MAYBE THE GIMMICK IS IN THE TIMING OF LEGION OF DOOM?

In my first post on this Yemen scare — which I will henceforth call "Legion of Doom" in honor of the Daily Beast source's use of the term — I suggested the big part of the plot might have already transpired.

> There's the increased drone activity in Yemen. Who knows! Maybe, like last year, the plot has already been rolled up and we're just waiting to confirm one of the several recent drone strikes have taken out our target?

I made that suggestion because of evidence that the US rolled up UndieBomb 2.0 on April 20-24 of last year, and **only then** deployed a bunch of Air Marshals and fear-mongering about Ibrahim al-Asiri for the days leading up to the May 1 anniversary of Osama bin Laden's killing. They eliminated the threat (which was minimal in any case, since the bomber was a British-Saudi-US mole), then rolled out fear-mongering about it, as if the threat still existed. Fairly clearly, the White House planned a big press conference on their operation once they killed Fahd al-Quso, and thus got furious when the AP managed to scoop their theater.

I increasingly think that may be the case. Whether or not there was ever a real threat, I suspect it may have partly passed before the big rollout of it last Friday (though the targeting of a top AQAP member, the presence of additional JSOC forces, or all the drone strikes may have increased the risk for Americans in Yemen).

Consider: back when Pentagon stenographer Barbara Starr was among the first to discuss the intercepts behind Legion of Doom, she suggested very fresh SIGINT chatter and a warning from President Abdo Rabi Mansour Hadi delivered on

July 31 or August 1 had led the US to close a bunch of embassies (though even there, they waited a few days to start closing embassies).

> **Fresh intelligence** led the United States to conclude that operatives of al Qaeda in the Arabian Peninsula were in the final stages of planning an attack against U.S. and Western targets, several U.S. officials told CNN.
>
> The warning led the U.S. State Department to issue a global travel alert Friday, warning al Qaeda may launch attacks in the Middle East, North Africa and beyond in coming weeks. The U.S. government also was preparing to close 22 embassies and consulates in the region Sunday as a precaution.
>
> **The chatter among al Qaeda in the Arabian Peninsula operatives had gone on for weeks but increased in the last few days**, the officials said.
>
> Taken together with a warning from Yemeni officials, the United States took the extraordinary step of shutting down embassies and issuing travel warnings, said the officials, who spoke on condition of anonymity.
>
> While the specific target is uncertain, U.S. officials are deeply worried about a possible attack against the U.S. Embassy in Yemen **occurring through Tuesday**, the officials said.
>
> [snip]
>
> **Yemeni intelligence agencies alerted authorities of the threat two days ago**, when the Yemeni president was in Washington, said the official, who spoke on condition of anonymity. [my emphasis]

And the original and an update to the NYT's original story on Legion of Doom says the intercept between Zawahiri and Wuhayshi came

sometime last week.

> The intercepted conversations last week between Ayman al-Zawahri, who succeeded Osama bin Laden as the head of the global terrorist group, and Nasser al-Wuhayshi, the head of the Yemen-based Al Qaeda in the Arabian Peninsula, revealed what American intelligence officials and lawmakers have described as one of the most serious plots against American and Western interests since the attacks on Sept. 11, 2001.

But the latest AP version of the intercept call says it was picked up "several weeks ago."

> A U.S. intelligence official and a Mideast diplomat said al-Zawahri's message was picked up several weeks ago and appeared to initially target Yemeni interests. The threat was expanded to include American or other Western sites abroad, officials said, indicating the target could be a single embassy, a number of posts or some other site. Lawmakers have said it was a massive plot in the final stages, but they have offered no specifics.

Perhaps the discrepancy comes from confusion about two different Zawahiri-Wuhayshi intercepts. In its conference call report, the Daily Beast reports that authorities picked up a communication, via courier, between Zawahiri and Wuhayshi "last month."

> An earlier communication between Zawahiri and Wuhayshi delivered through a courier was picked up last month, according to three U.S. intelligence officials.

That earlier conversation may simply have been Zawahiri naming Wuhayshi his deputy, but the role of a courier in the interception suggests

they may have gotten far more intelligence — perhaps not just intelligence tipping the US off to whatever conference call protocol AQ was using, but also to the location of Wuhayshi and other figures.

Now consider the drone strikes. After a lapse of 6 weeks (and an overall quiet back to the Brennan confirmation), there have been ~~5~~ 6 attacks reported as drone strikes in the last several weeks. One would hope the intensity of the drone strikes represents some kind of new intelligence. But if it does, it represents intelligence dating back to before July 28, the date of the first strike in this series. That would coincide between with the AP's timing and/or the timing of the capture of the courier.

Finally, consider Iona Craig's fact check from Saturday of this Guardian article. She notes that while the Guardian bylines the article from Sanaa, the reporter is actually elsewhere. She notes several errors in the description of a clash that took place on Friday, and notes the British warning to leave Yemen has been in place since March 2011.

It's this item, though, I find most interesting. The Guardian quotes an anonymous "security source" saying that a recent IED explosion at a checkpoint led security forces to believe someone was testing security on approaches to the British and US embassies.

> A security source in Sana'a said: "After an improvised explosive device (IED) exploded at a checkpoint in Al-Hasabah [a district in the capital] a week ago, more IEDs were discovered in and around the capital at checkpoints that lead to and from the embassies of the UK and the US. This prompted the capital's security forces to think their security protocol was being 'tested' for a larger attack."

But Craig notes,

> The explosion in Hasaba was a month ago. Not a week ago.

The blast was reported on July 8 — which was the first day of Ramadan — but it appears the blast took place 2 days earlier, on July 6. The story itself contributes nothing to the actual news (or that being treated as news) about Legion of Doom. But it reveals that either the Guardian is very confused (which certainly seems possible), and/or a security source is trying to suggest the origin of Yemeni threat intelligence relating to perceived IED threats at checkpoints is more recent than it really is, the last week rather than the entire month of Ramadan.

