



RAND *Europe*



The New Terrorism and the Information Society


Cyber-Threats in the Information Age

Presentation to CASIS – 27 September 2002, Ottawa

Dr Kevin A. O'Brien
Senior Policy Analyst

RAND Europe – Using Partnerships in Europe to Create Awareness in the Information Society

www.randeurope.org



These are personal reflections and do not necessarily represent the views of RAND Europe, its parent RAND, or of any of its sponsors

- What is the CNI?
- What is terrorism? What is cyber-terrorism?
- Asymmetric Actors and Cyber-Threats
- Hype or reality? Security in the Information Age
- Terrorism in Cyber-Space: threats and TTOs
- Cyber-Threats: Evolution, Indicators & Warning
- CIP & Intelligence: Centralisation & Information-Sharing

The Critical National Infrastructure (CNI)

Those physical and information technology facilities, networks and assets whose disruption or destruction would have serious impact on the health, safety, security, economic well-being of citizens or on the effective functioning of governments and businesses

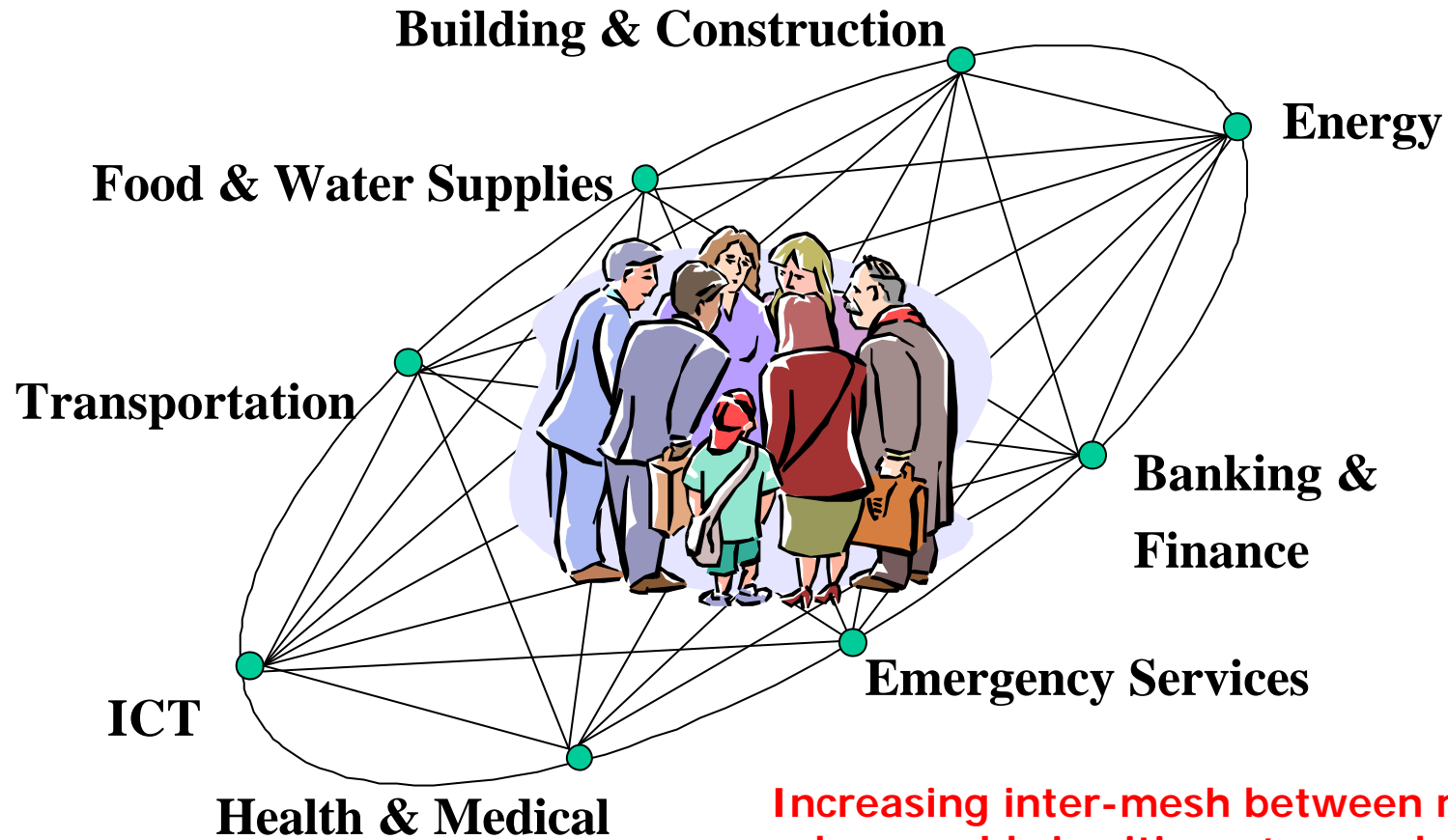


See definition on terrorism later

Critical Infrastructures are:

- systems whose incapacity or destruction would have a debilitating impact on the defense or economic security of the nation (US PDD-63)
- Essential focus on Critical National Infrastructure (CNI) & Critical National Information Infrastructure (CNII)
 - Including concern with International Information Infrastructures (III)
- Currently (post-9/11) entwined with Homeland Security approach in US, UK and elsewhere

The Critical National Infrastructure (CNI)



