CYBER WARFARE

Estonia

- On April 27, 2007, Estonian officials moved a Soviet-era memorial celebrating an unknown Russian who died fighting the Nazis during In anticipation of the move, thousands of ethnically Russian Estonians protested."
- The protests eventually turned violent, and led to rioting, hundreds of arrests, and one death. This event began a series of Distributed Denial-of-Service (DDoS) attacks launched against several Estonian national websites.
- Estonian government websites that would generally receive 1,000 visits a day were receiving 2,000 visits every second, causing the websites to be shut down for several hours at a time.
- The attacks became more sophisticated and persisted for several weeks until NATO and the United States sent security experts to Estonia to investigate and protect the computers from further attack. Estonia initially blamed the Russian government for the attacks; World War II.
- investigations indicate the attacks were not affiliated with the Russian government, but rather the product of "spontaneous anger from a loose federation of separate attackers.

Stuxnet

- On June 1, 2012, officials of President Barack Obama's administration admitted that the computer worm, Stuxnet, was a joint project between the United States and Israel designed to disrupt Iran's nuclear program.
- Stuxnet was designed to suddenly speed up or slow down the spinning of centrifuges used to enrich uranium, causing their parts to break and thereby crippling the entire uranium enrichment operation. Stuxnet was programmed to self-destruct on June 24, 2012

Flame

- On May 28, 2012, the Kaspersky Lab in Moscow announced the discovery of malicious software codenamed Flame.
- The primary function of Flame is to collect information. It steals valuable information from infected computers ranging from, but not limited to, computer display contents, documents, stored files, password information, contact data, audio conversations, and monitoring of Skype.
- Flame, introduced in 2010, is nearly sixty times the average size of other known malicious programs.

- Kaspersky found that most of the infected computers were in the Middle East.
- Iran had the highest number of Flame infections; Israel, the Palestinian territories, Sudan, Syria, and Lebanon also had substantial numbers of infected computers.
- Many commenters suspect that Israel is responsible for the Flame program, and while Israel has not taken responsibility for Flame

- Computer network operations (CNOs) have been defined by the United States Joint Chiefs of Staff as being used to "attack, deceive, degrade, disrupt, deny, exploit, and defend electronic information and infrastructure.
- **Article 2(4)** of the U.N. Charter sets forth the fundamental international law prohibition on the use of force, stating that, "all members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the purposes of the United Nations."

- **U.N. Charter provisions can be applied to cyber attacks**?

- Articles 2(4), 39, 42, and 51 do not list or refer to any specific weapons but the **International Court of Justice** in its advisory opinion on nuclear weapons found that these provisions "**apply to any use of force, regardless of the weapons employed. The Charter neither expressly prohibits, nor permits, the use of any specific weapon".**
- In May 2011, the United States Department of Defense concluded in its first formal cyber-strategy that the laws of armed conflict can be expanded to include cyber-warfare thereby allowing the application of both Article 2(4) and Article 51 to cyber attacks.

Prohibition on the Use of Force: Article 2(4)

- Article 2(4) include "verbal threats, initial troop movements, initial movements of ballistic missiles, massing of troops on a border, use of fire control radars, and interference with early warning or command and control systems."
- Cyber-attacks will be compared to the items on this non-exhaustive list to determine whether they constitute a threat of force.
- No clear definition of what constitutes use of force. The U.N. Charter does not define use of force, nor has any international body.
- The International Court of Justice - in the case of Nicaragua v. United States of America -that arming and training a rebel group constituted a use of force, but supplying of funds to a rebel group and United States military maneuvers held near the border did not involve the threat or use of force.

- Under Article 51, a classic military armed attack activates the target nation's right to respond in self-defense.
- A nation responding to an armed attack must fulfill the requirements of necessity, proportionality, and immediacy.
- **The principle of necessity requires that "non-forcible remedies must either prove futile in limine or have in fact been exhausted in an unsatisfactory manner**."'

Issues with cyber crime in I-Law

- identifying the location of a cyber-crime raises numerous questions.
- Is the source of the electronic communication the location?
- Where it was originally received?
- What if criminal conduct in furtherance of the offense occurred in the jurisdiction?
- Or did the offender simply access a computer in that state?
- It can also be very difficult to tell where the criminal act actually takes place.

- Proposals for the establishment of an International Criminal Tribunal for Cyberspace (ICTC).
- cyber-crimes of most serious concern to the international community, including violations of a global treaty or set of treaties on cyber-crime, or coordinated global cyber-attacks against critical national infrastructure are the subject matter

Cyber-espionage

- "Cyber-espionage is defined as the intentional use of computers or digital communications activities in an effort to gain access to sensitive information about an adversary or competitor for the purpose of gaining an advantage or selling the sensitive information for monetary reward”
- Espionage does not reach the level of use of force under the U.N. Charter

- cyber-espionage should, in some situations, be treated as a use of force or threat of use of force under the U.N. Charter.
- China has gained substantial military advantages in recent years by stealing information on some of the most advanced weapons systems in the American arsenal, including jet fighters and unmanned submersible vehicles.

- In 2009, the North Atlantic Treaty Organization Cooperative Cyber Defence Centre of Excellence ("NATO CCD COE"), a renowned cyber research and training institution in Tallinn, Estonia, invited an independent group of experts to compile a manual on the international law governing cyber warfare.
- This effort brought together a group of international law scholars and practitioners—the International Group of Experts ("Experts")—to explore and articulate how extant legal norms apply to cyber warfare.
- The original Tallinn Manual on International Law Applicable to Cyber Warfare was published in 2013.

Cyber crime and international law

- At the international level two new treaty instruments provide a sound basis for the essential cross-border law enforcement cooperation required to combat cyber-crime.
- The first of these instruments, **the Council of Europe's (CoEs) Cyber-crime Convention, is purpose built and although designed as a regional** mechanism has global significance.
- The second is the **United Nations (UN) Convention against transnational organized crime**, which is global in scope but indirectly deals with cyber-crime when carried out by criminal networks in relation to serious crime.

- a UN draft resolution in 2003 at the 58th session of the General Assembly (GA) on "**Cyber security and the protection of critical information infrastructures“.**
- The passage of the CoE's Cyber-crime Convention in December 2001 and its activation in July 2004 provides for the first time an international legal mechanism for cooperation in law enforcement and harmonisation of laws

International treaties

- Forty-two states have signed the Convention (including non-council member states: Canada, South Africa, Japan and the USA) but as of 2005 only 11 states had ratified the convention.
- The cumbersome nature of treaty ascension processes the ratification and activation (a minimum of five ratifications are necessary) of this Convention in less than three years has been extraordinarily rapid.
- The Convention's "First Additional Protocol to the Convention on Cyber-crime on the criminalisation of acts of a racist or xenophobic nature committed through computer systems" that extends "content" cyber-crime to include "hate speech" as well as child pornography has been signed by 25 states and awaits the ratification process.

- The Convention, apart from enhancing MLA, provides comprehensive powers to expedite preservation of stored computer data and partial disclosure of traffic data;
- to make production orders; to search computer systems;
- to seize stored computer data;
- to enable real-time collection of traffic data;
- and to intercept the content of questionable electronic data.

- Beginning with the Eighth UN Congress on the Prevention of Crime and the Treatment of Offenders in 1990, the UN, with its network of institutes on crime prevention and criminal justice, has been actively involved in addressing problems of transnational crime and cyber-crime.

United Nations Convention against transnational organized crime

- The TOC Convention significantly extends the reach of the 1988 Vienna Convention against illicit traffic in narcotics and psychotropic substances.
- The TOC Convention enables establishes several offence categories:
- participation in an organised criminal group, money laundering, corruption and obstruction of justice as well as protocols in respect to trafficking in women and children (117 states and 64 parties with effect from 25 December 2003);
- illicit manufacturing and trafficking in firearms (52 states and 22 parties but not yet in force);
- and smuggling of migrants (112 states and 57 parties with effect 28 January 2004).
- Serious crime is defined broadly (conduct attracting punishment of four or more years' imprisonment).

TOC

- The TOC Convention, defines an offence as "transnational" if it is:
- " committed in more than one state;
- " committed in a single state but planned, prepared, directed or controlled in another state";
- committed in one state but involving an organised group whose activities cross national boundaries;
- committed in a single state but has "substantial effects" in another state.

“serious crime”

- "serious crime" (as defined in the Convention), "where the offence is transnational in nature and involves an organized criminal group“.
- Every cyber crime is "serious crime" because such offences usually affect more than a single jurisdiction, often involve at least three or more actors, and are committed with the aim of achieving some financial or material benefit.

The Council of Europe Cyber-crime Convention

- The CoE, founded in 1949, comprises 45 countries, including the members of the EU (a separate entity), as well as countries from Central and Eastern Europe. Headquartered in Strasbourg, France, the CoE was formed as a vehicle for integration in Europe, and its aims include agreements and common actions in economic, social, cultural, legal and administrative matters.
- As one of the two principal supranational organisations in Europe (the other being the EU), the CoE is responsible for creating and implementing a wide variety of measures aimed at international crime and has adopted a number of widely used conventions on interstate cooperation in penal matters.
- In 1996, the CoE's European Committee on Crime Problems established a committee of experts to address cyber-crime, which completed its work late in 2001.

- The resulting Cyber-crime Convention has three aims: to lay down common definitions of certain criminal offences - nine are mentioned in the Convention - thus enabling relevant legislation to be harmonised at national level;
- to define common types of investigative powers better suited to the information technology environment, thus enabling criminal procedures to be brought into line between countries; and
- to determine both traditional and new types of international cooperation, thus enabling cooperating countries to rapidly implement the arrangements for investigation and prosecution advocated by the Convention in concert, for example, by using a network of permanent contacts.

- The Convention, has received strong support from lawmakers and practitioners throughout Europe and beyond. But both the Convention and its additional protocol have been criticised on various grounds by a number of associations, particularly those active in the protection of freedom of expression, and also by industry elements.
- The CoE Convention on Cyber-crime (the "Convention") obligates signatories to criminalise a minimum list of specific offences where there was consensus and thus harmonised offences to eliminate problems of dual criminality.
- The basic structure and content of the convention is outlined below. The CoE Convention on Cyber-crime (the "Convention") obligates signatories to criminalise a minimum list of specific offences where there was consensus and thus harmonised offences to eliminate problems of dual criminality.
- The basic structure and content of the convention is outlined below.

Computer-related offences: Title 1

- addresses offences against the confidentiality, integrity and availability of computer data such as:
- * illegal access of a computer system;
- * interception of non-public transmissions of computer data to, from, or within a computer system;
- * interference with computer data;
- * interference with computer systems, such as computer sabotage; and
- * the misuse of computer-related devices (e.g. "hacker tools"), including the production, sale, procurement for use, import or distribution of such devices.

- Title 2 covers the traditional offences of fraud and forgery when carried out through a computer system. For forgery, the intent of this provision is to protect computer data in the same manner as tangible documents, where such data may be acted upon or used for legal purposes.
- Title 3 seeks to control the use of computer systems as a vehicle for the sexual exploitation of children and acts of racists or xenophobic nature. This category of offences concerns the subject or contents of computer communications and focuses on offences related to children. The Convention makes various acts (from the possession to the intentional distribution of child pornography) criminal offences, thus covering all links in the chain. This provision criminalises various aspects of the electronic production, possession and distribution of child pornography.

- **Title 4** criminalises wilful infringements of copyright and related rights when such infringements have been committed by means of a computer system and on a commercial scale. This section targets the large-scale distribution of illegal copies of works protected by intellectual property rights (TPR). Infringements of IPR, in particular of copyright, are among the most commonly committed offences on the internet, and cause concern both.

- Jurisdiction Among the various important matters addressed by the Convention, was the question of jurisdiction in relation to information technology offences, for example, to determine the place where the offence was committed and which law should accordingly apply, including the case of multiple jurisdictions and the question of how to solve jurisdictional conflicts. This provision establishes criteria under which contracting parties are obliged to establish jurisdiction over the criminal offences in the Convention. The provision concerning jurisdiction also requires states exercising jurisdiction to coordinate when victims are located in different countries.

- The Convention also creates the legal basis for an international computer crime assistance network, a network of national contact points permanently available (the "24/7 network").
- The network established by the Convention is based on experience gained from the network created by the G8 and co-ordinated by the US Department of Justice.
- Under the Convention, states are obligated to designate a point of contact available 24 hours a day, seven days a week, in order to ensure immediate assistance to investigations within the scope of the Convention. The establishment of this network is one of the most important provided by the Convention to ensure states can respond effectively to the law enforcement challenges posed by computer crime. This network will supplement the more traditional channels of cooperation. Each national 24/7 contact point is to either facilitate or directly carry out technical or legal advice, preservation of data, collection of evidence, and locating of suspects. The Convention also requires that national network team be properly trained to respond to computer-related crime.

Budapest Convention: scope

Criminalising conduct

- Illegal access
- Illegal interception
- Data interference
- System interference
- Misuse of devices
- Fraud and forgery
- Child pornography
- IPR-offences

Procedural tools

- Expedited preservation
- Search and seizure
- Interception of computer data

+

International cooperation

- Extradition
- MLA
- Spontaneous information
- Expedited preservation
- MLA for accessing computer data
- MLA for interception
- 24/7 points of contact

Harmonisation

The only binding international instrument and guiding legislative tool in the fight against Cybercrime

Budapest Convention: The role of the Cybercrime Convention Committee (T-CY)

(Committee of Parties to the Budapest Convention)

Established under Article 46 Budapest Convention

Membership (November 2016):

- 50 Members (State Parties)
- 17 Observer States
- 12 organisations (African Union Commission, Commonwealth Secretariat, ENISA, European Union, Eurojust, Europol, INTERPOL, ITU, OAS, OECD, OSCE, UNODC)

Functions:

- Assessments of the implementation of the Convention by the Parties
- Guidance Notes
- Draft legal instruments

Two plenaries/year as well as Bureau and working group meetings

- ► An effective follow-up mechanism;
- ► The T-CY appears to be the main inter-governmental body on cybercrime matters internationally

CYBER TERRORISM

Introduction

- Cyberspace is considered **by** many to be a new war fighting domain.
- 2001 European Convention on Cybercrime -the focus on inter-State issues and State-sponsored cyber operations.
- that non-international armed conflict today ranging from low-intensity armed conflicts between organized armed groups in failed-State scenarios like Somalia' to traditional types of civil war like the ongoing armed conflict in Syria to "internationalized" scenarios like the armed conflict in **Afghanistan**
- Such attacks may lead to death or bodily injury, or cause explosions, plane crashes, water contamination, severe economic loss or serious attacks against critical infrastructure, attacks against life and electronic infrastructure which are directed **against national security** establishments and critical infrastructure.
- In the context of post **9/11,** the threat of cyber terrorism is often linked to **Al-** Qaeda and other terrorist organisations.

