

TOP SECRET STRAP 1



# Next Generation Events

---

TOP SECRET STRAP 1

23 March 2009



## What is NGE?

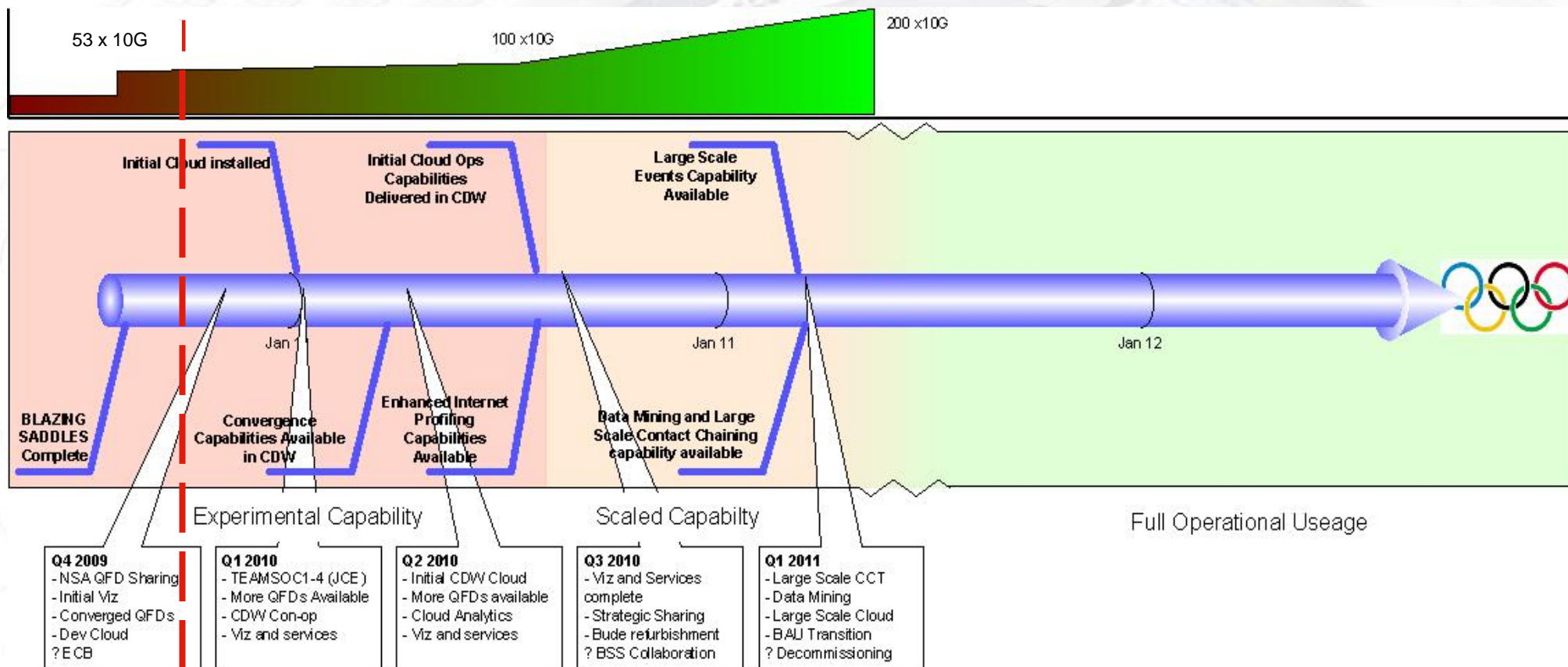
- **Systems like HAUSTORIUM reaching ingest capacity**
  - **But scale and variety both increasing**
- **5-Eyes also far-apart on “metadata” requirements, need to get closer together**

### The Answer?

- **NGE: A multi-stage project that tackles a series of the problems, at increasing scale, and with increasing collaboration**



# Next Gen Events: High-level Plan



- Q4 2009**
  - NSA QFD Sharing
  - Initial Viz
  - Converged QFDs
  - Dev Cloud
  - ? E CB
- Q1 2010**
  - TEAMSOC1-4 (JCE)
  - More QFDs Available
  - CDW Con-op
  - Viz and services
- Q2 2010**
  - Initial CDW Cloud
  - More QFDs available
  - Cloud Analytics
  - Viz and services
- Q3 2010**
  - Viz and Services complete
  - Strategic Sharing
  - Bude refurbishment
  - ? BSS Collaboration
- Q1 2011**
  - Large Scale CCT
  - Data Mining
  - Large Scale Cloud
  - BAU Transition
  - ? Decommissioning

