

# RSA® Conference 2015

San Francisco | April 20-24 | Moscone Center

SESSION ID: MASH-F01

## Cyber Security & Aviation

### **Lawrence D. Dietz, Esq.**

General Counsel & Managing Director Information Security

TAL Global Corporation  
@TALGlobalCorp

### **Erroll G. Southers, DPPD**

Managing Director, Counter-Terrorism & Infrastructure Protection

TAL Global Corporation  
@TALGlobalCorp

# CHANGE

Challenge today's security thinking



# “The Economic Impacts of a Terrorist Attack on the U.S. Commercial Aviation System”

## October 2005

### 7-Day Shut-Down:

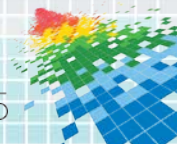
- ◆ \$13.5 - \$21.3 Billion

### Two-Year Projection:

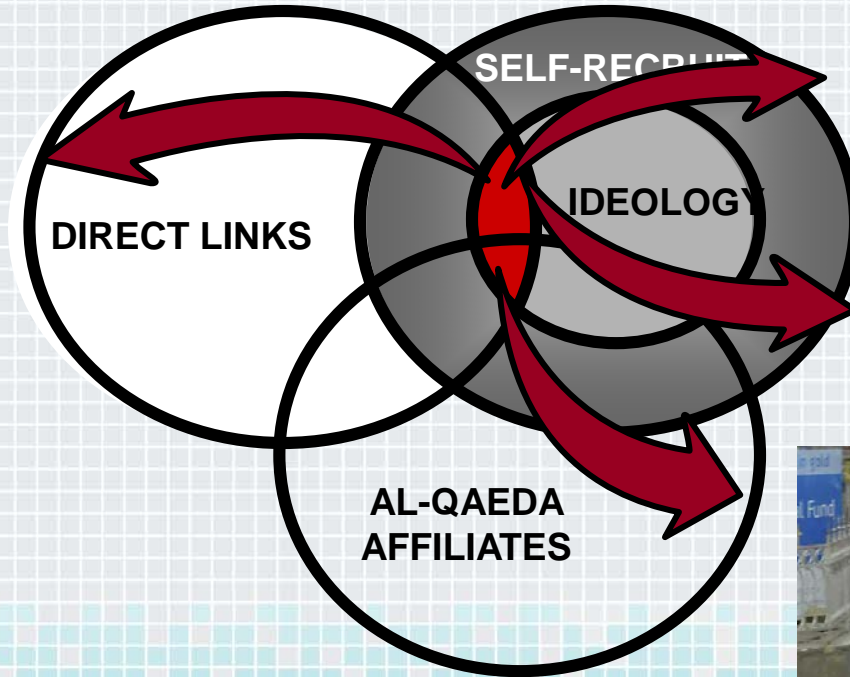
- ◆ \$249 - \$394 Billion

### Direct Costs:

- ◆ \$27 Billion



# Emerging Threats



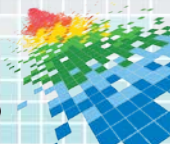
