Global and Modern Terrorism/Cyber Terrorism

February 9, 2016 By Pierluigi Paganini

In the following brief I will describe kinetic plot based modern terrorism/Cyber-terrorism and religious affiliations.□

Both Jihadist and Non-Jihadist, organized crime associations, data and statistics to show that Radical Muslim Terrorism is the most prominent form in America today.

Modern terrorism and cyberterrorism display the use of violence and threats to intimidate or coerce, normally for political purposes. The state of fear and submission produced by terrorism is known as terrorization. Both are found underlying in espionage, targeted penetrated breaches and kinetic plots. I will outline and compare the plots based on past history.

A brief history according to James Clapper, Director of National Intelligence; in 2011 alone there were over 13,000 reported attacks. This is a 45-year people arrested in 43 plots.

From January 2015 to December of 2015 there were 23 plots of Cyber Terrorism reported and 43 people arrested in 189 plots of terrorism with 454 arrests. Out of 44 plots like Boston, where a kinetic plot was tried and successful; Salafist plots totaled□ 99%, Non-Jihadist- 3% 14 are Jihadist and led to between 900-1,000 active investigations. Out of 35 plots 70% led to arrest. Out of the targets most are Islamic Driven by Terrorist Radicalization noted by James Comey FBI Director.

Here are some results of terrorism related events following 9/11 and the window of opportunity that it created. There were 288 plots following 9/11 and 170 of those were kinetic plots on the homeland. A whopping 59% of these plots led to arrest.

The Islamic extremists plots equaled 90%, 86 were Jihadist and led to 167 investigations. Out of the 167 investigations 8 were successful plots that reached fruition. Out of the 167 investigated, 78 were interdicted, resulting in 37 murders, and 49 injuries. The Islamic state produced 10-11% splinter groups, 5% women, and 7% bad girls.

In regard to Non-Islamic there were 84 plots resulting in 228 investigations. Out of the 228, 25 kinetic plots on the homeland were successful. There were a total of 59 plots interdicted resulting in 77 deaths and 60 injuries caused by crazy white people.

Official ISIS/ISIL terrorism involved 76 plots from 2014-2016. ISIS produced 60% of these and 18 were on US soil. 26 of these attacks produced violence and 26 were kinetic plots. 14% of total attacks were originating from ISIS. One example is Emanuel Luthchman who tried to capture, bomb, and behead Merchants Grill patrons on New Year's in New York the name of ISIS. In addition, 4 marines were killed in Tennessee by Isis bred Shiite prisoners and 14 were recently slain in the San Bernardino attacks which were insider attacks.

Global Terrorism is on the rise in greater numbers than US soil, 17 were killed in the Paris attack. 21 Coptic Christians were murdered on the Libyan Coast. In Tunisia, 137 were killed in a Yemen Mosque. In Kuwait, 39 French and Tunisians were killed at a beach resort. Another 27 killed in a Shiite Mosques and many others remain unreported.

On US Soil, 4 marines were killed in Tennessee, In Akron, OH Terrence Joseph McNeil plots to kill100 US service Members, a terrorist stabbed 5 in Mencer, CA.

In the Federal Spectrum, Government contracts and private sector breach is on the rise. Economic espionage has increased at an alarming rate from 1945-2010. There were 200 arrest were made, 90 in Washington DC Metro area, 40% New York State. Much of these attacks resulted in economic loss from the Chinese. There were 4 confirmed plots in California in 2015. Internationally there were 3 major plots, resulting in a total of 9 indictments which were focused on technology transfer in Government Trade Secrets focused on Corporate Espionage.

This is becoming more and more of the normal trend, instead of the old fashioned classic terrorism through traditional bombings. This modern day terrorism is focused on intellectual theft, theft of personally identifiable information that could lead to easy coercing and manipulation of the person in control of the property. It is focused on theft of trade secrets from the inside out; corporate cyber espionage.

Insider attack history includes the terrorist attacks on London in 2005 which came from their own British Citizens. The Boston Marathon attack was carried out by US citizens and the Paris attacks by French Citizens.

US Cyber Command Commander Admiral Mike Rogers noted that the breach of 22 million records from OPM was simply a part of China's huge data spying ring from Beijing. The records collected were of those with extensive background checks related to (TSSCI) Top Secret Compartmented Information security clearances. This data will likely lead to identification of spies in China and interruption of their activities.

Big Data Analytics made it possible for large bulk data stolen to be scanned for vital information such as Personally Identifiable Information. PII consists of health, medical, dental, birth, marriage, and or death records leading to next of kin or blood relative threat or coercement.

The pertinent PII; Social Security numbers, mother's maiden name and or health records can be used and tailored for an intelligence perspective and gain pertinent life details about said individuals or for social engineering and manipulation of said data to alter the individual's original identity and recruited as double agent and or dual spy.

