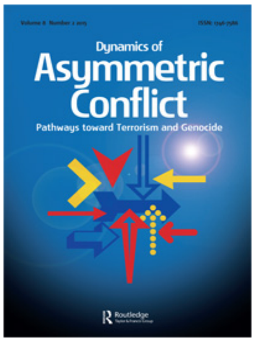

Dynamics of Asymmetric Conflict

Pathways toward terrorism and genocide

ISSN: 1746-7586 (Print) 1746-7594 (Online) Journal homepage: http://www.tandfonline.com/loi/rdac20

Terrorism, counterterrorism, and the Internet: The American cases

John Mueller & Mark G. Stewart

To cite this article: John Mueller & Mark G. Stewart (2015) Terrorism, counterterrorism, and the Internet: The American cases, Dynamics of Asymmetric Conflict, 8:2, 176-190, DOI: 10.1080/17467586.2015.1065077

To link to this article: http://dx.doi.org/10.1080/17467586.2015.1065077

Published online: 12 Sep 2015.

Submit your article to this journal

Article views: 6

View related articles

View Crossmark data

Dynamics of Asymmetric Conflict: Pathways toward terrorism and genocide

Volume 8, Issue 2, 2015

Special Issue: Computer-Assisted Terrorism. Guest Editors: John Horgan, Max Taylor and Marc Sageman

Select Language▼

Dynamics of Asymmetric Conflict, 2015
Vol. 8, No. 2, 176–190, http://dx.doi.org/10.1080/17467586.2015.1065077

Terrorism, counterterrorism, and the Internet: The American cases

John Mueller[a]* and Mark G. Stewart[b]

[a]*Cato Institute and Department of Political Science, Ohio State University, Columbus, Ohio, USA;* [b]*Centre for Infrastructure Performance and Reliability, University of Newcastle, New South Wales, Australia*

This article assesses the cases that have come to light since 9/11 of Islamist extremist terrorism, whether based in the United States or abroad, in which the United States itself has been, or apparently has been, targeted. Information from them is used to evaluate how the Internet (including various forms of electronic communication) has affected several aspects of the terrorism enterprise in the United States: radicalization, communication, organization, and the gathering of information. In general, it is found that the Internet has not been particularly important. Although it has been facilitating in some respects, it has scarcely ever been necessary. In some respects, the Internet more fully aids efforts to police terrorism – although this is mainly due to the incompetence and amateurishness of would-be terrorists. In other respects, however, the Internet, and the big data compilations it makes possible, greatly increase the costs and complications of the counterterrorism quest.

Keywords: terrorism; counterterrorism; Internet; cyberterrorism

Introduction

Since 9/11, some 61 cases have come to light of Islamist extremist terrorism, whether based in the United States or abroad, in which the United States itself has been, or apparently has been, targeted. These are summarized in Appendix 1. In this article, we apply information from the case studies on which these summaries are based to assess how the Internet (including various forms of electronic communication) has affected several aspects of the terrorism enterprise in the United States: radicalization, communication, organization, and the gathering of information. We also assess the potential for cyberterrorism within the United States.

In general, we find that the Internet has not been particularly important to the terrorism enterprise. Although it has been facilitating in some respects, it has scarcely ever been necessary. That is, much of what has taken place could have happened if the Internet had never been invented.

The Internet does have special relevance, however, to the counterterrorism enterprise. In some respects, the existence of the Internet facilitates the efforts to police terrorism – although this is mainly due to the incompetence and amateurishness of would-be terrorists. In other respects, however, the Internet, and the big data compilations it makes possible, greatly increase the costs and complications of the counterterrorism quest.

Except in passing, we do not deal with three elements of the terrorism enterprise. We do not assess the efforts of some would-be terrorists in the United States to go abroad to join the fight against American interests there, although the full array of case studies does include two of that sort (Cases 98 and 99). We do not evaluate terrorism cases that have not come to light because they have been deterred or have been disrupted at such

*Corresponding author. Email: bbbb@osu.edu

a low level of planning that the authorities have not been able to bring terrorism charges.[1] And we do not deal with terrorism in other parts of the world, although it seems likely that many of our conclusions about the terrorism issue may apply to other developed countries as well as to many countries that are not consumed by civil war.

Terrorism and the Internet

The Internet has affected terrorism in the United States in a variety of ways. None of them, it appears, has proved to be terribly significant.

Radicalization

Although it is common to assess the process by which potential terrorists become "radicalized", it is not at all clear that this is a good way to look at the phenomenon (see also Brooks, 2011, pp. 12–14; Patel, 2011; Sedgwick, 2010). The concept tends to suggest that there is an ideological motivation to the violence. However, these would-be terrorists in the cases are not set off so much by anything theoretical but rather by intense outrage at American and Israeli actions in the Middle East and by a burning desire to seek revenge, to get back, to defend, and/or to make a violent statement expressing their hostility to what they see as a war on Islam.

The authors of the case studies were specifically asked to assess the motivations driving the people in their cases. There were a few in which it could probably be said there was no notable motivation at all (Cases 5, 10, 19). However, in almost all the other cases, the overwhelming driving force was simmering, and more commonly boiling, outrage at American foreign policy – the wars in Iraq and Afghanistan in particular and also the country's support for Israel in the Palestinian conflict.

Religion was a key part of the consideration for most, but it was not that the plotters had a burning urge to spread Islam and Sharia law or to establish caliphates – indeed few would probably be able to spell either word. Rather it was the desire to protect their religion and religious heritage against what they commonly see to be a concentrated war upon it in the Middle East by the United States government and military (see also Bergen, 2011; Fallows, 2006, p. 142; Ignatius, 2015; Mearsheimer, 2011, p. 24; Pape & Feldman, 2010, pp. 76–79; Sageman, 2008, pp. 72–82, 91–92; Walt, 2009). None seems to remember (or perhaps in many cases ever knew) that the United States strongly favored the Muslim side in Bosnia and in Kosovo in the 1990s – as well as, of course, in the Afghan war against the Soviet Union in the 1980s.

In stark contrast, there is remarkably little hostility to American culture or society or to its values or to democracy. Almost none of the terrorist characters in the cases had any problem with American society – indeed, a number of them show a deep and quite nuanced appreciation for American girls. This is particularly impressive because many of the people under examination (though certainly not all) were misfits, suffered from personal identity crises, were friendless, came from broken homes, were often desperate for money, had difficulty holding jobs, were on drugs, were petty criminals, experienced various forms of discrimination, and were, to use a word that pops up in quite a few of the case studies and fits even more of them, "losers".

