Forensics for Critical Information Infrastructure Protection

By

Ian Bryant

Presented At

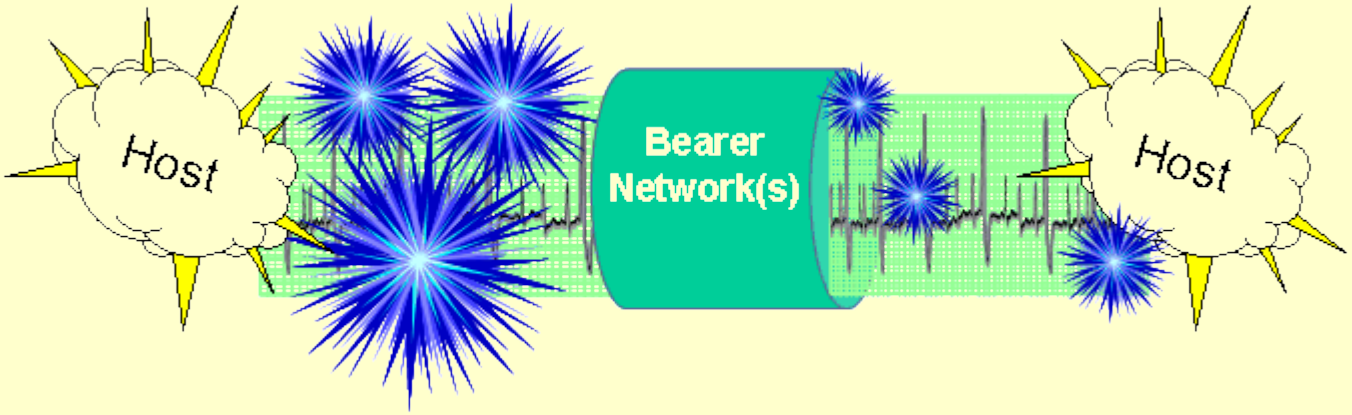
The Digital Forensic Research Conference

DFRWS 2004 USA Baltimore, MD (Aug 11th - 13th)

DFRWS is dedicated to the sharing of knowledge and ideas about digital forensics research. Ever since it organized the first open workshop devoted to digital forensics in 2001, DFRWS continues to bring academics and practitioners together in an informal environment. As a non-profit, volunteer organization, DFRWS sponsors technical working groups, annual conferences and challenges to help drive the direction of research and development.

http:/dfrws.org

Forensics for Critical Information Infrastructure Protection (CIIP)