In an attempt to protect the persons identified in the breach, OPM has transferred the personal data on cleared individuals to the Pentagon. They will take over the monitoring and background to create a secure environment for future individual data security. The annual fiscal cost is estimated at $600,000.00.

In contrast, (then and now) with the recent cross over to Cyber Espionage and Global Terrorism manifestation in Going Dark. Some other terms are rogue, and under the radar through hidden applications and data. These new tactics are through apps which can be download through various applications to the cell phone which cannot be traced by government authorities. Espionage related actions totaled 781, over a span of 20 years in which 565 or 21% Russian and 155 cases confirmed China Based Espionage with many diverted cases through proxy hopping.

The Government cannot gain access to the encrypted communications in applications such as WhatsApp, Snap Chat, Confide, and Signal, just to name a few. The latest encryption methods disappear in a matter of seconds after the message is displayed preventing duplication of said message.

Some popular platforms are gaming platforms which can be used to send encrypted messages under false names. These are used to send and receive plots and plans for attacks. Some other targets through Cyber espionage and hacking are to gain access to PII, Personally Identifiable Information through social media, Twitter, LinkedIn, Face Book, and Dark Mafia, to gather intelligence and or compromise personal data.

In comparison, modern terrorism and cyber terrorism has manifest itself primarily through Islamic radical terrorism in various forms. It comes in many names and under various headings. The primary target is to kill the infidel: (anyone not bowing to the name of Allah). Often times the youth and the weak are recruited as targets for ISIS and ISIL because of their desire to fit in and a need to be a part of something. They are targeted to convert to Islam and radicalized via the internet.

In summary, Terrorism and modern Cyber Terrorism will not go away. This is history repeating itself. Just as many years ago Protestants fought against Catholics, now Christianity fights Muslim.   In 2014, 2.6% of terrorism victims lived in Western Countries. This is likely to get worse before it gets better. There is not one easy way to combat terrorism as you see it comes in now in your hand-set, head-set, at your finger-tips. Be wise with your choices as it may come knocking at your door.

About the Author Theresa Frush:

Theresa Frush is a former AmeriCorps Vista Fellow who served as a Special Projects Coordinator amongst various federal agencies. Ms. Frush was instrumental in the development and implementation of strategic planning geared towards the partnership building required to coordinate and mitigate the effects of natural *disasters. Ms. Frush specialized in organized disaster planning, roundtable discussions and mock exercises to coordinate the mobilization of volunteers and the appropriate allocation of resources and supplies for special needs groups.*

Ms. Frush was also the co-founder of Chesapeake Youth Summit, whereby she provide training and opportunities for r effective dialogue and civic engagement between government, law enforcement and military agencies aimed at the reduction of recidivism among low income *youth population*

Edited by Pierluigi Paganini

(Security Affairs – Terrorism, cybersecurity)

References:

Bill Gerts 25Jan2016 CyberCom OPM hack highlights China big data spying

Brooks, Rosa 20Nov15 the threat is already inside

David Major, www.Spypedia.com

Share it please ...

SHARE ON

Pierluigi Paganini

Pierluigi Paganini is Chief

Information Security Officer at□ Bit4Id, firm leader in identity□ management, member of the ENISA (European Union Agency for Network and Information Security)Treat Landscape Stakeholder Group, he is also a Security Evangelist, Security Analyst and Freelance Writer. Editor-in-Chief at "Cyber Defense Magazine", Pierluigi is a cyber security expert with over 20 years experience in the field,□ he is Certified Ethical Hacker at□ EC Council in London. The passion for writing and a strong belief that security is founded on sharing and awareness led Pierluigi to find the security blog□ "Security Affairs" recently named a Top National Security Resource for US. Pierluigi is a member of the "The Hacker News" team and he is a writer for some major publications in the field such as Cyber War Zone,□ ICTTF, Infosec Island, Infosec Institute, The Hacker News Magazine and for many other Security magazines. Author of the Books "The Deep Dark Web" and “Digital Virtual Currency and Bitcoin”.

PREVIOUS ARTICLE

CVE-2016-0603 - Oracle Issues out-of-box Java emergency patch for Windows

NEXT ARTICLE

Carbanak cybergang is back and it is not alone

[redacted]

[redacted]

- +Pierluigi Paganini

Pierluigi Paganini is Chief Information

Security Officer at Bit4Id, firm leader in□ identity management, member of the ENISA (European Union Agency for Network and Information Security) Threat Landscape Stakeholder Group, he is also a Security Evangelist, Security Analyst and Freelance Writer. Editor-in-Chief at "Cyber Defense Magazine".

Back to top ^