# Chemical Attack Path Evolution



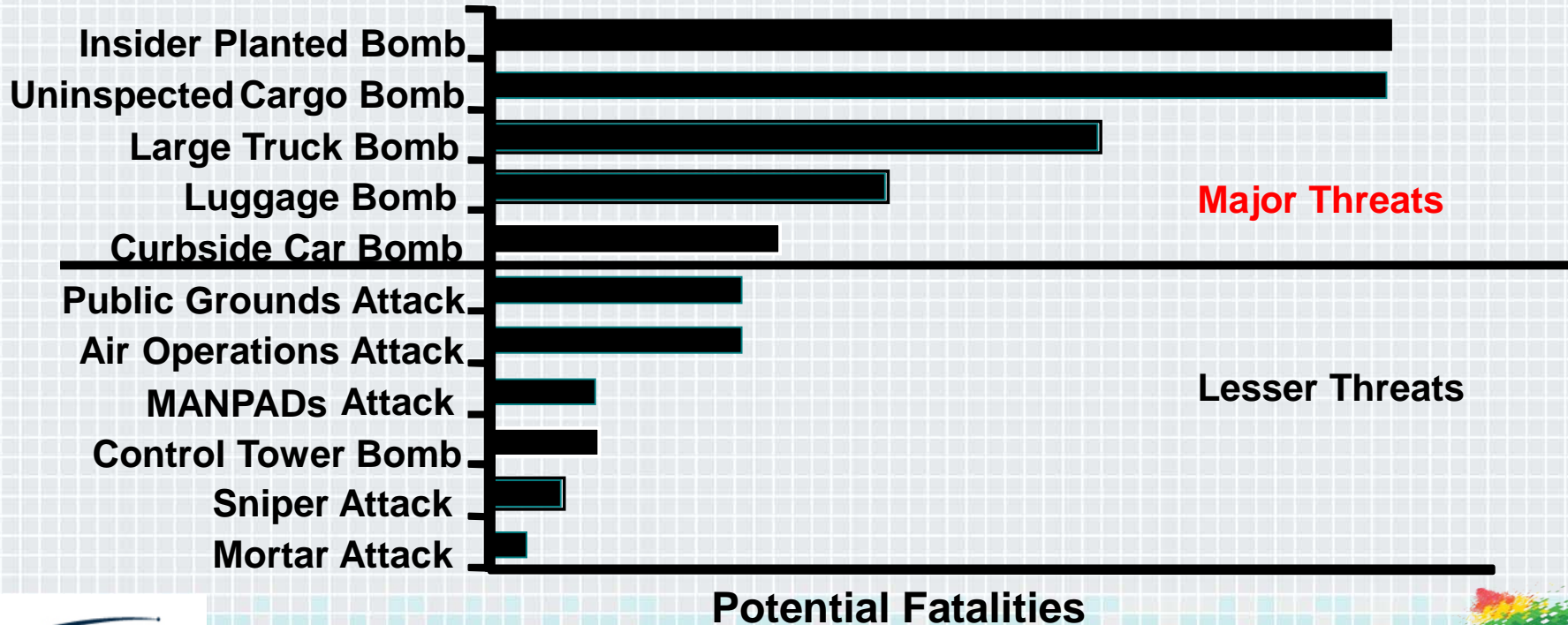
1994

2001

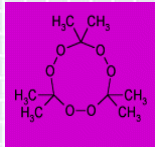
2009



# Aviation Terrorist Scenarios (RAND)



# “Operation Hemorrhage”



TATP



# “Destroying the target is not necessary!”



Bryant Neal Vinas

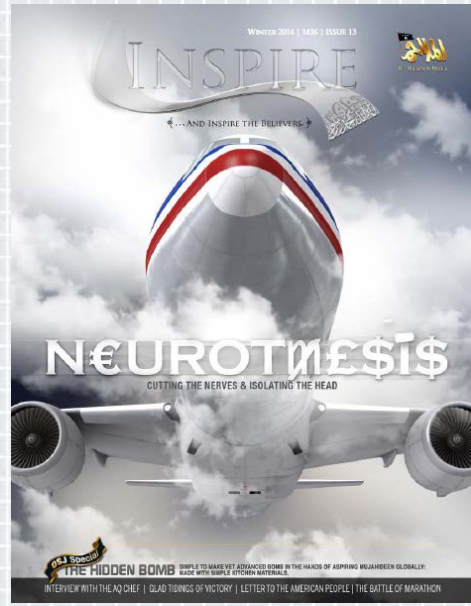


Faisal Shahzad



# Jihad

**OS Special**  
**OPEN SOURCE JIHAD**  
 FROM AQ'S KITCHEN: THE HIDDEN BOMB  
 1. BREACHING AIRPORT SECURITY  
 2. MAKING THE HIDDEN BOMB  
 3. FIELD TACTICS



@heartheworld

A collection of quotes from friend and foe



**MAJOR NIDAL HASSAN, Soldier of Allah - Fort Hood Shooter** (Court Sabre):  
 I am the Shooter.... The evidence will show I was on the wrong side. The evidence will also show that I then switched sides. The evidence will show we Mujahideen are imperfect soldiers trying to establish a perfect religion in the Land of the Supreme God.



