WHAT WE DO &
WHAT WE NEED……

Presentation by

POLICE

&

LAW ENFORCEMENT AGENCIES

Tasks

- INVESTIGATION/ ENQUIRY
- LAW & ORDER/ VIP SECURITY
- INTELLIGENCE GATHRING

USE OF TECHNOLOGY IS PERTINENT FOR ALL THE TASKS LISTED ABOVE

POLICE AS A GROUP IS A NON-TECHNICAL USER OF TECHNOLOGY- THE BIGGEST BOTTLE-NECK

Tasks :INVESTIGATION/ ENQUIRY

- **Organized criminals of urban/ sub-urban background**
- **Anti-national activities**
- **Narcotics**
- **Illegal weapon**
- **Kidnapping for ransom**
- **Wild life syndicate**
- **Fake Indian Currency Notes (FICN)**
- **Bank/Financial frauds**
- **Cyber crimes**
- **Frauds including internet lottery scams**
- **Dacoits**
- **On going heinous crimes**

Task: LAW & ORDER/ VIP SECURITY

- DAY-TODAY
- SPL OCCASSIONS-festivals, rallies, VIP visits
- FALL OUT OF SITUATIONS

Task: Intelligence gathering

- Ground information
- Tech-int (Technological intelligence)
- Source based

Intelligence

- Intelligence refers to discrete information with some relevance.
- Intelligence Analysis is the processing of raw intelligence into finished intelligence through
  - abstraction,
  - evaluation, and
  - understanding

  of such information for its **accuracy** and **value**.

Actionable intelligence

Actionable intelligence

is

conclusive component

within a larger pool of

the secret, covert or otherwise "intelligence"

Ground information: Collection and Collation

- Identification through
  - Trust worthy informers
  - Election voter list
  - Bills and payments in govt/private/other offices such as telephone/ mobile/ Electricity/ Nagar Nigam
  - Land registration record
  - Vehicle registration record – RTO data
- Movement information through
  - Informers
  - Other relevant sources
- Professional ground information workers

Tech-int-Technological intelligence

- **Electronic Surveillance**
  - CDR/ Log
  - Interception of mobile/ internet
  - Dump data analysis
  - Bank account, ATM, Credit card
  - Movement tracking through usage of banking instrumentsAccount_ststement._628301028330-Complete(1).xlsx ▶
  - Identification through ATM/Credit card usage clippings ▶

Tech-int-Technological intelligence

- **Railway/ Airlines reservation servers**
    - Search based on combination of parameters such as name, age, gender, train number, boarding station, destination and so on ▶
    - Airlines servers
- **Feed from**
    - CC TV data
    - Access control data
    - X-ray scanners

Tech-int-Technological intelligence

- Internet as a source of actionable intelligence may be used for
    - Investigation
        - Retrieving user data
        - Tracking user
        - Collecting digital evidence
    - Keeping oversight
        - Internet patrolling
        - Advanced Electronic Surveillance

Oversight

- There is growing trend of keeping oversight on Target activities on internet through search engines like Google, AltaVista, Yahoo, Wikipedia, and alike
- **Internet patrolling** is the new term coined for this oversight activity
- It is equally important from the point of view of LEAs to have an oversight without involving any of the internet agencies.

STEPS INVOLVED IN INTERNET PATROLLING

1. Identification of sites
2. Identification of transactions
3. Identification of seriousness of transactions
4. Tracking transactions

