Exploiting Emotions About Paris to Blame Snowden, Distract from Actual Culprits Who Empowered ISIS

Whistleblowers are *always* accused of helping America's enemies (top Nixon aides accused Daniel Ellsberg of being a Soviet spy and causing the deaths of Americans with his leak); it's just the tactical playbook that's automatically used. So it's of course unsurprising that ever since Edward Snowden's whistleblowing enabled newspapers around the world to report on secretly implemented programs of mass surveillance, he has been accused by "officials" and their various media allies of Helping The Terrorists™.

Still, I was a bit surprised just by how quickly and *blatantly* — how shamelessly — some of them jumped to exploit the emotions prompted by the carnage in France to blame Snowden: doing so literally as the bodies still lay on the streets of Paris. At first, the tawdry exploiters were the likes of crazed ex-intelligence officials (former CIA chief James Woolsey, who once said Snowden "should be hanged by his neck until he is dead" and now has deep ties to private NSA contractors, along with Iran–obsessed Robert Baer); former Bush/Cheney apparatchiks (ex-White House spokesperson and current Fox personality Dana Perino); right-wing polemicists fired from *BuzzFeed* for plagiarism; and obscure *Fox News* comedians (Perino's co-host). So it was worth ignoring save for the occasional Twitter retort.

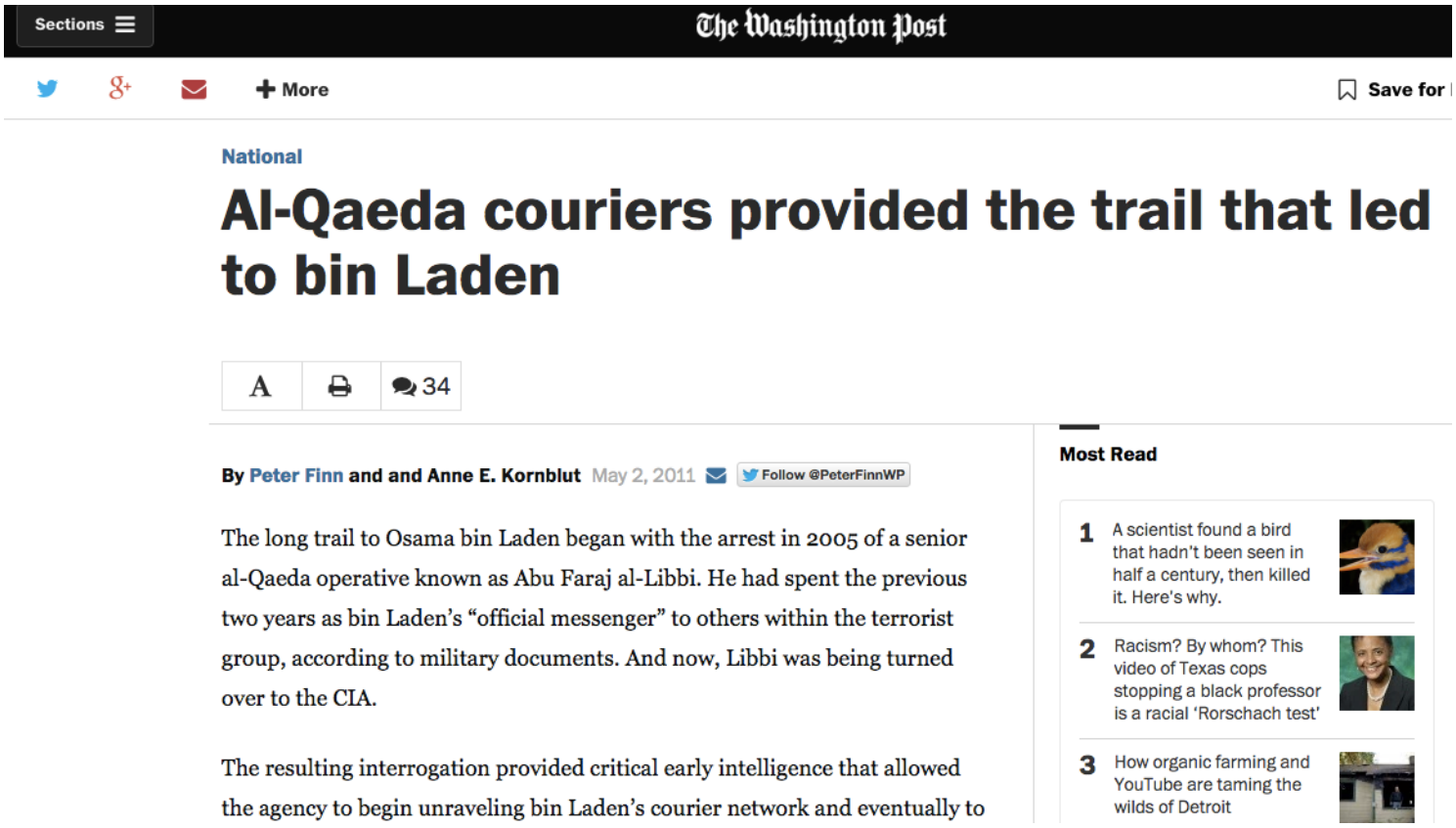
But now we've entered the inevitable "U.S. Officials Say" stage of the "reporting" on the Paris attack — i.e., journalists mindlessly and uncritically repeat whatever U.S. officials whisper in their ear about what happened. So now credible news sites are regurgitating the claim that the Paris Terrorists were enabled by Snowden leaks — based on no evidence or specific proof of any kind, needless to say, but just the unverified, obviously self-serving assertions of government officials. But much of the U.S. media loves to repeat rather than scrutinize what government officials tell them to say. So now this accusation has become widespread and is thus worth examining with just some of the actual evidence.