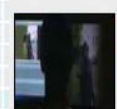
**ROBERT MUELLER, Former FBI Director** (AP):  
 Lone wolf or solo terrorists are much more difficult for us to identify and to disrupt for an attack to take place. It's hard to quantify (the threat) because you have one metric and that is preventing all attacks. If there's one attack, you're unsuccessful... It (Fort Hood shooting) is part of a pattern we've seen recently but a pattern that probably will be replicated in the future. The existence of "lone wolves" is why telephone and Internet surveillance programmes are "tremendously important."



**BARACK OBAMA, US President** (CNN):  
 Across the political spectrum, Americans recognize that we had to adapt to a world in which a bomb could be built in a basement. (In a recent speech of his justifying NSA's mass surveillance.)



**DR. CORNEL WEST, American Philosopher & Civil Rights Activist** (Associated Press):  
 I think we have to acknowledge that President Obama has very little moral authority at this point, because we know anybody who tries to rationalize the killing of innocent people, a criminal - George Zimmerman is a criminal - but President Obama is a global George Zimmerman (pointing to Obama's attempt to rationalize the killing of innocent children in U.S. drone strikes).



**JEREMIAH ADEBOLA, Teacher of the Woolwich Mujahid** (Qigeesa International):  
 People may say, "Well, he (Woolwich Mujahid) is a violent individual, and he proved that on the day of Woolwich." But I would say, "Was Lee Rigby a violent individual? Are other British soldiers, who go to Afghanistan and Iraq and kill, violent individuals?"

@heartheworld

A collection of quotes from friend and foe



**ADAM GADANI, Al-Qaeda Mujahid** (Je Sais Mésic):  
 Stand, revenge on America the enemy of Islam and Muslims. Remind us of the glories of Khatmül, Dar-es-salam, Aden, New York, Washington, Fort Hood, Benghazi and Boston. Defend your religion, Ummah and honors from America and the crusades, by hitting their interests in our countries and theirs. The war with the crusades and Jews is global, it does not acknowledge boundaries and there are no restrictions except those brought by the just Sharf'ah or those advantageous to Islam and Muslims as seen by the trusted Ummah scholars and Mujahideen leaders.



**MUSTAFA QADRI, Amnesty International, Researcher** (France 24):  
 We're really concerned about the US drone program, because it claims it can use them anywhere in the world because it has a global war against Al-Qaeda and its allies. But we have to take the US on its word, because it has provided us with no information. This is a secret program. In fact, in our case we've found at least in some cases they're clearly killing civilians, and some of these cases might be war-crimes.



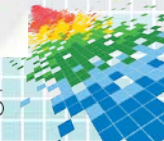
**REP. TOM COTTON, Former Soldier in Iraq and Afghanistan** (American Enterprise Institute):  
 The president likes to say that Al-Qaeda is on the run, maybe so. But only in one regard. As for many have learned the basic infantry doctrine, the Infantry is on offense when it is moving, and is in defense when it is not moving. Al-Qaeda is only on the run in the sense that Al-Qaeda is on the offense around the world.



**ERROLL G. SOUTHERS, Expert on Counter-Terror** (Interview with Hersh):  
 Homegrown actors can successfully attack a U.S. target with little or no resources. We have always known this was a possibility, but Boston reminded us of the adaptive nature of the threat we face. The Iraqis came to attack a marathon - a particularly difficult target to secure. This speaks to the issue of soft targets and their relative vulnerability, and the fact that violent actors seek out public gatherings that, by their nature, cannot be made totally secure.



