



(b) (6), (b) (7)(C) **Director, Counterintelligence**  
(b) (6), (b) (7)(C)

**No Active Alerts**

**TYPES OF ADVISORIES**

**Bulletin**

Describes current developments or general trends regarding threats of terrorism.

**Elevated Alert**

Warns of a credible terrorism threat against the United States.

**Imminent Alert**

Warns of a credible, specific and impending terrorism threat against the United States.

**NASA CI/CT MONTHLY NEWS UPDATE – January 2016**

*This monthly newsletter is published to increase NASA personnel awareness of significant current issues related to counterintelligence, counterterrorism, and counterintelligence cyber matters. To learn more about CI/CT awareness, or to schedule a CI/CT presentation, please contact the CI POC located on the last page.*

**Significant Counterterrorism (CT) Issues:**

**STUDY: UNPRECEDENTED SUPPORT FOR ISIS IN THE U.S.**

Support for ISIS in America has reached an unprecedented level with several thousand U.S.-based sympathizers and more terrorism-related arrests in 2015 than any year since 9/11.

<http://www.cnn.com/2015/12/01/politics/isis-in-united-states-research/index.html>



**THE ISIS TRAIL OF DEATH**



Since October 10<sup>th</sup> 2015, ISIS and its sympathizers around the world have killed at least 525 people in six attacks in six countries outside its so-called caliphate. American CT officials say that of the six attacks, three were directed by ISIS from its territory in Syria/Iraq and another two were so-called "announcement" attacks — local ISIS elements revealing their existence in dramatic fashion.

<http://www.nbcnews.com/storyline/isis-terror/isis-trail-death-n475861>

**Significant Counterintelligence Issues:**

**PUTIN SALUTES RUSSIA'S INTELLIGENCE AGENCIES ON 'SPIES' DAY'**

Vladimir Putin has honored members and veterans of the Russian security services on their annual professional holiday – which marks the day that the dreaded Cheka secret police was formed in 1917. He said Russian security agencies had exposed 320 foreign spies in 2015 and prevented “more than 30 crimes of a terrorist nature”.



<http://www.theguardian.com/world/2015/dec/20/putin-salutes-russias-intelligence-agencies-on-national-spies-day>

**ECONOMIC ESPIONAGE: THE GLOBAL WORKFORCE & THE INSIDER THREAT**



Today's CEOs, be they from large multinational enterprises or smaller shops, need to think about the effects economic espionage may have on their companies. Their own intellectual property, trade secrets and personnel are all of interest to others. In addition, data provided to and received from customers, clients and employees may prove to be the most sensitive.

<https://securityintelligence.com/economic-espionage-the-perfect-storm/>



## **Significant Cyber Issues:**

### **CYBER ESPIONAGE IS REACHING CRISIS LEVELS**

Cyber espionage has reached crisis levels. One study puts the cost of cybercrime at \$24 billion to \$120 billion in the U.S. and up to \$1 trillion globally. For modern corporations, the cross-border aspects of cyber espionage can cause significant challenges.

<http://fortune.com/2015/12/12/cybersecurity-amsc-cyber-espionage/>



### **OUR BEST FRENEMY**



When it comes to global cyber threats, you could say there's the whole rest of the world, and then there's China. The victims of Chinese hacking cover every sector of the U.S. economy, from banks and tech firms to energy giants and government agencies.

<http://www.politico.com/agenda/story/2015/12/china-us-cyber-attack-hacks-000332>

### **Analyst Notes – Items to Watch:**

The multiple attacks outside of the Middle East (The Russian airliner crash and the gun/grenade attacks in Paris/San Bernardino) have shown that ISIS is morphing from a serious problem in the Middle East to being a worldwide terrorism threat. In addition, attacks in Mali, Yemen and Libya are showing the resilience of Al Qaeda and its affiliates. With the success of the ISIS attack in California and the multiple threats issued by ISIS, it is obvious that the threat to the United States is rising. The number of ISIS plots in the United States is at an all-time high and both the FBI and DHS expect more “lone wolf” type attacks to be forthcoming. Russia and China continue their conventional espionage efforts and cyber-attacks against the United States and other Western nations. This effort at “Nation State Theft” is in spite of public agreements and signed treaties. Economic espionage and insider threats within the United States continue to cost this nation billions in profits as well as significant sensitive technology losses. The NASA CI/CT division continues to monitor these threats and any others that have the potential to harm NASA or its equities.

### **NASA CI Offices:**

- Ames Research Center: (b) (6), (b) (7)(C)
- Armstrong Flight Research Center: (b) (6), (b) (7)(C)
- Glenn Research Center: (b) (6), (b) (7)(C)
- Goddard Space Flight Center: (b) (6), (b) (7)(C)
- Jet Propulsion Laboratory: (b) (6), (b) (7)(C)
- Johnson Space Center: (b) (6), (b) (7)(C)
- Kennedy Space Center: (b) (6), (b) (7)(C)
- Langley Research Center: (b) (6), (b) (7)(C)
- Marshall Space Flight Center: (b) (6), (b) (7)(C)
- NASA Headquarters: (b) (6), (b) (7)(C)
- Stennis Space Center: (b) (6), (b) (7)(C)