One key premise here seems to be that prior to the Snowden reporting, The Terrorists helpfully and stupidly used telephones and unencrypted emails to plot, so Western governments were able to track their plotting and disrupt at least large-scale attacks. That would come as a massive surprise to the victims of the attacks of 2002 in Bali, 2004 in Madrid, 2005 in London, 2008 in Mumbai, and April 2013 at the Boston Marathon. How did the multiple perpetrators of those well-coordinated attacks — all of which were carried out prior to Snowden's June 2013 revelations — hide their communications from detection?

This is a glaring case where propagandists can't keep their stories straight. The implicit premise of this accusation is that The Terrorists didn't know to avoid telephones or how to use effective encryption until Snowden came along and told them. Yet we've been warned for years and years before Snowden that The Terrorists are so diabolical and sophisticated that they engage in all sorts of complex techniques to evade electronic surveillance.

By itself, the glorious mythology of How the U.S. Tracked Osama bin Laden should make anyone embarrassed to make these claims. After all, the central premise of that storyline is that bin Laden only used trusted couriers to communicate *because al Qaeda knew for decades to avoid electronic means of communication because the U.S. and others could spy on those communications.* Remember all that? *Zero*

Dark Thirty and the “harsh but effective” interrogation of bin Laden’s “official messenger”?



Sections

The Washington Post

+ More

Save for

National

Al-Qaeda couriers provided the trail that led to bin Laden

A 34

By Peter Finn and and Anne E. Kornblut May 2, 2011 Follow @PeterFinnWP

The long trail to Osama bin Laden began with the arrest in 2005 of a senior al-Qaeda operative known as Abu Faraj al-Libbi. He had spent the previous two years as bin Laden’s “official messenger” to others within the terrorist group, according to military documents. And now, Libbi was being turned over to the CIA.