International cooperation

- The Convention on Cyber Crime **(ETS** no **185) ("ECCC")** is the first international treaty addressing crimes committed via the Internet and other computer networks.
- articles **2-6** which address offences against the confidentiality, integrity and availability of computer data and systems, may be used to address the offence of cyber terrorism.
- South Africa is the only African country to sign the European Convention on Cyber crime **(ECCC).**

Some incidents…….

- Rami Yousef who orchestrated the **1993** World Trade Center bombing **by** using encryption to store details of his scheme on his laptop computer, is a case in point **.**
- It has also been reported that the first known attack **by** terrorists against a country's computer system took place in Sri Lanka in **1998,** when the ethnic Tamil Tigers guerrillas overwhelmed Sri Lankan embassies with **800** e-mails a day over a two week period.
- During the war in Kosovo in **1999,** Serb sympathisers tried to target the **NATO** website with viruses.
- In another incident, cyber attacks were launched against the Estonian state during April **2007.** The targets were the Estonian Parliament, banks, media houses and government departments.

Definition of cyber terrorism

- "premeditated use of disruptive activities, or the threat thereof, in cyber space, with the intention to further social, ideological, religious, political or similar objectives, or to intimidate any person in the furtherance of such objectives".
- The United Kingdom has introduced a number of anti-terrorist legislation, namely, the Terrorism Act of 2000, the Anti-Terrorism, Crime and Security Act 2001 and the Terrorism Act of **2006.**

Legislations on cyber terrorism

- The United States of America introduced the Patriot Act of 2001 in response to the **9/11** attacks.
- South Africa :legislations on cyber terrorism and terrorist financing- 1. the Prevention of Organised Crime Act **38** of **1999 ("POCA"),**
- **2.** the Financial Intelligence Centre Act 38 of 2001 ("FIGA"),
- 3. the Electronic Communications and Transactions Act 25 of 2002 ("ECT),
- 4. Protection of Constitutional Democracy against Terrorism and Related Activities Act **33** of 2004 ("PCDTRA").

USA, PATRIOT ACT, **Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism**.

- The Act has eased restrictions on electronic surveillance to facilitate the capture of terrorists.
- contains anti-money laundering provisions in order to prevent terrorists from achieving any financial gain from their actions.
- includes terrorism and computer crimes on its list of offences. However, the Act has been criticized for violating the civil rights of ordinary American citizens.

- Cell phones have also been used to track terrorists and to provide evidence against them. South Africa has introduced the Regulation of Interception of Communication Act 2002 (RICA) for this purpose.

UK

- The Terrorism Act of 2000 was introduced to address terror attacks in the United Kingdom. The listed prohibited actions include endangering another person's life or creating a serious risk to the public health or safety, acts designed to seriously interfere with or disrupt an electronic system and acts involving serious violence to or death to another person or serious property damage.
- Section 1(2)(e) of the Terrorism Act 2000 describes a terrorist act as one that "is designed seriously to interfere with or seriously disrupt an electronic system"

- On 14th December 2001, the British Anti-Terrorism, Crime and Security Act
- the United Kingdom government is seeking protective measures against the cyber terrorist threat. IT HAS SET UP National Technical Assistance Centre which is a surveillance advice and interception facility

Definitions.....

- Dorothy Denning defines cyber terrorism as "the convergence of terrorism and cyberspace. It is understood to mean unlawful attacks and threats of attack against computers, networks and the information stored therein when done to intimidate or coerce a government or its people in the furtherance of political or social objectives".
- Mark Pollit defines cyber terrorism as a"premeditated, politically motivated attack against information, computer systems,computer programmes, and data which result in violence against noncombatanttargets **by** sub national groups or clandestine agents".

What is cyber terrorism

- An attack that undermines the confidentiality or availability of a computer, information resident on it.
- Some offences under Computer Misuse and Cybercrime Act 2003:
- Unauthorised access to data
- Access with intent to commit offences
- Unauthorised access to and interception of computer service
- Damaging or denying access to computer system

THREATS TO INDIA

- The Intelligence Bureau(IB) has warned India regarding the cyber threat to India.
- Dr. A.P.J. Abdul Kalam warned in a 2005 lecture regarding the cyber terrorism
- Mr.Ankit, said India lacks training for cyber security experts.
- Cyber crime experts say this is a dangerous scenario.

ESTIMATED ENEMY COUNTRIES

- Two countries are estimated in cyber attack towards India. Namely China and Pakistan.
- China may try to destabilize our economy.
- Pakistan, may attack ESCOMs.

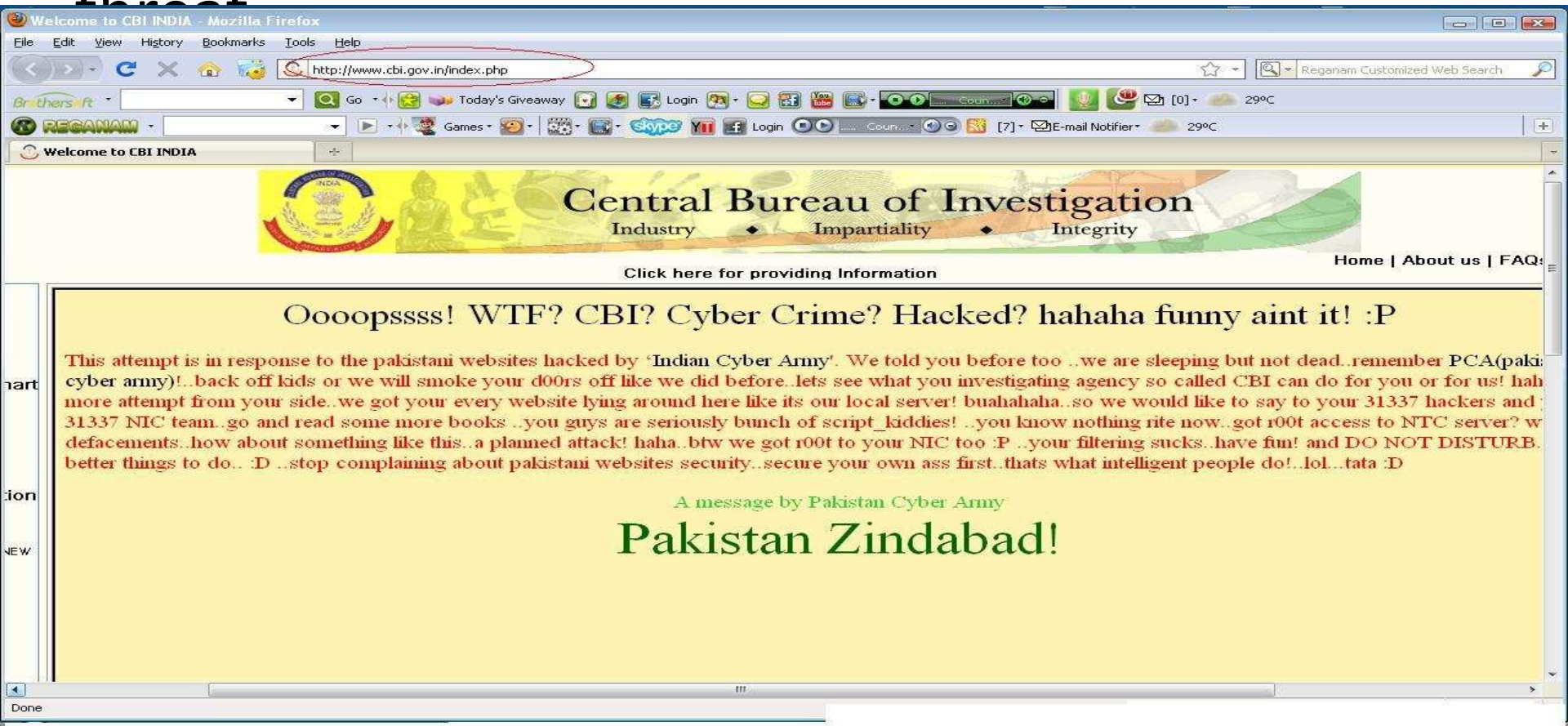
INITIAZATION OF CYBER TERRORISM IN INDIA

- Police on October 6,2008 arrested 20 suspected members ,who had played a role in the serial blasts in Ahmadabad , Surat and New Delhi.

- And found that they played a role in sending the e-mail messages before and after the blasts in New Delhi and Ahmadabad.

- It is found that the Google maps has been used as the source of information for intruding into the city of Mumbai.

- The CBI of India too suffered in the international security that the Pakistani cyber terrorist was able to break into the Indian websites and were making a open statement threat



CYBER TERRORISM TOOK PLACE WORLD WIDE

- Cyber crime has emerged as a new level of terrorism world wide. Which may even happen in India.
- Jamming the power of the whole city.(i.e.)The blocking of the power stations.
- The breakage to the banking of the country.
- Flooding the whole city with sewage waste.

- The bombarding of the computers connected to internets.
- Robbery of the international banks.
- Breaking into a plane's onboard computer systems forcing it to crash.
- The complexity of the cyber terrorism is that this attack can be carried out by terrorists any where in the world without even touching our soil with free of cost.

HACKERS CAN TURN YOUR HOME COMPUTER INTO A BOMB

HACKERS CAN TURN YOUR HOME COMPUTER INTO A BOMB

... & blow your family to smithereens!

By RANDY JEFFRIES / Weekly World News

WASHINGTON — Right now, computer hackers have the ability to turn your home computer into a bomb and blow you to Kingdom Come — and they can do it anonymously from thousands of miles away!

Experts say the recent "break-ins" that paralyzed the Amazon.com, Buy.com and eBAY websites are tame compared to what will happen in the near future.

Computer expert Arnold Yabenson, president of the Washington-based consumer group National CyberCrime Prevention Foundation (NCPF), says that as far as computer crime is concerned, we've only seen the tip of the iceberg.

"The criminals who knocked out those three major online businesses are the least of our worries," Yabenson told *Weekly World News*.

"There are brilliant but unscrupulous hackers out there who have developed technologies that the average person can't even dream of. Even people who are familiar with how computers work have trouble getting their minds around the terrible things that can be done.

"It is already possible for an assassin to send someone an e-mail with an innocent-looking attachment connected to it. When the receiver downloads the attachment, the electrical current and molecular structure of the central processing unit is altered, causing it to blast apart like a large hand grenade.

"As shocking as this is, it shouldn't surprise anyone. It's just the next step in an ever-escalating progression of horrors conceived and instituted by hackers."

Yabenson points out that these dangerous sociopaths have already:

- Vandalized FBI and U. S. Army websites.
- Broken into Chinese military networks.
- Come within two digits of cracking an 87-digit Russian security code that would have sent deadly missiles hurtling toward five of America's major cities.

"As dangerous as this technology is right now, it's going to get much scarier," Yabenson said.

"Soon it will be sold to terrorists cults and fanatical religious-fringe groups.

"Instead of blowing up a single plane, these groups will be able to patch into the central computer of a large airline and blow up hundreds of planes at once.

"And worse, this e-mail bomb program will eventually find its way into the hands of anyone who wants it.

"That means anyone who has a quarrel with you, holds a grudge against you or just plain doesn't like your looks, can kill you and never be found out."

KABOOM! It might not look like it, but an innocent home computer like this one can be turned into a deadly weapon.

Sickos can wreak death and destruction from thousands of miles away!

Arnold Yabenson.

LACKING OF CYBER SECURITY IN INDIA

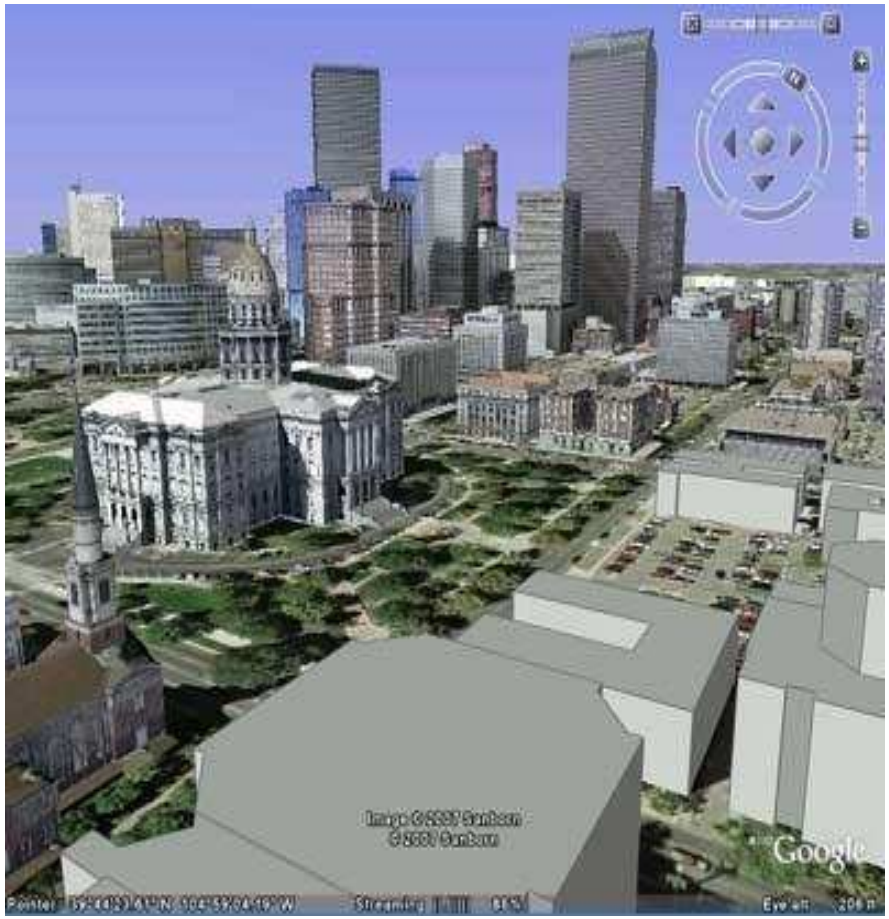
- It is estimated that 5 thousand of corporate networks have no protection from cracking.
- at Home the internet facilities still suffers security. Which causes cyber hacking of the banking of that house
- India becoming the developed nation the number of transactions has made to digital via Internet has increased . The work of almost all branches of the country like economy, energy, transport and communications, banking uses computer networks.

