International Data Exchange architecture for cooperation on cyber security and intelligence

BIC Discussion Paper **22-JUN-2011**

John C. Mallery [1]

1 CSAIL, Massachusetts Institute of Technology. USA

This project is supported within the portfolio of the European Commission's DG-CNECT Unit H.4, Trust and Security, and has received funding by European Commission's Seventh Framework ICT Programme under grant number 25258655 for the period January 2011 to December 2013.

Introduction

International collaboration and coordination can rapidly reduce defensive gaps across the individual countries and build capacities for crisis response. Without systematic and expeditious international coordination, attackers can replay attacks across different countries. This structural advantage for attackers can only be offset by collective defences incorporating rapid international learning to identify, disrupt and defend against innovative attacks across their lifecycles from reconnaissance and testing to deployment.

Collective cyber defence against threats from cybercriminals, hacktivists, terrorists and nation-states in peace or in war requires an effective architecture for scalable real-time data sharing, collaborative analysis, and rapid threat mitigation. Development of such real-world defensive capabilities poses challenges that can drive both applied and fundamental research.

An international program of research will broaden awareness, understanding and capacity across participating countries, and deepen technical knowledge around data sharing and analysis tasks. The integration of national expertise and experience can facilitate faster learning and transfer new and effective concepts into operational practice to fight crime, close defensive gaps, protect intellectual property and coordinate defences against malicious state actors. Objectives include creation of shared data collection, analysis and protection methodologies. International aggregation of cyber data on crime and law enforcement, black markets, economics, state interactions, long-term cyber-fuelled transformations will enable tracking trends as they emerge and counteracting malicious techniques, tools and procedures before they diffuse widely. These transnational datasets on breaches, attack patterns, best practices, and defensive coordination will enhance common situational awareness and will enable retro-dictive metrics of efficacy for countermeasures.

Legal and regulatory barriers to cyber data sharing remain a significant challenge to defensive coordination. Thus, international cooperation can also drive legal harmonization to support shared collection, fusion, analysis, and response capabilities. Legal and policy incentives, in combination with actionable results, will also need to motivate private and public actors to coordinate at the sectoral and national levels.

International dimension and its challenges

The first step in an international initiative is to engineer a cyber data strategy that recommends what to collect in each domain prioritized by its purpose, and how to harmonize processing and analysis. The strategy needs to identify clear procedures for sharing various data according to sensitivity, for sanitization based on concerns about privacy or sources and methods, and for defining exchange formats and delivery times. They should include context, specific sharing purpose, and ultimately lifespan of the sharing. Importantly, the strategy needs to identify synergies arising from integrating data across national boundaries and its impact on the participating countries.

Numerous precedents can inform the strategy across a range of sectors and issue areas. The European Network & Information Security Agency[2] (ENISA) collects, analyzes, disseminates data on InfoSec in a pan European context. DHS Predict[3] (US) has developed a legal framework for sharing cyber data within the United States, which has been extended to Canada and soon to the European Union. The European Commission funded Wombat Project[4] has fielded collaborative sensors for Internet malware and attack data. The European Public-private Partnership For Resilience[5] has focused on critical information infrastructure protection. The Financial Services Information Sharing and Analysis Center[6] (FS-ISAC) brings together US financial sector entities and aggregates data collected from its members after anonymizing it. The non-profit National Cyber Forensics and Training Alliance[7] (US) integrates information and analysis for the financial services sector across private, public and academic communities. The Confickr Working Group is a well-known example of informal but effective cooperation as are the Anti-Phishing Working Group and Digital Phishnet. Lessons can be drawn from these and other collaborations to architect effective international cyber data collection and analysis.

2 European Network & Information Security Agency, http://www.enisa.europa.eu/
3 DHS Predict, https://www.predict.org/
4 European Commission FP7 Wombat Project, http://www.wombat-project.eu/
5 European Public-private Partnership For Resilience, http://ec.europa.eu/information_society/policy/nis/strategy/activities/ciip/impl_activities/index_en.htm
6 Financial Services Information Sharing and Analysis Center (FS-ISAC), http://www.fsisac.com/
7 National Cyber Forensics and Training Alliance, http://www.ncfta.net/