The resulting interrogation provided critical early intelligence that allowed the agency to begin unraveling bin Laden’s courier network and eventually to

Most Read

1 A scientist found a bird that hadn't been seen in half a century, then killed it. Here's why.

2 Racism? By whom? This video of Texas cops stopping a black professor is a racial ‘Rorschach test’

3 How organic farming and YouTube are taming the wilds of Detroit

Any terrorist capable of tying his own shoe — let alone carrying out a significant attack — has known for *decades* that speaking on open telephone and internet lines was to be avoided due to U.S. surveillance. As one Twitter commentator put it yesterday when mocking this new *It’s-Snowden’s-Fault* game: “Dude, the drug dealers from the Wire knew not to use cell phones.”

The Snowden revelations weren’t significant because they told The Terrorists their communications were being monitored; everyone — especially The Terrorists — has known that forever. The revelations were significant because they told the world that the NSA and its allies were collecting *everyone else’s* internet communications and activities.

The evidence proving this — that The Terrorists have been successfully using sophisticated encryption and other surveillance-avoidance methods for many years prior to Snowden — is so overwhelming that nobody should be willing to claim otherwise with a straight face. As but one of countless examples, here’s a *USA Today* article from **February 2001** — more than 12 years before anyone knew the name “Edward Snowden” — warning that al Qaeda was able to “outfox law enforcement” by hiding its communications behind sophisticated internet encryption:

USA TODAY

Tech

▪ E-mail this story ▪ Subscribe to t[illegible]ewspaper ▪ Si[illegible]

February 5, 2001

02/05/2001 - Updated 05:17 PM ET

Terror groups hide behind Web encryption

By Jack Kelley, USA TODAY

WASHINGTON — Hidden in the X-rated pictures on several pornographic Web sites and the posted comments on sports chat rooms may lie the encrypted blueprints of the next terrorist attack against the United States or its allies. It sounds farfetched, but U.S. officials and experts say it's the latest method of communication being used by Osama bin Laden and his associates to outfox law enforcement. Bin Laden, indicted in the bombing in 1998 of two U.S. embassies in East Africa, and others are hiding maps and photographs of terrorist targets and posting instructions for terrorist activities on sports chat rooms, pornographic bulletin boards and other Web sites, U.S. and foreign officials say.

AP

U.S. officials say Osama bin Laden is posting instructions for terrorist activities on sports chat rooms, pornographic bulletin boards and other Web sites.

Read more

Related story • Bin Laden notes hidden in sites

"Uncrackable encryption is allowing terrorists — Hamas, Hezbollah, al-Qaida and others — to communicate about their criminal intentions without fear of outside intrusion," FBI Director Louis Freeh said last March during closed-door testimony on terrorism before a Senate panel. "They're thwarting the efforts of law enforcement to detect, prevent and investigate illegal activities."

A terrorist's tool

The *Christian Science Monitor* similarly reported on February 1, 2001, that "the head of the U.S. National Security Agency has publicly complained that al Qaeda's sophisticated use of the internet and encryption techniques have defied Western eavesdropping attempts."

After 9/11, we were constantly told about how wily and advanced The Terrorists were when it came to hiding their communications from us. One scary graphic from the November 2001 issue of *Network World* laid it out this way:

network

Al Qaeda suspected of using everything from advanced steganography over the Internet to couriers carrying messages across the desert.

BY SHARON GAUDIN

terror

The U.S. and its allies

The U.S. is employing spy satellites and imaging software to track Al Qaeda. The very technology the terrorists use to communicate can give away their positions, with the U.S. scanning for cell phone radiation emissions, satellite signals and e-mail. And with some of the top encryption experts on its team, the U.S. is throwing its might into cracking Al Qaeda's code and weeding out the cells worldwide.

• Spy satellites
The U.S. has a network of spy satellites orbiting the globe. During the Gulf War, some of those satellites were trained on Iraq and Kuwait, but now the U.S. satellite system is believed to be scanning the Afghan mountains and surrounding areas for bin Laden.

• Imaging software
Using imaging software, the U.S. and its allies are able to pick out ground movement, such as transport trucks, tanks and troop movements.

• Triangulating cellular signals
By using three cellular towers, the source of a cell phone call can be pinpointed to within a few feet.