New technologies (particularly from JCE) incorporated into solution as they are de-risked / proven

We Are Here

29 September 2009



## NGE: The Last Three Months

- **Sharing Enriched Metadata (HARBOUR PILOT)**
  - Moving towards metadata standards across 5-Eyes
  - Invisible to GCHQ analysts
- **Internet Profiling (BLAZING SADDLES)**
  - Taking ICTR ideas on how to process Events at scale, and scale even more
  - Required significant effort on End-to-End Sigint process



## Plug 1 - Internet Profiling: The BLAZING SADDLES Delivery

- **What It Does:**
  - Takes 8 ICTR QFD's and scales them for up to 100 x 10G bearers
  - Allows the analyst to see large amounts of a targets online activity
  - Metadata – MUTANT BROTH, AUTO ASSOC, KARMA POLICE, SOCIAL ANIMAL, INFINITE MONKEYS, HRMAP
  - Content – MEMORY HOLE, MARBLED GECKO
- **Why You Care:**
  - Want to know alternate online accounts?
  - Quickly build up a picture of someone's online MO and interests?
  - Identify for further exploitation (with other techniques) a targets network/machines?
  - Success across IP/X – CP, SIMMER, Mumbai, G20 – and ask around in your IPT!
- **How You Get Access:**
  - Currently instigating corporate process (based on C2C skill level)
  - Interim – see your Tech Director or Tech Ex



## NGE: The Next Three Months

- **ROCK RIDGE**
  - **Continuing QFD roll-out**
    - SAMUEL PEPYS
    - CAFFEINE HIT
  - **Sharing some QFD's with (initially) NSA**
- **Converged Events**
  - **Ensuring we don't perpetuate the C2C/Telephony divide**
  - **Specific QFD's that enhance our ability to exploit converged**
    - Evolved MUTANT BROTH
    - LAUGHING HYENA
  - **Exit strategy for SALAMANCA/HAUSTORIUM**
- **CLOUD Experiments at Bude**
  - **JCE and TINT**
    - Developing/testing technologies for later in the roadmap
- **ICTR (and others!) continue to develop new ideas**



## NGE: And After That?

- **Capability Development Workspace**
  - Bulk datamining capability
  - Use existing sources, and new cloud capabilities
- **Large-scale contact chaining**
  - MOAG – but anyone can create
  - Using both GCHQ and NSA datastores
- **MO/Profiling based discovery**
  - Always been the goal for events-led analysis
  - Dependent on technological advancements, but looking good
- **Events/Content Fusion & Visualisation**
  - Seamless navigation between Events and Content
  - Making sure we continue the MONTE VISTA/LOOKING GLASS ideas



## Next Generation Content..?

- **Not yet...but thinking and delivery is happening**
  - **TIPC using TDI's**
  - **Expand XKS use**
  - **Trial new ways of collecting/processing content (TINT)**





## Plug 2: TIPC Expansion

- **What It Does**
  - Full client IP stream collection triggered by known selector
  - Expanded to STM-64 environment as well as STM-1/4
  - Now triggered by TDI's, not just gmail, yahoo and maktoob
- **Why You Care**
  - Unique Intelligence material that can't be strong selected – web visits/searches etc
  - Find new protocols used by targets – you, tech trends, T development
  - Contextless
  - New dictionary – old one completely erased
- **How Do You Get Access?**
  - Talk to your C2C Tech Ex – they are running pre-requisite briefings as there are some dangers...(full IIB!)



## Plug 3: XKS & TINT @Bude Experiments

- **What It Will Do:**
  - **Promotion from XKS to IIB**
  - **Integration into LOOKING GLASS**
  - **Connection to Native File Viewer (FUME CUPBOARD)**
  - **Continuing to work on the NSA data access issue**
  - **The TINT@Bude Experiments Attempt To:**
    - Re-sessionise *everything*
    - Tag traffic, based on
      - strong selector/ geography/ application
      - contextual fingerprints:
    - Extract metadata in bulk
    - Retain a 3-day rolling buffer of 'interesting' content
      - for retrospective/protocol/network/analysis
      - for refining fingerprints/selectors
    - Do this on 20 x 10G's!
- **Why You Care:**
  - **Packet processing approach misses stuff**
  - **Strong selection only**
  - **Too much data retained is unused (97% unviewed)**
  - **Promote only the good stuff to long-term storage**
  - **Aim: to automatically promote to long term storage**
- **When Do You Get Access?**
  - **New XKS capabilities will be rolled out to GCHQ KS's when available**
  - **TINT PUT in place, but experimental, not operational use only**