Context

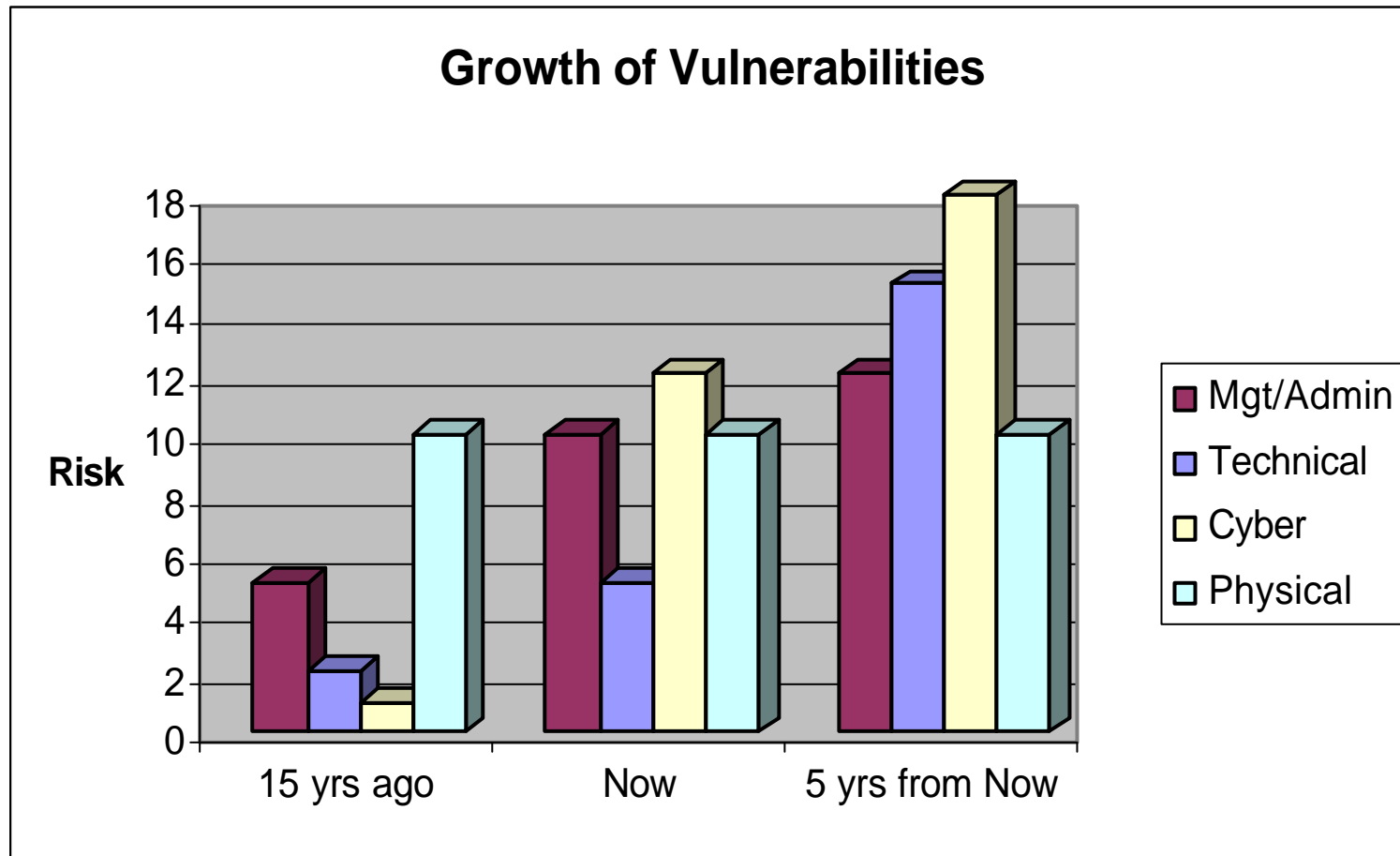
- Development of IT & Communications a critical component of globalisation
- E-Commerce, Evolution in Military Affairs, Business Efficiencies, Critical Infrastructures
- Rapid Growth translating into Dependence and Interdependence
- Sophistication and attendant Dependencies also source of vulnerabilities

- Globalised, interconnected world
 - Fashion, music, finance ... computer viruses
- In C20th, massive societal disruption required aerial bombardment, blockade
 - Now, can be undertaken by asymmetric opponents
- Post Sept-11, disruption was only a by-product...

- The problem is threefold
 - contemporary society is inherently more vulnerable to malicious attacks
 - terrorists use modern infrastructures to attack them
 - shocks to one infrastructure may cause ripple effects in others

- The means of possible attacks on our infrastructures are varied
 - include physical attacks, cyber-attacks, NBC attacks and psychological attacks (e.g. through market and media manipulation)
 - “old terrorism” – focusing on individuals as targets and using conventional weapons – has not been replaced by the new terrorism

- The transition to a more technology-intensive economy, demographic and societal change, and growing interdependencies look set to increase the vulnerabilities of major systems in the 21st Century
- The provision of health services, transport, energy, information and telecommunications, food and water supplies, safety and security are all examples of vital systems which can be severely damaged by a single catastrophic event, a chain of events, or the disastrous interaction of complex systems (OECD)



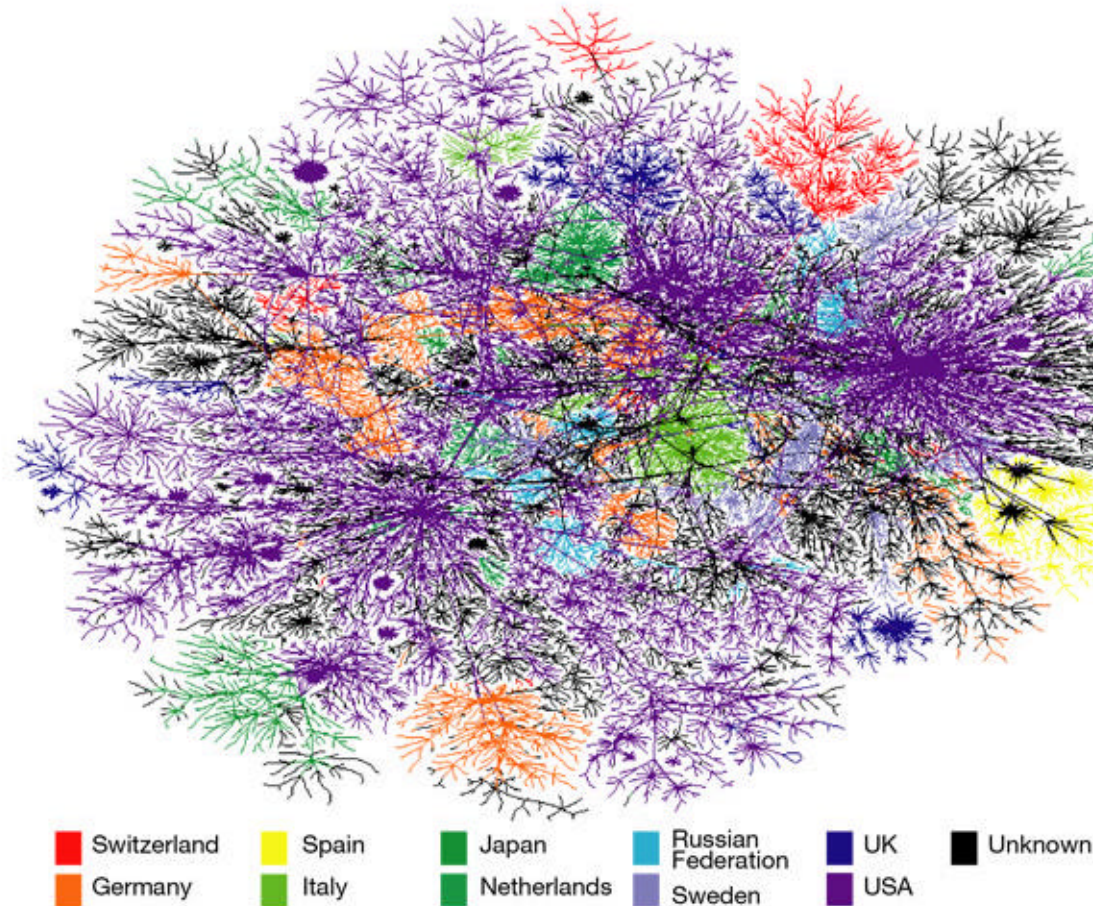
- Redirecting terrorist violence away from humans to infrastructures
 - 1990s: IRA use this concept very effectively, sufficiently occupying the resources of the British government through infrastructural attacks (as opposed to direct attacks against people)
 - In the future, stock markets or other primary financial institutions might become high-profile targets and the most effective means of accomplishing a terrorist's goal
 - More damage would be accomplished by taking the New York Stock Exchange offline for a few days rather than actually bombing a building

Danger of increasing moves towards Nuclear,
Biological, Radiological, Chemical attacks – forgets...