As noted, with two exceptions (Cases 98 and 99) the cases examined do not include those dealing with people seeking to go abroad to fight against American interests there by joining the insurgencies in Iraq and Afghanistan or to defend Somalia against Ethiopian invaders.[2] However, hostility to American foreign and military policy was obviously the primary motivator for these individuals.

The role of the Internet in this process may be facilitating, but it scarcely seems to be required. In particular, it does not seem to be necessary for the process of stoking outrage at American foreign and military policy. For the most part, any stoking stems from information readily available in the evening news: abuse of Iraqi prisoners at Abu Ghraib, torture by the CIA, "collateral" damage from American air and drone strikes, the mounting body count in Iraq and Afghanistan, instances of American troop abuse of Muslim civilians, Israeli bombings of Lebanon and Gaza.

The people in many of the cases did go to the Internet for further information, and they frequently sought out the most radical sites, of which there are a large number (Jenkins, 2011, pp. 15–17; Weimann, 2006). For example, as they searched for information congenial to their proclivities, several were impressed by the works of the radical American cleric Anwar al-Awlaki who hid out in Yemen from 2002 until his death by drone strike in 2011. However, this process simply supplied information that in earlier days might have been furnished by incendiary paper pamphlets – a relatively minor change. It is the message that is vital, not the medium for delivering it.

Authorities can often make domestic terrorists seem more threatening by suggesting they have grand ideological plans to radically change Western society – to establish "caliphates" there and to spread and then rigidly enforce an extreme version of Sharia law. The "radicalization" syndrome – with its apparent stress on ideology – plays nicely into this narrative. The process can be seen in the case of two men who were picked up for planning to machine gun, and lob grenades at, a local military processing center in Seattle (Case 44). According to news reports, the men said that they were motivated by a desire to retaliate for crimes by US soldiers in Afghanistan and that they wanted to kill military personnel to prevent them from going to Islamic lands to kill Muslims. However, the official Department of Justice press release on the case merely says that the men were "driven by a violent, extreme ideology".

In a similar manner, when the New York Police Department report, *Radicalization in the West* (Silber & Bhatt, 2007), discusses an embryonic plot to bomb Herald Square (Case 12), there is a great deal of material about "extremist literature" and "jihadi ideology", but almost nothing to suggest that, as even the prosecutors in the case contended, the perpetrators were driven by anger over American foreign policy in the Middle East, the war in Iraq, and abuse by American soldiers of Iraqi prisoners at Abu Ghraib (Rashbaum, 2006).

And after an (incredibly inept) effort by a terrorist to bomb Times Square in 2010 (Case 34), New York Mayor Michael Bloomberg was quick to conclude that "There are some people around the world who find our freedom so threatening that they're willing to kill themselves and others to prevent us from enjoying it" (Chang, 2010). Far from warring against freedom, however, the would-be bomber was primarily motivated by (or radicalized by) a desire to be "part of the answer to the U.S. terrorizing Muslims nations and the Muslim people", and he was particularly angered by America-led drone strikes in Pakistan and Afghanistan (Mueller, 2015).

It should be stressed in all this, however, that, although hostility toward American policy is a primary motivator in these cases, there are a huge number of people who have also been strongly opposed to American policy in the Middle East – including for most of the time a very large percentage of the Americans who identify themselves as Democrats (Jacobson, 2006). Although the tiny number of people plotting terrorism in the United States display passionate hostility to American foreign policy, there is a far, far greater number of people who share much of the same hostility but are in no sense inspired to commit terrorism to express their deeply held views (see also Brooks, 2011; Horgan, 2012; Jenkins, 2011, p. 17; Patel, 2011).

Communication

The Internet played a considerable role in many of the cases in allowing people to communicate with each other, and e-mail was often a useful medium for this. However, the bulk of the communication, and the most important, was face-to-face. As this may suggest, there are few connections, and therefore communications, between the cases. Though often inspired by the violent jihadist movement, almost all were essentially planned in isolation from the others (see also Jenkins, 2011, p. 21; Sageman, 2008).

For the most part, the Internet played only a limited, or even perverse, role in plotting terrorism. There are cases in which the would-be perpetrator used chat rooms or Facebook or Twitter to seek out like-minded souls and potential collaborators (Cases 16, 30, 39, 40, 41, 48, 49, 55, 56, 57, 60). Usually, they simply got connected to the FBI. This phenomenon will be discussed more fully later.

For quite some time after 9/11 – especially during the early years when it was thought that there were many sleeper cells imbedded in the country – authorities worried intensely that al-Qaeda central might use the Internet to communicate coded signals to its operatives (Lustick, 2006, p. 172n32).[3] The worry, it turns out, was not necessary: there were no sleeper cells (Mueller, 2006, pp. 37–38; Sageman, 2008, p. 106).

Organization

The notion that an attack can be effectively organized by means of the Internet is something of a fantasy. More generally, as Mette Eilstrup-Sangiovanni and Calvert Jones (2008) point out, setting up a networked terrorist plot is extremely difficult under the best of circumstances. Doing so entirely, or largely, through the Internet is even more problematic.

Case 18 is the only one in the set where this was attempted, and it suggests the difficulties. It involves a deeply religious, drug-addicted professor of economics at Lebanese International University in Beirut (he taught business ethics and human resources), aged 28, who plotted with seven people he met in virtual space to go to Canada, obtain explosives, and then journey south to set them off on a PATH commuter train as it traveled under the Hudson River in New York. The conspirators never actually met in person and, while they were able to Google tunnels in New York, none of them ever made it into the country to have a look at one in three dimensions. By 2005, the FBI had uncovered the plot – and possibly participated in it. It tipped off the Lebanese police, and the professor was arrested in 2006.

The lead FBI official on this case asserted that the conspirators were “about to go into a phase” in which they would “attempt” to surveil the target, figure out “a regimen of attack”, and acquire explosives. It was, he said, “the real deal”. Other officials, however, anonymously suggested to reporters that the plot was essentially “aspirational” and characterized by “jihadi bravado”. But, as one put it, “somebody talks about tunnels, it lights people up”. And, indeed, New York City officials were quick to see the light: they immediately used the disclosure about the virtual plot to try to get more funding from the federal government (Hsu & Wright, 2006).

Information

The Internet could be useful to the would-be terrorists in their plotting, in particular for obtaining information about potential targets. However, the plotters scarcely needed it to select targets.