• Electronic footprints
Intelligence agencies around the world are watching for signal sources and even cellular radiation.

Additional tracking methods
- Watching e-mail traffi
- Wire tapping
- Online tapping
- Monitoring software
- Decryption software
- Software to sniff out steganography

• Human courier network
Al Qaeda's leaders are too wary of letting the U.S. pinpoint their locations by tracing electronic footprints, so they pass communications through a network of close, trusted human runners who slip through the Afghan countryside, moving farther away from bin Laden and his lieutenants.

• Cell phones, e-mail, satellite phones
Once beyond Afghanistan's borders, Al Qaeda's operatives will often go to populated areas — Baghdad, London, Islamabad — where communications can be veiled in the millions of other phone calls, cell phone calls or e-mails being sent out. Communications using these technologies are generally encrypted or use code phrases.

• Online semaphores
Using prearranged signals, a terrorist could set up a Web page with a blue background. A change in background color could signal a warning or call to action.

• Steganography
This is the art of digital camouflage, hiding an image, audio file or even a spreadsheet in a larger digital file, such as a photo.

• Front companies
Al Qaeda members use the cover of front companies to disguise phone calls, faxes and even terrorism-related travel. The companies also bring in money that can fund the Jihad.

• Anonymizers and remailers
This lets Al Qaeda members hide their identities when sending e-mail to their colleagues or those outside the terrorist group.

• Encryption
It's widely used to cloak communications that are being transmitted online or even passed hand-to-hand on a disk.

• Coded messages
Prearranged codes are used over telephones, cell phones, satellite phones, e-mail and even in person to disguise actual messages.

Message in a bitmap

Steganography is thought to be among Al Qaeda's high-tech communication tools.

Steganography is the art of hiding information in plain sight. Some security and terrorism experts say soldiers inside the Al Qaeda terrorist network could be using steganography to send each other secret messages embedded in ordinary looking digital photos.

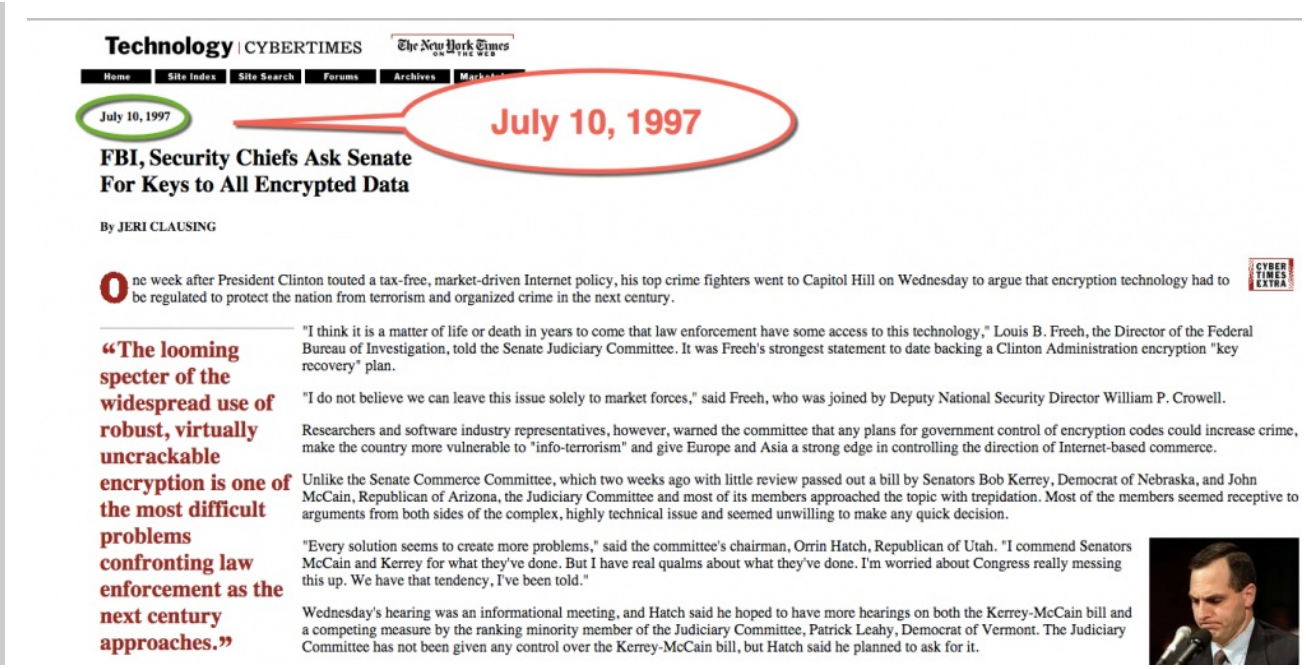
A variety of files, ranging from photos to text documents, audio and spreadsheets, can be hidden inside a simple digital photo, says Chet Hosmer, CEO or WetStone Technologies, a security company in Cortland, N.Y. There's a variety of steganography software available that will make tiny adjustments to the bits in an image and then insert the new file into open spaces.