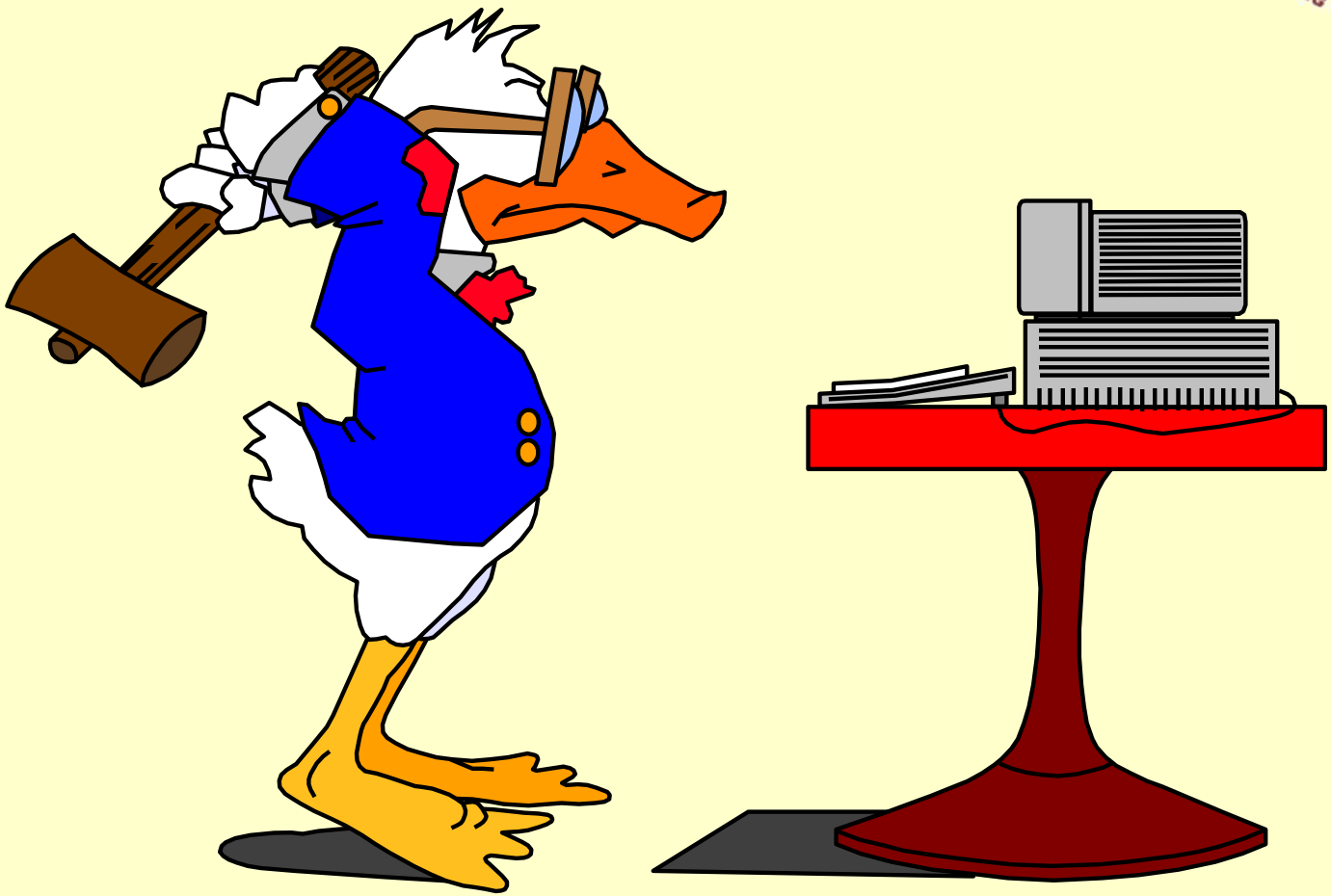
Ian Bryant
Head NISCC Research & Technology Group
& MOD Permanent Representative to NISCC

