## International Data Exchange and A Trustworthy Host: Focal Areas For International Collaboration In Research And Education – John C. Mallery

**Speaker:** John C. Mallery, Massachusetts Institute of Technology, Computer Science & Artificial Intelligence Laboratory, Cambridge, MA, United States
John C. Mallery is a research scientist at the Massachusetts Institute of Technology, Computer Science & Artificial Intelligence Laboratory. He is concerned with cyber policy and has been developing advanced architectural concepts for cybersecurity and transformational computing for the past decade.

A key message is the acknowledgement that international cooperation is nascent and a more global approach is urgently needed because there is ultimately just one, single global information environment, consisting of the interdependent networks of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.

Table 1 enumerates asymmetries within cyber attack and defense that today disproportionately favor the attacker. The attacker benefits from the initiative (A) and the large defender value at risk (B), whereas the defender controls more knowledge (L), architects the systems (M) and the criminal justice system (N). In between (C – K), the attacker has many advantages but international data sharing and defensive coordination can deny advantage to the attacker by improving communication (F), enhancing situational awareness (G), providing mechanisms for coordination (I), speeding up decision cycles (J), increasing agility (K), encouraging more defensible architectures (M) and supporting or incentivizing defensive coordination with the legal system.

**Table 1.** International data exchange can reduce asymmetries between attack and defence.

| | *Mode* | *Attacker* | *Defender* |
|---|---|---|---|
| A | Initiative | Chooses the best place, time and means of attack | Must defend everywhere, all the time, against any attack |
| B | Value At Risk | Small (terror or criminal actors) | Large |
| C | Code Size | Small (often 100s of lines) | Large (>20-50 million lines) |
| D | Software Control | High | Supply chain → Low |
| E | Software Abstraction | Good, integrated for purpose | Poor, evolutionary tower |
| F | Communication | Organized around attack → Good | Organized around products → Poor |
| G | Situational Awareness | High | After-market bolt-on → Low |
| H | Accountability | Low (terror or criminal actors) | High |
| I | Coordination | Small group → high | Non-scalable → low |
| J | Decision cycle | Fast | Slow |
| K | Agility | High (apparent) | Low |
| L | Domain Knowledge | Low, narrow & concentrated | High, broad but diffuse |
| M | Architectural Control | Low | High, but slow |
| N | Legal/Justice Systems | Low | High, but slow & political |

It is essential that we have the ability to conduct comprehensive intelligence collection and evaluation on any developing situation that threatens our cyberspace activity, followed by near-simultaneous processing, exploiting and disseminating of the information. This depends on collaboration, data exchange and sharing (and also knowledge sharing) between countries. We need comprehensive research towards international intelligence, surveillance, and reconnaissance (ISR) in the cyberspace domain.

Mallery characterized these challenges as follows.

- **Problem:** Attackers can replay attacks across different countries without rapid international learning to defend against attacker innovations
- **Benefits:** International collaboration and coordination can rapidly reduce defensive gaps across the OECD and build crisis-response capacities
- **Leverage:** Bias work factors in favour of defense and against cyber attack
- **Approach:** Exchange data related to cyber crime, attack patterns and best defense practices
- **Research:** Motivate technical research via needs of realistic data sharing scenarios

An architecture for international and cross-sector sharing of cyber threat and attack data will ensure a more effective collective cyber defense than countries, sectors or organizations might otherwise achieve individually.