This is all, obviously, wildarsed speculation based on some pretty crazy reporting.

Whatever the timing of whatever the big news, it seems clear the US is settling in for a larger operation in Yemen, which will likely further obscure what is really going on.

But given the precedent of UndieBomb 2.0, in which the government pretty demonstrably carried out a fear-mongering campaign after the threat had already been thwarted, I'll raise again the possibility that these events actually could mean to obscure big news that has already occurred.

Update: Restructured original post somewhat.

July, unknown date: Communication between Ayman al-Zawahiri and Nasir al-Wuhayshi via courier picked up

July 8: Ramadan begins

July 16: AQAP confirms death of Said al-Shihri, reportedly in fourth drone strike that targeted him

July 19: Spokesperson for Yemeni Embassy tweets, "With the death of #AQAP cofounder Saeed alShihri & **the absence of #alQaeda's Emir Nasir**

alWehayshi, who is running the #AQ network in Yemen;" John Pistole ratchets up Ibrahim al-Asiri fear-mongering again

July 21: Abu Ghraib prison break

July 23: Abdulelah Haider Shaye released

July 23: Hadi in Qatar

"Several weeks ago:" per the AP when communication between Zawahiri and Wuhayshi intercepted

July 24: Hadi leaves for the US

July 25: Hadi visit to DC
formally announced (see discussion of whether it was planned in advance)

July 28: Drone strike # 1, Abyan, kills 6;
report Ibrahim al-Asiri killed in drone strike (his escape announced August 3)

July 29: Hadi meets with John Kerry and John Brennan; drone strike in Waziristan, including possible high profile figure

July 30: Hadi meets with Jacob Lew and Chuck Hagel; Pakistani prison break; Drone strike #2, Shabwa, kills 3, potentially including Al Khidr Husayn al Ja'dani

July 31 – August 1: Hadi delivers intelligence on threat

August 1: Hadi meets Obama; Drone strike #3, Hadramout, kills 5

August 2: US announces Embassy closures;
reported date of Tor compromise

August 3: Saudi King Abdullah hosts Hadi; Yemeni Embassy promises "major development" to be announced (a Saudi "suicide bomber" captured in Yemen just before the meeting)

August 4: Intercepted date planned for attack, Embassy closures start; first reports of Tor compromise

August 5: Yemen offers rewards for 25 AQAP

operatives

August 6: Yemen Foreign Minister says Embassy shutdowns help extremists; US “evacuates” staff; Drone strike #4, Marib, kills 4

August 7: 15 year anniversary of African Embassy bombings, Ramadan ends; Drone strike #5, Shabwa, kills 7; Update: and Strike #6, details to come

---

THE OOGA BOOGA* CONTINUES TO WEAR OFF

Two and a half years ago, I noted how TSA head John Pistole pointed to a plot the FBI created while he was still its Deputy Director to justify the use of VIPR teams to stop people on non-aviation public transportation.

> A couple of weeks back, I pointed to John Pistole’s testimony that directly justified the expansion of VIPR checkpoints to mass transport locations by pointing to a recent FBI-entrapment facilitated arrest.
>
> > Another recent case highlights the importance of mass transit security. On October 27, the Federal Bureau of Investigation (FBI) arrested a Pakistan-born naturalized U.S. citizen for attempting to assist others whom he believed to be members of al Qaida in planning multiple bombings at Metrorail stations in the Washington, D.C., area. During a sting operation, Farooque Ahmed allegedly conducted surveillance of the Arlington National Cemetery,

> > Courthouse, and Pentagon City Metro stations, indicated that he would travel overseas for jihad, and agreed to donate $10,000 to terrorist causes. A federal grand jury in Alexandria, Virginia, returned a three-count indictment against Ahmed, charging him with attempting to provide material support to a designated terrorist organization, collecting information to assist in planning a terrorist attack on a transit facility, and attempting to provide material support to help carry out multiple bombings to cause mass casualties at D.C.-area Metrorail stations.
>
> > While the public was never in danger, **Ahmed's intentions provide a reminder of the terrorist attacks on other mass transit systems: Madrid in March 2004, London in July 2005, and Moscow earlier this year. Our ability to protect mass transit and other surface transportation venues from evolving threats of terrorism requires us to explore ways to improve the partnerships between TSA and state, local, tribal, and territorial law enforcement, and other mass transit stakeholders. These partnerships include measures such as Visible Intermodal Prevention and Response (VIPR) teams we have put in place with the support of the Congress**. [my emphasis]

Now to be clear, as with Mohamed Mohamud's alleged plot, Ahmed's

> plot *never existed* except as it was performed by FBI undercover employees. In fact, at the time the FBI invented this plot, now TSA-head Pistole was the Deputy Director of FBI, so in some ways, Ahmed's plot is Pistole's plot. Nevertheless, Pistole had no problem pointing to a plot invented by his then-subordinates at the FBI to justify increased VIPR surveillance on "mass transit and other surface transportation venues." As if the fake FBI plot represented a real threat.

Today, a NYT piece raises questions about VIPR's efficacy (without, however, noting how TSA has pointed to FBI-generated plots to justify it).

> T.S.A. and local law enforcement officials say the teams are a critical component of the nation's counterterrorism efforts, but some members of Congress, auditors at the Department of Homeland Security and civil liberties groups are sounding alarms. The teams are also raising hackles among passengers who call them unnecessary and intrusive.
>
> "Our mandate is to provide security and counterterrorism operations for all high-risk transportation targets, not just airports and aviation," said John S. Pistole, the administrator of the agency. "The VIPR teams are a big part of that."
>
> Some in Congress, however, say the T.S.A. has not demonstrated that the teams are effective. Auditors at the Department of Homeland Security are asking questions about whether the teams are properly trained and deployed based on actual security threats.

It'd really be nice if NYT had named the "some"

in Congress who had raised concerns. Particularly given its focus on TSA's expanding budget, which Congress has the ability to cut.