- But still we don’t have cyber security..
- The breakage of these networks may paralyze the whole country.
- India being IT superpower is in need of cyber security

WAY OF SECURITY

- cyber crime police stations must be established soon.
- The recruitment of professionals is must.
- The latest updating of security software's must be done in companies, schools, colleges and other sectors.
- The pirated soft wares must be put to an end.

- The Google maps showing the higher security parts of the nation must be disabled.
- The unauthorized GSM Sims must be deactivated by the mobile companies .



- The mobiles with out IP address must be banned.
- The selling of smarter mobiles must be only to certified people cause the interaction between those mobile cant be tracked.
- The recording between blackberry mobiles

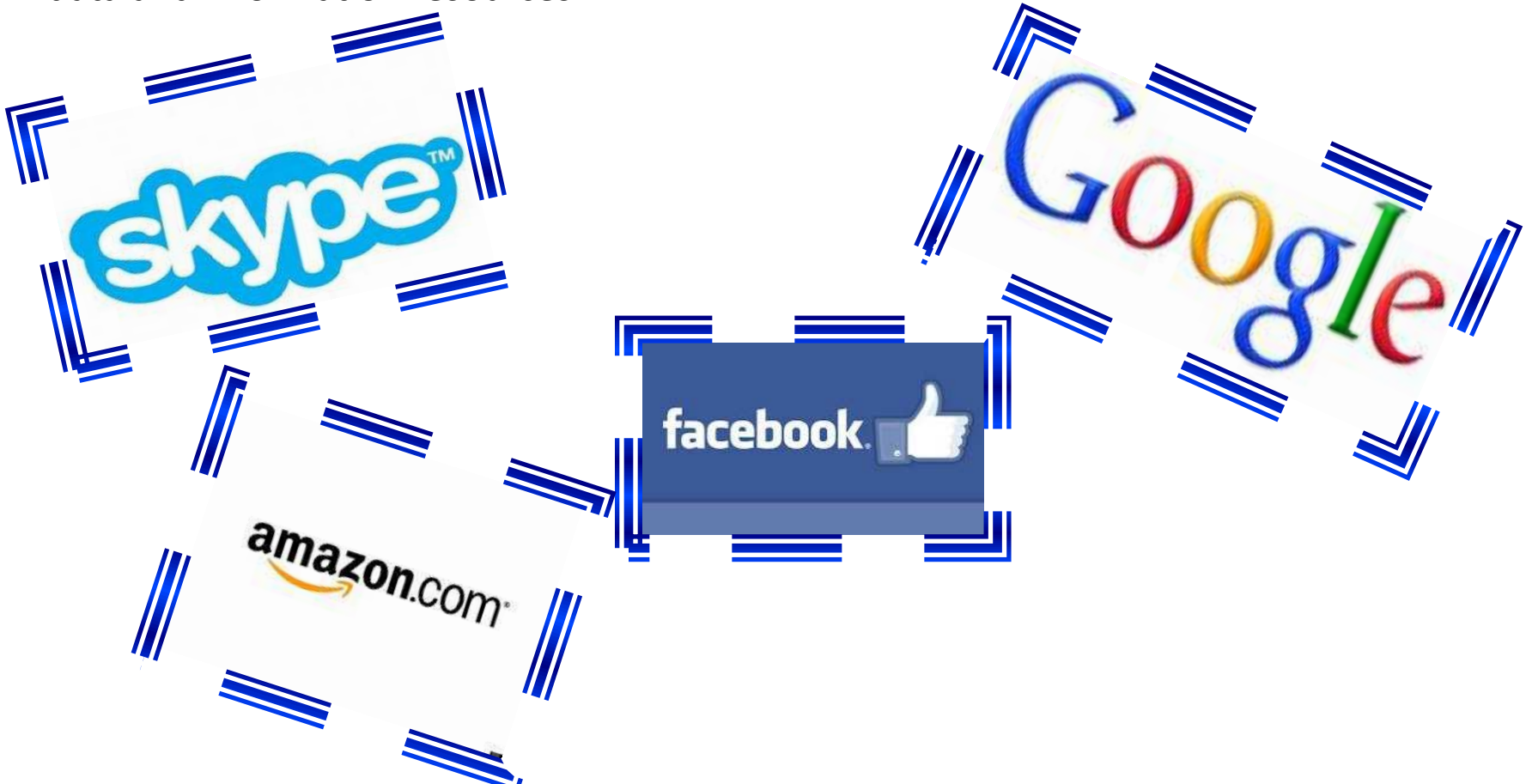
- The education of the security system must be made from school level to colleges.
- The banning of the sites regarding manufacture of bombs and hacking and other offensive sites must be done.

TERRORISM AND THE USE OF INTERNET

Terrorism and the use of Internet

The Internet

- The Internet is an infrastructure combining different kinds of media – email, chat groups, World Wide Web etc.
- The Internet makes it possible to disseminate and transmit different sets of data and information resources.



The Internet

- The internet is subject to very little regulation – was developed as an open, interoperable network without hierarchical disbursing - regulations are generally few in number and impose only minimal constraints

The Dark side

Nefarious Intentions → Heinous uses → Digital menace

- Virtual geographical footpr
- Fragmented structure
- Rapidly evolving technology

- This is where the use of the internet by terrorists fits in.
- *"Terrorists use the Internet just like*

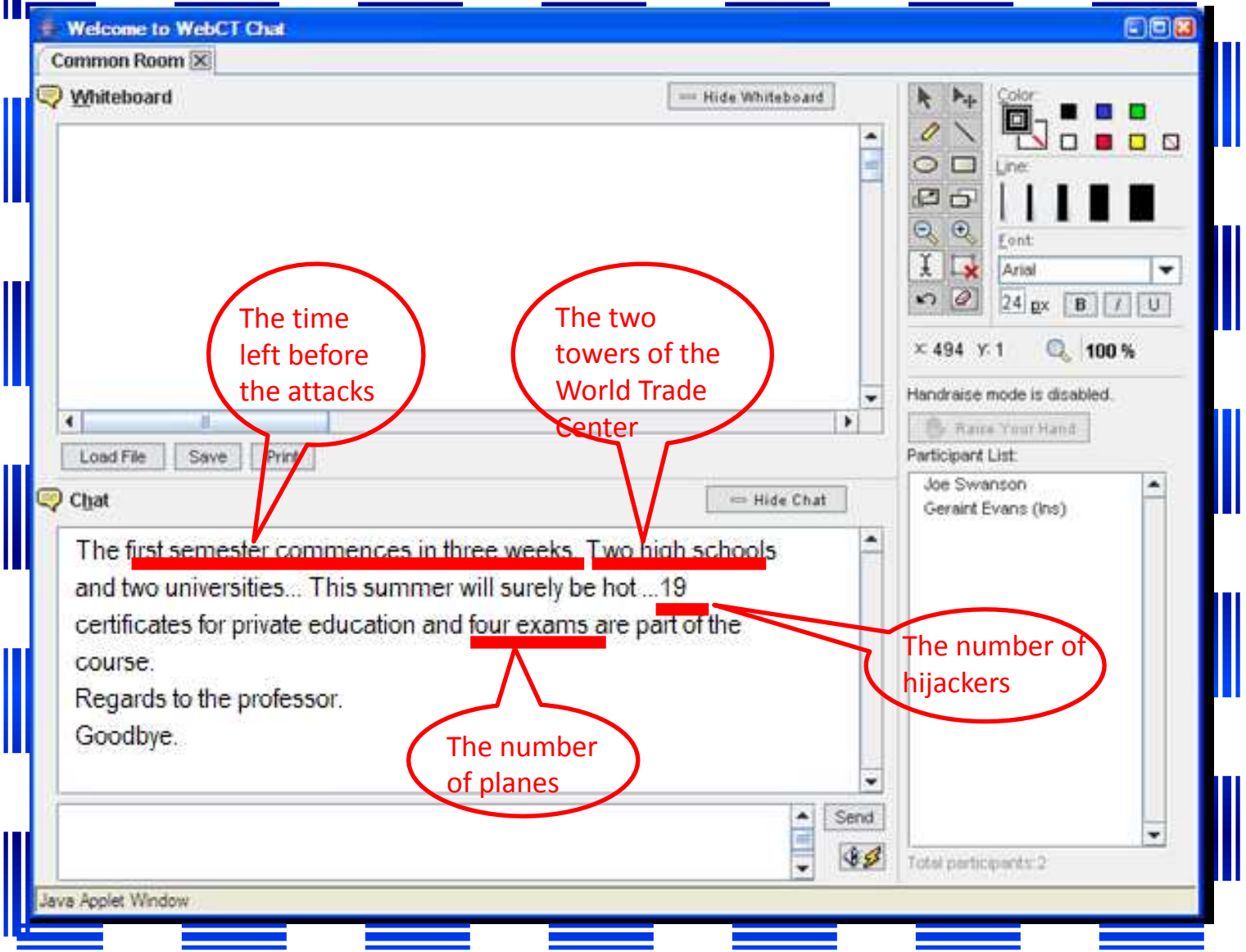
See, Freiburger, T. and S. Crane, J. 2008. A Systematic Examination of Terrorist Use of the Internet. *International Journal of Cyber Criminology*, 2 (1), pp. 309-319.

The uses of Internet: Access to Information

Every minute more than two million Google searches are conducted

The uses of Internet: Communication

The uses of Internet: Communication



Information Disbursing

Every minute more than 70 new domains are Registered.

The uses of Internet: Social networking

Every minute Facebook is logged in six million times

The Growing threat: The internet as pivotal to terrorist attacks

- 9/11 was made possible only because of the intensive use of internet which went into the planning to cull out intelligence on the targets as well as exchange information—to collect information regarding the flight timings, steal Social Security Networks and driver licenses, and more importantly – to execute the major planning for the attacks through emails sent in code words and to communicate in real time and coordinate the attacks
- 2001 Parliament Attacks - the internet was used by terrorists for making fake identity cards and fake Home Ministry stickers in the Attack on the Parliament House.^
- Nearly all terrorist attacks in India between 2008 and 2012 were the end results of extensive usage of the internet.^^

^See, *State v. Mohd. Afzal and Ors*. 107(2003)DLT385

^^Strategy Page. 2013. *Counter-Terrorism: India's Internet Threat*. [online] Available at: http://www.strategypage.com/htmw/htterr/20120616.aspx [Accessed: 29 Sep 2013].

The use of internet by terrorists in India

- Nearly all terrorist attacks in India between 2008 and 2012 were the end results of extensive usage of the internet.
- In India, like elsewhere, the internet is used for planning, communications during the attacks as well as for initial planning and recruitments.
- Whereas in the initial planning stages the information is encrypted or erased quickly so that it is never traceable as evidence, in the actual execution of the attacks even extensive usage of the internet for communication is difficult to trace and even more difficult to act upon.

- **Voice Over Internet Protocol , VOIP, is one of the most important tools which is used by terrorists for being able to send encrypted and extremely hard to detect voice calls over the internet.**
- **Terrorists in India have been found to extensively use Gmail for most of the primary communications**
- **Google News Alerts on the internet to keep a tab on police movement and thus sharpen their movement and evade entrapment.**

Why the internet?

1) surreptitious command, control and communications capabilities;

2) enhanced access to information of all types;

3) a ubiquitous source of funding, money laundering, and electronic transfers;

4) a means to conduct asymmetric, offensive information operations, and

5) global publicity and recruiting.

Cyber terrorism as opposed to the use [illegible] oses

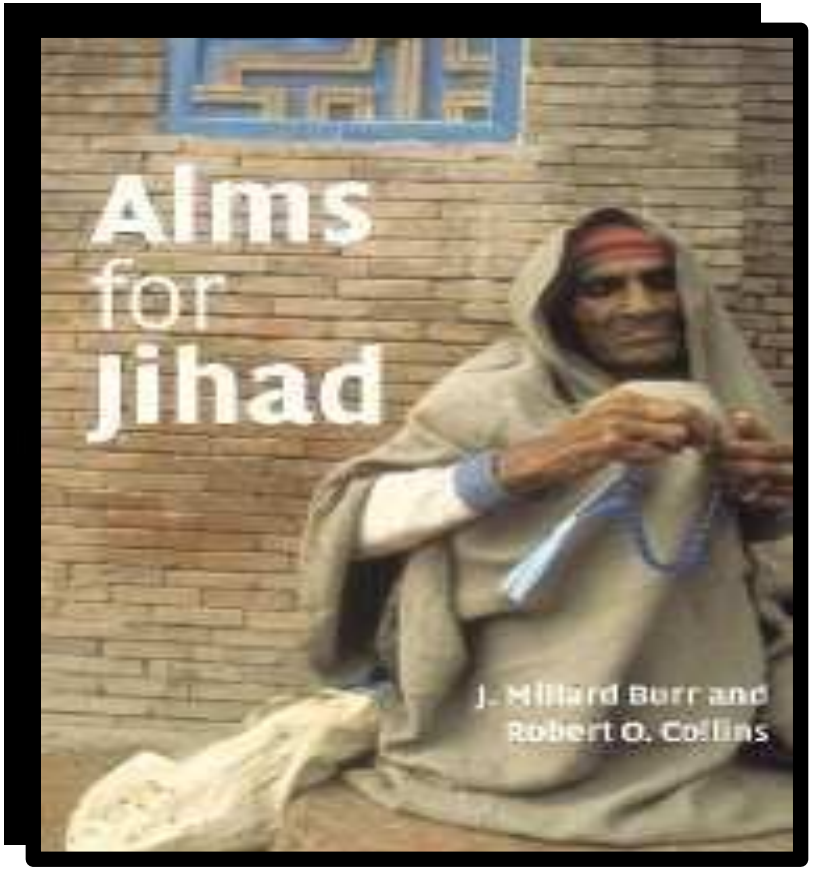
[illegible]ernet

Why this study?