Working Document for Discussion ONLY

Forensics in CIIP

- **The CIIP Context**
- **Forensics and Triage**
- **Questions**

The CIIP Context

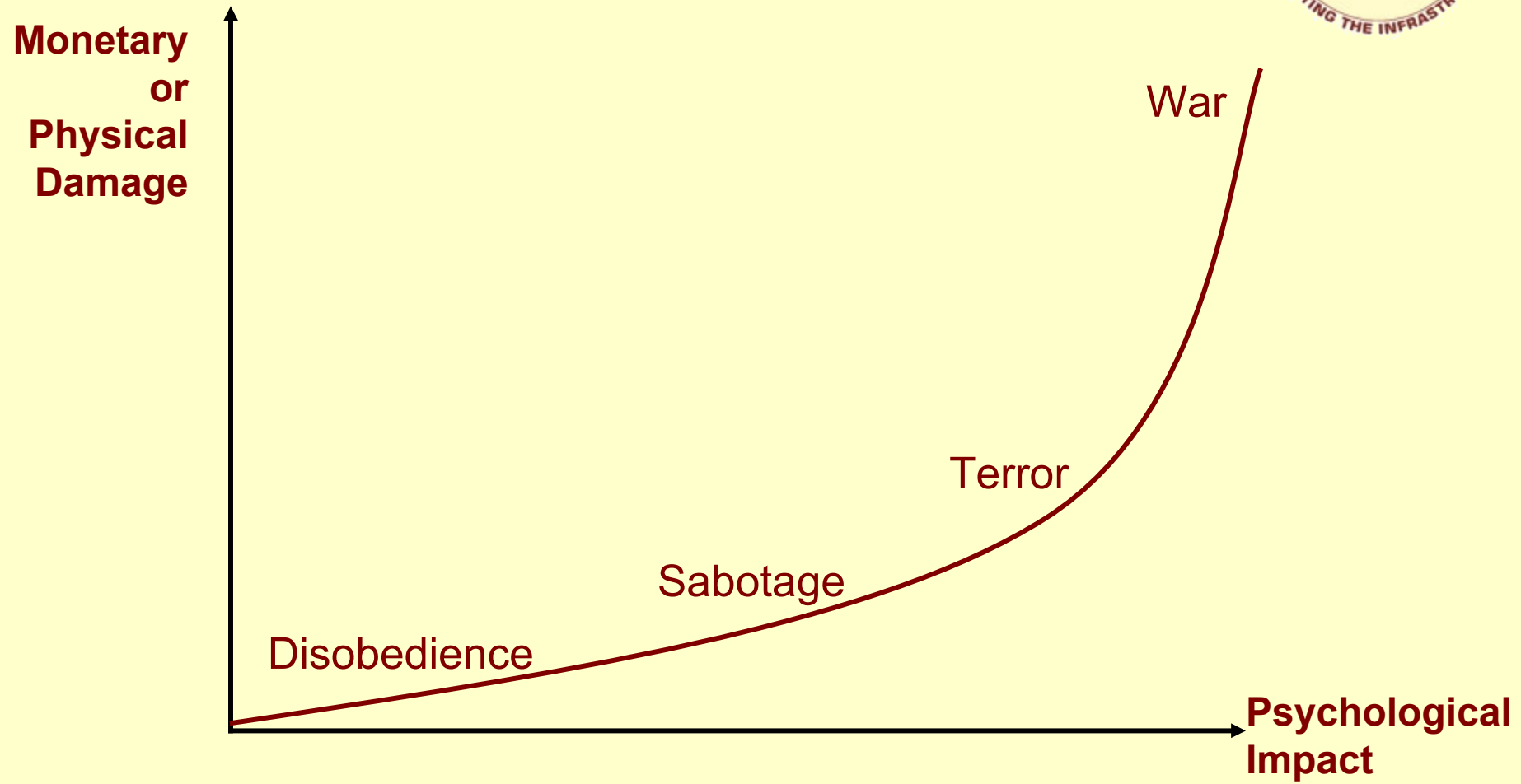


Working Document for Discussion ONLY

Cyber Attack

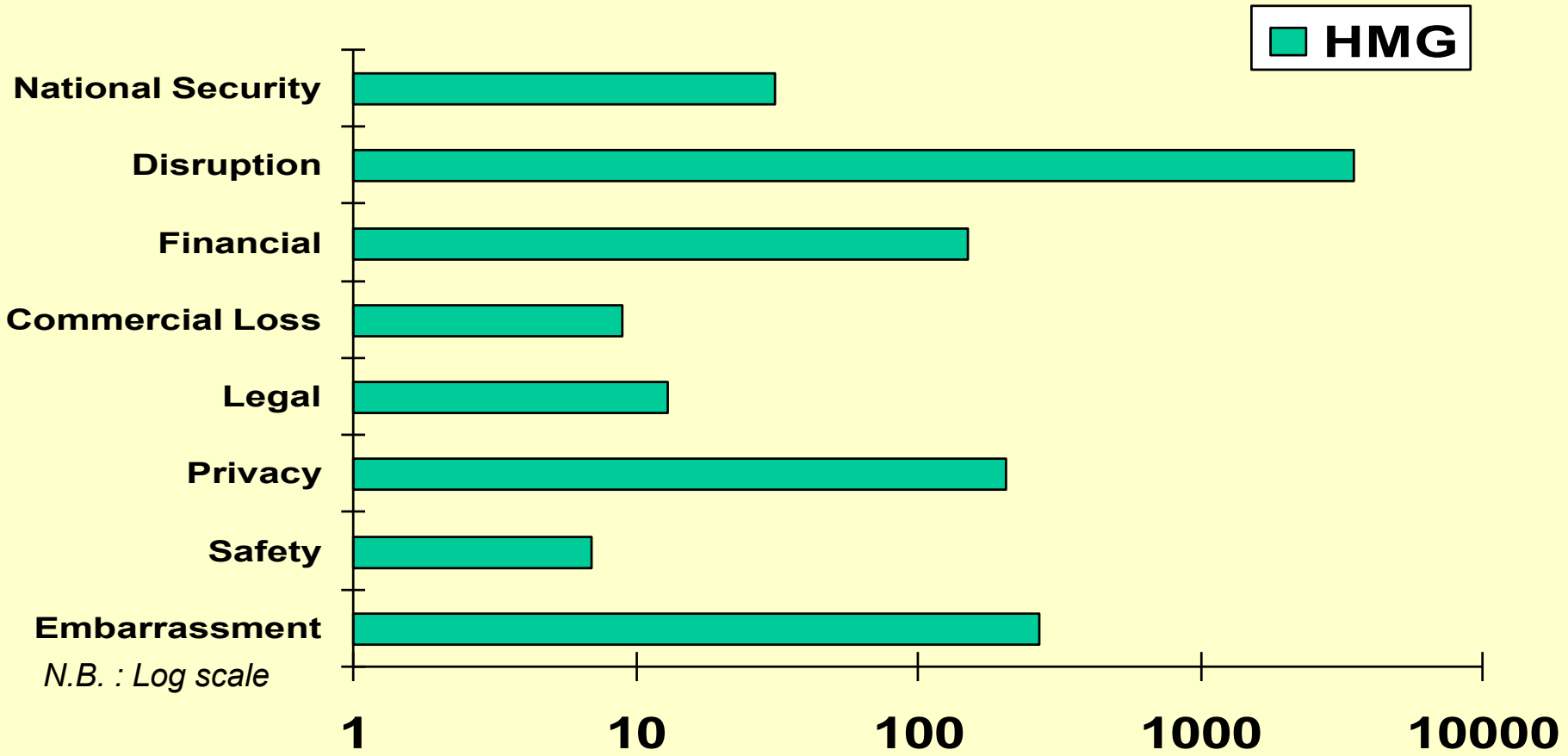
- **Selection of mechanisms**
  - **1st Order Cyber effects**
    - **MalWare (Collateral) ; DDOS (Directed)**
  - **2nd Order Cyber effects**
    - **Collateral Physical effects of Cyber acts**
    - **Cyber PsyOps e.g. Threats to HLS personnel**
  - **2nd / 3rd / nth Order Kinetic effects**
    - **Physical attack causing Cyber impact**