**SUHEIB AMIN, Former Brooklyn College Student** (Qigeesa America):  
 I remember we had, you know, a political discussion in class that I really didn't want to get involved in. I remember I had one professor that said that if he was in Iraq, he'd probably be on the other side. And I remember I was just looking at him thinking "I'll be in jail if I thought (off) that."







**Junaid Hussain** @AllahuAhkbar911 3h  
 @FOXNEWS WE HAVE PLANTED EXPLOSIVES ON DELTA FLIGHT #1061 FROM LA TO ORLANDO, WE ARE ISIS, WE ARE HERE, YOU WONT BE

**Junaid Hussain** @AllahuAhkbar... 3h  
 @DeltaAssist @do2 WE PLANTED EXPLOSIVES ON BOARD FLIGHT #1061 HEADING TO ORLANDO OUR SOLDIERS WAITING FOR SIGNAL

**COMMANDER DATA** @SETHDSTEWART  
 @DELTAASSIST HEY DELTA, I JUST PUTTED A BOMB INSIDE 4 PLANES DELTA FLIGHT 4459, DELTA FLIGHT 5811, DELTA FLIGHT 1880, DELTA FLIGHT 2566.

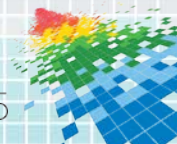
**COMMANDER DATA** @SETHDSTEWART  
 @AMERICANAIR AMERICAN AIRLINES FLIGHT 197 HAS A BOMB INSIDE AND IT'S GOING TO EXPLODE IN 50 MINUTES.

**COMMANDER DATA** @SETHDSTEWART  
 @SOUTHWESTAIR SOUTHWEST AIRLINES FLIGHT 306 HAS A BOMB INSIDE AND IT'S GOING TO EXPLODE. IF IT DOESN'T EXPLODE. I WILL PUT DYNAMITE.



# Physical World Conclusions

- Aviation is a visible, vulnerable and attractive target.
- The enemy is resilient and adaptive.
- Today's attack vectors may not be tomorrow's attack vectors.
- Attacks can be sophisticated and coordinated or they can be lone wolf efforts.
- Attackers many not fit the 'traditional' picture.

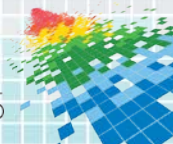


# The Clausewitz Trilogy



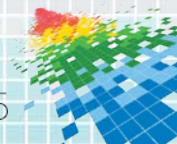
## Ends – What you want to accomplish.

- ◆ Casualties & Property Damage
- ◆ Media & Propaganda Exploitation
- ◆ Psychological Impact
- ◆ Economic Impact



# Means – Resources/Vectors

- ◆ People
- ◆ Aircraft
- ◆ Luggage
- ◆ Cargo
- ◆ ???????



# Ways – Tactics - Aircraft

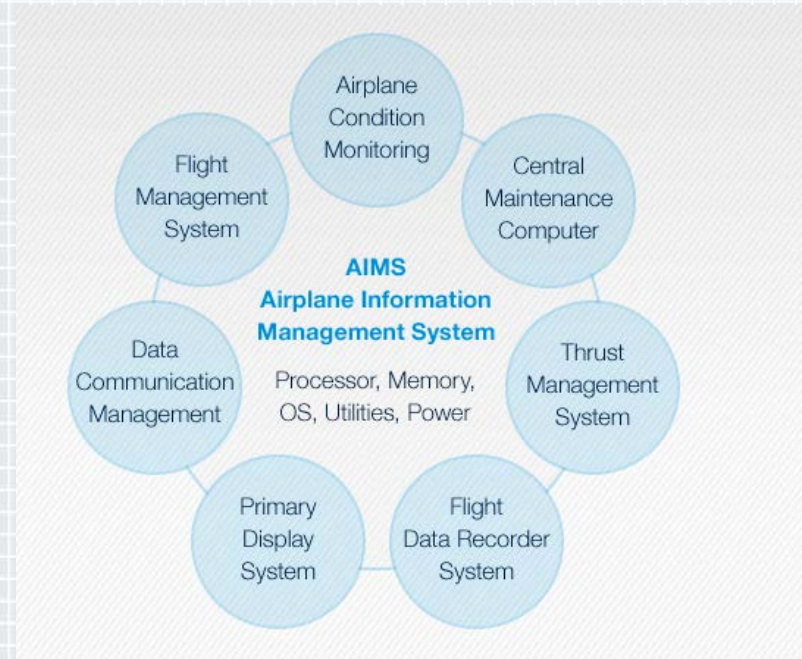
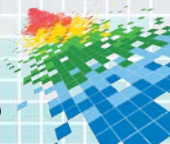