> The program now has a $100 million annual budget and is growing rapidly, increasing to several hundred people and 37 teams last year, up from 10 teams in 2008. T.S.A. records show that the teams ran more than 8,800 unannounced checkpoints and search operations with local law enforcement outside of airports last year, including those at the Indianapolis 500 and the Democratic and Republican national political conventions.

But I'm most fascinated by TSA's second (again, unnamed) defense of the program.

> T.S.A. officials would not say if the VIPR teams had ever foiled a terrorist plot or thwarted any major threat to public safety, saying the information is classified. But they argue that the random searches and presence of armed officers serve as a deterrent that bolsters the public confidence.

As with the telephone metadata dragnet, they won't say whether they've actually thwarted a plot. Instead, they effectively say security theater "bolsters the public confidence."

Let's hope those "some in Congress" the NYT won't identify do act to defund this.

Foreign Policy's Editor-at-Large David Rothkopf expresses optimism that we have finally begun to wake up from the spell the decade of fearmongering has put us under.

> We have come to what could be seen as the end of an ignominious period in U.S. national security history, one that might be called the Decade of Fear. And though it was the 9/11 attacks that

> ushered this period in, our response in the months and years afterward defined it far more than those blows ever could. At a moment when the United States could have seen the terrorist threat as being as limited and peripheral, we over-reacted – grotesquely.
>
> We didn't react to the moment. We didn't seize it. We succumbed to it.
>
> Instead, we allowed our fear to drive the creation of a massive government security apparatus, huge expenditures, and reckless global programs. Compared to the number of people, groups, or weapons systems threatening us, our investment in our response to said threats redefines "disproportionate" in the annals of a government where excess has been a hallmark of our military-industrial complex. And that's saying something.
>
> Gradually, this excess came to haunt us. War spending with its $2-3 trillion price tag exacerbated our national financial burdens at a time of great economic crisis. Our wars of over-reach and ideological hysteria damaged our international standing and incited political backlash at home. Recently, some of the secret initiatives launched to contain the perceived (but amorphous and largely illusory) were revealed to have risked not only American personal freedoms but also international relationships in ways that no terrorist could ever hope to achieve.
>
> This in turn has finally created a reaction, a retrenchment, and, thankfully, a movement back to a more rational national security.

Certainly the polling on the balance between security and liberty after the Boston Marathon

attack reflects this. As does polling on whether Edward Snowden is a whistleblower or villain. So, too, does the widespread skepticism about the latest Yemen scare.

Rothkopf endorses something I and others suggested after Janet Napolitano announced her departure: either give Department of Homeland Security a mandate that includes real urgent threats to the "homeland," such as resilience in the face of climate change related disasters and possibly even mitigation approaches, or shut it down.

If Rothkopf is right that the spell is beginning to wear off (it may be wearing off in flyover country, but members of Congress and their lobbyist funders still seem to buy it), then we really need to take several big picture steps back to discuss what the real risks to the country are. Before we waste more trillions on security theater and pointless wars.

---

*Note, the term Ooga booga clearly has racist roots. I use it here to convey, in part, that the fearmongering relies in part on racially-coded fears.

WHAT IF THE TOR TAKEDOWN RELATES TO THE YEMENI ALERT?

Eli Lake and Josh Rogin reveal that the intercept between Ayman al-Zawahiri and Nasir al-Wuhayshi was actually a conference call between those two and affiliates all over the region.

> The Daily Beast has learned that the discussion between the two al Qaeda

> leaders happened in a conference call that included the leaders or representatives of the top leadership of al Qaeda and its affiliates calling in from different locations, according to three U.S. officials familiar with the intelligence. All told, said one U.S. intelligence official, more than 20 al Qaeda operatives were on the call.
>
> To be sure, the CIA had been tracking the threat posed by Wuhayshi for months. An earlier communication between Zawahiri and Wuhayshi delivered through a courier was picked up last month, according to three U.S. intelligence officials. But the conference call provided a new sense of urgency for the U.S. government, the sources said.

The fact that al Qaeda would be able to have such conference calls in this day and age is stunning. The fact that US and Yemeni sources would expose that they knew about it is equally mind-boggling.

But one thing would make it make more sense.

On Sunday, Tor users first discovered the FBI had compromised a bunch of onion sites and introduced malware into FireFox browsers accessing the system. Since then, we've learned the malware was in place by Friday, the day the US first announced this alert (though the exploit in FireFox has been known since June).

> The owner of an Irish company, Freedom Hosting, has allegedly been providing turnkey hosting services for the Darknet, or Deep Web, which is "hidden" and only accessible through Tor .onion and the Firefox browser. The FBI reportedly called Eric Eoin Marques "the largest facilitator of child porn on the planet" and wants to extradite the 28-year-old man. About that time, Freedom Hosting went down; Tor users discovered

> that someone had used a Firefox zero-day to deliver drive-by-downloads to anyone who accessed a site hosted by Freedom Hosting. Ofir David, of Israeli cybersecurity firm Cyberhat, told Krebs on Security, "**Whoever is running this exploit can match any Tor user to his true Internet address, and therefore track down the Tor user**."
>
> If you've never visited the Hidden Wiki, then you should be fully aware that if you do, you *will* see things that can never be unseen. Freedom Hosting maintained servers for "TorMail, long considered the most secure anonymous email operation online," wrote Daily Dot. "Major hacking and fraud forums such as HackBB; large money laundering operations; and the Hidden Wiki, which, until recently, was the de facto encyclopedia of the Dark Net; and virtually all of the most popular child pornography websites on the planet."
>
> But if you use Tor Browser Bundle with Firefox 17, you accessed a Freedom Hosting hidden service site since August 2, and you have JavaScript enabled, then experts suggest it's likely your machine has been compromised. In fact, E Hacking News claimed that almost half of all Tor sites have been compromised by the FBI. [my emphasis]

So what if this takedown was only secondarily about child porn, and primarily about disabling a system al Qaeda has used to carry out fairly brazen centralized communications? Once the malware was in place, the communications between al Qaeda would be useless in any case (and I could see the government doing that to undermine the current planning efforts).