The change is undetectable to the human eye, and the only way someone would know to check for a hidden message in a particular picture is if there were a predetermined type of picture to be on alert for. An operative might be told to watch for a picture of a brown-haired girl holding a flower, for instance. A software program would be used to scan the image for a hidden file and then extract it. The hidden file often would be encrypted, as well.

— Sharon Gaudin

All the way back in *the mid-1990s*, the Clinton administration exploited the fears prompted by Timothy McVeigh's Oklahoma City attack to demand backdoor access to all internet communications. This is what then-FBI Director Louis Freeh told the Senate Judiciary Committee in July 1997 — almost 20 years ago:

> *The looming spectre of the widespread use of robust, virtually uncrackable encryption is one of the most difficult problems confronting law enforcement as the next century approaches. At stake are some of our most valuable and reliable investigative techniques, and the public safety of our citizens. We believe that unless a balanced approach to encryption is adopted that includes a viable key management infrastructure, the ability of law enforcement to investigate and sometimes prevent the most serious crimes and terrorism will be severely impaired. Our national security will also be jeopardized.*



Technology | CYBERTIMES The New York Times ON THE WEB

Home | Site Index | Site Search | Forums | Archives | Market

July 10, 1997

July 10, 1997

FBI, Security Chiefs Ask Senate For Keys to All Encrypted Data

By JERI CLAUSING

One week after President Clinton touted a tax-free, market-driven Internet policy, his top crime fighters went to Capitol Hill on Wednesday to argue that encryption technology had to be regulated to protect the nation from terrorism and organized crime in the next century.

CYBER TIMES EXTRA

"The looming specter of the widespread use of robust, virtually uncrackable encryption is one of the most difficult problems confronting law enforcement as the next century approaches."

"I think it is a matter of life or death in years to come that law enforcement have some access to this technology," Louis B. Freeh, the Director of the Federal Bureau of Investigation, told the Senate Judiciary Committee. It was Freeh's strongest statement to date backing a Clinton Administration encryption "key recovery" plan.

"I do not believe we can leave this issue solely to market forces," said Freeh, who was joined by Deputy National Security Director William P. Crowell.

Researchers and software industry representatives, however, warned the committee that any plans for government control of encryption codes could increase crime, make the country more vulnerable to "info-terrorism" and give Europe and Asia a strong edge in controlling the direction of Internet-based commerce.

Unlike the Senate Commerce Committee, which two weeks ago with little review passed out a bill by Senators Bob Kerrey, Democrat of Nebraska, and John McCain, Republican of Arizona, the Judiciary Committee and most of its members approached the topic with trepidation. Most of the members seemed receptive to arguments from both sides of the complex, highly technical issue and seemed unwilling to make any quick decision.

"Every solution seems to create more problems," said the committee's chairman, Orrin Hatch, Republican of Utah. "I commend Senators McCain and Kerrey for what they've done. But I have real qualms about what they've done. I'm worried about Congress really messing this up. We have that tendency, I've been told."