Since terrorist motivation seems mainly to arise from hostility to American foreign and military policy abroad and not from some sort of broader ideology, military installations within the country were fairly common targets even though they are not very good ones if one is seeking to do maximum damage and to inflict maximum shock. The easiest military targets to find are recruitment centers within cities, and would-be terrorists have frequently plotted to attack them. Military targets, including members of the military, were explicitly considered in Cases 15, 22, 25, 26, 27, 32, 35, 40, 43, 44, 45, 46, 48, 56, 58, and 60. As it happens, 14 of the 19 deaths caused by Islamist extremists since 9/11 were inflicted on or at military installations – and only one of the victims was a civilian (Cases 26 and 32) (see also Brooks, 2011, p. 38).

But the Internet was hardly required to find the location of military recruitment centers. If there were no Internet, they would be conveniently listed in the phone book. Moreover, in many cases, target selection is effectively a random process, not one worked out with guile and careful planning. Often, it seems, targets have been chosen almost capriciously and simply for their convenience. Thus, a would-be bomber targeted a mall in Rockford, Illinois because it was nearby (Case 21). Terrorist plotters in Los Angeles in 2005 drew up a list of targets (some of which, as it happens, did not exist) that were all within a 20-mile radius of their shared apartment (Case 15). And one of the Boston Marathon bombers lived within three miles of the site of the attack (Case 54). Or there was the terrorist who, after several failed efforts, went home and, with no plan at all, shot at a military recruiting center three miles from his apartment, killing one recruiter who was out on a smoke break (Case 26).

Some plotters did go to the web to find information about bombs. But, except for the Boston Marathon terrorists (Case 54), it clearly did not convey enough information to build a successful bomb since none of the people in these cases was able to do so – though one potential perpetrator (Case 41) seemed to think he had acquired the relevant knowledge.

The popular notion that the Internet can be effective in providing useful operational information, particularly about making bombs, seems to be severely flawed. In one study, for example, Michael Kenney (2010) notes that it is filled with misinformation and error and that it is no substitute for direct, on-the-ground training and experience.[4] Anne Stenersen is similarly unimpressed: the Internet manuals she has examined are filled with materials hastily assembled and "randomly put together" and contain information that is often "far-fetched" or "utter nonsense" (Stenersen 2009, p. 56; see also Brooks, 2011, pp. 30–34; Eilstrup-Sangiovanni & Jones, 2008, p. 32; Stenersen, 2008; and, in contrast, Weimann, 2006).

Moreover, as David Benson (2014, pp. 306–307) points out, even if the information is valid, "it does not necessarily follow that one can actually carry out the task". Interaction with an instructor is often necessary. Thus, many are unable to prepare food correctly from Internet instructions, "let alone master gourmet cooking". No one seems to be contending that surgeons, arc-welders, explosives technicians, or combat soldiers be trained entirely from the web. And unlike failure at fudge-making, failure at explosive-making carries considerable danger.

Ramzi Yousef, who was primarily responsible for the failed 1993 effort to topple the World Trade Center, is widely considered to be an "explosives genius", a "genius bomb-maker", and a "master of explosives". Asked if he considered himself to be a genius, Yousef responded strongly in the affirmative. However, as a bomb-maker he was given to splashing acid in his face and detonating bombs by accident. During his bomb work, he also started a small fire in a cooking pot in his apartment, leading to a search by police that turned up a laptop that contained plans for his plot (Mueller & Stewart, 2015, ch. 4).

In addition, as political scientist Louis Klarevas (2011) has noted, “sophisticated explosives are nearly impossible to manufacture in the United States as the necessary precursor chemicals are not available to the general public”. Would-be bombers who are incapable of getting around these restrictions need, then, to pursue simpler explosives like pipe bombs, which are, continues Klarevas, “least likely to inflict mass casualties”.

In at least two of the American cases – the Boston Marathon one and the one involving the hapless, zombie-like Jose Pimentel (Cases 54 and 48) – terrorists were working from an article published in the summer 2010 issue of *Inspire*, an English-language online “periodical magazine” issued by the al-Qaeda organization in Yemen. The article was written by someone calling himself “The AQ Chef” and is entitled “Make a bomb in the kitchen of your Mom”. The clumsy title is rendered in white lettering on a dark grey background in the magazine, but the words “bomb” and “Mom” are in light blue, presumably in an effort to highlight the author’s cleverness at rhyme to his less perceptive, or more humorless, readers.

In the *Inspire* article, AQ Chef instructs the would-be bomber to paste nails to the outside of a pipe elbow-joint, fill it with a mixture of crushed match-heads and sugar, and then detonate it through a drilled hole with a contraption consisting of a broken Christmas tree light, a bit of wire, a small battery, and a clock with a nail pounded into its face. Although AQ Chef does note that one could use gunpowder extracted from “cartilages” rather than crushed match-heads for the core “inflammable substance”, he mainly focuses on the match-head approach and suggests that 80 match-heads per bomb would do the trick.

As Klarevas points out, however, experiments on the Discovery Channel’s “Mythbusters” program suggest AQ Chef was rather off the mark. The television hosts first tried setting off 30,000 match heads in a bucket and did produce a colorful flameout, but no explosion, and the bucket itself emerged from the experiment singed, but whole. They tried again with a million match-heads and got a flameout perhaps three times as impressive. The collected match heads in either experiment were far too voluminous to fit inside a standard pipe elbow-joint.

In the day between the arrest of Pimentel and the press conference touting his arrest, the New York Police Department put together three pipe bombs of the sort he was striving to create. Presumably, they used gunpowder rather than match scrapings, and they detonated the three bombs *simultaneously* – a feat he was unlikely to be able to accomplish – in a small four-door Mazda. A video recording of this effort was shown at the start of the press conference (see http://www.youtube.com/watch?v=poV6lc2b070). As Klarevas points out, the explosion and fire shown in the video would probably have proved fatal to anyone who was sitting in the car and possibly to anyone who was standing outside very close to it.

The limitations of such bombs is also suggested by the fact that the two somewhat larger bombs set off in a crowd at the Boston Marathon in 2013 killed but three people. It would be quite possible and far easier, notes Klarevas, to kill more people with a single handgun.

Cyberterrorism

Much the same holds for increasingly popular concerns about cyberterrorism.[5] Although many of the people in the cases did use the Internet for communication and for information, none showed much ability at, or interest in, committing cyberterrorism.