The timing would all line up — and it would explain (though not excuse) why the government is boasting about compromising the

communications. And it would explain why Keith Alexander gave this speech at BlackHat.

> terrorists … terrorism … terrorist attacks … counterterrorism … counterterrorism … terrorists … counterterrorism … terrorist organizations … terrorist activities … terrorist … terrorist activities … counterterrorism nexus … terrorist actor … terrorist? … terrorism … terrorist … terrorists … imminent terrorist attack … terrorist … terrorist-related actor … another terrorist … terrorist-related activities … terrorist activities … stopping terrorism … future terrorist attacks … terrorist plots … terrorist associations
>
> [snip]
>
> Sitting among you are people who mean us harm

Just one thing doesn't make sense.

Once NSA/FBI compromised Tor, they'd have a way to identify the location of users. That might explain the uptick in drone strikes in Yemen in the last 12 days. But why would you both alert Tor users and — with this leak — Al Qaeda that you had broken the system and could ID their location? Why not roll up the network first, and then take down the Irish child porn guy who is the likely target?

I'm not sure I understand the Tor exploit well enough to say, but the timing does line up remarkably well.

Update: Some re-evaluation of what really happened with the exploit.

> Researchers who claimed they found a link between the Internet addresses used as part of malware that attacked Freedom Hosting's "hidden service" websites last week and the National Security Agency (NSA) have backed off substantially from

> their original assertions. After the findings were criticized by others who analyzed Domain Name System (DNS) and American Registry for Internet Numbers (ARIN) data associated with the addresses in question, Baneki Privacy Labs and Cryptocloud admitted that analysis of the ownership of the IP addresses was flawed. However, they believe the data that they used to make the connection between the address and the NSA may have changed between their first observation.

Update: On Twitter, Lake clarifies that this conference call was not telephone-based communications.

US JUSTICE: A ROTTING TREE OF POISONOUS FRUIT?

Saturday, the NYT reported that other agencies within government struggle to get NSA to share its intelligence with them.

> Agencies working to curb drug trafficking, cyberattacks, money laundering, counterfeiting and even copyright infringement complain that their attempts to exploit the security agency’s vast resources have often been turned down because their own investigations are not considered a high enough priority, current and former government officials say.

Of the 1,410 words in the article, 313 words are explicitly attributed to Tim Edgar, who used to work for ACLU but starting in 2006 worked first

in the Office of Director of National Intelligence and then in the White House. Another 27 are attributed to "a former senior White House intelligence official," the same description used to introduce Edgar in the article.

The article ends with Edgar expressing relief that NSA succeeded in withholding material (earlier he made a distinction between sharing raw data and intelligence reports) from agencies executing key foreign policy initiatives in the age of cyberwar and Transnational Criminal Organizations, and in so doing avoid a "nightmare scenario."

> As furious as the public criticism of the security agency's programs has been in the two months since Mr. Snowden's disclosures, "it could have been much, much worse, if we had let these other agencies loose and we had real abuses," Mr. Edgar said. "That was the nightmare scenario we were worried about, and that hasn't happened."

Today, San Francisco Chronicle reminds that NSA does hand over evidence of serious criminal activities if it finds it while conducting foreign intelligence surveillance, and prosecutors often hide the source of that original intelligence.

> Current and former federal officials say the NSA limits non-terrorism referrals to serious criminal activity inadvertently detected during domestic and foreign surveillance. The NSA referrals apparently have included cases of suspected human trafficking, sexual abuse and overseas bribery by U.S.-based corporations or foreign corporate rivals that violate the Foreign Corrupt Practices Act.
>
> [snip]
>
> "If the intelligence agency uncovers

> evidence of any crime ranging from sexual abuse to FCPA, they tend to turn that information over to the Department of Justice," Litt told an audience at the Brookings Institution recently. "But the Department of Justice cannot task the intelligence community to do that."
>
> [snip]
>
> "The problem you have is that in many, if not most cases, the NSA doesn't tell DOJ prosecutors where or how they got the information, and won't respond to any discovery requests," said Haddon, the defense attorney. "It's a rare day when you get to find out what the genesis of the ultimate investigation is."
>
> The former Justice Department official agreed: "A defense lawyer can try to follow the bouncing ball to see where the tip came from – but a prosecutor is not going to acknowledge that it came from intelligence."

And (as bmaz already noted) Reuters reminds that the DEA has long had its own electronic surveillance capability, and it often hides the source of intelligence as well.

> Although these cases rarely involve national security issues, documents reviewed by Reuters show that law enforcement agents have been directed to conceal how such investigations truly begin – not only from defense lawyers but also sometimes from prosecutors and judges.
>
> The undated documents show that federal agents are trained to "recreate" the investigative trail to effectively cover up where the information originated, a practice that some experts say violates a defendant's Constitutional right to a fair trial. If defendants don't know how

> an investigation began, they cannot know to ask to review potential sources of exculpatory evidence — information that could reveal entrapment, mistakes or biased witnesses.

As bmaz also noted, none of this was very secret or new. The FISA sharing is clearly permitted by the minimization procedures. Litigation on it 11 years ago suggested it may be even more abusive than laid out under the law. And bmaz has personally been bitching about the DEA stuff as long as I've known him.

These articles suggesting there may be more sharing than the NYT made out on Saturday, then, are primarily reminders that when the fruits of this intelligence get shared, the source of the intelligence often remains hidden from those it is used against.

Which brings me to this WSJ op-ed Edgar published last week. In some ways the op-ed makes a laudable case for more transparency.