- Cyber terrorism is defined, however for the use of the internet by terrorists there has not been the coinage of either a term or a definition.
- The use of internet is made by terrorists for
  - perpetrating psychological warfare
  - for recruitment
  - for financial support for networking
  - for planning
- The use of internet by terrorists can be said to be the biggest contributing factor for the success of many terrorist attacks
- This is widely acknowledged but very less concrete action has been taken very less concrete action on and this is where this paper finds its launching platform.

Why is The Internet an attractive choice for financing terrorism?

- Anonymity of the internet is expedient
- Web-based financial transactions can be carried out with users or server in foreign country anywhere in the world
- Internet based financial transactions are subject to very little regulation
- Al-Qaeda, Hamas, Laskhar-e Taiba, and Hizballah have been confirmed to extensively use the internet to finance their terrorist activities^



*Washington Institute. 2013. *Terrorist Financing on the Internet: Policy Analysis*. [online] Available at: http://www.washingtoninstitute.org/policy-analysis/view/terrorist-financing-on-the-internet [Accessed: 30 Sep 2013].

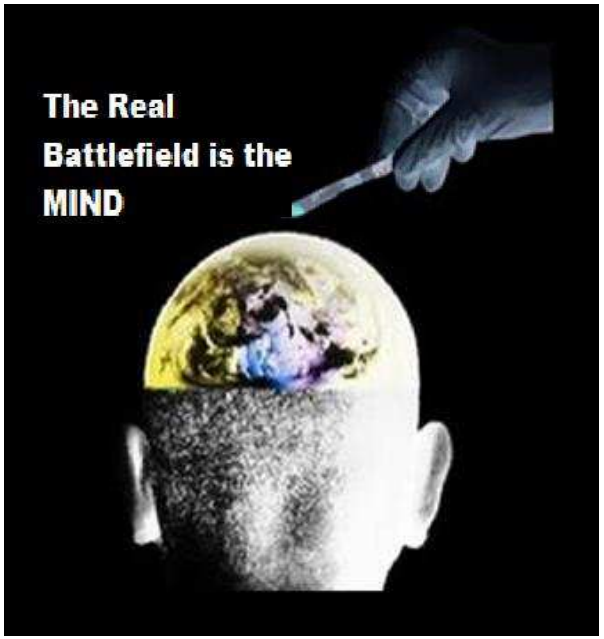
India is at special risk

- The International Monetary Fund has pointed out how India is at a especially huge risk of being home to terrorist financing
- India is a member of the multi-national Financial Action Task Force (FATF), an inter-governmental organization founded in 1989 by the G7 which was created to develop policies to counter terror financing and this very Task Force has questioned India's efficacy in the same domain.^
- Section 17 of the Unlawful Activities (Prevention) Act makes raising funds an offence where there is likelihood that they will be used for terrorist acts.

^'Indian laws cannot counter terror-funding'. 2010.*The Indian Express*, [online] July 18th. Available at: http://www.indianexpress.com/news/indian-laws-cannot-counter-terrorfunding/648241/ [Accessed: 30 Sep 2013].

Psychological Warfare: PSYWAR

- The radicalization process for terrorism has been academically explained through two main concepts:
  - triggers
  - motives
- While triggers have been understood to be usually geopolitical like the Palestinian problem, the motives are both psychological and ideological and the massive use of the internet by terrorists only flames the psychological motives by further flaming the feeling of being wronged, of desiring revenge.

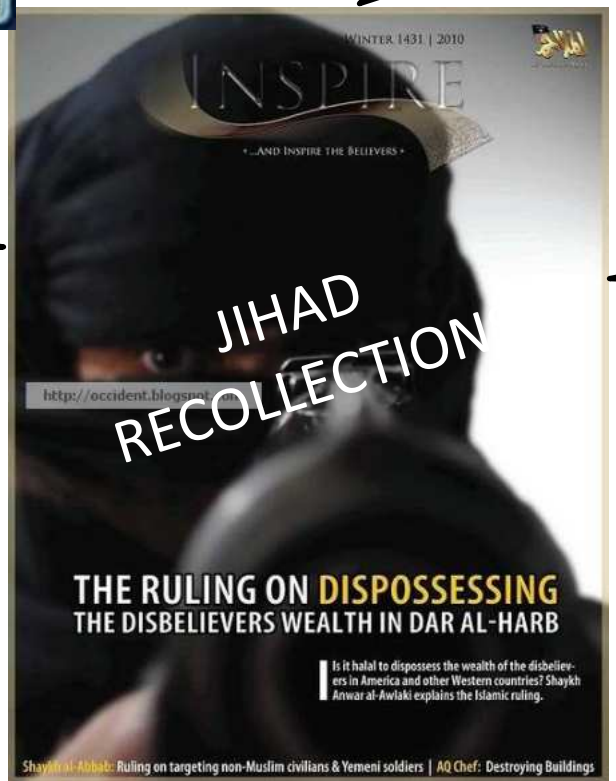


See the transcript of Mathieu Guidère's interview available at: Naravane, V. 2012. 'Home-grown western terrorists are new threat to India'. .

Psychological Attack

"Militant training is an obligation in Islam upon every sane, male, mature Muslim, whether rich or poor, whether studying or working and whether living in a Muslim or non-Muslim country"

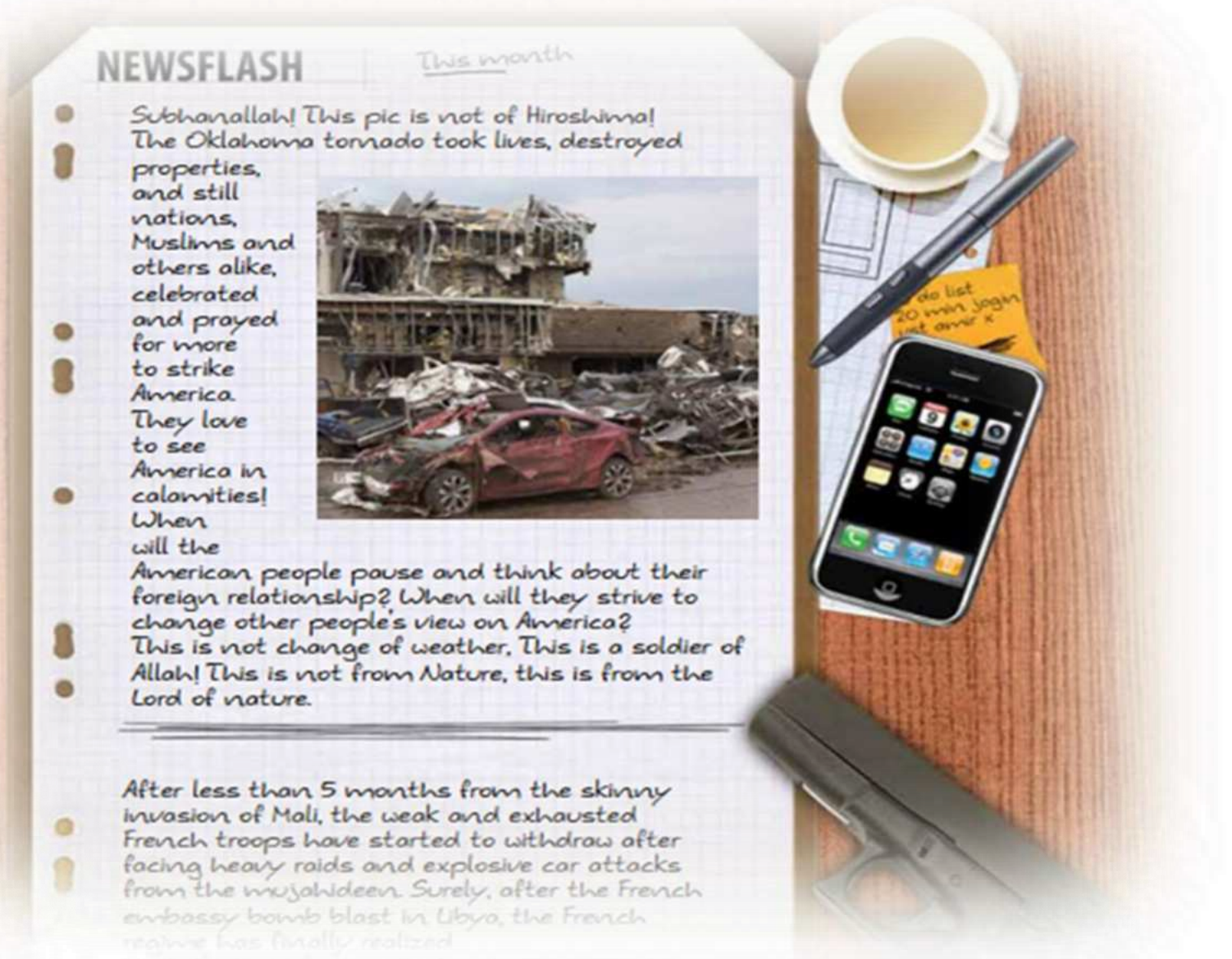
"It is your freedom to ignite a firebomb"



"It is either Jihad or Disgrace. You Choose".

"The peace you enjoyed before September 11 is merely just part of history. In other words, you will never enjoy peace until we live it practically in Palestine and all the infidel forces leave the Peninsula of Muhammad ﷺ and all other Muslim lands."

Spring, 2013, Inspire



"The Oklahoma tornado took lives, destroyed properties, and still nations, Muslims and others alike,
celebrated and prayed for more to strike America. They love to see America in

Sheikh Ibrahim Ar-Rubaysh

Allah will restrain the evil might of those who disbelieve

﴿So fight (O Muhammad) in the Cause of Allah; you are not held responsible except for yourself. And inspire the believers (to fight), it may be that Allah will restrain the evil might of those who disbelieve. And Allah is Stronger in Might and Stronger in punishing﴾ [4: 84]

In this holy verse, Allah commands His Messenger ﷺ to fight in His cause even if he is to do that alone. He then lays out the goal: He will restrain the evil might of those who disbelieve, Allah is Stronger in Might and He can punish whomever He wants among His enemies. Bear in mind, Allah orders the believers to fight so as to honor them and take among them martyrs. Allah says, ﴿And if Allah had willed, He could have taken vengeance upon them (Himself), but (He ordered armed struggle) to test some of you by means of others﴾ [47: 4]

Imam Al-Baghawy comments on this verse: "It means: do not abandon waging *Jihad* on the enemy and supporting the oppressed even if you are alone. Indeed, Allah has promised victory and punished others for abandoning *Jihad*."

The Potency of the PSYWAR: Recruitment and Manpower

- Potential recruits continue to be 'incited, infected and radicalized' on the web.

- Home Secretary, GS Pillai, acknowledged how, particularly in India the internet is a 'potent tool' used by terrorists for recruiting youth and expanding their networks.

- Section 18B of the UAPA provides that whoever recruits or causes to be recruited any person or persons for commission of a terrorist act shall be punishable with imprisonment for a term which shall not be less than five years but which may extend to imprisonment for life, and shall also be liable to fine.

Investigative Project. 2012. *Glossy Internet Magazine Targets Americans for Jihad Training :: IPT in the News :: The Investigative Project on Terrorism*. [online] Available at: http://www.investigativeproject.org/1027/glossy-internet-magazine-targets-americans-for [Accessed: 27 Sep 2013].

Jihad Recollections, Issue 6, page 55

"Net a recruitment tool for terrorist in India". 2011.*Times of India*, [online] May 7th. Available at: http://articles.timesofindia.indiatimes.com/2011-03-07/internet/28665443_1_cyber-security-cyber-crimes-lab [Accessed: 29 Sep 2013].

Control and Command

- Terrorists have been found to make use of real time communication to better control the execution of attacks.
- Interception of such communication is considered to be extremely difficult if not impossible at least until it is too late to take action.
- The accounts used for these purposes are deleted after the job is over and thus the evidence is easily erasable and the requisite software is deleted from the computer's hard disk so that absolutely no trace is left.

Tibbetts, P. 2002. Terrorist Use of the Internet and Related Information Technologies.