Counterterrorism and the Internet

The Internet has furnished both assistance and hindrance to the counterterrorism enterprise.

Assistance

In some respects, the Internet has been an important aid to counterterrorism efforts (see also Benson, 2014; for a similar conclusion about policing international crime, see Andreas, 2013). It is far easier and far less costly to intercept electronic communications (preferably, one hopes, with a warrant to do so) than to intercept paper letters, steam them open, and then reseal them and send them on their way. And it is also far easier to get into computer files than into paper ones.

However, many of the advances stem primarily from the stupidity and incompetence of the would-be terrorists. As noted earlier, quite a few of them advertise their radical views or seek out collaborators on the web. Similar incompetence is seen in Case 28 concerning Najibullah Zazi and two other Afghan-Americans who were recruited in Pakistan by al-Qaeda to set off bombs on the New York transit system (Apuzzo & Goldman, 2013, pp. 109–114). In preparation, Zazi received explosives training and e-mailed nine pages of bomb-making instructions to himself. FBI Director Robert Mueller asserts that this training gave Zazi the "capability" to set off a bomb (Frieden, 2009). That, however, seems to be a substantial overstatement. Even with the training and material at hand, Zazi *still* apparently could not figure it out, and he frantically contacted an unidentified person overseas for help several times (Moreno & Banda, 2009).[6] Each of these communications was "more urgent in tone than the last", according to court documents (Johnson, 2009; Temple-Raston, 2009). Communications between Zazi and al-Qaeda leaders were being monitored because Zazi was using a known overseas terrorist address that had long been under surveillance (Bergen, Sterman, Schneider, & Cahall, 2014, pp. 20–21; British spies help prevent attack, 2009; Smith, 2013). The communications naively used "wedding" as a code word for the planned terrorist attack even though authorities had long been on to that rather childish Aesopian euphemism (Apuzzo & Goldman, 2013, p. 9).

There is considerable reason to expect that the counterterrorist advantage will persist. For decades, top terrorist operatives have been careful about their communications. Terrorists have surely known at least since the 1990s that United States intelligence is searching communications worldwide to track them down: it was then that Osama bin Laden ceased talking on a satellite phone (Carnevale, 2008). Year after year we have heard about "chatter" that has been picked up by official agencies, and one certainly has to conclude that it has dawned on the chatterers that there are extensive efforts to listen in and that the NSA, in its tireless quest to conduct its very global war on terror, might well be on their case. Moreover, it is quite clear that international jihadists have for over a decade had manuals and handbooks containing detailed information about how to keep communications secure (Greenwald & Fishman, 2014), and the 9/11 hijackers took considerable precautions (Arkin, 2006).

However, as Eilstrup-Sangiovanni and Jones (2008) note, people attempting to set up clandestine networks "are far from nimble learners" (p. 33) and, in particular, "many are strikingly naïve about security" (p. 37). As Benson (2014, pp. 309–310) points out, terrorists continually inadvertently disclose information about themselves when using the Internet. The continuing profligate use of social networking on the Internet by Islamic State members is also relevant (Byman & Shapiro, 2014).

Hindrance

On the other hand, there is a danger that counterterrorism will, on balance, actually be hampered by the ready availability of electronic data and information. There has been a tendency to collect everything in part because it has become technologically possible to do so. Dana Priest and William Arkin noted in 2011 that the National Security Agency was then intercepting and ingesting 1.7 billion communication elements every day including "telephone calls, radio signals, cell phone conversations, emails, text and Twitter messages, bulletin board postings, instant messages, website changes, computer network pings, and IP addresses" (Priest & Arkin, 2011, p. 77).

Combined with the "9/11 Commission Syndrome" – which dictates that all leads must be followed up because the one you skip might be the next 9/11 – the result has been a costly, even absurd, surfeit of information, commonly rendered in snappy nautical terms like engulfing, deluge, wave, ocean, or tsunami (Mueller & Stewart, 2015; Priest & Arkin, 2011; Sageman, 2014).

Central to this massive enterprise is what in the FBI has often come to be called "ghostchasing" (Graff, 2011, p. 398; Mudd, 2013, pp. 69, 213). Agencies like theirs, redirecting much of their effort from organized crime and white collar embezzlement, have kept their primary focus on the terrorist threat and each day follow up on more than 5000 tips or leads – or "threats" as they are called internally (Graff, 2011, p. 399). That would total well over 10 million since 2001. Even under very generous assumptions about how many of these contain true grist, only one alarm in 10,000 fails to be false – the rest all point to ghosts. And the vast majority of the leads deemed worthy of pursuit seem to have led to terrorist enterprises that were either trivial or at most aspirational.

Chasing ghosts is an expensive, exhausting, bewildering, chaotic, and paranoia-inducing process (Mueller & Stewart, 2015, ch. 1). At times, in fact, it seems to be an exercise in dueling delusions: a Muslim hothead has delusions about changing the world by blowing something up, and the authorities have delusions that he might actually be able to overcome his patent inadequacies to do so.

A considerable contribution to this extravagant exercise has been generated by big data collections, particularly those gathered by the NSA. There is a tendency to believe – very attractive to data-gathering geeks – that, with enough data to sort through, one can come up with algorithms that will point to the solution even without knowing very much substantively about the actual phenomenon of interest – in this case, terrorism.[7] However, under the sway of the 9/11 Commission Syndrome, the geeks are wary of casting the identifying algorithm too tightly. Consequently they tend to pass on potential leads in great numbers.