> What, then, accounts for the public mistrust? Intelligence officials forget that the public sees none of this. Where the government sees three branches of government working together in harmony, the public sees a disturbing pattern of secret law and secret government accompanied by demands to "trust us, we are keeping you safe." Secret checks and balances appear to be nothing more than a pale shadow of our constitutional design.
>
> [snip]
>
> President Obama should go further, wresting control from the leakers and restoring trust with the public. He should ask Mr. Clapper to look across the intelligence community and disclose to the public the types of large databases it collects in bulk, under what legal powers or interpretations,

> and pursuant to what safeguards to protect Americans' privacy—while keeping necessary details secret.
>
> [snip]
>
> Openness is a value in itself, but it is also a necessary precondition to the effective functioning of our three branches of government.

Though it seems to contradict itself as to whether the NSA is collecting everything.

> 'Big data" is one name for the insight that collecting all the information in a massive database will uncover facts that collecting only some of the information cannot. This is not news to Gen. Keith Alexander, director of the National Security Agency. Gen. Alexander is a zealous advocate of getting it all whenever practically and legally possible.
>
> [snip]
>
> Despite what Americans see in the movies, the NSA doesn't actually collect everything.

But the truly bizarre part of this op-ed that endorses more transparency is this claim about Amnesty v. Clapper.

> The ACLU has challenged the constitutionality of NSA surveillance programs for years, but that case never got to the issue of constitutional rights. The intelligence community argued, and the Supreme Court agreed, that the civil-liberties groups couldn't maintain their lawsuit. Civil-liberties advocates represented a variety of people with entirely reasonable fears of monitoring. Whether they were actually under surveillance was a secret (**and properly so**). The government argued

> vigorously that this secrecy meant the case could not go forward, and the court agreed. [my emphasis]

Remember, as a threshold matter, what we're talking about. Amnesty v. Clapper's plaintiffs included human rights organizations like Amnesty International and Human Rights Watch; criminal defense attorneys including Khalid Sheikh Mohammed and Mohamedou Ould Salahi's attorneys by name, the Nation and Chris Hedges, and SEIU.

Since SCOTUS rejected the plaintiffs' case on standing, leaked minimization standards have made it clear Section 702 surveillance provides no protection for human rights workers, journalists, political organizations, or even attorneys representing people — like Salahi — who have not yet been criminally charged. While none of the plaintiffs in the case could be directly targeted, their communications with people they have every business to be talking to easily could be. And we'd never know whether these entities — whose work makes them adversaries to the government — were surveilled unless the government decided to charge them or their interlocutors and reveal that fact.

And Tim Edgar, civil libertarian, thinks it is "proper" that all these people, most of whose activities are protected under the Constitution, should never know if the government is surveilling their work.

Then there's the other problem with Edgar's endorsement of secrecy surrounding whether Amnesty v. Clapper plaintiffs have been surveilled: the government has reneged on the several promises it made over the course of that litigation to reveal when this surveillance is used on defendants (precisely the issue the SFChron and Reuters stories emphasize).

> What we have learned since the *Clapper* decision, however, has revealed a yawning chasm between the government's words and actions. Faced

> with recent revelations_about the FAA surveillance program, intelligence officials have raced to defend the controversial law. And, in doing so, they have touted at least four cases where warrantless FAA surveillance was purportedly critical to preempting terrorist plots. Yet not one of the defendants in these prosecutions was told that the government's evidence was obtained from FAA surveillance, and thus they had no opportunity to challenge the statute. This fact runs directly contrary to the arguments that lawyers for the government paraded before the Supreme Court just last fall.
>
> Indeed, the government has openly departed from its previous position. Criminal defendants in Chicago and Florida have filed motions seeking to compel the government to provide notice of its intent to rely on evidence obtained from warrantless wiretapping under the FAA, yet the government is now arguing that it has no obligation to do so.

This extends to the program Edgar specifically defends in his op-ed, the Section 215 dragnet, where the government never told Basaaly Saaed Moalin it used the Section 215 dragnet — apparently accessed by claiming al-Shabaab's pre-terrorist designation effort to expel US-backed invaders of Somalia amounted to plotting against "the homeland" — to identify and justify wiretaps on him.

Given Edgar's enthusiasm for the surveillance of even protected activities to remain secret, taken in tandem with all the known examples where the government hides the source of this surveillance, there is no reason to believe an article based significantly on his claims that NSA's information (whether in raw data form or as intelligence reports) is not shared widely in the government. Maybe it's true.

But ultimately we have one way of testing such claims: in the courts. And if even defendants are never given an opportunity to challenge not just the constitutionality of the programs themselves, but also potentially dubious claims made to justify the surveillance, all the so-called transparency from those already caught in lies is of limited use.

SHUT DOWN CYBERCOMMAND — US CYBERCOMMANDER KEITH ALEXANDER DOESN'T THINK IT'S IMPORTANT

Back on March 12 — in the same hearing where he lied to Ron Wyden about whether the intelligence community collects data on millions of Americans — James Clapper also implied that "cyber" was the biggest threat to the United States.

> So when it comes to the distinct threat areas, our statement this year leads with cyber. And it's hard to overemphasize its significance. Increasingly, state and non-state actors are gaining and using cyber expertise. They apply cyber techniques and capabilities to achieve strategic objectives by gathering sensitive information from public- and private sector entities, controlling the content and flow of information, and challenging perceived adversaries in cyberspace.

That was the big takeaway from Clapper's Worldwide Threat Assessment. Not that he had

lied to Wyden, but that that cyber had become a bigger threat than terrorism.

How strange, then, that the US CyberCommander (and Director of National Security) Keith Alexander mentioned cyber threats just once when he keynoted BlackHat the other day.

> But this information and the way our country has put it together is something that we should also put forward as an example for the rest of the world, because what comes out is we're collecting everything. That is not true. What we're doing is for foreign intelligence purposes to go after counterterrorism, counterproliferation, **cyberattacks**. And it's focused. [my emphasis]

That was it.

The sole mention of the threat his boss had suggested was the biggest threat to the US less than 5 months earlier. "Counterterrorism, counterproliferation, cyberattacks. and it's focused."