Threat Spectrum



Working Document for Discussion ONLY

Incidents Reported to UNIRAS



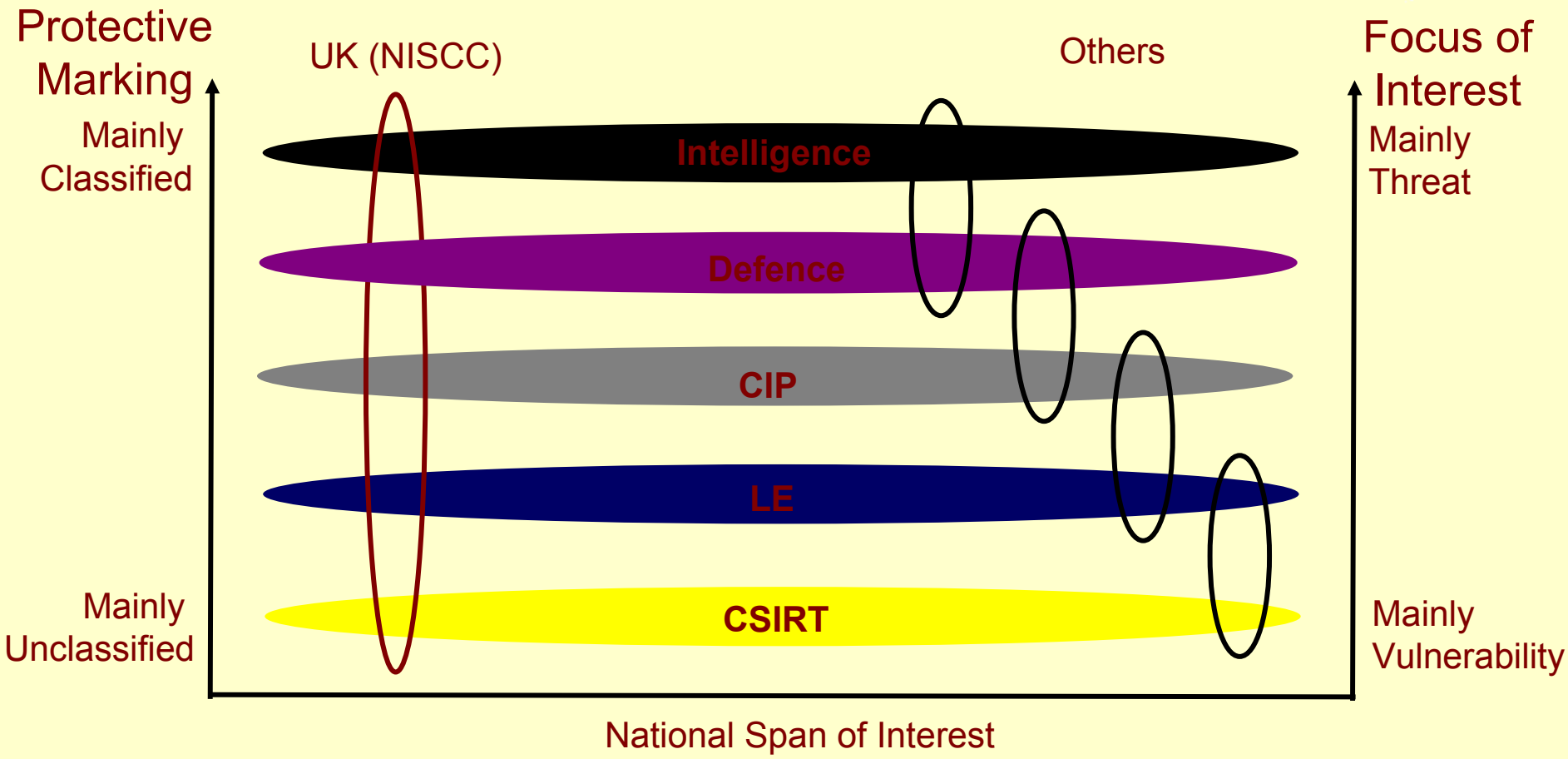
Working Document for Discussion ONLY

The Multipartite Problem

- **Variety of interested parties**
  - **Organisations detecting an Incident**
  - **Security Staffs**
  - **Law Enforcement**
  - **Technical Staffs**
  - **National CIIP organisations**
- **Dependencies**
  - **Avoiding actions of one party adversely impacting on others' interests**
  - **Biggest challenge is to prevent Evidential contamination during Detection / Triage**

Working Document for Discussion ONLY

Communities of Interest



Working Document for Discussion ONLY

Is this Forensics ?

Frequency	Ports
Very High	**21 (FTP),** 80 (HTTP)**, 111 (SunRPC), 139 (NetBIOS-SSN), 1433 (MS-SQL)**
High	**22 (ssh), 23 (telnet),** 25 (smtp)**, 53 (domain), 137 (NetBIOS-NS),** 443 (HTTP-S)**, 445 (MS-DS), 515 (lpdw0rm), 1080 (SOCKS), 1524 (Ingreslock), 3128 (Squid), 6112 (dtspc),** 8080 (HTTP-alt)**, 27374 (SubSeven)**
Medium	**3 (compressnet), 57 (privterm), 1024 (Jade), 1214 (Grokster), 1243 (Backdoor-G), 3072 (CSDmonitor), 3389 (MSTermSvc), 5800 (VNC), 6588 (AnalogX), 8000 (irdmi), 8888 (ddi-tcp-1)**
Low	**135 (epmap), 1434 (MS-SQL), 2049 (NFS), 4000 (BackBackDoor), 4001 (newoak), 4002 (pxc-spvr), 4003 (pxc-splr), 8081 (BlackIce)**
Very Low	**(All others)**

Working Document for Discussion ONLY

Forensics and Triage

Working Document for Discussion ONLY

Triage

(Tr-äzh, Träzh)

1. **A process for sorting injured people into groups based on their need for or likely benefit from immediate medical treatment.**

2. **A system used to allocate a scarce commodity**

3. **A process in which things are ranked in terms of importance or priority**

Incident Triage

Main Categories

- **Offensive Information Operations**
- **Serious Security Breach**
- **Serious Criminal Offence**
- **Other Electronic Attack**
- **Other Technical Incident**
- **Other Criminal Offence**
- **Other Security Incident**

Response Profile (1)