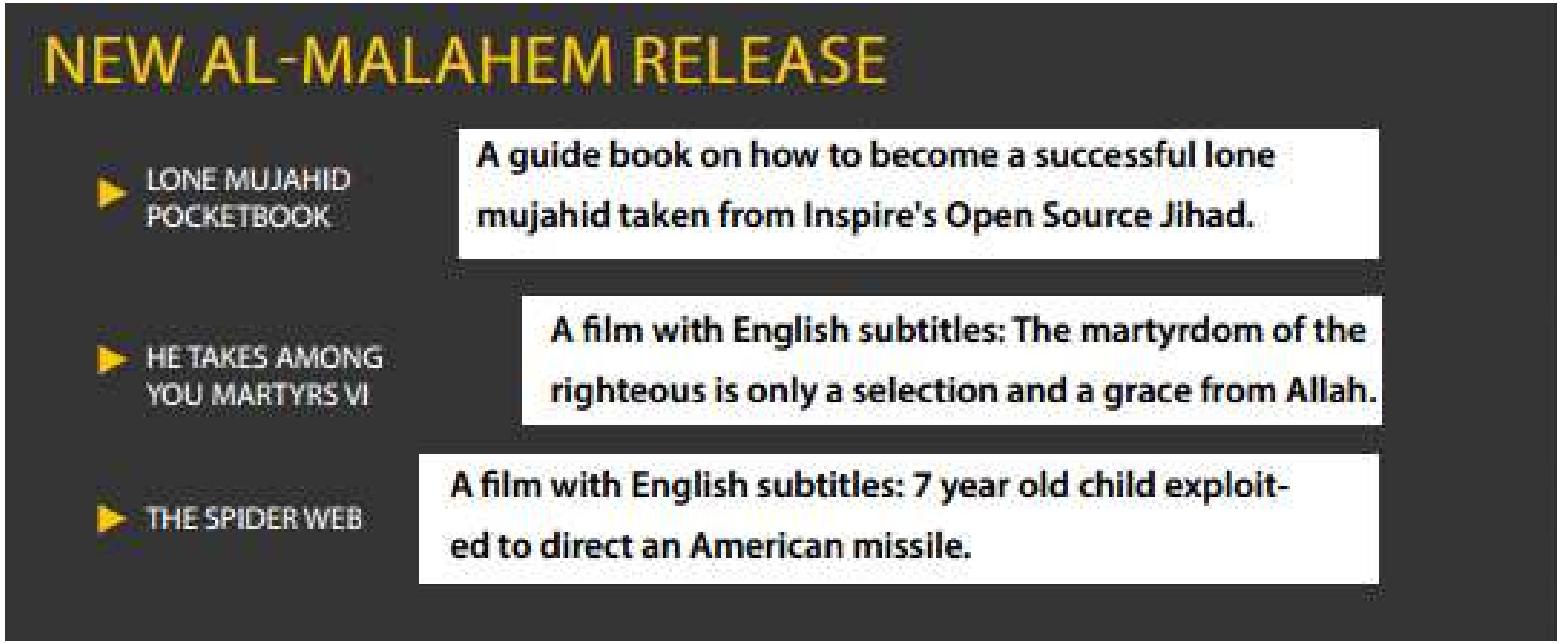
Dead Drops and steganography

- An extremely creative way devised by terrorists of using the internet is of dead drops. Dead drops are traditionally associated with the world of espionage as depictive of exchange of information without the two parties actually ever having to meet. This way there is never any evidence of there being a conspiracy. Internet dead drops go a step further by also erasing the very information which is exchanged. After creating free email accounts the information is saved in an email draft without being sent, later the other participant is given the adequate account details and accesses the draft.
- Another way in which terrorists use the internet is one which is even more veiled and concealed below the layers. This way is of steganography though which information is hidden in different media so it is not visible to others apart from the intended recipient.^

^See, Hummel, M. 2008. Internet terrorism. *Homeland Security Rev.*, 2 p. 117 - 130

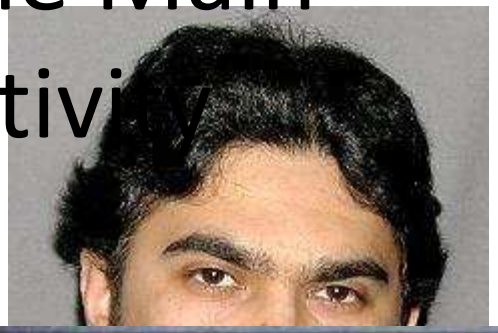
Details about Weapons

- *Jihad Recollections* provides for articles on "Remote Control Detonation", "Training with

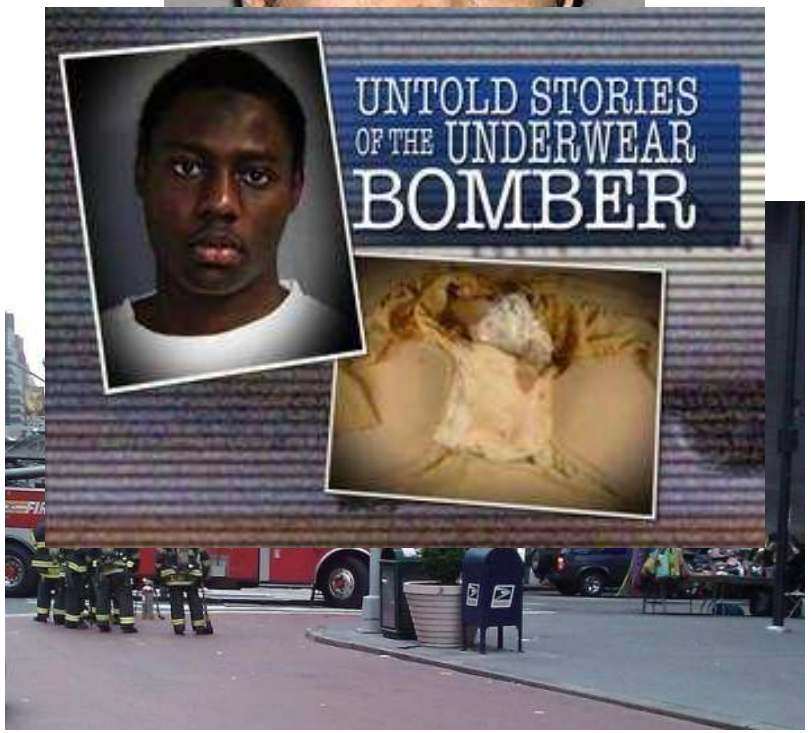


Inspire Magazine Issue 8, p. 33

Online incitement as the Main cause of terrorist activity



- Faisal Shahzad, failed to successfully detonate a time bomb in Times Square, New York, admitted to be influenced heavily by Anwar al-Awlaki whose videos of extremely convincing rhetoric were widely available online.
- Umar Farouk Abdulmutallab was significantly influenced by many fundamentalist Islamic chat rooms before he attempted to detonate explosives hidden in his underwear on board a Northwest Airlines flight.



See, Rollins, J. and Theohary, C. 2011. Terrorist Use of the Internet: Information Operations in Cyberspace. *Congressional Research Service*,
See, Council on Foreign Relations. 2013. Terrorists and the Internet.
See, Alia E. Dastagir, U. 2013. *Internet has extended battlefield in war on terror*

"bin Laden of the internet“: Online terrorism training

- **Anwar al-Aulaqi,** a fluent English speaker, al-Awlaki had used contemporary technology to communicate with a wide circle of people in the West.
- Despite being banned from entering the UK in 2006, al-Awlaki spoke via video-link in 2007–09 on at least seven occasions at five different venues in Britain.
- He gave a number of video-link lectures at the East London Mosque during this period.
- Abu Musab al-Zarqawi has an Al-Qaeda cell in Iraq which is exemplary in its use of the internet especially through posting extensive footage of bombings, decapitate hostages, two just before they were executed.

The Use of internet by terrorists is

The Indian Journey

Information Technology Act of 2000

Indian Computer Emergency Response Team (CERT-In). 2003

Section 66 F of the Act deals exclusively with cyber terrorism and punishes those who with intent to "threaten the unity, integrity, security or sovereignty of India or to strike terror in the people or any section of the people" carry out
denial of service attacks,
attempt to penetrate a computer source without authorization
or introducing any computer contaminants
And it is likely to cause death, destruction of property, damage, or disruption of supplies and services.
Section 84B makes abetment an offence.
Section 84C makes attempt to commit an offence also punishable

???

ion 69 of the IT Act deals with interception, ring and decryption of information .
s for the Controller to direct any agency of ernment to intercept any information through any computer resource if he it is expedient to do so in the interest of ereignty of the state.

Information Technology (Amendment) Act 2008.

which deals with requests of
directions to the Department
ations to remove websites.
hecks and balances on the guidelines required to block websites.

2012, 2013– mandatory VOIP encryption and Real Time Information Sharing

ncy and also has tie ups with onal bodies.

ation
Without authorization knowing that it might be used to damage the security of the State, lead to defamation, or incitement to an offense.
The punishment is imprisonment for life.

Responses of other States

- *United States of America's Patriot Act of 2001*
- *United States of America v.*
- *UK approach v. US approa speech*
- *United States of America v. Emerson Begolly*

United States of America v. Emerson Begolly, July 2013

"For those who decide to download, please keep in mind:

... Please use precautions when downloading by using appropriate anonymizing software.

Also, save it to a flash drive, not your hard drive.

And use extreme caution if attempting anything mentioned in this booklet; I don't want to see posted in the Ummah section "Suspected Islamist killed while mixing chemicals for bomb making."

Security Blogs CNN. 2013. *Prison for man who used Internet to encourage terrorism*. See *United States of America v. Emerson Begolly*,

Winning the War on terror

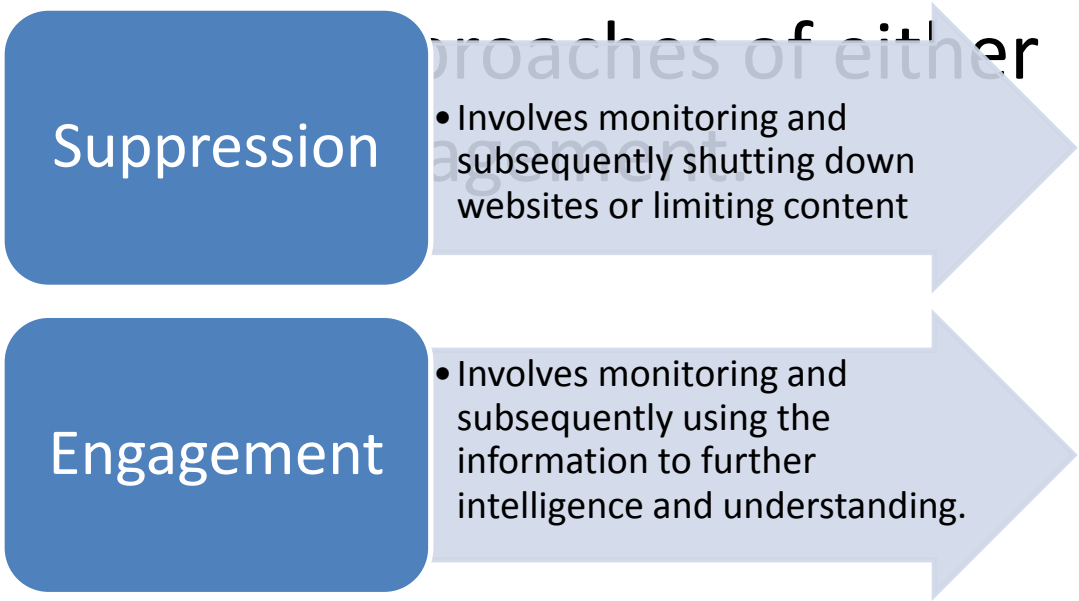
- It is impossible to win the war on terror unless the use of internet by terrorists is effectively monitored.^
- The United Nations has stated that the use of the Internet for terrorist purposes is a phenomenon which is growing rapidly and requires proactive response by all member states.^^

^ See, Dark Web Terrorism Research. 2013. *Dark Web Terrorism Research: Artificial Intelligence Laboratory : Eller College of Management : The University of Arizona*. [online] Available at: http://ai.arizona.edu/research/terror/ [Accessed: 26 Sep 2013].

^^2012. Use of the Internet for Terrorist Purposes. *United Nations Office on Drugs and Crime*, p. v. Available at: http://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf [Accessed: 29 Sep 2013].

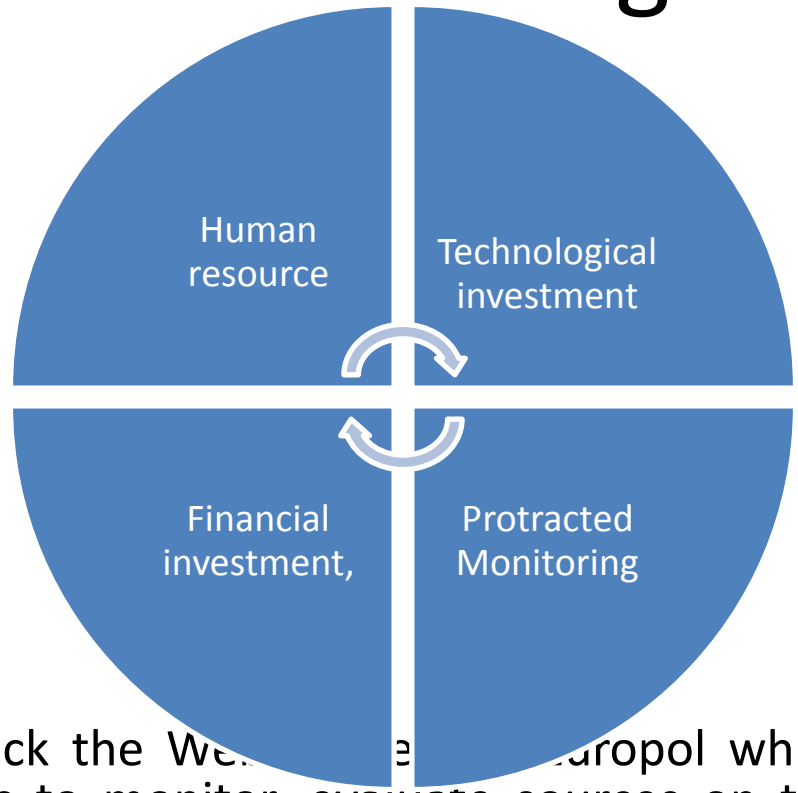
The Context of Policy

- The requisite policy in the context of the use of internet by terrorists can be viewed through t[illegible]proaches of either suppressi[illegible]agement.



Lewis, J. 2005. The Internet and Terrorism. *American Society of International Law Procedure*, 99 pp. 112-115.