Increasing
propensity towards
Infrastructural
Attacks

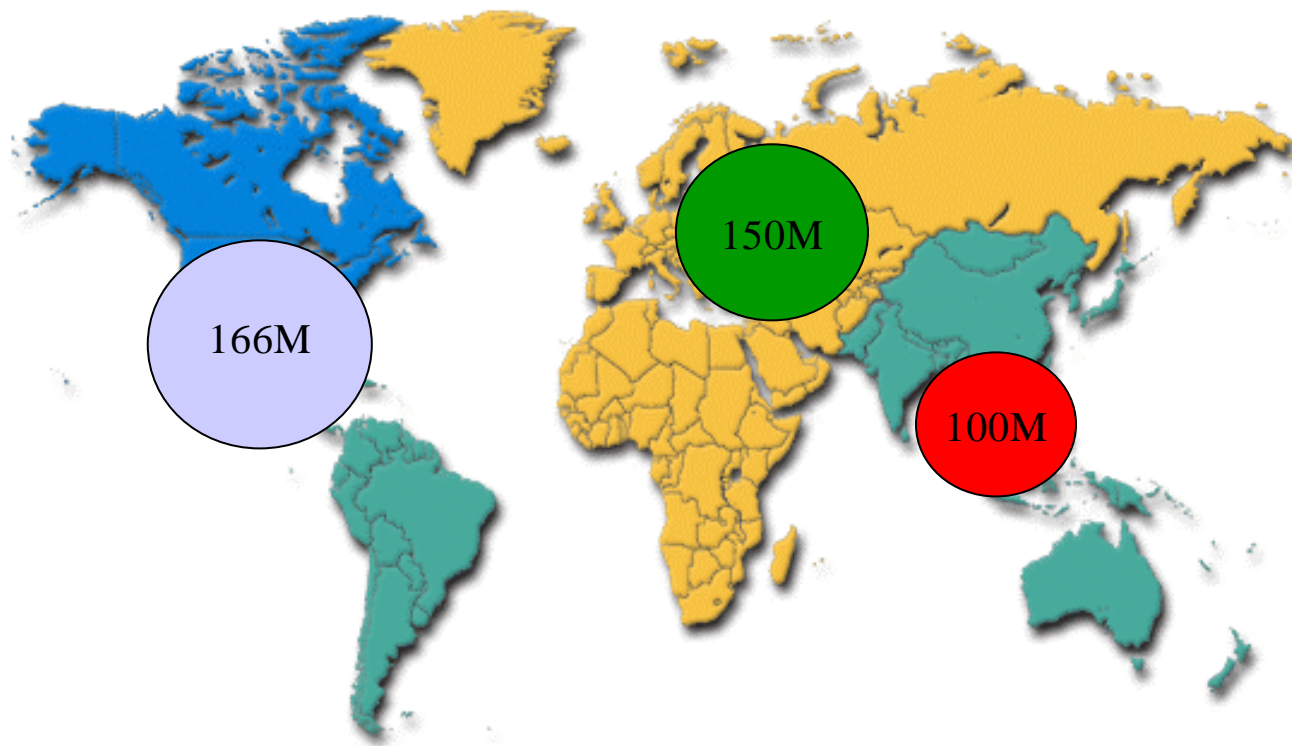


The Vulnerable Internet?



Changing Face of the Internet

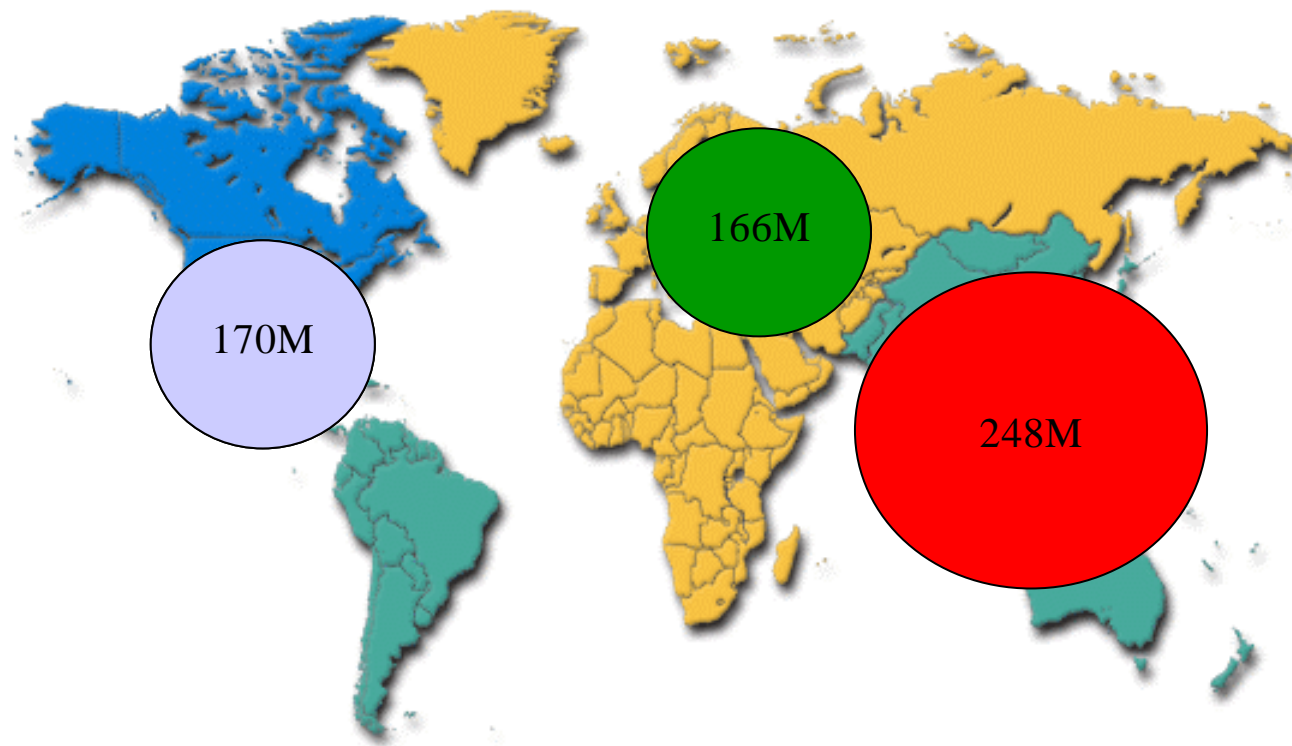
2002



Source: Cisco

Changing Face of the Internet

2005



Source: Cisco

The unlawful use of – or threatened use of – force or violence against individuals or property to coerce or intimidate governments or societies, often to achieve political, religious, or ideological objectives