**Fig. 1.** Straw man architecture for international data sharing and collaboration.

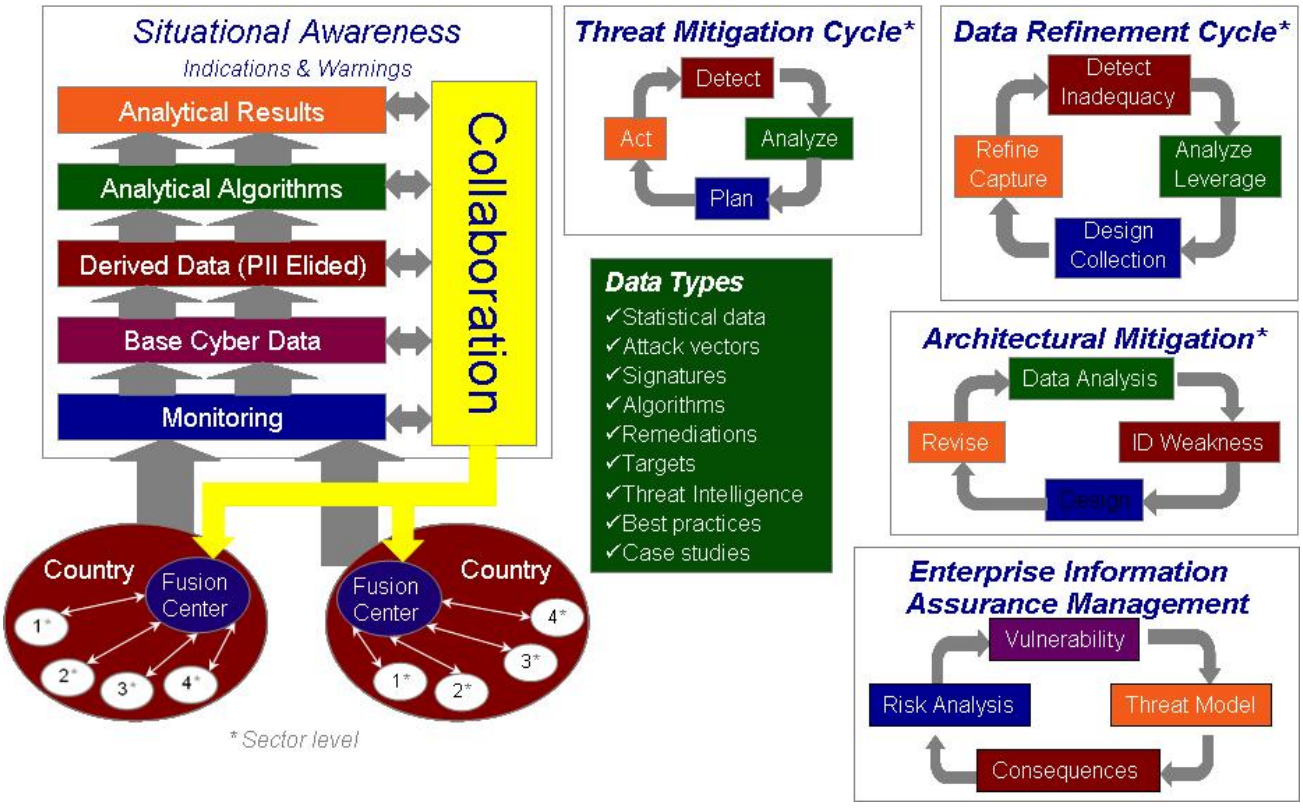

Figure 1 illustrates an international cyber data sharing architecture that integrates data from multiple countries and sectors and returns collaboratively produce analytical products and threat mitigation techniques. Country fusion centers integrate country information and expertise internationally. Within each country and across its sectors, shared monitoring infrastructures capture base cyber data at sources. This data is processed to remove personally identifiable information (PII) before being analyzed using shared algorithms to produce results fed back into shared situational awareness. The architecture supports sector-based threat mitigation cycles as well as enterprise information assurance management of value at risk. The architecture supports learning modalities like data refinement to improve data capture, analysis and utility in threat mitigation. Based on knowledge gained about vulnerabilities and attacker vectors, the architecture helps drive improvement of enterprise and infrastructure architectures to improve defensibility.

This kind of sharing scenario can drive research along many trajectories. The type of data collected needs to be effective and offer leverage for cyber defense. Large-scale analytics over the data need to reveal important patterns in real time and lead to timely threat mitigation. Given an effective sharing architecture, major malicious actors will endeavor to corrupt the data and subvert its operation, and so resilient and trustworthy engineering will be needed for all components from sensors to hosts, monitoring, analysis and mitigation actions. At the same time, PII and enterprise information must be protected to respect important societal values and incentivizing sharing. Difficult technical, legal and administrative challenges in international authentication, authorization, encryption and remote policy enforcement must be overcome to reach higher levels of trust and sharing necessary for weaponizable data like critical infrastructure attacks and mitigations.

Mallery characterized the goals of cyber data sharing and collaborative analysis as follows:

- Build shared awareness and understanding of cyber phenomena across countries
    - Employ shared data collection methodologies
    - Integrate measurements of phenomena across borders
    - Focus early on cyber crime and economic incentives
- Create comparable transnational data sets
    - Capture cyber breaches, attack patterns, best practices, defensive coordination
    - Include aggregate data on crime, black markets, economics, state-state interactions, long-term transformations
- Field a cyber data sharing framework that helps countries to:
    - Collect cyber data for compatible sharing
    - Fuse data to create common situational awareness
    - Manage national legal impediments to sharing via derived or aggregate data or by recommending harmonization steps
    - Exchange derived data in real time
    - Provide mechanisms for controlled drill down needed for law enforcement, advanced persistent threats (APT) or cyber emergencies
- Build shared collection, fusion, analysis, and response capabilities

In addition to cyber data sharing and collaborative analysis, Mallery introduced the idea of raising the work factors for malicious actors worldwide by collaboratively

developing an open-source trustworthy host platform for collaborative research and education. Mallery characterized the challenge as follows:

- Problem: Attackers are subverting legacy architectures which are inadequate for current threats
- Benefits: Development and evolution of a clean-slate trustworthy host will:
  - Create reference host architecture for computing, routers, cloud, embedded, wireless
  - Integrate best information assurance (IA) engineering from the open literature
  - Provide a reference paradigm for cumulative research and education
  - Drive higher assurance for open source and commercial software
- Leverage: Raise work factors required to compromise commodity hosts
  - Eliminate remote access penetration vectors
  - Prevent privilege escalation
  - Manage information leakage
  - Verify tool chain and resulting software
  - Rapidly detect and remediate flaws or breaches
- Approach: Pool research efforts across OECD countries to create and evolve a shared host platform reflecting best IA engineering practices
- Research: Motivate technical research via needs of an existing and readily-accessible free implementation

Finally, Mallery presented 10 technical features for a trustworthy operating system.

1. Safe Language*: No penetration vectors
   - Clean semantics – lambda calculus, extensible
   - Design for verification
   - Composability (practical even if incomplete)
2. Trusted Operating System*: Enforce least privilege
   - Separation kernels or hypervisors
   - Factored into well-defined independent cooperating components
   - Critical components verified
3. Binary Hygiene*: Eliminate return oriented programming
   - Control function entry/exit points (gates)
4. Information Flow Control: Manage side channels
   - Leak resistance
5. Monitoring: Audit & Accountability
   - Multi-scale reference models
   - Privacy awareness
6. Recovery: Efficient diagnosis and rollback to known states
   - Transactional persistent memory
7. Safe Networking Stack: Enforce least privilege
   - Protocol and channel separation by application, process or thread
8. Authorization & Authentication System: Manage least privilege
   - Non-by-passable
9. Separation User Interface:
   - Manage domain crossings explicitly
10. High Productivity Trusted Software Engineering*:
    - Inside industry development Cycles
    - Verified tool chain

During the discussions, Bart Preneel suggested cryptographic software stack as an additional requirement and everyone agreed.