Wednesday's hearing was an informational meeting, and Hatch said he hoped to have more hearings on both the Kerrey-McCain bill and a competing measure by the ranking minority member of the Judiciary Committee, Patrick Leahy, Democrat of Vermont. The Judiciary Committee has not been given any control over the Kerrey-McCain bill, but Hatch said he planned to ask for it.

How dumb do they think people are to count on them forgetting all of this, and to believe now that The Terrorists only learned to avoid telephones and use encryption once Snowden came along? Ironically, the Snowden archive itself is full of documents from NSA and its British counterpart, GCHQ, expressing deep concern that they cannot penetrate the communications of Terrorists because of how sophisticated their surveillance-avoidance methods are (obviously, those documents pre-date Snowden's public disclosures).

As but one example, the GCHQ files contain what the agency calls a "Jihadist Handbook" of security measures, dated 2003, that instructs terror operatives in the use of sophisticated surveillance-avoidance techniques that — as we noted when we first reported it — are very similar to what GCHQ *still* tells its own operatives to use:

In light of all this, how can "officials" and their media stenographers persist in trying to convince people of such a blatant, easily disproven falsehood: namely, that Terrorists learned to hide their communications from Snowden's revelations? They do it because of how many benefits there are from swindling people to believe this.

To begin with, U.S officials are eager here to demonize far more than just Snowden. They want to demonize encryption generally as well as any companies that offer it. Indeed, as these media accounts show, they've been trying *for two decades* to equate the use of encryption — anything that keeps them out of people's private online communications — with aiding and abetting The Terrorists. It's not just Snowden but also their own long-time Surveillance State partners — particular Apple and Google — who are now being depicted as Terrorist Lovers for enabling people to have privacy on the internet through encryption products.

As I documented last November, the key tactic of American and British officials is to wage a P.R. war against Silicon Valley companies who offer encryption by accusing them of Helping The Terrorists. Last September, FBI Director James Comey actually said, "What concerns me about this is companies marketing something

expressly to allow people to hold themselves beyond the law," while the *New York Times* gave anonymity in that article to a security official to link the new iPhone 6 to terrorism. The head of GCHQ called Apple and Google "the command-and-control networks of choice for terrorists and criminals" as part of what the *New York Times* called "a campaign by intelligence services in Britain and the United States against pressure to rein in their digital surveillance after disclosures by the American former contractor Edward J. Snowden."

Mail Online

Home | News | U.S. | Sport | TV&Showbiz | Australia | Femail | Health | Science | Money

Latest Headlines | News | World News | Arts | Headlines | Pictures | Most read | News Board | Wires

Twitter and Facebook are helping terrorists says new GCHQ chief: Fanatics using social media as 'command and control networks'

- **Privacy campaigners slam the claims and demands by Robert Hannigan**
- **Big Brother Watch's Emma Carr accuses him of 'perpetuating falsehoods'**
- **Mr Hannigan started at GCHQ on Monday after working in Foreign Office**
- **Insisted some firms 'in denial' about way fanatics misuse their services**

By JAMES SLACK, HOME AFFAIRS EDITOR FOR THE DAILY MAIL

PUBLISHED: 21:58 GMT, 3 November 2014 | **UPDATED:** 23:13 GMT, 4 November 2014

Share 252 shares 180 View comments

Global internet companies have become 'the command and control networks of choice' for terrorists, claims the new head of Britain's electronic spying agency.

Then there's the blame-shifting benefit. For most major terror attacks, the perpetrators were either known to Western security agencies or they had ample reason to watch them. All three perpetrators of the *Charlie Hebdo* massacre "were known to French authorities," as was the thwarted train attacker in July and at least one of the Paris attackers. These agencies receive billions and billions of dollars every year and radical powers, all in the name of surveilling Bad People and stopping attacks.