(US Dept. of Defense)

Terrorism is the “**use or threat of action** [which]:

- involves **serious violence against a person**;
- involves **serious damage to property**;
- **endangers a person's life**, other than that of the person committing the action;
- **creates a serious risk to the health or safety** of the public or a section of the public; or
- is designed seriously to interfere with or seriously to disrupt an **electronic system** [– and]
- the use or threat is designed to **influence the government** or to **intimidate the public** or a section of the public; and the use or threat is made for the purpose of **advancing** a political, religious or ideological cause (UK *Terrorism Act 2000*)

1. political borders are irrelevant to the group's objectives, and they do not act on behalf of any particular state
2. membership and resources are drawn from supporters in more than one state
3. area-of-operations, including targeting, transcends state borders

- **Large Transition States** (China, Russia, and India)
- **Rogue States** (Syria, Libya, Iran, North Korea, Indonesia, Zimbabwe, Liberia, or Burma)
- **Failed States** (ruled by warlords and despots – with the patronage of organised crime, trafficking in weapons, narcotics, stolen goods and human beings)
- **Transnational Organised Criminality** (becoming much more sophisticated, transnational, and involved in conflicts in a manner similar to a rogue actor or terrorist)
- **Transnational Terrorism (including extremist religious, anarchist, or patriotic forces)** (large groups have come to the fore, including Islamic fundamentalist factions – many of which are linked to al-Qaeda)

**Rogue States, Transnational
Organised Crime (TOC), &
Transnational Terrorist
Organisations (TTOs) now
making the migration to cyber-
space**

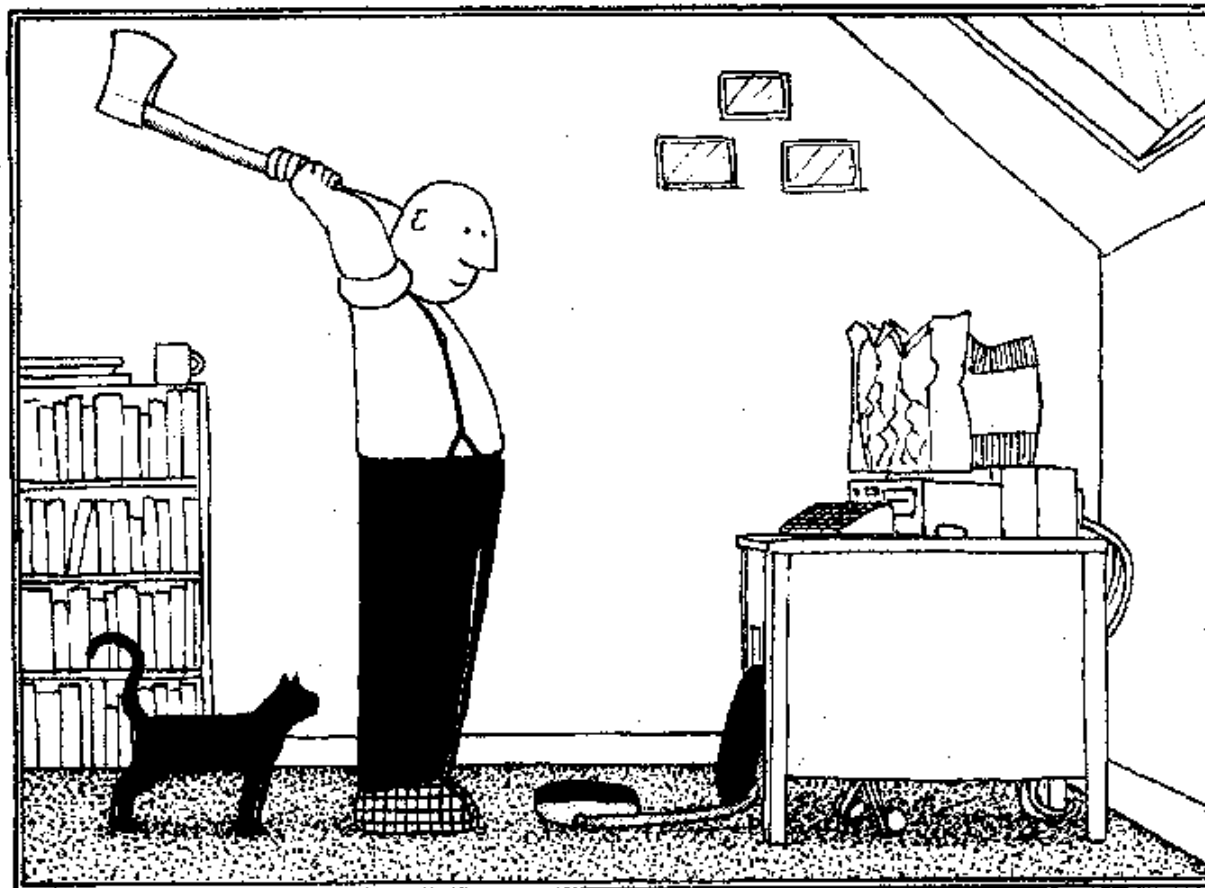
"Cyber-Terrorism" in criminal statutes on terrorism:

- designed seriously to interfere with or seriously to disrupt an electronic system (UK *Terrorism Act* 2000)
- In warfare as well as in business, IT is the great equaliser: its low financial barrier to entry relative to heavy industry allows even the poorest organisations an IT effectiveness equal (or nearly equal) to large corporations

"Cyber-terrorism" vs. "cyber-crime"

- **Cyber-crime:** real-world traditional criminal activities carried-out using computers, networks and other hi-tech means (ie. fraud, paedophilia)
- **Cyber-terrorism:** malicious activities carried-out against networks, networked systems and the Internet
- ↳ **Hacking and viruses, Cyber-terrorism, Spoof websites, Virtual countries, Distributed denial-of-service attacks**
- Legislation does not differentiate but can contradict (ie. *Computer Misuse Act 1992* vs. *Terrorism Act 2000* – "hi-tech crime" vs. "cyber-terrorism")

Destruction of Information & Computer Networks



Actual nature of the threat

- Is this "terrorism"??
 - Do cyber-attacks cause (mass) casualties?
 - Does it "terrorise"? Propaganda factor: "to be seen"
 - Certainly "(organised) political violence"

CRIME ➡ TERRORISM ➡ WAR

- Danger not from "electronic Pearl Harbour" but from "electronic Exxon Valdez" or "electronic Bhopal"

Hype or Reality?