Big data are likely to have value in establishing, or nailing down, correlations that may lurk within vast data collections.[8] The problem with big data in the terrorist quest, however, is that analysts are not looking simply for correlations or connections. In contrast, when Amazon.com routinely sifts through its huge customer database, it is not concerned that there may be a considerable error rate when correlating the buying or surfing habits of one customer with another one. But there are, in fact, very few likely terrorists in the information haystack, and few of those are actually capable or dedicated enough to justify concerted, and therefore costly, policing efforts. Thus, it is important to be precise, not just co-relative, when searching for them. A high error rate wastes time and effort, has considerable civil liberties complications, and may dim the senses of the chasers, making the quest less likely to succeed. Adding huge amounts of hay only exacerbates the problem. The issue is put in more general form by Marc Sageman (2014):

"Throwing more analysts at the problem compounds the issue as it creates more false leads for analysts who err on the side of security" (p. 573).[9]

Walter Pincus (2013) explains that if operatives at NSA, sorting through their massive databases, uncover "a questionable pattern" such as "calls to other suspect phones", they send a report to the FBI for investigation. In NSA this process has sometimes been called "We Track 'Em, You Whack 'Em" (Priest, 2013). The FBI, then, is routinely supplied with what Garrett Graff calls "endless lists of 'suspect' telephone numbers". When followed up, these leads virtually never go anywhere: of 5000 numbers passed along, only 10 – two-tenths of 1% – panned out enough for the bureau to bother to get court permission to follow them up. At the FBI, NSA tips are often called "Pizza Hut leads" because, following them up, FBI agents "inevitably end up investigating the local pizza delivery guy". There is, in other words, not much of anything to "whack". At one point, the generally diplomatic director of the FBI, Robert Mueller, bluntly told NSA director Keith Alexander: "You act like this is some treasure trove; it's a useless time suck." An agent in the trenches puts it a bit less delicately: "You know how long it takes to chase 99 pieces of bullshit?" (Graff, 2011, p. 527; see also Jenkins, 2011, p. 18). Moreover, to the degree that attitude prevails, investigators, overwhelmed by the trivial, may well be inclined to fail to treat NSA tips with much seriousness.

If 1 million of the over 10 million leads the FBI has fruitlessly followed up derived from NSA tips, and if the cost of following up each is a mere $1000, the NSA leads have led to a billion dollars in unnecessary expenditures – or to the equivalent of 75 million large pepperoni pizzas.

Another problem arises from the fact that big data sets are often literally unfathomable: that is, essentially bottomless. Thus, the fact that none of the leads dredged up from a dataset has yet led anywhere is not necessarily deflating to the quest. There is still a great amount of unplumbed information out there, and rather than giving up, there is a consequent temptation to re-jig the algorithm in an increasingly straw-grasping hope for success. The larger the haystack, the less likely it will ever be deemed to be free of needles.

Conclusion

For the most part, terrorism's virtual army in the United States has been, as Brian Jenkins (2011, p. 17) puts it, remained exactly that: virtual. "Talking about jihad, boasting of what one will do, and offering diabolical schemes egging each other on is usually as far as it goes." This "may provide psychological satisfaction" and "win accolades from other pretend warriors, but it is primarily an outlet for verbal expression, not an anteroom to violence".

To the degree that the Internet has contributed to the process, it seems mainly to have benefited the counterterrorists.

Disclosure statement

No potential conflict of interest was reported by the authors.

Notes

1. For a discussion of this issue, see Mueller and Stewart (2015, ch. 3).
2. Marc Sageman (2008, pp. 74–75) has provided an arresting comparison with Jewish youths who felt called upon to go abroad to fight for besieged Israel in wars in 1948, 1967, and 1973.
3. See also the bizarre case described in Risen (2014, ch. 2).

4. And even that may not be enough. The Times Square bomber (Case 34) had weeks of direct training in Pakistan. His bomb is said to have "almost succeeded" by John Yoo (2011, p. 278) and Ali Sofan (2013). However, the bomb was reported from the start to be "really amateurish", with some analysts charitably speculating when it was first examined that it might be "some sort of test run" created by "someone who's learning how to make a bomb and will learn from what went wrong with this". Apparently because it is difficult to buy explosive fertilizer, the bomber purchased the non-exploding kind instead. It is not clear why he did not use dirt or dried figs for his explosive material since these are cheaper, easier to find, and will fail to explode with same alacrity as non-explosive fertilizer. He also threw in some gasoline – which does not explode either, though it does burn – as well as some propane, that will explode only when it is mixed precisely with the right amount of air, a bomb design nicety he apparently never learned.
5. In early 2005, Richard Clarke, counterterrorism coordinator from the Clinton administration, issued a scenario that appeared as a cover story in the *Atlantic*. In it he darkly envisioned terrorist shootings at casinos, campgrounds, theme parks, and malls in 2005, bombings in subways and railroads in 2006, missile attacks on airliners in 2007, and devastating cyberattacks in 2008. He has now become an energetic figure in the escalating, and lucrative, concern about cyberterrorism (Clarke & Knake, 2010). For critiques of this position, see the sources arrayed at http://www.cato.org/research/cyberskeptics.
6. Zazi also foolishly attracted attention by racing at more than 90 miles per hour across the country in his bomb-material-laden car (Apuzzo & Goldman, 2013, p. 10).
7. James Risen (2014, p. 234) relays the joke that an extrovert in NSA is one who looks at *your* shoes when talking to you.
8. However, there is also a danger that the common problem of confusing statistical significance with substantive significance will be embellished: the larger the data set, the more likely a relationship will be deemed to be statistically significant (on this issue, see Ziliak & McCloskey, 2008).
9. Relevant here is a study finding that, as more information becomes more readily available to scientists, they can "more easily find prevailing opinion" and are "more likely to follow it". This leads to "more citations referencing fewer articles" even as "findings and ideas that do not become consensus" are "forgotten quickly" (Evans, 2008, p. 398; see also Benson, 2014, p. 306).

References

Andreas, P. (2013). *Smuggler nation: How illicit trade made America*. New York, NY: Oxford University Press.

Apuzzo, M., & Goldman, A. (2013). *Enemies within: Inside the NYPD's secret spying and Bin Laden's final plot against America*. New York, NY: Simon and Schuster.

Arkin, W. M. (2006, March 30). What the 9/11 plotter tells us. *washingtonpost.com*.

Benson, D. C. (2014). Why the Internet is not increasing terrorism. *Security Studies*, *23*, 293–328.

Bergen, P. (2011, May 6). Five myths about Osama bin Laden. *washingtonpost.com*.

Bergen, P., Sterman, D., Schneider, E., & Cahall, B. (2014, January). *Do NSA's bulk surveillance programs stop terrorists?* Washington, DC: New America Foundation.

British spies help prevent attack. (2009, November 9). *Telegraph*.

Brooks, R. A. (2011). Muslim "homegrown" terrorism in the United States: How serious is the threat? *International Security*, *36*(2), 7–47.

Byman, D., & Shapiro, J. (2014, October 9). We shouldn't stop terrorists from tweeting. *washingtonpost.com*.

Carnevale, M. L. (2008, May 28). Tracking use of Bin Laden's satellite phone. Washington Wire, blogs.wsj.com.

Chang, A. (2010, May 2). Bloomberg in Times Square: "We're not going to let them win". WNYC News, wnyc.org.