So when they fail in their ostensible duty, and people die because of that failure, it's a natural instinct to blame others: *Don't look to us; it's Snowden's fault, or the fault of Apple, or the fault of journalists, or the fault of encryption designers, or anyone's fault other than ours.* If you're a security agency after a successful Terror attack, you want everyone looking elsewhere, finding all sorts of culprits other than those responsible for stopping such attacks.

Above all, there's the desperation to prevent people from asking how and why ISIS was able to spring up seemingly out of nowhere and be so powerful, able to blow up a Russian passenger plane, a market in Beirut, and the streets of Paris in a single week. That's the one question Western officials are most desperate not to be asked, so directing people's ire to Edward Snowden and Apple is beneficial in the extreme.


SECTIONS HOME SEARCH

The New York Times

Obama Calls Paris Events 'an Attack on the Civilized World'

After Outcry, Ireland Adjusts Its Corporate Tax Draw

Three Teams of Coordinated Attackers Carried Out Assault on Paris, Officials Say...

Attackers in P Give Anybody

EUROPE

Tony Blair Says Iraq War Helped Give Rise to ISIS

By KIMIKO DE FREYTAS-TAMURA OCT. 25, 2015

Email Share Tweet Save

LONDON — Tony Blair, the former British prime minister, suggested on Sunday that the United States-led invasion of Iraq in 2003, which removed Saddam Hussein from power, helped give rise to the Islamic State, even as he said it was "hard to apologize for removing Saddam."

Mr. Blair, whose decision to involve Britain in the military mission made him deeply unpopular at home, told CNN that "there are elements of truth" to the view that the war in Iraq helped pave the way for the Islamic State.

The origins of ISIS are not even in dispute. The *Washington Post* put it simply: "*almost all of the leaders of the Islamic State are former Iraqi officers*, including the members of its shadowy military and security committees, and the majority of its emirs and princes." Even Tony Blair — *Tony Blair* — admits that there'd be no ISIS without the invasion of Iraq: "'I think there are elements of truth in that,' he said when asked whether the Iraq invasion had been the 'principal cause' of the rise of ISIS." As *The New Yorker*'s John Cassidy put it in August:

> *By destroying the Iraqi state and setting off reverberations across the region that, ultimately, led to a civil war in Syria, the 2003 invasion created the conditions in which a movement like ISIS could thrive. And, by turning public opinion in the United States and other Western countries against anything that even suggests a prolonged military involvement in the Middle East, the war effectively precluded the possibility of a large-scale multinational effort to smash the self-styled caliphate.*

Then there's the related question of how ISIS has become so well-armed and powerful. There are many causes, but a leading one is the role played by the U.S. and its "allies in the region" (i.e., Gulf tyrannies) in arming them, unwittingly or (in the case of its "allies in the region") otherwise, by dumping weapons and money into the region with little regard to where they go (even U.S. officials openly acknowledge that their own allies have funded ISIS). But the U.S.'s own once-secret documents strongly suggest U.S. complicity as well, albeit inadvertent, in the rise of ISIS, as powerfully demonstrated by this extraordinary four-minute clip of Al Jazeera's Mehdi Hasan with Gen. Michael Flynn, former head of the Defense Intelligence Agency:

Given all this, is there any mystery why "U.S. officials" and the military-intelligence regime, let alone Iraq War-advocating hacks like Jim Woolsey and Dana Perino, are desperate to shift blame away from themselves for ISIS and terror attacks and onto Edward Snowden, journalism about surveillance, or encryption-providing tech companies? Wouldn't you if you were them? Imagine simultaneously devoting all your efforts to depicting ISIS as the Greatest and Most Evil Threat Ever, while knowing the vital role you played in its genesis and growth.

The clear, overwhelming evidence — compiled above — demonstrates how much deceit their blame-shifting accusations require. But the more important point of inquiry is to ask why they are so eager to ensure that everyone but themselves receives scrutiny for what is happening. The answer to that question is equally clear, and disturbing in the extreme.

Research: Margot Williams

"