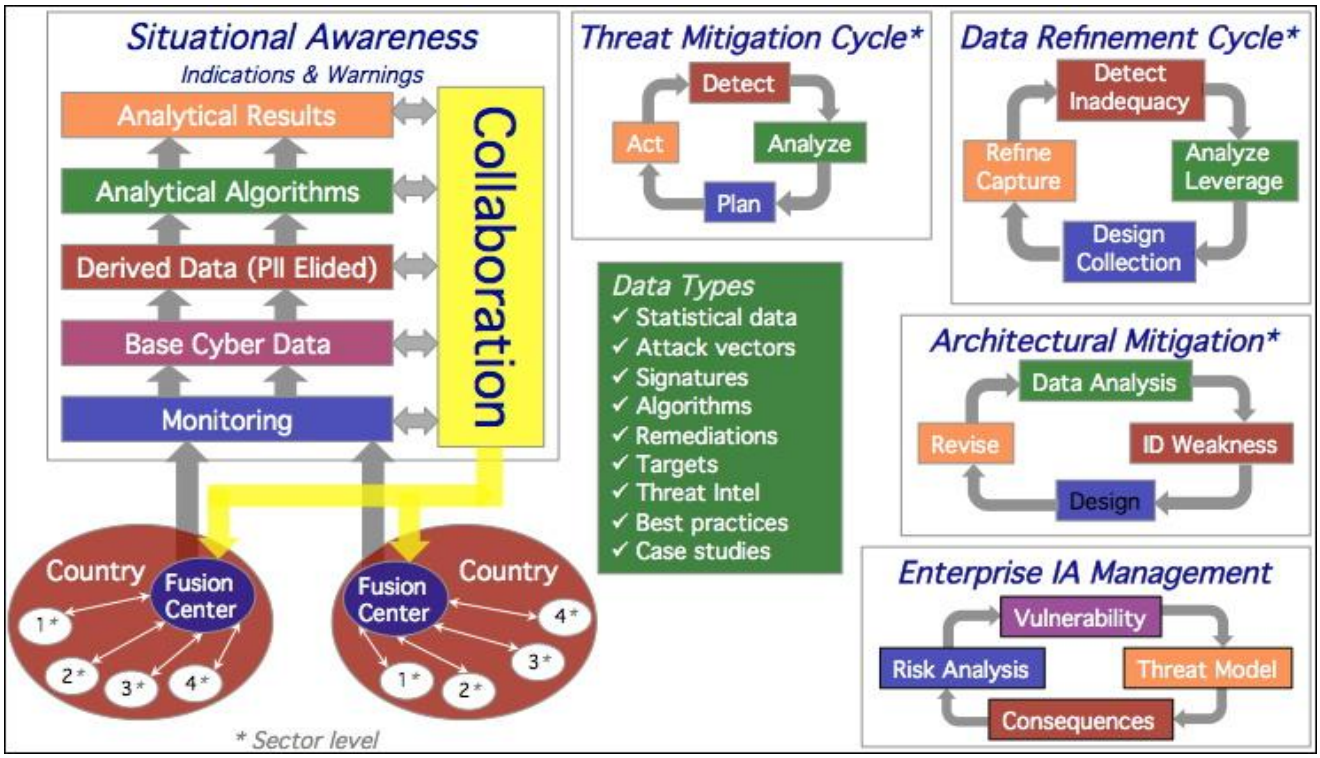

Figure 1 - A strawman international cyber data sharing architecture

The critical ingredient for success is incentivizing participation of national governments and private actors by demonstrating the advantages of multinational scale, the synergies of international cooperation and the direct benefits to participants. International scale can help drive increased quality and integrity of data. Guidelines for managing data collection and sharing that respect local law and cultural sensitivities can reduce impediments to participation. Finally, clear identification and mitigation of the risks of sharing can assuage concerns of governments and private actors. Furthermore, security solutions[8] for acquisition, storage, processing and transfer of data can be deployed to reduce risks while enabling benefits.

Some of the research and development areas necessary to support this effort include:

- Architectures for collection, analysis, policy enforcement
- Representation and structure of data
- Policy representation and understanding
- Implementation of data sharing, including data formats, standards, tools, usability
- Security, including secure host with strong isolation, access control management, policy enforcement, data integrity, provenance tracing
- Cryptographic techniques, including data splitting, differential privacy, cypher text arithmetic
- Development of a trustworthy platform for data sharing and analysis
- Creation of a test bed for concept demonstration.

As shown in Figure 1, a strawman architecture has been generated and this was described in more detail at the workshop. Due to the duration of the session, it wasn't possible to get into very technical discussions but there was instead a focus on advancing this work to the next level and commitment to formulate a strategy for research and development coordination, which will enhance the outcomes through tactical planning, leveraging and combining task-relevant national expertise.

Malicious actors in cyberspace actively exploit the shortcomings in the ability of defenders to coordinate their activities. They can rerun the same attacks against different countries, sectors and organizations so long as cyber data and countermeasures are not being shared effectively.

An architecture for international and cross-sector sharing of cyber threat and attack data will ensure a more effective collective cyber defense than

[8] Security solutions will include operating system security, cryptographic techniques, harmonized vetting procedures and access control mechanisms, and data protection techniques like slicing, aggregation or incremental revelation.

countries, sectors or organizations might otherwise achieve individually.

Figure 1 illustrates an international cyber data sharing architecture that integrates data from multiple countries and sectors and returns collaboratively produced analyses 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.

The goals of cyber data sharing and collaborative analysis were characterized as follows:

- Build shared awareness and understanding of cyber phenomena across countries
  - o Employ shared data collection methodologies
  - o Integrate measurements of phenomena across borders
  - o Focus early on cyber crime and economic incentives
- Create comparable transnational data sets
  - o Capture cyber breaches, attack patterns, best practices, defensive coordination
  - o Include aggregate data on crime, black markets, economics, state-state interactions, long-term transformations
- Field a cyber data sharing framework that helps countries to:
  - o Collect cyber data for compatible sharing
  - o Fuse data to create common situational awareness
  - o Manage national legal impediments to sharing via derived or aggregate data or by recommending harmonization steps
  - o Exchange derived data in real time
  - o 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

We need to look at optimising the integration of both technical and economic perspectives to favour defensive interventions that disrupt malicious business models. Figure 2 illustrates the limited scope of conventional technical approaches to cyber defence. By integrating understanding of the attack business model, defenders gain additional opportunities to disrupt the attacker anywhere on his value cycle using passive or active means. Additionally, the resources, capabilities and motivations of the attacker provide constraints on the range of technical defences necessary for effective defence.

At the workshop, there was strong agreement to identify the stakeholders in the architecture diagram (Figure 1) and to assemble a team to begin developing an international project consortium together, perhaps starting with a smaller number of countries and advancing to more later.

About the Author

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. He has been very active in both the INCO-Trust and BIC projects since the beginning.

Figure 2 - Optimising integration of technical and economic perspectives for cybersecurity