

**Steps towards Better e-Crime Management:
Mapping Cybercrime Problems and the Ways they are Combated**
(Parliament and the Internet Conference, 14th October 2010)

Presentation by Dr. Michael Levi, Professor of Criminology, Cardiff University
Levi@Cardiff.ac.uk, 44-29-20874376, London, October 2010

=====

Organised crimes, frauds and terrorism – cyber-enabled or not - are shaped by and respond to the environments provided by the licit world: private & public sectors, plus law enforcement.

So this calls for rethinking traditional divisions of interest into ‘public’ and ‘private’ since they are interdependent but not identical.

National boundaries are unhelpful for problem identification and solution.

But they are an essential jurisdictional basis for public sector and some private sector bodies.

Framework assumptions

=====

Key Points

1. We need to know what we know and don't really know about the scale and impact of cybercrimes.
2. There may be no consistent pattern about who benefits the most from public-private partnerships: but perhaps all that matters is that ‘both/multiple parties’ benefit!
3. Not every party will benefit from each initiative – have to see this as a process that develops over time (like the Wolfsberg private banks and their AML initiatives).
4. The private sector can gain if public authorities do not just collect their intelligence about crimes against business but also use this to deal jointly with threats – parts of the business sector must be seen as ‘deserving victims’ and as co-preventers.

=====

The Need for Audit

- Confusion/struggles over labelling of acts
 - Identity theft is often better described as ‘identity duplication’
 - Same act as damage, espionage, fraud, play, theft, warfare
- Elision of threat and manifest harm
- What are our knowledge gaps about different types of cyber-risks & how are they likely to change over time?
- Can we sensibly predict more than short-term trends in risks?
- How and in what terms do we measure cyber-harms?
- Is there any reason to think that some measures are better?
- How are we actually organised (a) to prevent and (b) to deal reactively with cyber-harms?
- How do we measure our individual and collective impact on cyber-harms, and can we do this better?
- How would we know that things were getting better or worse?

=====

Research Design

Phase 1: Secondary Data Collation (Duration: 3 months)

- Rapid Evidence Assessment (REA) of published academic and industry research and Government reports on the prevalence and impact of cybercrime
 - British Crime Survey
 - Information Security Breaches Survey (BIS)
 - Former NHTCU/NOP surveys
 - Audit Commission surveys
 - British Chambers of Commerce surveys
 - Federation of Small Businesses surveys
 - CIFAS & UKPA reports
 - Symantec/Cybersource/other industry reports
- Collation and analysis of official offence data from police databases
 - Home Office
 - SOCA
 - Constabularies
 - Central e-Crime Unit
 - Action Fraud/NFIB

=====

Research Design

•Phase 2: Primary Data Collation

–Interviews on perceptions of the cybercrime problem and mapping cybercrime control:

- Policy makers
- Criminal justice and security agencies
- Industry partners
- Academic experts

–Need info on what people want and expect to give and to receive from other parties, and how satisfied they are

–Online Delphi Group focused on establishing a partnership approach to controlling cybercrime

=====

•Phase 3: Analysis and Report Writing