New Concepts of Security

Cyber

Risk & Vulnerabilities

**Critical National
(Information) Infrastructure**

Attack & Early Warning

Brand

4 levels of threat

Real

Security Intelligence loss

**National security & well-
being**

Attack warning

Prestige

Multi-levels

Quantifying & Valuing the Threat

Cyber-Threats

- Cyber-terrorism is not only about damaging systems but also about intelligence gathering
- Intense focus on 'shut-down' scenarios and tight analogies with physically-violent techniques ignore other more potentially effective uses of IT in terrorist warfare: intelligence-gathering, counter-intelligence and disinformation
 - ↳ For example, attacking an information system would be a good way to either distract the target or otherwise enable the terrorist to perform a physical attack

Transnational Terrorist Organisations in Cyber-space

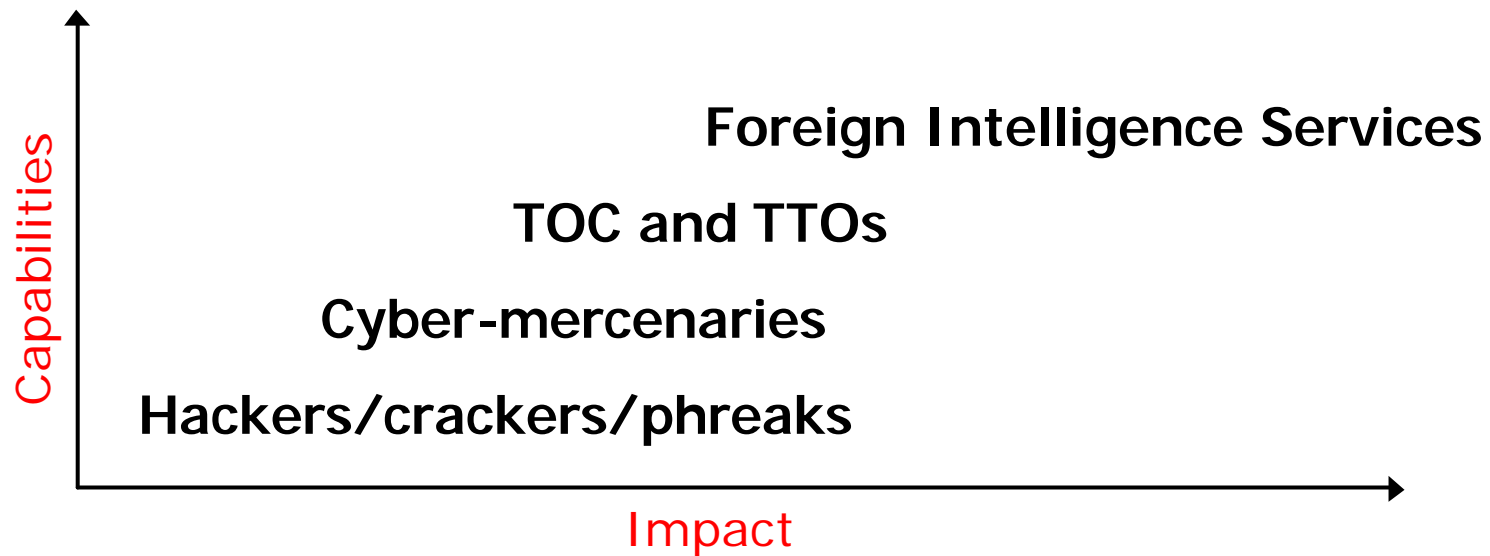
- use of new/Internet-based technologies for coordinating, communicating and supporting the planning of terrorist (cyber-based and real-world) activities
- “Virtual sanctuaries”
- Emigration: LTTE & SNLA cyber-attacks
- al-Qaeda & Cyber-space
- Aum Shinriyko & Tokyo Subway Attack

Terrorists Using Cyber-space & New Technologies

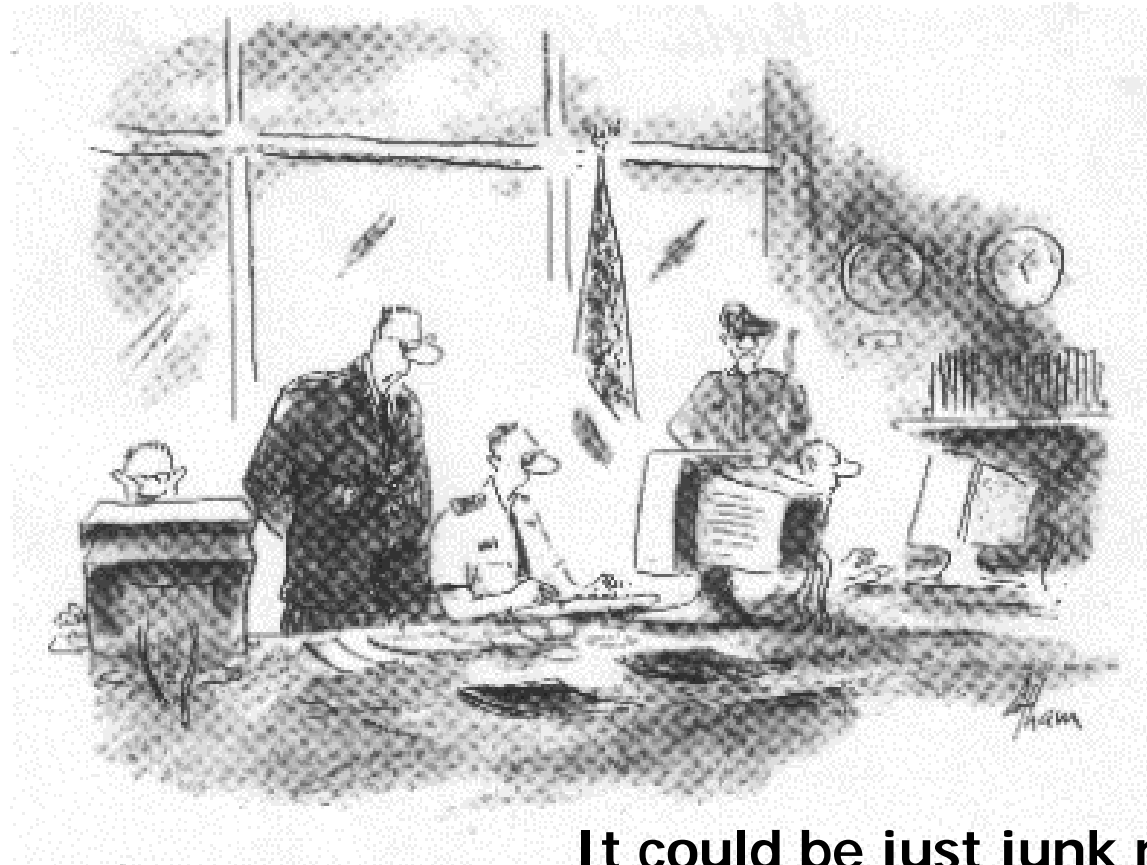
- The threat from cyber-terrorism as well as the significant use of cyber-space continues to grow exponentially
- “The advent of new technologies, advanced means of communication and ever-more sophisticated ways of moving money around have already influenced the way terrorists operate and will continue to do so. Terrorist organisers and fundraisers no longer have to be in the same country as their target or indeed as each other. Their communications to each other can be encrypted. And there is the potential, if the right targets are hit (such as strategic computer systems running banking or air traffic control operations), to affect thousands or even millions of people.” (UK Home Secretary 1998)