Type	**Offensive Information Operations**
Characteristics	**Malicious Electronic Attack (MEA)** • **HERF weapons** • **Denial of Service (DOS)** • **Targeted MalWare**
Threat Actor(s)	• **Hostile Power(s)** • **Empowered Small Agent(s)**
Lead	**National Government**
Forensics Requirement	• **2 phase : Rapid Assessment followed by Post Event Analysis** • **Evidential quality not usually paramount** • **Rapid restoration of service**
Remarks	**Typically Military response** ***(if permitted by Rules of Engagement (RoE))***

Working Document for Discussion ONLY

Response Profile (2)

Type	**Serious Security Breach**
Characteristics	**Compromise of:** **• Highly Sensitive Information** **• Highly Critical Systems**
Threat Actor(s)	**• Hostile Intelligence Service(s)** **• Individuals**
Lead	**Security / Counter-Intelligence Staffs**
Forensics Requirement	**• 2 phase: Assessment, then Comprehensive Incident Analysis** **• Evidential quality will vary** **• Timely restoration of service**
Remarks	**Forensic requirement will vary with Attribution, as actions by Individuals may lead to a Prosecution**

Working Document for Discussion ONLY

Response Profile (3)

Type	**Serious Criminal Offence**
Characteristics	**Typical categories** • **Theft** • **Misuse (obscene material)**
Threat Actor(s)	• **Individuals**
Lead	**Law Enforcement**
Forensics Requirement	• **1 phase: Comprehensive Incident Analysis** • **Evidential quality paramount** • **Timely restoration of service**
Remarks	**Police and Criminal Evidence Act, and ACPO Code of Practice, govern Evidential Requirements**

Response Profile (4)

Type	**Other Electronic Attack**
Characteristics	**Directed attack, or Collateral Attack with Major Impact :** **• DDOS** **• Defacement** **• MalWare with malicious payload**
Threat Actor(s)	**• Empowered Small Agent(s)** **• Individual(s)**
Lead	**CSIRTs ("CERTs")**
Forensics Requirement	**• 2 phase: Assessment, then Comprehensive Incident Analysis** **• Evidential quality will vary** **• Rapid restoration of service**
Remarks	**Forensic requirement will vary with Attribution, as if perpetrator can be identified, may lead to a Prosecution**

Working Document for Discussion ONLY

Response Profile (5)

Type	**Other Technical Incidents**
Characteristics	**Typically "undirected", but of significant impact:** **• Intensive Scans and Probes** **• Spamming** **• MalWare without malicious payload**
Threat Actor(s)	**• Individual(s)**
Lead	**CSIRTs ("CERTs") or WARPs**
Forensics Requirement	**• Normally only Assessment required** **• Occasional need for Comprehensive Incident Analysis** **• Rapid restoration of service**
Remarks	**Forensic requirement will vary with both Novelty and Attribution:** **• If event is unique or unusual, Technical details of most interest** **• If clear perpetrator can be identified, may lead to a Prosecution**

Working Document for Discussion ONLY

Response Profile (6)

Type	**Other Criminal Offence**
Characteristics	**Major categories** • **Misappropriation** • **Criminal Damage**
Threat Actor(s)	• **Individuals**
Lead	**Law Enforcement**
Forensics Requirement	• **1 phase: Comprehensive Incident Analysis** • **Evidential quality paramount** • **Timely restoration of service**
Remarks	**Police and Criminal Evidence Act, and ACPO Code of Practice, govern Evidential Requirements**