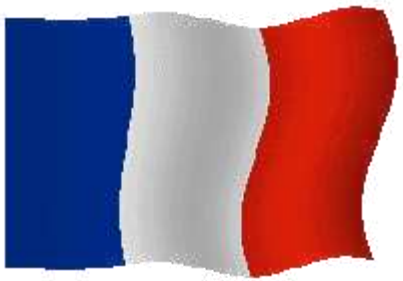
Monitoring



- Europe has Check the We[illegible]e [illegible]uropol which encourages all member nations to monitor, evaluate sources on the internet which further terrorism and pool in all the information at the Europol Office.
- Project Tempora under the aegis of the British Government Communications Headquarters(GCHQ) where electronic surveillance carried out clandestinely

Filtering

- Filtering is used by at least forty countries all around the world for issues related to religion, culture, politics, and sexuality among others.
- France uses limited filtering for websites that promote terrorism. These provisions were judicially held to be valid in the light of the fact that these were considered a reflection of balancing public order and freedom of communication.
- Australia, in May 2008, came up with a cyber-safety plan which aimed towards bringing in a cyber-security plan according to which Internet Service Providers necessarily had to filter out content which furthered terrorism.



Ronald J. Deibert, John G. Palfrey, Rafal Rohozinski and Jonathan Zittrain, 2008, *Access Denied—The Practice and Policy of Global Internet Filtering*, MIT Press, pp. 320

See, Breindl, Y. and Wright, J. 2012. Internet Filtering Trends in Western Liberal Democracies: French and German Regulatory Debates. *Internet Policy Review*, Available at: http://policyreview.info/articles/analysis/internet-filtering-trends-liberal-democracies-french-and-german-regulatory-debates [Accessed: 26th September, 2013].

Prosecuted only for the use of internet for terrorist purposes

Younis Tsouli, 2005, UK - for “the purchase, construction and maintenance of a large number of Web sites and Internet chat forums on which material was published which incited acts of terrorist murder, primarily in Iraq.”

Samina Malik, 2007, UK - found guilty of “possessing information of a kind likely to be useful to a person committing or preparing an act of terrorism.” Malik had downloaded and saved on her hard drive The Terrorist’s Handbook, The Mujahideen Poisons Handbook and other documents that appeared to support violent jihad.

India: The Way Forward

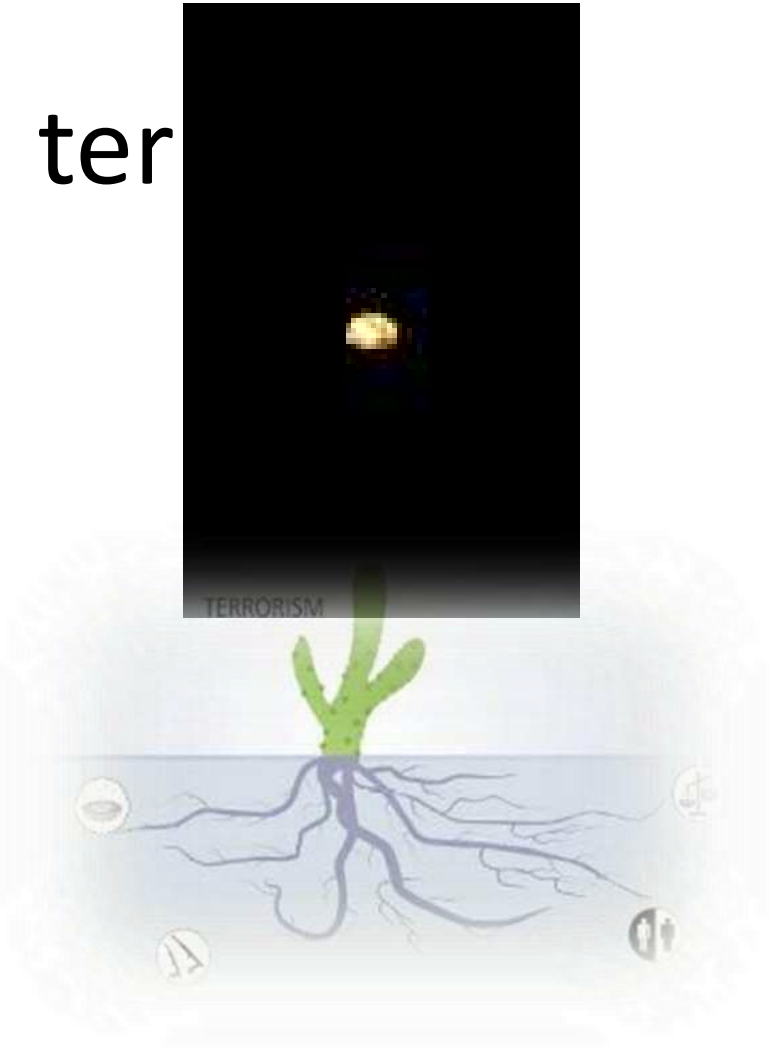
- Section 17 of the Unlawful Activities (Prevention) Act makes raising funds where there is likelihood that they will be used for terrorist acts an offence. Many websites, however, solicit contributions in kind in the form of supplies, or other fungible contributions like gold. To this extent there is a requirement for having a provision which specifically deals with material support is required.
- *"17. Punishment for raising ~~fund~~ material resources for terrorist act. Whoever raises ~~fund~~ material resources for the purpose of committing a terrorist act shall be punishable with imprisonment for a term which shall not be less than five years but which may extend to imprisonment for life, and shall also be liable to fine."*

India: The Way Forward

- **Section 18. Punishment for conspiracy, etc -Punishment for conspiracy, etc.** Whoever conspires or attempts to commit, or advocates, abets, advises or incites or knowingly facilitates the commission of, a terrorist act or any act preparatory to the commission of a terrorist act, shall be punishable with imprisonment for a term which shall not be less than five years but which may extend to imprisonment for life, and shall also be liable to fine.
- Instigation where there is no preparation or commission is left out.

the very root of ter

Terrorism never emerges in a vacuum but is a confluence and convergence of a multitude of interrelated factors.
The roots have to be uprooted for the cause to be solved.



Sinai, J. 2007. New trends in terrorism studies: strengths and weaknesses. *Mapping terrorism research: State of the art, gaps and future direction*, pp. 31-50.

We swear by Almighty Allah we will never stop fighting you. The only reasons we have done this is
because Muslims are dying every day. This British soldier is an eye for an eye a tooth for a tooth. We apologise that women had to see this today but in our lands our women have to see the same. You people will never be safe. Remove your government. They

WHY DID I CHOOSE AL QAEDA?

SHAYKH ABU MUSAB AL-AWLAKI

Because of the offers and warnings given to leave this path:

When I first pursued the path of jihad with Al-Qaeda, I faced many hindrances, among them:

a) Offers of desires:

Once I was told : you are a respected man, you are a caller of Islam, why will you distort your reputation by following Al-Qaeda? Then I was offered money indirectly.

b) Warnings:

They threatened me that people will be warned from me, they will hate and banish me from their *masajid*.They threatened me with jail, death and freezing my wealth and assets.

A number of months passed by without being called, no one would visit me and the brothers from Al-Qaeda had not assigned any work to me at that time. Those on the right path should always face trials, especially in the era of the enemy's dominance.

Allah says, ‹Do the people think that they will be left alone because they say, "We believe" and they

Because of logic reasons:

If we compare the *manhaj* of the *mujahideen* with their dissidents, we will find that the *mujahideen* confront force with force, strength with strength and iron is not dented except by iron. However, some think we do not have enough strength while they witness America's blood being spilled in large quantities, its war machines being destroyed, its prestige being degraded and its supporters being demolished. After all this, they call this *ummah* to truce and being soft with the infidels?! Where are their minds?!

A sane person stands for fighting the rulers, because they have supported the occupier with wealth, military, politics and media so that they maintain their thrones. This is oppression towards muslims. According to a sane mind, the oppressed should be supported until he retains his rights from the oppressors, because this is justice, and sound minds agree with justice.

Why did I choose Al Qaeda??


ISLAMIC EMIRATE OF
AFGHANISTAN
VOICE OF
JIHAD
Home
News
Weekly Analysis
Statements
Articles
Movies
Interviews
Contact us
WEBSITES
Islam
PASHTO
Arabic
Urdu
Farsi
Movie Section
Alsomod Website
LOGIN
COMMANDER SENATOR HAYATULLAH AND 3 GUNMEN KILLED IN GHOR
AMBUSH AND ARMED ATTACKS IN BADGHIS KILLS 2 PUPPETS, WOUND 2 OTHERS
8 INVADERS KILLED AS TANK OBLITERATED BY POWERFUL LANDMINE
TANK OF ROMANIAN INVADERS BLOWN APART BY ANTI-TANK MINE
LANDMINE TAKES OUT ENEMY VEHICLE IN TERENKOT
ENEMY VEHICLE DESTROYED BY LANDMINE
Comments of spokesman of Islamic Emirate for consideration by media outlets
-
Thursday, 02 August 2012 10:35
Thursday, 14 Ramadan

AQTWEETS

Comments on the Boston Operation

Collected by Al-Malahem Media from the mujahideen in the Arabian Peninsula

Abu Omar

I wish I was u #Tamerlan , u made a mother whose son has bn killed by US 2 smyl, I ask Allah to join us in Jannah.

Suleiman khan

I'm happy the 2nd anniversary of Sheikh Usama's martyrdom came while Americans mourn for the casualties of the blessed #Boston Bombing.

Abu Sameer Al-Amriki

We are drainin these kuffar's economy, no money no war no cry. Hope they increase the intelligence budget, wow! mo #taxes ! Thats all folks :)

Enemy of Tyrants

#Boston Bombings: Good planning, even better is turning the plan into action, and the best thing is that the operation exceeded expectations

Isaac X

Pressure cooker is well named by Jose Martinez, the #Marathon cooker raised Obama's blood pressure,oh! he became over-cooked by Boston steam.

Abu Shamel

Allahu Akbar, I feel so happy, only 2 soldiers of Allah defeated America, its army & #intel America can never stop the decree of Allah.

Abul Kheir Al-'Adany

They say the bros arent AlQaeda, they are lone wolves. That z wat ALQ wants, the #jihad project to be da ummah's prjct, I blve we are winning.

Abu Zaid

In other marathons the winners wear metallic medals, in this #marathon even the supporters got their metallic share ;)

HOW TO COMMUNICATE WITH US

Al-Malahem Media

If you are interested in contributing to this magazine with any skills - be it writing, research, editing, or advice - or have any questions for us, you can contact us at any of the email addresses below. We strongly encourage everyone to use the Asrar al-Mujahideen program to get in touch with us as was explained in our first issue. Please take special precautions when using the program in order to avoid detection from the intelligence services. Our public key can be obtained below.

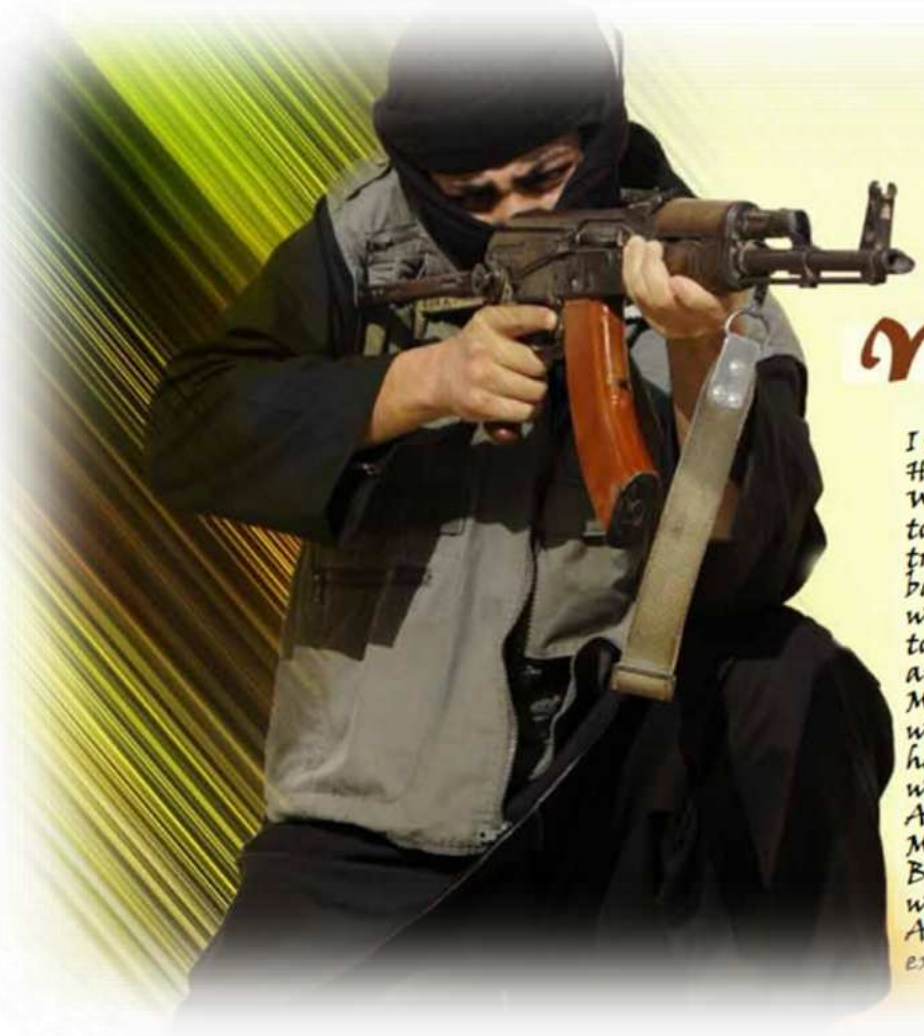
inscont@yahoo.com

pirezine@yahoo.com

Public Key for Asrar Mujahideen

pyHAv2KZ9gRLgLtwb4spOh0Xb1cFjsZ3tcbo6CnuUT+wOy74p7
uZnEbshDmLZFXVSe5RntWOI5m8+6rdl2HRcC401JZIgxsmMI5I
KaSLmepn6dElNoWTbVAjtsFERXcjtEOYkZvhQN3JCIAlNTs6Xk
I8zxI4U7VU2LoZzJw4QEdRcWutnZ3yCS5VxLnTOUtIawwZKd3C
HFLrkzmhEr5G1Nxe6+OlU6ZI8aomCOfwFkYLao28RLDL8vGag7
JFbxSXy7f6LOBrCCO8Mu4lfUpUGOZCGP4RXJfRLTEEmH9sFf/C
ZEwJEeWm9o2fo2yU/4nXMZIxN441iVzvlGTPbuPxy2f0+p/NMV
X+orew/pvkoofnw0lxFhVxYU99eixHBEgEQCAusw7FVGHbpRJg
gULtulLCd9VLAZRFvhyUk+lHPpsoedrQLvSoHlVC/Ga7ZIMJYX
ZPNuYqbafJpUZAqU1Ghq/YKIlCeClbLuWSaDErp+K3kMz0m6Ay
qCFcrv6gcxMqzHPIj9VJ3ZS97vMqgux3VeZKRG1TCV+Jm1whg8
/32OnzZILNtYBWLvWavpum

USA SHOULD WEIGH THE PRIORITY IT GIVES TO TRANSNATIONAL ATTACKS ON MUSLIMS AGAINST ITS HOMELAND SECURITY



Mujahid's Wish

I wish I am in America. It seems odd, right?
Hijra is not the end of a mujahid's ambition.
Walking with an AK is not the end of the road. I used to think the same as you, until I met brothers in the training camps, brothers who look into the enemies' barrels and see Jannah. Surprisingly, many of them wish to live in America. They have one gentle project to carry out; detonating even one bomb in any crowded area. They wish to be lone mujahideen like Tamerlan.
Many of the brothers who made Hijrah from the West wish they have a return ticket, returning home heading for mom's kitchen. Not to serve the kuffar with delicious and exotic meals, but to terrorize the American society until they cease to fight and assault Muslims.
Brother residing in the West, grab your chance and walk steadfastly towards your goal.
As for me here in Yemen, whenever I move around with explosives around my waist, I wish I am in America.