Clarke, R. (2005). Ten years later. *Atlantic* (January/February), 61–77.

Clarke, R. A., & Knake, R. K. (2010). *Cyber war: The next threat to national security and what to do about it*. New York: Ecco.

Eilstrup-Sangiovanni, M., & Jones, C. (2008). Assessing the dangers of illicit networks. *International Security*, *33*(2), 7–44.

Evans, J. A. (2008). Electronic publication and the narrowing of science and scholarship. *Science*, *321*, 395–399.

Fallows, J. (2006). *Blind into Baghdad: America's war in Iraq*. New York, NY: Vintage.

Frieden, T. (2009, September 30). Top U.S. security officials share Afghan–Pakistan border concerns. *cnn.com*.

Greenwald, G., & Fishman, A. (2014, August 12). NPR is jaundering CIA talking points to make you scared of NSA reporting. *firstlook.org/theintercept*.

Graff, G. (2011). *The threat matrix: The FBI in the age of terror*. New York, NY: Little, Brown.

Horgan, J. (2012, September 28). *Discussion point: The end of radicalization?* College Park, MD: National Consortium for the Study of Terrorism and Responses to Terrorism.

Hsu, S. S., & Wright, R. (2006, July 8). Plot to attack N.Y. foiled: Transit tunnels to N.J. called targets. *Washington Post*.

Ignatius, D. (2015, January 15). The Internet isn't to blame for radicalization. *washingtonpost.com*.

Jenkins, B. M. (2011). *Stray dogs and virtual armies: Radicalization and recruitment to jihadist terrorism in the United States since 9/11*. Santa Monica, CA: RAND Corporation.

Jacobson, G. C. (2006). *A divider, not a uniter*. New York, NY: Pearson.

Johnson, K. (2009, September 8). Weakened al-Qaeda is still a threat. *USA Today*.

Kenney, M. (2010). Beyond the Internet: *Mētis, techne*, and the limitations of online artifacts for Islamist terrorists. *Terrorism and Political Violence*, *22*(2), 177–197.

Klarevas, L. (2011, December 1). The idiot Jihadist next door. *foreignpolicy.com*.

Lustick, I. S. (2006). *Trapped in the war on terror*. Philadelphia, PA: University of Pennsylvania Press.

Mearsheimer, J. J. (2011). Imperial by design. *National Interest*. (January/February), 16–34.

Moreno, I., & Banda, P. S. (2009, September 26). Prosecutor: Terror plot focus was 9/11 anniversary. Associated Press.

Mueller, J. (2006). *Overblown: How politicians and the terrorism industry inflate national security threats, and why we believe them*. New York, NY: Free Press.

Mueller, John (Ed.). (2015). *Terrorism since 9/11: The American cases*. Columbus, OH: Mershon Center, Ohio State University. Retrieved from http://www.politicalscience.osu.edu/faculty/jmueller/since.html.

Mueller, J., & Stewart, M. G. (2015). *Chasing ghosts: The policing of terrorism*. New York, NY: Oxford University Press.

Mudd, P. (2013). *Takedown: Inside the hunt for Al Qaeda*. Philadelphia: University of Pennsylvania Press.

Patel, F. (2011). *Rethinking Radicalization*. New York: Brennan Center for Justice at New York University School of Law.

Pape, R. A., & Feldman, J. K. (2010). *Cutting the fuse: The explosion of global suicide terrorism and how to stop it*. Chicago, IL: University of Chicago Press.

Pincus, W. (2013, July 29). NSA should be debated on the facts. *washingtonpost.com*.

Priest, D. (2013, July 21). NSA growth fueled by need to target terrorists. *Washington Post*.

Priest, D., & Arkin, W. M. (2011). *Top secret America: The rise of the new American security state*. New York, NY: Little, Brown.

Rashbaum, W. K. (2006, May 10). S.I. man describes shattered life, then a plot to bomb a subway station. *New York Times*.

Risen, J. (2014). *Pay any price: Greed, power, and endless war*. Boston, MA: Houghton, Mifflin, Harcourt.

Sageman, M. (2008). *Leaderless Jihad*. Philadelphia, PA: University of Pennsylvania Press.

Sageman, M. (2014). The stagnation in terrorism research. *Terrorism and Political Violence*, *26*(4), 565–580.

Sedgwick, M. (2010). The concept of radicalization as a source of confusion. *Terrorism and Political Violence*, *22*(4), 479–494.

Silber, M. D., & Bhatt, A. (2007). *Radicalization in the West: The homegrown threat*. New York, NY: New York City Police Department.

Smith, B. (2013, June 7). Public documents contradict claim email spying foiled terror plot. *buzzfeed.com*.

Sofan, A. (2013, January 23). Enemies domestic. *Wall Street Journal*.

Stenersen, A. (2008). The Internet: A virtual training camp? *Terrorism and Political Violence*, *20*(2), 215–233.

Stenersen, A. (2009). Al-Qaeda's thinking on CBRN: A case study. In M. Ranstorp & M. Normark (Eds.), *Unconventional weapons and international terrorism: Challenges and new approaches* (pp. 50–64). London: Routledge.

Temple-Raston, D. (2009, October 3). Terrorism case shows range of investigators' tools. *NPR*.

Walt, S. (2009, November 30). Why they hate us (II): How many Muslims has the U.S. killed in the past 30 years? *foreignpolicy.com*.

Weimann, G. (2006). *Terror on the Internet: The new arena, the new challenges*. Washington, DC: United States Institute of Peace.

Yoo, J. (2011). Conclusion. In D. Reuter & J. Yoo (Eds.), *Confronting terror: 9/11 and the future of American national security* (pp. 277–290). New York: Encounter.

Ziliak, S. T., & McCloskey, D. N. (2008). *The cult of statistical significance: How the standard error costs us jobs, justice, and lives*. Ann Arbor, MI: University of Michigan Press.

Appendix 1. The cases: Terrorism in the United States since 9/11

Cases that have come to light of Islamist extremist terrorism since 11 September 2001, whether based in the United States or abroad, in which the United States itself has been, or apparently has been, targeted. Drawn from Mueller (2015).