The sole mention of the threat that his audience of computer security professionals are uniquely qualified to help with.

Compare that to his 27 mentions of "terror" (one — the one with the question mark — may have been a mistranscription):

> terrorists … terrorism … terrorist attacks … counterterrorism … counterterrorism … terrorists … counterterrorism … terrorist organizations … terrorist activities … terrorist … terrorist activities … counterterrorism nexus … terrorist actor … terrorist? … terrorism … terrorist … terrorists … imminent terrorist attack … terrorist … terrorist-related actor … another terrorist … terrorist-related activities … terrorist activities …

> stopping terrorism … future terrorist attacks … terrorist plots … terrorist associations

That was the speech the US CyberCommander chose to deliver to one of the premiere group of cybersecurity professionals in the world.

Terror terror terror.

> Sitting among you are people who mean us harm

… US CyberCommander Alexander also said.

Apparently, Alexander and Clapper's previous intense focus on stopping hacktavists and cyberattacks and cybertheft and cyber espionage have all been preempted by the necessity of scaring people into accepting the various dragnets that NSA has deployed against Americans.

Which, I guess, shows us the true seriousness of the cyber threat.

To be fair to our CyberCommander, he told a slightly different story back on June 27, when he addressed the Armed Forces Communications and Electronics Association International Cyber Symposium.

Sure, he started by addressing Edwards Snowden's leaks.

But then he talked about a debate he was prepared to have.

> I do think it's important to put that on the table, because as we go into cyber and look at—for cyber in the future, **we've got to have this debate with our country**. How are we going to protect the nation in cyberspace? And I think this is a debate that is going to have all the key elements of the executive branch—that's DHS, FBI, DOD, Cyber Command, NSA and other partners—with our

> allies and with industry. We've got to figure how we're going to work together.

How are we going to protect the nation in cyberspace? he asked a bunch of Military Intelligence Industrial Complex types.

At his cyber speech, Alexander also described his plan to build, train, and field one-third of the force by September 30 — something you might think he would have mentioned at BlackHat.

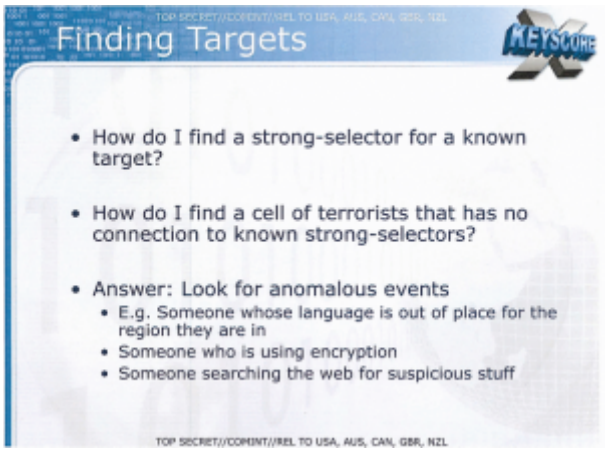
Not a hint of that.

Our US CyberCommander said — to a bunch of industry types — that we need to have a debate about how to protect the nation in cyberspace.

But then, a month later, with the group who are probably most fit to debate him on precisely those issues, he was all but silent.

Just terror terror terror.

ON SAME DAY ALEXANDER TELLS BLACKHAT, "THEIR INTENT IS TO FIND THE TERRORIST THAT WALKS AMONG US," WE SEE NSA CONSIDERS ENCRYPTION EVIDENCE OF TERRORISM



Thirty minutes into his speech at BlackHat yesterday, Keith Alexander said,

> Remember: their intent is not to go after our communications. Their intent is to find the terrorist walks among us.

He said that to a room full of computer security experts, the group of Americans probably most likely to encrypt their communications, even hiding their location data.

At about the same time Alexander made that claim, the Guardian posted the full slide deck from the XKeyscore program it reported yesterday.

> How do I find a cell of terrorists that has no connection to known strong-selectors?
>
> Answer: Look for anomalous events

Among other things, the slide considers this an anomalous event indicating a potential cell of terrorists:

- Someone who is using encryption

Meanwhile, note something else about Alexander's speech.

13:42 into his speech, Alexander admits the Section 702 collection (this is true of XKeyscore too — but not the Section 215 dragnet,

except in its use on Iran) also supports counter-proliferation and cybersecurity.

That is the sole mention in the entire speech of anything besides terrorism. The rest of it focused exclusively on terror terror terror.

Except, of course, yesterday it became clear that the NSA considers encryption evidence of terrorism.

Increasingly, this infrastructure is focused intensively on cybersecurity, not terrorism. That's logical; after all, that's where the US is under increasing attack (in part in retaliation for attacks we've launched on others). But it's high time the government stopped screaming terrorism to justify programs that increasing serve a cybersecurity purpose. Especially when addressing a convention full of computer security experts.

But maybe Alexander implicitly admits that. At 47:12, Alexander explains that the government needs to keep all this classified because (as he points into his audience),

> Sitting among you are people who mean us harm.

(Note after 52:00 a heckler notes the government might consider BlackHat organizer Trey Ford a terrorist, which Alexander brushes off with a joke.)

It's at that level, where the government considers legal hacker behavior evidence of terrorism, that all reassurances start to break down.

Update: fixed XKeystroke for XKeyscore—thanks to Myndrage. Also, Marc Ambinder reported on it in his book.

Update: NSA has now posted its transcript of Alexander's speech. It is 12 pages long; in that he mentioned "terror" 27 times. He mentions "cyber" just once.

MIT RELEASES ITS OWN SWARTZ INVESTIGATION AFTER STALLING RELEASE OF SECRET SERVICE'S

MIT has just released its report on the university's role in the investigation into Aaron Swartz.

Part of it explains how the Secret Service came to be involved in the investigation.