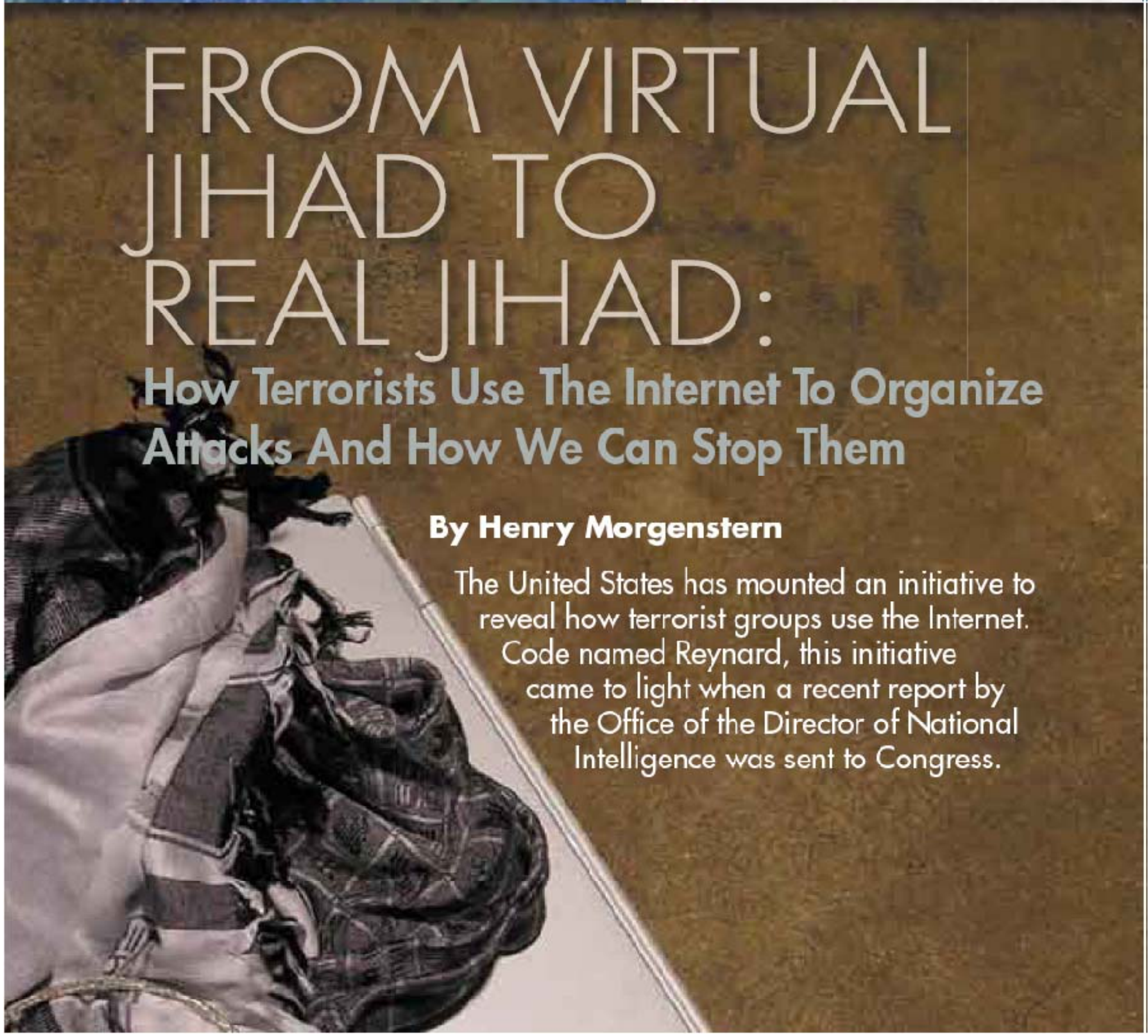
From Virtual Jihad to Real Jihad

New home of

Terror – Internet

authored by

Henry Morgenstern



FROM VIRTUAL JIHAD TO REAL JIHAD:

How Terrorists Use The Internet To Organize Attacks And How We Can Stop Them

By Henry Morgenstern

The United States has mounted an initiative to reveal how terrorist groups use the Internet. Code named Reynard, this initiative came to light when a recent report by the Office of the Director of National Intelligence was sent to Congress.

Going Dark program

- Known as "**Going Dark**, the program is designed to beef up the FBI's already formidable electronic surveillance, intelligence collection and evidence gathering capabilities”

Going Dark program

"seven core capabilities":

- Digital Forensics;
- Electronic Surveillance;
- Physical Surveillance;
- Special Technology and Applications;
- Tactical Communications;
- Tactical Operations and
- Technical Support/Coordination.

WHAT DO WE NEED……

Effective solutions for

- Tracking VOIP calls
- Internet Patrolling
- Data-mining
- GSM/SGSN switches eliciting valuable intelligence
- Identification of suspected mobile user within

  a sector of a cell tower
- Some sort of behavioural capturing of people in queue at scanning points

And so on…….

SUGGESTIONS TO ORGANIZERS

- CII has taken exceptional initiative to bring together the industry, government and the end users
- But some very vital sectors using advanced security systems, have been overlooked such as banking, aviation and transport
- Police/LEA’s should have been given half a session to put forth their view on technology need and their absorption

Thank you……..

Dr. Aravind Chaturvedi
Dy. SP UP STF, Lucknow
+91-9838503310
+91-9454401826
ac@upstf.com

Investigation

- Cases of impersonation, defamation, threat, ransom, anti-national activities etc. on e-mail, instant messaging, social networking sites and so on have risen exponentially
- At the same time, internet provides irrefutable digital evidence to prosecute cases effectively

Investigation

Cases of

- phishing,
- vishing,
- spoofing,
- online banking frauds and
- other fraudulent activities through internet

are traced by tracking IP address of internet connectivity and other digital parameters

Investigation

- The primary task remains to identify the perpetrator. In all such cases, IP address stored in the mail header provides key info
- Further, inbox /outbox / address book , usage details , registration details etc of such suspect is retrieved through the concerned service provider

Investigation

- Sequence of steps involved in tracing perpetrator through internet
  - Mail header
  - ISP tracing national international
  - Connectivity tracing
  - CBI/INTERPOL contact in case of foreign ISP/ telephone connectivity

Investigation

- Further possibilities
  - ATM clipping in case of online banking/credit card etc. frauds

IDENTIFICATION OF SITES

- Match –making sites
- Pornographic sites
- Dating sites
- Social networking sites
- C2C(CUSTOMER TO CUSTOMER) transaction sites such as ebay
- Prior known sites involved in terrorist activities or transactions

IDENTIFICATION OF TRANSACTIONS

- Cost involved in the transaction- usually high value
- Type/mode of transaction- cash involvement is suspicious
- Parties involved- anonymous names may be used
- Past record of the transactions conducted by the involved parties-grey list
- Geographical location of the transaction process

IDENTIFICATION OF THE SERIOUSNESS OF THE TRANSACTIONS

- This can be achieved by having a thorough knowledge of
  - the present & past threats
  - Latest activities carried out by the terrorist organizations
  - Ability & capacity of the terrorist organization in question
  - Technology acquisition of the terrorist organization

TRACKING TRANSACTIONS

- Once the role of the involved parties is ascertained/confirmed, their ID’s have to be established.
- Track the IP & ISP of the people involved in the transaction
- Track their e-mail records
- Track their networking site profiles (to identify their network/a suspect/black listed)
- Track their previous e-transaction records & bank statements to identify the type of amount involved

Internet Patrolling: Terrorist module

- LEA’s may be interested in terrorist’s activities
  - Planning
  - Motivation
  - Action
  - Communication within group
  - Feedback

VoIP

- Voice Over Internet Protocol is communication of voice/text/video over internet similar to that of regular telephone/mobile connection
- It turns out to be very cheap as the actual voice/text/video traffic is carried over Internet more so for those with always-on broadband Internet connections.