “utter lack of evidence that a terrorist attack has ever been prevented because searching the NSA database was faster than other investigative tactics,” he had “serious doubts about the efficacy of the metadata collection program as a means of conducting time-sensitive investigations in cases involving imminent threats of terrorism.”**15

**No risk of nuclear terrorism**

**Mueller 9** (Prof Political Science @ Ohio State University, John, “The Atomic Terrorist?”, Paper Prepared for the International Commission on Nuclear Non-Proliferation and Disarmament, April 30, http://www.icnnd.org/research/Mueller\_Terrorism.pdf)

**Thus far terrorist groups seem to have exhibited only limited desire and even less progress in going atomic.** This may be because, after brief exploration of the possible routes, they, unlike generations of alarmists on the issue, have discovered that **the tremendous effort required is scarcely likely to be successful**.**It is highly improbable that a would-be atomic terrorist would be given or sold a bomb by a generous like-minded nuclear state because the donor could not control its use and because the ultimate source of the weapon might be discovered.** Although there has been great worry about terrorists illicitly stealing or purchasing a nuclear weapon, **it seems likely that neither “loose nukes” nor a market in illicit nuclear materials exists.** Moreover, **finished bombs have been outfitted with an array of locks and safety devices.** There could be dangers in the chaos that would emerge if a nuclear state were utterly to fail, collapsing in full disarray. However, even under those conditions, **nuclear weapons would likely remain under heavy guard by people who know that a purloined bomb would most likely end up going off in their own territory, would still have locks, and could probably be followed and hunted down by an alarmed international community.** The most plausible route for terrorists would be to manufacture the device themselves from purloined materials. This task requires that a considerable series of difficult hurdles be conquered in sequence, including the effective recruitment of people who at once havegreat technical skills and will remain completely devoted to the cause. In addition, a host of corrupted co-conspirators, many of them foreign, must remain utterly reliable, international and local security servicesmust be kept perpetually in the dark, and no curious outsider must get consequential wind of the project over the months or even years it takes to pull off. In addition, **the financial costs of the operation could easily become monumental.** Moreover, **the difficulties are likely to increase because of enhanced protective and policing efforts by self-interested governments and because any foiled attempt would expose flaws in the defense system, holes the defenders would then plug.** The evidence of al-Qaeda’s desire to go atomic, and about its progress in accomplishing this exceedingly difficult task, is remarkably skimpy, if not completely negligible. The scariest stuff—a decade’s worth of loose nuke rumor—seems to have no substance whatever. For the most part, terrorists seem to be heeding the advice found in an al-Qaeda laptop seized in Pakistan: “Make use of that which is available ... rather than waste valuable time becoming despondent over that which is not within your reach.” In part **because of current policies—but also because of a wealth of other technical and organizational difficulties—the atomic terrorists’ task is already monumental, and their likelihood of success is vanishingly small.** Efforts to further enhance this monumentality, if cost-effective and accompanied with only tolerable side effects, are generally desirable

**Turn, Federal programs actually create terrorists**

**Berkowitz 14**

SUNDAY, AUG 3, 2014 10:00 AM MDT How the FBI is creating terrorists

A damning new report suggests the bureau facilitates and sometimes even invents its targets' willingness to act By BILL BERKOWITZ.

Let’s start with a premise I think we can all agree with: **There have been no 9/11-type attacks on United States soil since,** well, 9/11. Here’s another statement we all probably agree with: **The federal government has all sorts of arrows in its quiver when it comes to gathering intelligence to thwart such attacks.** And that is where it begins to gets dicey: Unfortunately, in its counterterrorism project, the government appears to be relying more and more on perhaps the most twisted of those arrows; the use of informants, coerced and/or rewarded, entrapment, and the sting. **Since the September 2001 terrorist attacks on the Twin Towers and the Pentagon, the federal government has obtained more than 500 federal counterterrorism convictions. According to a new Human Rights Watch report (produced in association with Columbia Law School’s Human Rights Institute), “nearly 50 percent of [those] … convictions resulted from informant-based cases; almost 30 percent of those cases were sting operations in which the informant played an active role in the underlying plot.”** The report, “Illusion of Justice: Human Rights Abuses in US Terrorism Prosecutions,” points out that, while “[m]any prosecutions have properly targeted individuals engaged in planning or financing terror attacks… many others have targeted individuals who do not appear to have been involved in terrorist plotting or financing at the time the government began to investigate them. “Indeed, in some cases the Federal Bureau of Investigation may have created terrorists out of law-abiding individuals by conducting sting operations that facilitated or invented the target’s willingness to act.” In addition, there is a good chance that, without the government’s active participation, many of those ensnared by the government did not have the mental or intellectual capacity to plan, finance and/or carry out a terrorist event. “Americans have been told that their government is keeping them safe by preventing and prosecuting terrorism inside the US,” said **Andrew Prasow, Human Rights Watch’s deputy Washington director**, in a statement. “But take a closer look and you realize that **many of these people would never have committed a crime if not for law enforcement encouraging, pressuring, and sometimes paying them to commit terrorist acts.”**