Evolution of the threat – Tracking

- 4 levels of threat

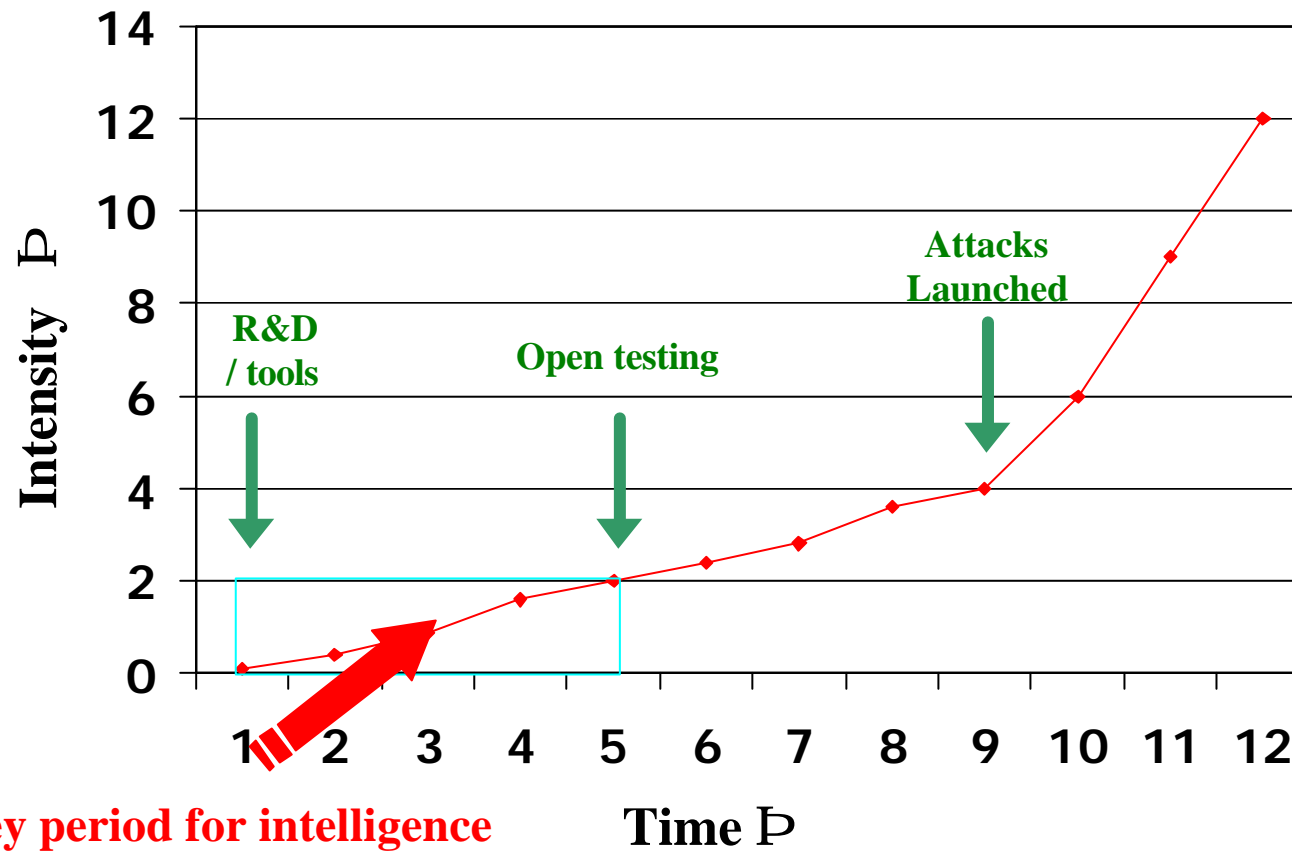


Evolution of the threat – Tracking – What do we know?



It could be just junk mail, Colonel, or the beginning of a major enemy attack...

Evolution of the threat – Tracking



Key period for intelligence detection & deterrence!!

Evolution of the threat – Incidents

- *Solar Sunrise* - not Iraq, but US & Israeli teens
- *Moonlight Maze* - ???
- E-Intifada – global not local
- China-Taiwan Cyber-war
- Guerrilla Warfare in Cyber-space?
- Attacks on the Internet itself – 13 root servers (.com, .net, .org)
- 9-11: what if al-Qaeda had impacted the NYC Emergency Response communications system, thus hampering the rescue and recovery efforts?

Evolution of the threat – Indicators & Warning

- Governments face a challenge in developing risk management strategies in response to vulnerabilities in society's critical and information infrastructures – and threats that range from the nuisance to the catastrophic
- Analysing the threat is normally key to risk management and to designing management strategies
- Problem is in adapting these mechanisms to the new risk environment
- Because of the difficulty of understanding cyber-threats, most focus has been upon vulnerability-based and impact reduction strategies that concentrate on identifying and mitigating societal vulnerabilities

Evolution of the threat – Indicators & Warning

- The current information systems security paradigm is a reactive model that involves detection of – and reaction to – attacks once they are underway
 - There is a pressing end-user need to increase warning time so that organisations can take preventive steps to minimise their losses from cyber-attacks
 - Require methodologies for predicting cyber-attacks, based on understanding, and thereby predicting, the activities of sub-state actors
- ↳ Devise and test pre-attack indicators and threat profiles in order to increase warning time

- Need to develop Predictive Indicator summaries focused upon the problem of defining, categorising and correlating indicators of potential computer network attack by looking outward at the threat spectrum as well as inward at the pattern of incidents
- This approach allows the warning mechanism to focus upon motives and intentions of potential attackers, in addition to capabilities

- Need to develop an understanding of how new threats can be used to craft coercive policies to affect the behaviour of these actors
 - Includes the use of criminological and coercive literature to match potential threat actors with potential policies
- An initial characterisation of these policies is
 - Denial; Detection/Apprehension; Punishment; Pre-emption

- Q: how should intelligence be perceived, used, etc in relation to cyber-space?
 - do traditional methodologies, norms and operational rules apply?
 - should cyber-space (for lack of a better term) be seen as another fully-developed operational environment much as the streets of Berlin are?
 - how does one conduct "operations" in cyber-space? are clandestine/covert actions applicable? if so, how?

"Cyber-intelligence"?

- ultimate aim being to develop new intelligence collection and operational methodologies to develop better threat profiles for indicators and warning of potential cyber-attack
- ⊕ differentiating between attacks which use cyber-space as a conduit AND attacks on cyber-space itself

- Issues to be considered:
 - use of new/Internet-based technologies for coordinating, communicating and supporting the planning of terrorist (cyber-based and real-world) activities
 - 'net camouflage' and anonymisers
 - the applicability of counter-intelligence practices to cyber-based information operations (including computer network operations)
 - the aspects of threat- and actor-profiling outlined above

"Cyber-intelligence"?