> The MIT Police decided that the situation required expertise in computer crime and forensics, which they did not have. They therefore telephoned the Cambridge Police Department detective who is their normal contact for assistance with computer-related crime activity.19 The Cambridge detective they contacted was a member of the New England Electronic Crimes Task Force.20 When he received the call for assistance from the MIT Police, the detective was working at the Task Force field office in a federal building in Boston, together with other law enforcement officers whose agencies participate in the Task Force. He responded to the call, accompanied by two other Task Force members: a special agent21 of the U.S. Secret Service; and a detective from the Boston Police Department. They arrived at the Building 16 closet around 11:00 a.m.
>
> We note that no one from MIT called the Secret Service. The MIT Police contacted the Cambridge detective by calling him on his individual cell phone. The

> special agent became involved because he accompanied the Cambridge detective. As a Task Force member, the detective would sometimes respond to calls alone, and sometimes respond in the company of other members of the Task Force. The MIT Police were aware that other members of the Task Force might accompany the detective, and that Task Force members included Secret Service agents.
>
> [snip]
>
> During the morning's activities in the basement closet, the special agent had asked for whatever electronic records MIT might have on the matter. As it is IS&T's protocol to obtain approval from MIT's Office of the General Counsel (OGC) before releasing information or materials to outside law enforcement agencies, IS&T contacted the OGC, which responded that it was appropriate to comply with the agent's request in view of the fact that law enforcement was conducting an investigation into what was potentially ongoing criminal activity of unknown scope, and it did not appear to OGC that such information would disclose personally identifiable information.

The report also provides this far less convincing description of how an MIT cop just happened to see Swartz close to his home and the Secret Service Agent just happened to be present at the time.

> At approximately 2:00 p.m. an MIT Police officer was driving to the Stata garage after his shift in an unmarked police cruiser. He was familiar with the investigation and had been informed by radio that the laptop had been removed from the basement closet. He had seen the January 4 video of the suspect, as well as stills made from the video, and

> he had a still with him in his cruiser. On Vassar Street, near Massachusetts Avenue, he saw a cyclist pass him heading in the opposite direction. Based upon the stills and video, and given the backpack and clothes the cyclist was wearing, the officer observed that the cyclist matched the description of the suspect from the basement closet. He made a U-turn to follow the cyclist, who turned onto Massachusetts Avenue and proceeded north towards Harvard Square. When the officer reached the cyclist and pulled alongside, he rechecked the still photos that he had in his car and concluded that the cyclist was in fact the person in the photos. He immediately called his department for backup. A second MIT Police officer, accompanied by the special agent, responded by car from the MIT Police station.

This may well be how the federal investigation into Aaron Swartz started and how it happened that the Secret Service immediately took the lead.

But I do find the timing of MIT's report release rather interesting. After all, just 12 days ago, they successfully moved to prevent the imminent disclosure of the Secret Service's own reports on the investigation to Wired's Kevin Poulsen.

STUDY SHOWS CYBERTHEFT REALLY ISN'T THE GREATEST TRANSFER OF WEALTH

IN HISTORY

I've long mocked the claim — often wielded by people like Sheldon Whitehouse and Keith Alexander — that cybertheft is the greatest transfer of wealth in history. Sure, cybertheft might be big. But bigger than colonization? Bigger than slavery?

But a new study shows that it is just a fraction of what cyber-boosters have been claiming: $25 to $100 billion rather than a $1 trillion.

The study does still show it is costly — leading to the lost of 508,000 jobs a year. And the study didn't account for something else I often harp on: the unknown role of Chinese hacking into weapons programs in degrading the effectiveness of those programs.

> Still unknown, for example, are the unseen costs of military cybertheft, said Mr. Lewis. "A lot of the cost overruns in some of our big programs are because they had to rewrite the code after the Chinese got in—and the real damage won't appear until we see how weapons actually perform," he said.

The study also did not calculate the effect of cybertheft on American competitiveness, which seems like a significant issue.

Ultimately, though, this is a problem that should be fought without the bluster. It is real. It is a threat, in large part, to private companies that don't pay their fair share in taxes. How we combat that problem should account for those factors.

NSA’S PRISM AND THE ODDITY OF PALTALK

Remember this presentation slide on PRISM from last month’s blockbuster report by the Guardian-UK?

Remember the one outlier right smack in the middle of the slide – the company name most folks don’t recognize?

PalTalk.

Very few news outlets tackled PalTalk, explaining what the business is and asking why it was included in the program. There was little more than cursory digging; Foreign Policy looked into PalTalk’s background, while PCMag merely asked in a snarky piece why PalTalk instead of a myriad of other larger alternative social media platforms.

It’s still a good question, but the answer might be right in front of us with a little more analysis.

PalTalk is an “online video chat community,” according to its own description. This means it is in the same competitive space as AOL and Skype, as well as Microsoft’s Hotmail IM and Yahoo Messenger.

The slide we’ve seen doesn’t tell us if access to AOL, Microsoft, and Yahoo was limited to email only, however. We can’t be certain PRISM and the other programs referenced in this particular NSA presentation weren’t also permitted access to live chat environments hosted by these companies. Foreign Policy sidled up to the issue, mentioning Yahoo as well as PalTalk, but didn’t follow through. It’s been relatively easy to see how interest veered away from this question; many news outlets focused on email metadata, not chat.

Squirrel away the unasked, unanswered question(s) about chat someplace for future reference.

With regard to PalTalk, Foreign Policy noted the organization was singular among the companies cited in the NSA slide as it was not a Silicon Valley firm. PalTalk is based in New York. The line of inquiry here went no further.

Hello, New York? This small business is co-located in an AT&T facility in Manhattan, and in New Jersey according the firm's CEO and founder Jeffrey Katz in a Forbes article dd. 2003 to which FP linked:

> "…He rents space in two AT&T data centers, one in Manhattan, another in Secaucus, N.J., with $700,000 worth of computer equipment, including 80 lower-end servers from Dell Computer and five IBM Unix servers. …"

This should raise numerous questions at this point. Manhattan must be an extremely expensive place to run a data center, cheek-and-jowl with financial traffic demanding extremely high uptime. Because of the frequency with which New York was mentioned in published content about PalTalk, the New Jersey location is likely a redundant facility for the purposes of business continuity if the main facility is disrupted.