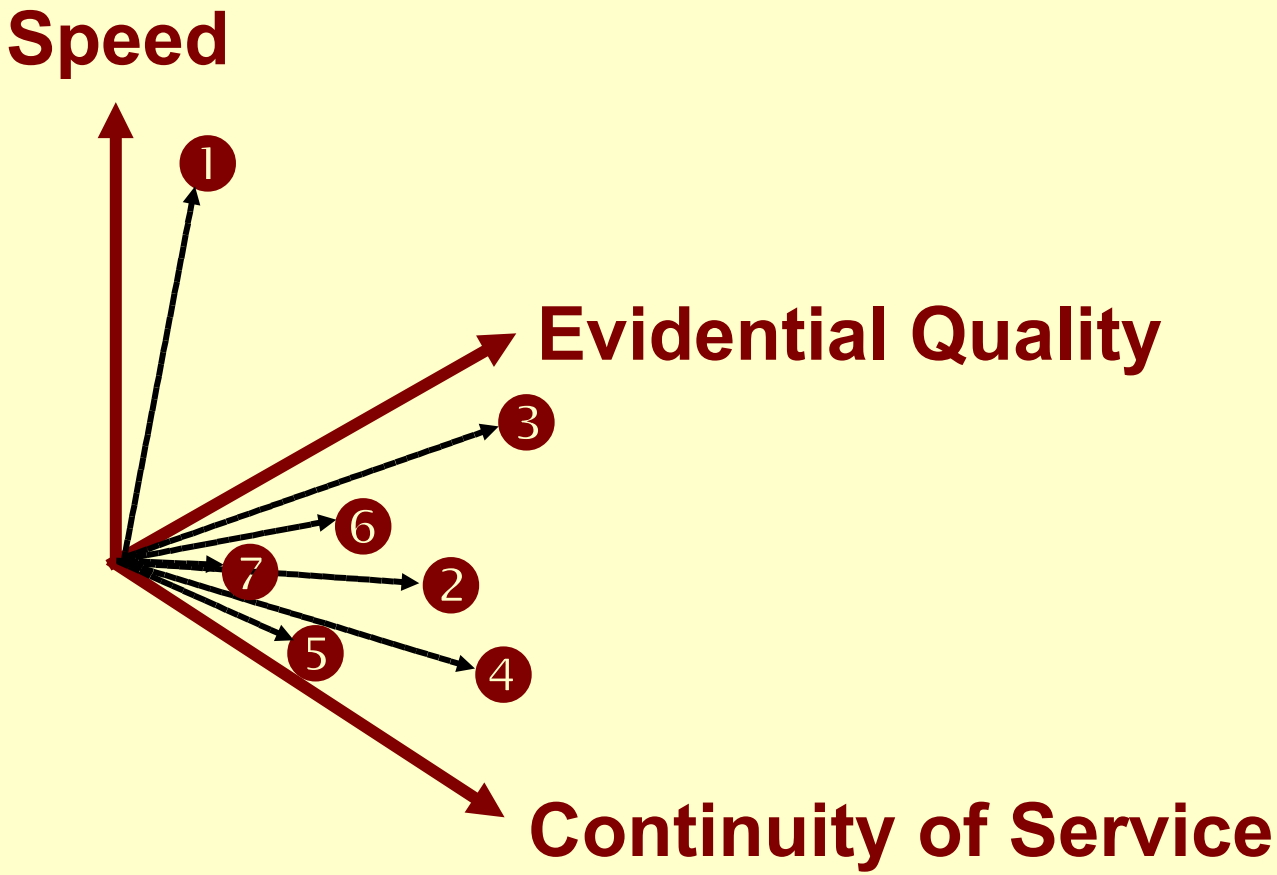
Response Profile (7)

Type	**Other Security Incident**
Characteristics	**Minor Impact** • **Misuse (excluding obscene material)** • **Failure to observe security regulations**
Threat Actor(s)	• **Individuals**
Lead	**Local Security Staffs**
Forensics Requirement	• **Not normally required** • **Minimal impact on service if invoked**
Remarks	**If Forensics required, will normally only be for limited Evidential quality for internal disciplinary concerns**

Summary

Working Document for Discussion ONLY

No "One Size Fits All" Solution



Working Document for Discussion ONLY

Conclusions

- **Widespread need for Forensic services in Information Assurance**
- **A Triage process is essential to determine speed, scope, and purpose when Forensic involvement required**
- **Forensics activity must not become a Denial of Service (DOS) itself**
- **Biggest challenge to Forensics is outside the control of its own community :**
  - **Prevention of Evidential contamination during Detection / Triage**

Working Document for Discussion ONLY

Questions ?

Working Document for Discussion ONLY

Contact Details

Ian Bryant

Head of Research & Technology

NISCC

PO Box 832, London, SW1P 1BG, England

Telephone: **+44-20-7821-1330 x 4565 (PA)**
+44-20-7821-1330 x 4561 (Direct)

Facsimile : **+44-20-7821-1686**

Internet

mailto:ianb@niscc.gov.uk

http://www.niscc.gov.uk

Working Document for Discussion ONLY