- Issues to be considered:
 - Search engines (Google primary)
 - Data mining/data dumping
 - Knowledge Management parameters
 - More...

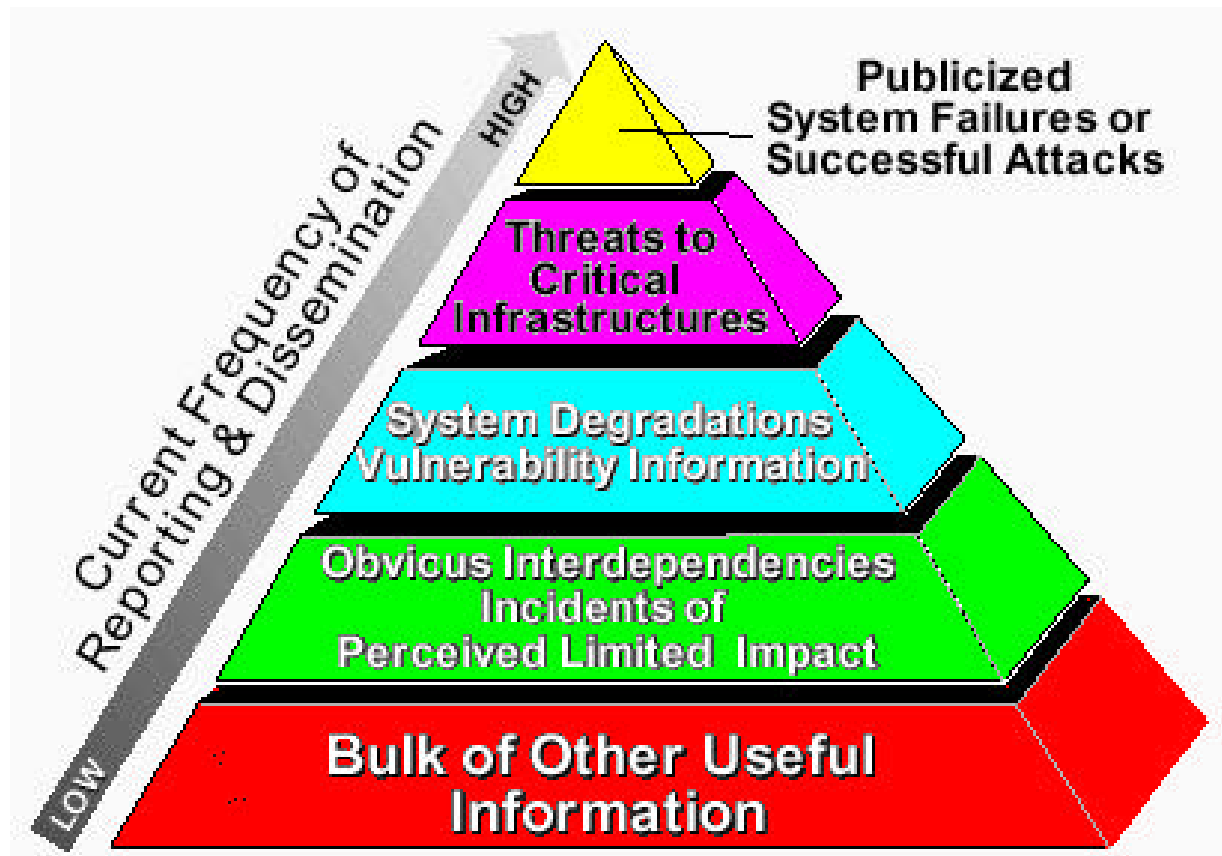
- ✍ Overwhelming problem of OTT collection capabilities vs. bare-bone analysis capabilities

"Cyber-intelligence"?

- Issues to be considered:
 - Time value of info & info-superiority
 - How to "kill/eliminate" actor? Can you?
 - Pursuit" in cyber-space considerations (legislation, security, borderless, ID switching, etc)
 - Legislation overall

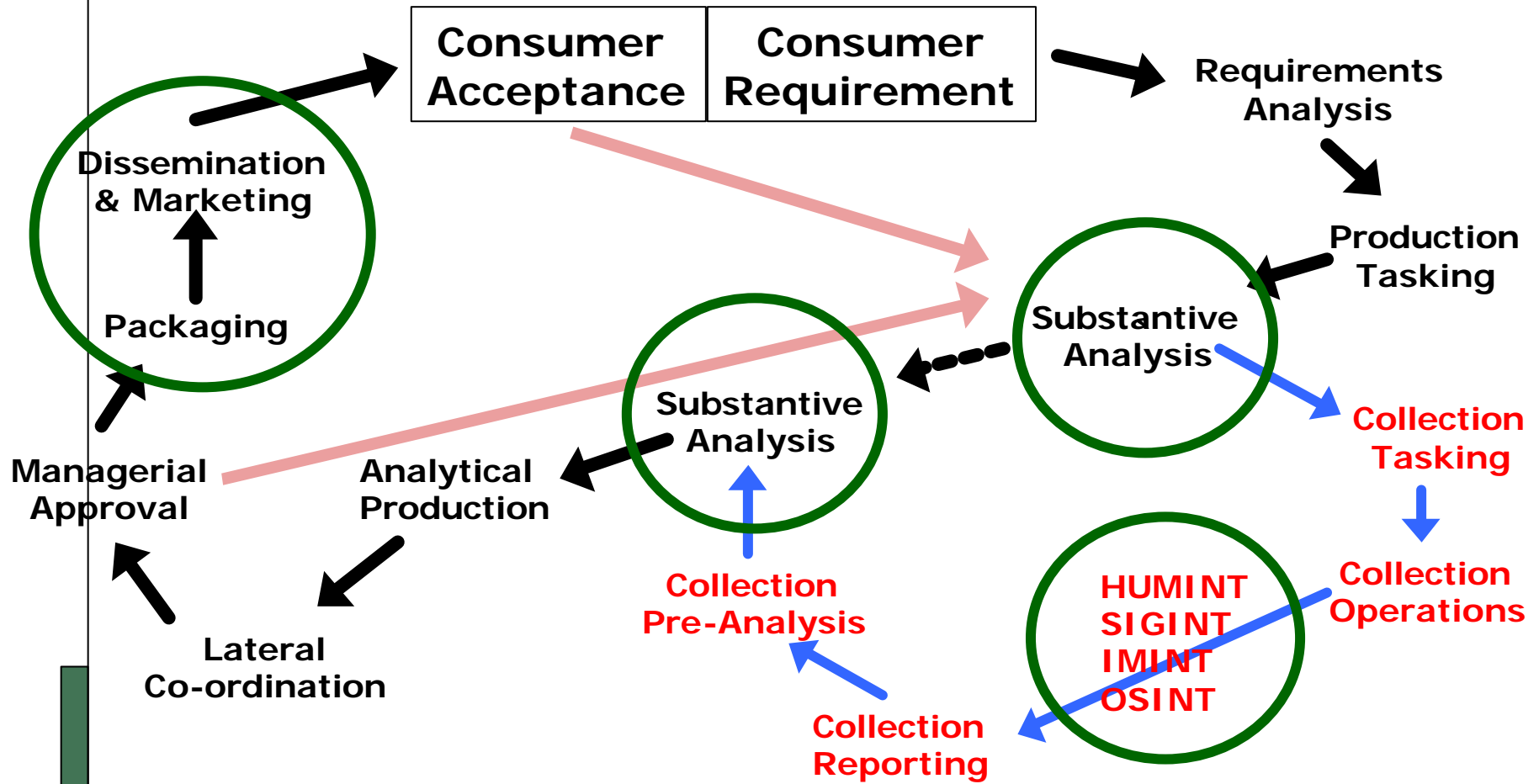
- Law Enforcement Intelligence – learning lessons for cyber-intelligence?
 - Intelligence-led policing is the LE community's response to the information revolution and to rising demands on limited resources
 - information technologies and KM tools enable more efficient utilisation of resources
 - aim is for smarter, more effective policing and improved allocation of policing resources
 - ultimate goal is deterrence, prevention and detection of crimes