You'll recall the last major disruptions to data traffic out of New York were due to Hurricane Sandy and 9/11.

Why would a tiny online video chat community need a data center likely to have world-class uptime and redundancy of a nature a company might need only twice a decade?

Another surprising matter is Foreign Policy's reference to earlier articles about Paltalk, while missing this key tidbit to which it linked from that same Forbes article:

> " A less savory crowd naturally migrates to such services. Katz reckons that about 5% of his traffic comes from folks using PalTalk to engage in a video-enhanced version of phone sex. But he

> prefers to talk about wholesome users, like Dennis Hill, a Marine at sea who uses his ship's Internet connection and PalTalk to reach his dad in Indiana. **Or Reza Pahlavi, son of the late shah of Iran, who last year addressed 700 PalTalk subscribers in an online video forum.** "We had people from all over the world," Katz marvels. "What other medium could do this?" …"

Of course the NSA might have some interest in a chat community where many Iranians congregate, especially Pahlavi loyalists.

Which brings us to a question which has been asked in a few different forms: What is it the domestic spying program really looking for in all the data from PalTalk along with the other Silicon Valley tech firms?

Whatever it is, it wasn't information to put the U.S. ahead of the curve on Arab Spring in Libya, Egypt, or now in Syria. PalTalk access was acquired in 2009; last year, British news outlets reported Al-Qaeda supporters used PalTalk as a venue for planning a bombing scheduled to detonate around Christmas Eve 2010. In spite of likely monitoring of PalTalk after the bomb plot was foiled, U.S. response to Arab Spring and Syria appears to have been rather reactive, not proactive.

An interesting facet of the reporting on the December 2010 UK bomb plot was the images of the suspects used in the reporting. Were some of these mug shots actually low resolution snaps from PalTalk video? Even if this isn't the case, is it PalTalk's video component which is most valuable to the NSA? The Telegraph-UK noted in 2010 that PalTalk was the largest online video chat service at that time, offering the ability to participate in multiple chats simultaneously. Was the network of contacts participating in multiple video chats what made PalTalk access critical to PRISM?

Perhaps there’s yet more revelatory information in all the content written to date about PalTalk. It’s worth another look. In the meantime the question remains: why PalTalk?

THE SHELL GAME: WHAT IS MICROSOFT DOING?

What is this so-called tech company doing?

Microsoft sees itself as going head-to-head with Apple and Google. The 10-year chart above comparing Microsoft, Apple, and Google stock tells us this has been a delusional perception.

It also sees itself in competition with IBM. Yet IBM surpassed it in market value two years ago, even after nearly a decade of ubiquity across personal computers in the U.S. and in much of the world. (IBM is included in that chart above, too.)

One might expect a sea change to improve performance, but is the shell game shuffling of Microsoft executives really designed to deliver results to the bottom line?

Tech and business sector folks are asking as well what is going on in Redmond; even the executive assignments seemed off-kilter. One keen analysis by former Microsoft employee Ben Thompson picked apart the company’s reorganization announcement last Thursday — coincidentally the same day the Guardian published a report that Microsoft had “collaborated closely” with the National Security Agency — noting that the restructuring doesn’t make sense.

The new organization pulls everything related to Windows 8 under a single leader, from desktop to mobile devices using the same operating system, migrating to a functional structure from a

divisional structure. There are several flaws in this strategy Thompson notes, but a key problem is accountability.

To tech industry analysts, the new functional structure makes it difficult to follow a trail of failure in design and implementation for any single product under this functional umbrella.

To business analysts, the lack of accountability means outcomes of successful products hide failed products under the functional umbrella, diluting overall traceability of financial performance.

But something altogether different might be happening beneath the umbrella of Windows 8.

There’s only one product now, regardless of device – one ring to rule them all. It’s reasonable to expect that every single desktop, netbook, tablet, cellphone running on Windows 8 will now substantially be the same software.

Which means going forward there’s only one application they need to allow the NSA to access for a multitude of devices.

We’ve already learned from a Microsoft spokesman that the company informs the NSA about bugs or holes in its applications BEFORE it notifies the public.

It’s been reported for years about numerous backdoors and holes built intentionally and unintentionally into Microsoft’s operating systems, from Windows 98 forward, used by the NSA and other law enforcement entities.

Now Skype has likewise been compromised after Microsoft’s acquisition of the communications application and infrastructure for the purposes of gathering content and eavesdropping by the NSA, included in the PRISM program.

Given these backdoors, holes, and bugs, Microsoft’s Patch Tuesday – in addition to its product registration methodology requiring online validation of equipment – certainly look very different when one considers each

opportunity Microsoft uses to reach out and touch business and private computers for security enhancements and product key validations.

Why shouldn't anyone believe that the true purpose of Microsoft's reorganization is to serve the NSA's needs?

Tech magazine The Verge noted with the promotion of Terry Myerson to lead Windows – it's said Myerson "crumples under the spotlight and is ungenerous with the press" – Microsoft doesn't appear eager to answer questions about Windows.

As ComputerworldUK's Glyn Moody asked with regard to collaboration with the NSA, "How can any company ever trust Microsoft again?"

If a company can't trust them, why should the public?

The capper, existing outside Microsoft's Windows 8 product: Xbox One's Kinect feature is always on, in order to sense possible commands in the area where Kinect is installed.

ACLU's senior policy analyst Chris Sogohian tweeted last Thursday, "… who in their right mind would trust an always-on Microsoft-controlled Xbox camera in their living room?"

One might wonder how often the question of trust will be raised before serious change is made with regard to Microsoft's relationship with the NSA. With political strategist Mark Penn handling marketing for the corporation and Steve Ballmer still at the helm as CEO, don't hold your breath.