Case number, title, *case type*, year, description

1 The shoe bomber *4* 2001 British man tries to blow up a US-bound airliner with explosives in his shoes but is subdued by passengers and crew

2 Padilla *1* 2002 American connected to al-Qaeda who had discussed a dirty bomb attack returns to US and is arrested

3 Mt. Rushmore *3* 2002 Two men in Florida, one of them possibly connected to an al-Qaeda operative, plot, crucially aided by an informant, to bomb local targets as well as Mt Rushmore before 9/11, and are arrested and tried the year after

4 El Al at LAX *4* 2002 A depressed anti-Israel Egyptian national shoots and kills two at the El Al ticket counter at Los Angeles airport before being killed himself in an act later considered to be one of terrorism

5 Lackawanna *1* 2002 Seven Americans in Lackawanna, NY, are induced to travel to an al-Qaeda training camp, but six return disillusioned, all before 9/11, and are arrested the next year

6 Paracha *2* 2003 A young Pakistani seeks to help an al-Qaeda operative enter the country to attack underground storage tanks and gas stations

7 Ali *2* 2003 A US citizen joins a terrorist cell in Saudi Arabia and plots to hijack a plane in the US and to assassinate President Bush when he is arrested by the Saudis and extradited to the US for trial

8 Columbus and the Brooklyn Bridge *2* 2003 American connected to al-Qaeda discusses shooting up a shopping mall in Columbus, OH, with two friends, then scouts taking down the Brooklyn Bridge for al-Qaeda, but decides it is too difficult

9 Barot and the financial buildings *2* 2004 Group in London tied to al-Qaeda scouts out financial buildings in US with an eye to bombing them, but never gets to the issue of explosives

10 Albany *3* 2004 Two men in Albany, NY, effectively help fund an informant's terror plot

11 Nettles *3* 2004 An American with a long history of criminal and mental problems plots under the nickname of "Ben Laden" to blow up a federal courthouse in Chicago and reaches out for help to a Middle Eastern terrorist group, but gets the FBI

12 Herald Square *3* 2004 Loud-mouthed jihadist in New York and a schizophrenic friend attract informant who helps them lay plans to bomb Herald Square subway station

13 Grecula *3* 2005 An American with visions of being an modern-day Spartacus agrees to build a bomb to be exploded in the US for undercover agents claiming to be al-Qaeda

14 Lodi *1* 2005 American in Lodi, California, who may have attended a training camp in Pakistan but with no apparent plan to commit violence is arrested with the aid of an informant

15 JIS *2* 2005 American in jail masterminds a plot by three others to shoot up military recruitment centers, synagogues, and a non-existent military base in the Los Angeles area but, although close to their first attack, the plot is disrupted when they leave a cell phone behind at a funds-raising robbery

16 The pipeline bomber and the terrorism hunter *3* 2005 An American offers on the Internet to blow up pipelines in Canada as an aid to al-Qaeda, and attracts the attention of freelance

informant

17 U of North Carolina *4* 2006 To punish the US government for actions around the world, a former student, after failing to go abroad to fight or to join the Air Force so he could drop a nuclear bomb on Washington, drives a rented SUV onto campus to run over as many Americans as possible and manages to injure nine

18 Hudson River tunnels *2* 2006 Angered by the US invasion of Iraq, several men based in Lebanon plot to flood railway tunnels under the Hudson river, but are arrested overseas before acquiring bomb materials or setting foot in the US

19 Sears Tower *3* 2006 Seven men in Miami plot with an informant, whom they claim they were trying to con, to take down the Sears Tower in Chicago, then focus on closer buildings

20 Transatlantic airliner bombings *2* 2006 Small group in London, under intense police surveillance from the beginning, plots to explode liquid bombs on US-bound airliners

21 Rockford *3* 2006 Loud mouthed jihadist attracts attention of an informant and together they plot exploding grenades at a shopping mall in Rockford, IL

22 Fort Dix *3* 2007 Small group target practices, buys guns, and plots to attack Ft Dix, NJ, with the aid of an informant who joins the group when the FBI is told they took a jihadist video into a shop to be duplicated

23 JFK airport *3* 2007 Small group, with informant, plots to blow up fuel lines serving JFK airport in New York

24 Vinas *2* 2008 New York man travels to Pakistan, is accepted into al-Qaeda, and plots to plant a bomb in the US, but is being watched and talks after being arrested

25 Bronx synagogues *3* 2009 Four men, with crucial aid from an informant, plot to bomb synagogues in Bronx, NY, and shoot down a plane at a military base

26 Little Rock *4* 2009 American man travels to Middle East to get training, but fails, and on return, working as a lone wolf, eventually shoots and kills one soldier at a military recruitment center in Little Rock, AK

27 Boyd and Quantico *2* 2009 Complicated conspiracy in North Carolina, including an informant, gathers weapons and may have targeted Quantico Marine Base

28 Zazi *2* 2009 Afghan-American and two friends travel to Pakistan to join Taliban, but are recruited by al-Qaeda to plant bombs on NY subways instead, and are under surveillance throughout

29 Springfield *3* 2009 Loud-mouthed jihadist plots, with informants, to set off a bomb in Springfield, IL

30 Dallas *3* 2009 Jordanian on a student visa rouses interest from the FBI in Internet postings and, together with three agents, tries to detonate a fake bomb in the basement of a Dallas skyscraper

31 Mehanna *2* 2009 Well-educated Muslim jihadist may have plotted briefly to shoot up a shopping center in the Boston area and tried to join insurgency in the Middle East, but is arrested for spreading jihadist propaganda

32 Fort Hood *4* 2009 Military psychiatrist, acting as a lone wolf, shoots up a military deployment center in Ft Hood, TX, killing 12 soldiers and one civilian, shortly before he is supposed to be deployed to the war in Afghanistan

33 The underwear bomber *4* 2009 Nigerian man tries to blow up a US-bound airliner with explosives in his underwear but is subdued by passengers and crew

34 Times Square *4* 2010 Pakistani-American gets training in Pakistan and on his own tries, but fails, to set off a car bomb at Times Square in New York

35 Alaska *3* 2010 Muslim convert in a remote Alaska town plots the assassination of 20 with the aid of an informant

36 Parcel bombs on cargo planes *2* 2010 An effort by al-Qaeda in the Arabian Peninsula to set off parcel bombs implanted in printer cartridges on cargo planes bound for the United States is disrupted

37 DC Metro-bomb plot *3* 2010 Pakistani-American aids FBI operatives posing as al-Qaeda in a plot to bomb the DC Metro

38 Oregon *3* 2010 Teenaged Somali-American jihadist, unable to go abroad to fight, works with FBI operatives, apparently alerted by his father, to set off a van bomb at a Christmas tree lighting ceremony in Portland, OR