Tamerlan

Prosecuting Dark Net Market Places : Challenges and Approaches

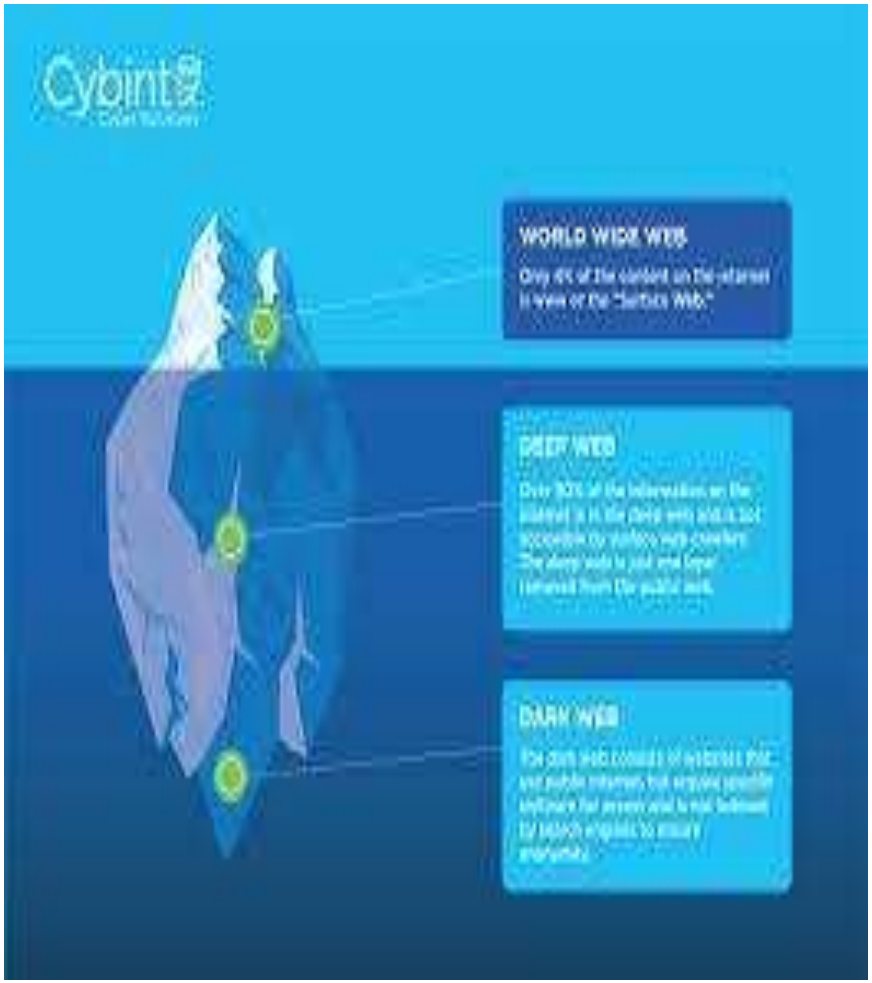
Introduction:

- Internet and the Dark Web

Introduction to the Dark Web and its functionality.

-
- What is Dark Web? -The non-www part of the web that uses internet but requires specific software, configurations, or authorization to access is known as Dark Web.
- This part is not navigable normally by using simple search engines.
- • How to access? – Using ‘the Onion Router’ (TOR). This TOR was designed by US Naval Research Lab as a pipeline to protect confidential government information. But there is absent of sufficient information as to how the usage changed. • Reason for the growth? – Anonymity.
- • Medium of Exchange? – Crypto currency.

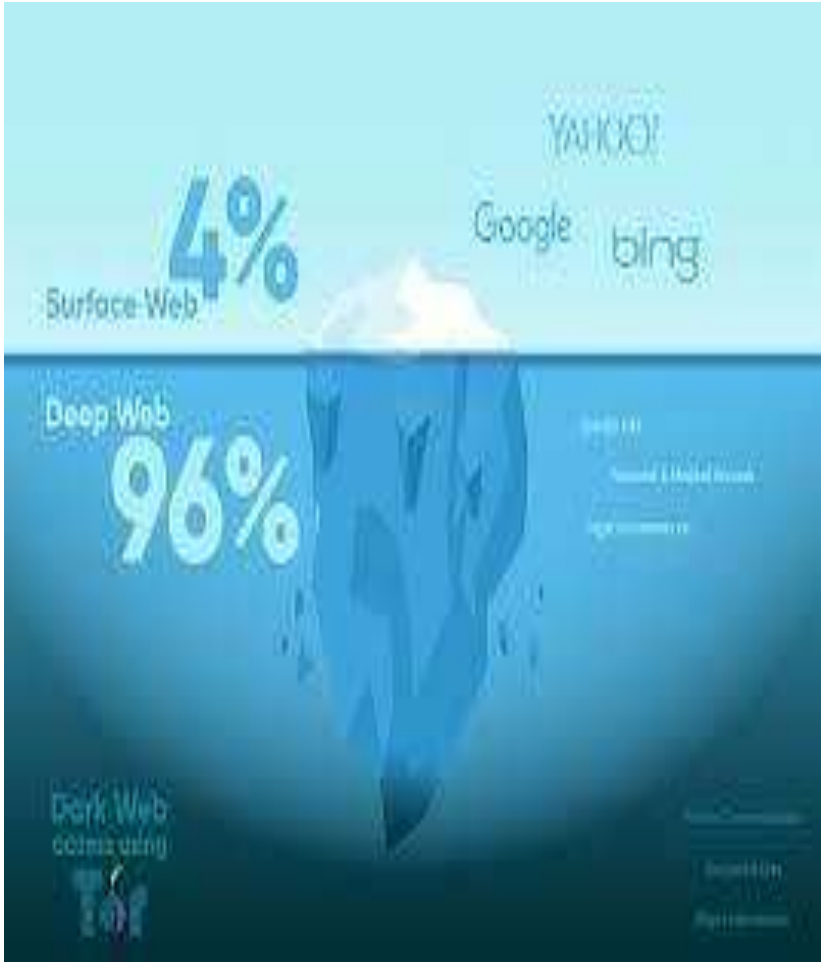
What exactly is Dark Net?



- Dark Net consist of the Deep Web and the Dark Web.
- WWW or the World Wide Web is only 4% of the content on the Internet which is often called the “clearnet” or “surface net”.
- Deep Web – 90 percent of the information on the internet is in the deep web and is not accessible by surface web crawlers.
- Dark Web – this consist of websites that use public internet but require specific software for access and is not indexed by search engines to ensure anonymity.

Dark Web - Marketplace

- An Amazon for Contrabands
- Examples of the kind of advertisements which are there on the dark net like “MDMA + free ecstasy”, “95% pure cocaine with world wide shipping!!” etc.



Various websites

- The Silk Road: A website primarily engaged in trade of illegal drugs. FBI was continuously trying to track the location of the server or the person involved, but all in vain. However, a mistake in the system allowed the FBI to trace it. The Mastermind was sentenced life imprisonment. •
- Playpen: A website primarily engaged in Child Pornography. Again, a glitch in the system allowed the seizure of the website. 186 people charged. However, the judge authorizing this charge was based in different jurisdiction from that of the server and hence, an issue of territoriality arose

- • Black Market Reloaded: A website engaged in huge trade of Illegal Weapons. Also Provided ancillary services like fake VISA, Passports, Counterfeit Money, etc. Michael Focia, the owner was arrested and prosecuted. •

- Darklode: An online, password-protected forum in which hackers and other cyber-criminals convened to buy, sell, trade and share information, ideas, and tools to facilitate unlawful intrusions on others' computers and electronic devices. Before becoming a member of Darklode, prospective members were allegedly vetted through a process in which an existing member invited a prospective member to the forum for the purpose of presenting the skills or products that he or she could bring to the group. Darklode members allegedly used each other's skills and products to infect computers and electronic devices of victims around the world with malware and, thereby gain access to, and control over, those devices.

lnkfzecnslxo6jqc.onion

Search

RAPTURE

EUR / BTC: 7,853.00 EUR / XMR: 270.79

Shop Messages Orders Account Profile Logout

0.0000 ฿
0.0000 ɱ

Barbiturates	6
Benzos	54
Cannabis	213
Digital Goods	7
Dissociatives	20
Ecstasy	55
Opioids	41
Other	414
Prescription	17
Psychedelics	19
RCs	0
Steroids	1
Stimulants	127
Weight Loss	0

Top 10 vendors

LetsWork 99 699
CokeCity 99 109
Suleyman 99 148
mdmaus 100 30
princess-peach 100 31
greenpirate 100 20
UKAlpzofficial 100 17
Mr.DT 100

Search | Select category | Relevance | Search

Afghan Heroin #3 // CLEAN and STRONG

0.1	8.22 EUR	0.3	22.6 EUR
0.5	35.96 EUR	1.0	61.64 EUR
3.5	205.48 EUR	7.0	400.67 EUR

Suleyman 99 148

AMNESIA DUTCH HAZE

3.5	42.41 EUR	7	70.1 EUR
14	132.17 EUR	28	247.08 EUR
56	482.68 EUR		

radarbreeder 97 32

Crack Cocaine // Pure Rock 10/10

0.1	9.62 EUR	0.3	26.02 EUR
0.5	36.22 EUR	1.0	62.24 EUR
3.5	237.67 EUR	7.0	424.42 EUR

Suleyman 99 148

Dexamphetamine 5mg - Original Aspen Pharma

5	29.53 EUR	10	52.51 EUR
30	137.85 EUR	50	196.93 EUR
20	98.46 EUR	40	170.67 EUR

SharkTank 100 3

Listing image STRAWBERRY DOG

3.5	41.67 EUR	7	65.32 EUR
14	120.5 EUR	28	236.51 EUR
56	461.75 EUR		

1 LB Light Dep Skittles

1372.2 EUR (0.173806 ฿)

Silk Road

anonymous market

Search

Drugs

Cannabis

Opioids

Stimulants

Cocaine

Other

Prescription

Psychedelics

Apparel

Art

Books

Collectibles

Computer Equipment

Custom Orders

Digital goods

Drug paraphernalia

Electronics

Erotica

Fireworks

Food

Forgeries

Hardware

Home & Gardening

Jewelry

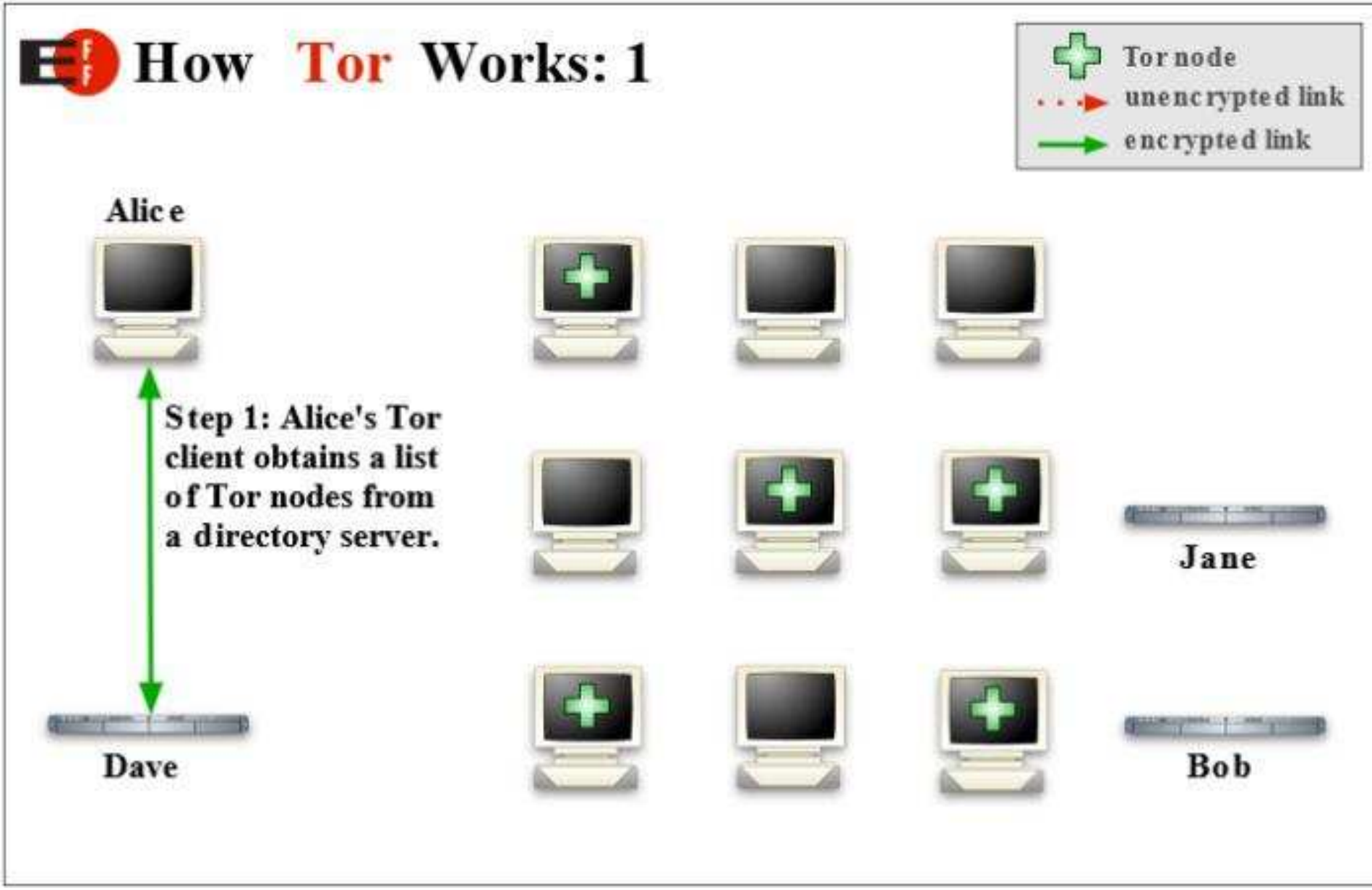
THE ONION ROUTER

- TOR or the onion router, in its most basic form, is an interconnected web of computers throughout the globe that allows for anyone to access the Internet with **COMPLETE ANONYMITY.**