Photo Source: Boeing Aircraft Company; [www.newairplane.com](http://www.newairplane.com)



# Ways – Airports & Cargo

- ◆ Airport Operations
  - ◆ Airport Operational Management
  - ◆ Departure Control Systems
  - ◆ Cargo Terminal Operations
  - ◆ Passenger Communications
  - ◆ Mobile Aps
- ◆ Cargo Terminal Operations
  - ◆ Unit Load Device (ULD) Management
  - ◆ Warehouse Management
  - ◆ Outbound/Export Operations
  - ◆ Bar Code Scanning
  - ◆ Service Level Agreement Management



# Cyber Elements

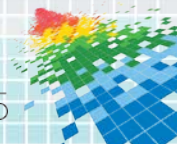
- ◆ Reservation Systems
- ◆ Flight Management Systems
- ◆ Access Control Systems (Badges)
- ◆ Flight Traffic Management
- ◆ Departure Control Systems
- ◆ Passport Control Systems
- ◆ Hazardous Materials Transportation Management
- ◆ Cargo Handling & Shipping
- ◆ Computers on the Aircraft
  - ◆ Flight Control Systems
  - ◆ GPS
  - ◆ Fuel gauges; fuel consumption
  - ◆ Maintenance Computer





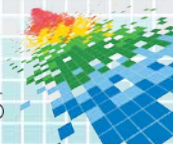
# Lessons For Other Industries

- ◆ Cyber attacks have downstream effects.
- ◆ Focus is on:
  - Harming People
  - Dramatic visual property damage.
- ◆ Secondary effects are likely to be emotional and economic.



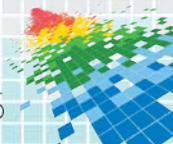
# Cyber Security Implications

- ◆ Networks are good means to achieve desired ends.
- ◆ Critical cyber vulnerabilities are:
  - Access Control
  - Control of Potential Kinetic Weapons (IOT)
- ◆ Need to secure unintended use and corruption of technology
  - Driverless Cars
  - Conveyer Systems



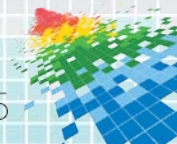
# Apply What You Have Learned Today

- ◆ Next week you should:
  - ◆ Identify critical ecosystems that serve your organization
- ◆ In the first three months following this presentation you should:
  - ◆ Understand the cyber vulnerabilities of these ecosystems
  - ◆ Define appropriate measures to reduce/mitigate these vulnerabilities
- ◆ Within six months you should:
  - ◆ Develop and implement policies and contractual modifications for the identified ecosystems to hold ancillary vendors to higher, stated security standards..



# Key Takeaways

- ◆ Tomorrow's threats will not be like today's.
- ◆ Don't underestimate your enemies.
- ◆ Think like an attacker, not a defender.
- ◆ Hold your suppliers and partners accountable to the same or a greater level of security than you have.
- ◆ Consider the psychological impact as well as actual damage.



# Thank You!

- ◆ [ldietz@talglobal.net](mailto:ldietz@talglobal.net)
- ◆ [esouthers@talglobal.net](mailto:esouthers@talglobal.net)