- Issues to be considered

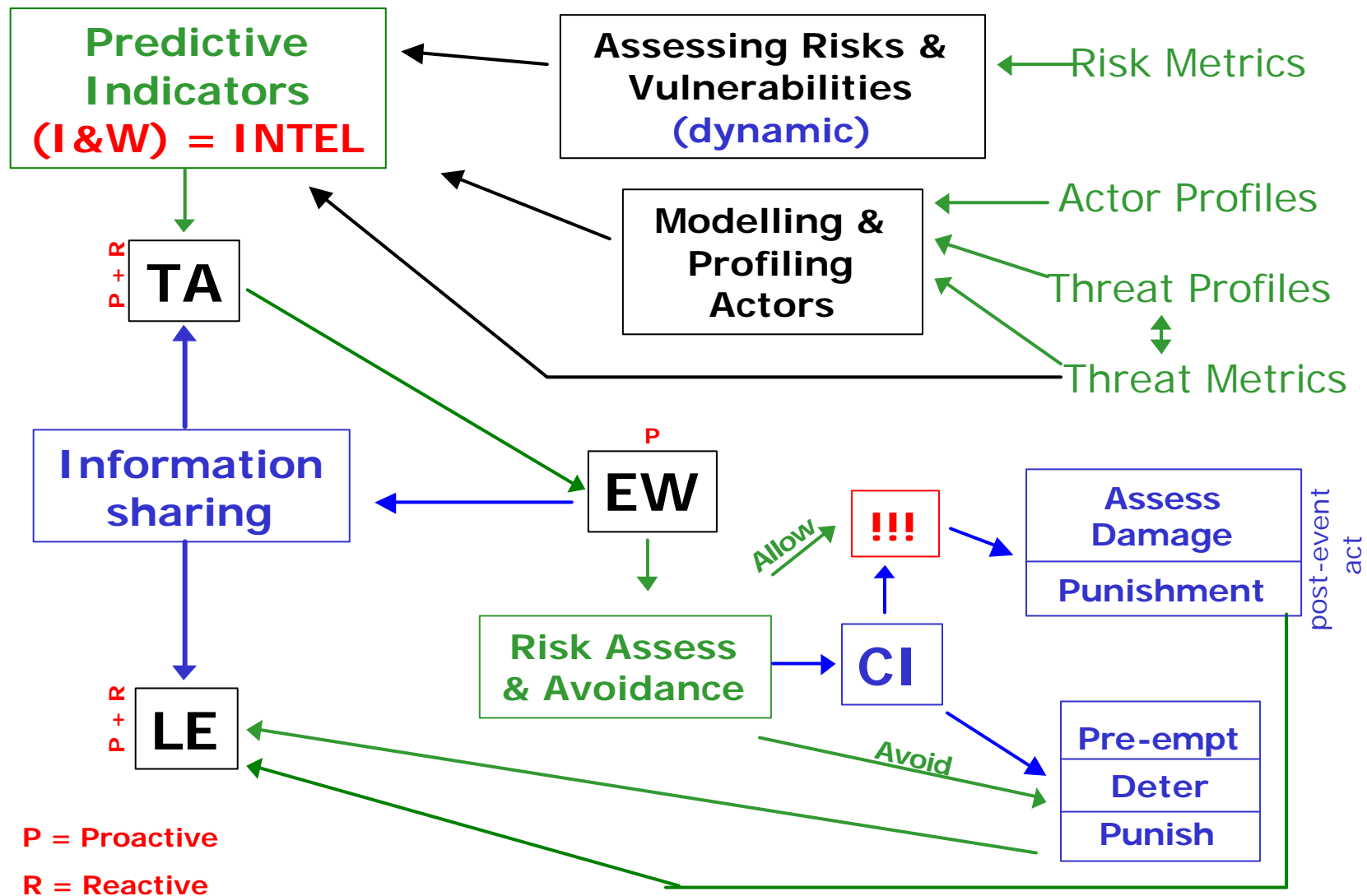


Source: EDS

Traditional Intelligence Cycle



"Cyber-Intelligence" Cycle?



Intelligence for CIP & Cyber-Threats

- Treat cyber-space as an operational environment
- Information-sharing is central: inter-agency, intra-governmentally, and internationally
 - **This is especially the based between law enforcement agencies and national security & intelligence agencies – this is a big failure right now on all levels**
 - **Essential to break-down traditional barriers and reluctance**
 - **Leads to better early warning**
- Enhance assessment to match collection efforts, which currently outweigh exponentially assessment and analysis resources

Intelligence for CIP & Cyber-Threats

- Enhance socio-cultural intelligence collection to better understand the sea in which these field swim
- Enhance HUMINT in these regions, including distasteful but necessary interaction with sub-state criminal, despotic and even terrorist elements closer to the target
- Public-private partnerships in information-sharing and intelligence are key (aforementioned emphasis on importance of business and industry in this area)
- clearly designate a lead agency in each country to lead these efforts: the current protectionist attitude of agencies vis-à-vis each other (so-called 'turf wars') are extremely counter-productive and can only contribute to the opponents' success

- Must differentiate between cyber-crime and other cyber-based threats
- Must ensure co-operation and co-ordination between the private sector and government
- Must ensure co-operation and co-ordination internationally as well as nationally
- Must approach cyber-threats differently from real-world threats – and all this means for intelligence operations and methodologies
- Must look for ways to enhance early-warning by developing effective predictive indicators

Thank you!!

Dr Kevin A. O'Brien

Senior Policy Analyst

RAND *Europe* Cambridge

Grafton House – 64 Maids Causeway

Cambridge CB5 8DD United Kingdom

+44(0)1223-353329 tel

+44(0)1223-358845 fax

obrien@rand.org

www.randeurope.org