About TOR:

- TOR in itself is not illegal. In fact it is partially supported by the US Govt and is used around the world to promote free speech and privacy.
- But the anonymity which TOR brings has a darker side – which is used by criminals to evade law enforcement detection.
- TOR requires only a download of the TOR Browser from the Internet.
- Once activated, TOR routes your Internet traffic, via an encrypted link, through three other computers (known as “nodes” or “relays”) that are part of thousand of computers in the TOR network, to reach its ultimate destination on a site on the Darknet.

How Tor Works: 1



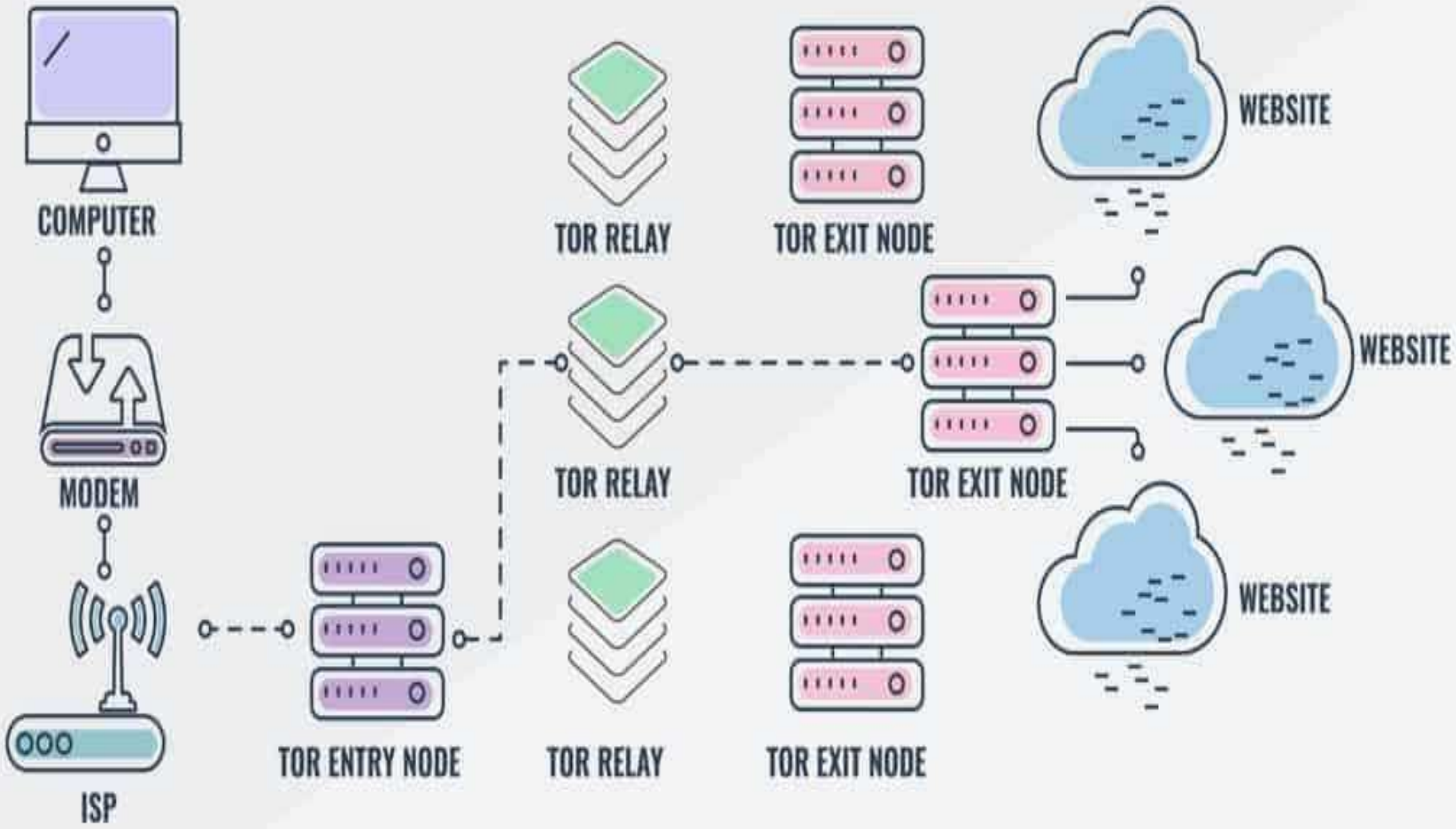


FIG: Simplified Tor Connection

Why does it use these multiple computers?

- Because the use of Encryption and relays through the TOR network renders the true Internet Protocol (IP) address for all traffic to and from the destination website on the darknet completely anonymous.
- Further, Marketplaces like these requires their users to transact in Cryptocurrencies which add another layer of anonymity. Like Bitcoin, Monero, Ethereum.

TOR uses a web address that end in “.onion” and not “.com” or “.org”

This makes the determination of true IP address of the Marketplace servers – a challenging task, since identifying such servers would ultimately be useful in identifying where these servers are located.

Scope of Problem:

- Deepdotweb.com – a site on the clearnet to educate the people about darknet reported that there are 23 darknet market places and vendor shops (single vendor) as of October 15, 2018.
- Top Markets includes – Dream Market, Wall Street Market and Point Free Market.
- Wall Street Market – the second largest marketplace on darnet according to this website has 3000 vendors and over 500,000 customers who sell and buy drugs, counterfeit items, jewellery, stolen credit cards, child pornography etc.

Identifying Darknet Market Places (Hallmarks of such Marketplaces)

- Although each darknet marketplace is different, they typically share similar organizational structures which is modeled after traditional e-commerce sites (Imagine Amazon).

- 3 main actors:
- Administrators
- Moderators
- Vendors (Sellers)

Administrators

A darknet marketplace has one or more founders, who are responsible for establishing the marketplace, developing the code that makes the marketplace run, and advertising the marketplace to attract vendors and buyers.

They have to maintain the Integrity of the Marketplace along with providing a good user experience for both vendors and buyers!!!

They may also hire “employees” for “tech support” who can help service user complaints regarding the functionality of the marketplace.

Moderators:

- They help to resolve disputes that arise between vendors and buyers.
- For example, if a buyer pays for Methamphetamine (an illegal drug), but does not receive the product or recieves inferior product, a moderator would need to resolve the dispute between the parties.

Use of Cryptocurrency:

- Integrity in the Dark Marketplace!!!
- Now, this need to ensure that orders are fulfilled faithfully – marketplaces hold cryptocurrencies in escrow.
- Escrow is basically when Buyers and Vendors are required to consign a certain amount of cryptocurrency with the marketplace, so that when a transaction takes place, it is paid for out of the escrow account.

Investigative Plan – New Means, Old Types of Crime

- There is an additional layer of Sophistication.
- The use of the darknet involves a layer of anonymity, and behind the layers of onion lies the traditional criminal enterprise.
- Accessing the dark marketplace is simply one component of the new criminal enterprise.
- Once this aspect is deciphered, the investigation reverts back to the classic law enforcement investigation involving narcotics, fraud, theft of identity, hacking etc.
- Compartmentalization – a hallmark of sophisticated conspiracy – only becomes more intricate with the injection of the darknet.

New Means, Newer Investigative Techniques

- Start off from the Clearnet.
- With these information, investigators and prosecutors should consider seeking non-content information, such as subscriber information, IP Address information, etc.
- Now, a unique component of investigation involves cryptocurrencies. Some of them has anonymity feature.
- Zeash and Monero has encrypted ledger making investigation more difficult.

Time is of the Essence

- Evidence is always fleeting on the internet.
- “Exit Scams” – Administrators and operators of Darknet Marketplace may wait for significant amount of virtual currency to sit in escrow, freeze the ability to transact with the escrow and then decide to instantly cease operation of the marketplace and pilfer all of the consumers funds that were pending release to various vendors.
- Once this is done, the entire marketplace is obliterated and investigation is set back.
- Thus, have to act fast.

Challenges and Opportunities:

- Now, the biggest challenge is that when law enforcement is able to locate the physical location of a server hosting a darknet marketplace, they are often in countries outside of where the crime has taken place. Here, USA [Example – The Silk Road Servers were in Reykjavik, Iceland].
- Data Exchange, Interpol – there are challenges to investigation when your evidence is located in different country. 70 countries agreed to have a designated point of contact to act on preservation requests for electronic evidence. [time pressure]

Even if Evidence is Preserved, it still has to be obtained

- To obtain evidence either electronic or otherwise, there are few alternatives:

1. Informal Cooperation.
2. Traditional Mutual Legal Assistance Treaty (MLAT) or other formal request
3. Open MLAT
4. Joint Investigative Team Agreement (JIT).

- Now, how the investigation authorities will proceed depends on the regime and preferences of the foreign country, the need of the investigation, and concerns about possible discovery obligations or litigation risk over Fourth and Fifth Amendment issues from foreign government action being considered part of a Joint Venture.

US Supreme court Decisions

- There is no U.S. Supreme Court decision yet.
- The appellate court decisions are very few in number and offer limited guidance.
- The basic legal analysis begins with the Fourth Amendment to the U.S. Constitution's protection against warrantless searches by law enforcement, absent special circumstances.
- Initially, the assumption was that the Fourth amendment rights are applicable only for physical searches. Hence, the Dark Web poses a new question. • Specific Cases:
- Katz v. United States: Accused involved in Illegal Gambling. Evidence obtained from a warrantless wiretapping of the phone. The Supreme Court held this evidence to be inadmissible.

- • Kyllo v. United States: The accused was growing Marijuana in his home. Police used an infrared radiation based device to obtain hot-spots in the home involved in the processing of marijuana. Thereafter, police obtained a search warrant on the basis findings of the infrared device. The Court held that Kyllo did have an expectation of privacy and that the use of the advanced infrared technology was beyond a simple observation by the naked eye, raising the technique to a search subject to the Fourth Amendment's protection.
- • United States v. Jones: The accused was involved in illegal trafficking of the Cocaine. The police installed a GPS based device to track the movement of his vehicle. The Supreme Court ruled that the placement and tracking of the GPS device was an unauthorized, warrantless search of the subject's vehicle.
- • Riley v. California, Carpenter v. United States: Search of the phones of the accused without warrant was held to be against the constitution.

4th 5th 6th Amendments in the US Constitution.

- 4th - The Constitution, through the **Fourth Amendment**, protects people from unreasonable searches and seizures by the government. The **Fourth Amendment**, however, is not a guarantee against all searches and seizures, but only those that are deemed unreasonable under the law.
- 5th - No person shall be held to answer for a capital, or otherwise infamous crime, unless on a presentment or indictment of a Grand Jury, except in cases arising in the land or naval forces, or in the Militia, when in actual service in time of War or public danger; nor shall any person be subject for the same offence twice
- 6th - In all criminal prosecutions, the accused shall enjoy the right to a speedy and public trial, by an impartial jury of the State and district wherein the crime shall have been committed, which district shall have been previously ascertained by law, and to be informed of the nature and cause of the accusation

Tricky Terrain: whether a method adopted will create more future headaches ?

- JIT and the Amendments
- JIT as opposed to other processes, would result in a court considering the foreign actor part of a joint venture which could have constitutional implications and create discovery obligations.
- Discovery – similar thorny area as well.
- The closer the degree of cooperation with the foreign officials, the more likely the US Prosecution will be held responsible for all Brady and Giglio materials in possession of foreign authorities.
- Brady v. Maryland – requires the prosecution to disclose all material exculpatory evidence.
- Giglio v. US – non disclosure of a promise not to prosecute a witness if he cooperated with the government was a violation of due process.

Legal Toolbox for attacking darknet market places and related actors

- Conspiracy – thus traditional charges
- Racketeer Influenced Corrupt Organization (RICO).
- Substantive other charges like access device fraud, identity theft etc.
- Asset forfeiture could be a powerful tool too.

Following Money : Targetting Exchangers

- All participants in the darknet are in it for the Money.
- Thus, another investigative approach is to target and identify vendors and/or higher level darknet marketplace operators is to focus on these exchanges of currencies.
- Undercover operations in US targeting darknet vendors (June 2018).
- Prosecuting person to person exchangers. Bitcoin exchangers has to register with Financial Crimes Enforcement Network (FinCEN) in compliance of Bank Secrecy Act.
- If not register – the actors of darknet violates US Penal Code.