39 DC Metro-Facebook *2* 2010 Virginia man brags without substance to a female Facebook correspondent that he will bomb the Washington Metro soon, and is quickly arrested for making interstate threats, receiving a light sentence

40 Baltimore *3* 2010 Baltimore man seeks allies on Facebook for violent jihad, and the FBI supplies him with an informant and with a fake SUV bomb with which he tries to blow up a military recruitment center

41 Texas *2* 2011 Saudi student in Texas, flunking out and displaying intense new discontent on his blog and Facebook profile, is arrested after buying bomb-making materials and considering potential targets including crowded streets in distant New York and a local residence of former President George W. Bush

42 Manhattan's pair of lone wolves *3* 2011 Mentally ill American citizen, with accomplice and undercover officer, upset with how the US treats Muslims around the world, purchases weapons as the first step in a plot to blow up synagogues, the Empire State Building, and other targets in New York and New Jersey

43 Pentagon shooter *2* 2011 A US marine reservist with jihadist literature shoots at military buildings in the DC area and is arrested as he seeks to desecrate the graves of veterans of the wars in Iraq and Afghanistan

44 Seattle *3* 2011 Two financially destitute men, exercised over US foreign policy, are arrested in Seattle after they purchase an FBI-supplied machine gun that they plan to use to attack a military recruiting center after they save up enough money to purchase bullets and other material

45 Abdo *2* 2011 A US Army Private, unwilling to wage war on Muslims, is arrested after he buys ammunition and bomb materials to explode in a restaurant popular with soldiers

46 Model planes *3* 2011 Seeking to "decapitate" the US "military center", a mentally ill hobbyist plots with police operatives to attack the Pentagon and Capitol with remote-controlled model planes bearing explosives and then to attack the buildings

47 Iran and Scarface *3* 2011 An Iranian-American used-car salesman from Texas, nicknamed "Scarface" from the results of an earlier street brawl, is engaged for a promised $1.5 million by members of the Iranian government to arrange for a Mexican drug cartel to blow up Saudi Arabia's ambassador in a Washington restaurant but is foiled by an undercover Drug Enforcement Agency operative who is wired $100,000 as a down payment

48 Pimentel *3* 2011 A naturalized US citizen and Muslim convert, hostile to US military ventures in the Middle East, seeks to make pipe bombs using match-heads to attack various targets

49 Tampa *3* 2012 Under suspicion after he walked into a store seeking to purchase an al-Qaeda flag, an Albanian-American loner plots in Tampa with a police operative to detonate a car bomb, fire an assault rifle, wear an explosive belt, take hostages, and bomb nightclubs, a police center, a bridge, and a Starbuck's coffee shop in order to avenge wrongs against Muslims and to bring terror to his "victims' hearts"

50 Capitol bomber *3* 2012 A Moroccan man who had overstayed his visa for years and had been thrown out of his apartment for non-payment of rent, concludes that the war on terror is a war on Muslims, plots with FBI operatives, and is arrested as he seeks to carry out a suicide bombing at the Capitol

51 Chicago bar *3* 2012 Drawn by the violent jihadist emails and Internet postings composed by an unemployed and apparently retarded 18-year-old Egyptian-American who felt the US was at war with Islam, FBI agents gain his confidence, supply him with a fake bomb which he parks outside a Chicago bar he said was filled with "the evilest people", and then arrest him when he attempts to detonate it from a nearby alley

52 Bombing the Federal Reserve Bank *3* 2012 A college flunk-out from Bangladesh uses his parents' life-savings to study in the US and, while working as a busboy in Manhattan, reaches out on Facebook, obtains the help of the FBI to do something that will "shake the whole country", and is arrested when he tries to set off an FBI-supplied bomb planted at the Federal Reserve Bank from a nearby hotel room

53 The brothers *2* 2012 Two brothers in Florida plot to set off a bomb in New York in revenge for US drone attacks in Afghanistan, but are arrested before getting very far beyond bicycling around Manhattan looking for targets

54 Boston Marathon *4* 2013 Two Chechen-American brothers, working alone, detonate two homemade bombs in a crowd at the Boston marathon, killing three, and then are killed or captured a few days later after an exhaustive and dramatic manhunt

55 Wichita airport *3* 2013 A worker at the Wichita, Kansas, airport plots with FBI agents to detonate a car bomb at dawn at the airport

56 Rochester *3* 2014 A local man, in sympathy with Islamic State militants, plots with FBI

operatives to shoot and kill members of the US military

57 Cincinnati *3* 2015 A young local loner, in sympathy with ISIS, plots with FBI operatives to set off a bomb at the Capitol in Washington, DC

58 Aurora *3* 2015 Unable to travel abroad to fight because of a felony conviction for trying to rob a McDonald's, an Illinois man plots with FBI operatives to "unleash the lion" by attacking a local National Guard Armory

59 Two women in Queens *3* 2015 Protesting that "It's war" and "Protest don't work" and "Why can't we be some real bad bitches?" two women, one in communication with al-Qaeda in Yemen, try to fabricate bombs with the aid of an undercover officer

60 Fort Riley *3* 2015 A young man enthusing on Facebook about being killed in jihad, plots with FBI operatives to explode a 1000-pound bomb at a nearby military base

61 Ohio returnee from Syria *2* 2015 A Somali-American, actively communicating about his plans on social media, travels to the Middle East, stays about a month, receives some training, returns, and may have planned to commit violence

Case types

1. An Islamist extremist conspiracy or connection that, in the view of the authorities, might eventually develop into a plot to commit violence in the United States
2. An Islamist extremist terrorist plot to commit violence in the United States, no matter how embryonic, that is disrupted
3. An Islamist extremist plot to commit violence in the United States that was essentially created or facilitated in a major way by the authorities and then rolled up by arrest when enough evidence is accumulated
4. An Islamist extremist terrorist or terrorist group that actually reaches the stage of committing, or trying to commit, violence in the United States

There are also two case studies concerning efforts by Islamist extremists to go abroad to inflict damage on US interests there:

98 New York Stock Exchange 2010 Three men seek to join the fight against the US in the Middle East and find a couple of operatives in Yemen who agree to help them (and after being arrested, identify them), but only after the men send over tens of thousands of dollars and case the New York Stock Exchange for a possible attack

99 Toledo 2006 Three men in Toledo, OH, seek to join the fight against the US in the Middle East but fail to get there while attracting the attention of an informant who trains them