BUILDING International Cooperation for Trustworthy ICT

European Commission Information Society and Media

BIC planning session on

Building a long term International Cooperation strategy in Trustworthy ICT

System Security and Cyber-Defence: requirements for an international approach to technological challenges and open issues.

BIC Partners

TSSG

Waterford Institute of Technology

TECHNISCHE UNIVERSITÄT DARMSTADT

TELECOM ParisTech

Atos

Amsterdam, Netherlands

6th July 2011

Table of Contents

EXECUTIVE SUMMARY

The EU FP7 BIC project [1], with the support of the SysSec project [2], organised a session as a step in the development of plans and proposals for international collaboration in research towards a vision of cyber-space that supports fundamental freedoms, privacy and the free flow of information in a secure and reliable manner, while protecting the essential information infrastructures on which we depend.

The session was held on 6th July 2011, during the afternoon of the SysSec workshop. The stated objectives of the session were:

- Address the general question of the scope and priorities, and initial planning considerations for international collaboration on R&D towards trustworthy ICT.
- Explore *Frameworks for Data Sharing*, as a specific enabler for collective defence and response to cyber-attack.
- Prepare the ground for the extended BIC workshop being planned for, Quarter 4 2011;
- Further clarify scope for international collaboration on cyber-security;
- Progress the Secure International Data Exchange Architecture for Cybersecurity, introduced at the May, 2010 workshop to explore the technical and organisational requirements and constraints.

Due to the nature of the SysSec workshop and expertise of the participants, the BIC session organisers placed a heavy emphasis on the continuation of the work started during the Inco-Trust project on scoping an International Data Exchange architecture, specifically for cybersecurity, which would enable exchange and sharing between responsible states and organisations of information and intelligence on cyber-attacks. The participants feel this would be an essential component of collective cyber-defence against malicious action (as well as accidents and flaws). It is central to the ability to anticipate and respond: longer-term in the preparation of strategic, collective defensive measures, and short-term in recognising, isolating, and recovering from, attack – threatened or actual.

The comprehensive ninety minute session was broken into the following sections with expert speakers from around the globe.

1. Motivation and vision
2. Threat models, actors and capabilities
3. Technologies to support the International Data Exchange Architecture
4. Legal, regulatory, political, social, economic, and environmental challenges
5. Next steps for planning

The organising committee of the BIC session included:

Jim Clarke,	Waterford Institute of Technology, IRL
Karl Levitt,	The University of California, Davis, USA
Evangelos Markatos,	FORTH, Greece,
Neeraj Suri,	TUD, Germany
John C. Mallery,	MIT, USA
Michel Riguidel,	Telecom Paris-Tech, France
Aljosa Pasic,	ATOS Origin, Spain
Rebecca Wright,	Rutgers University, USA.

INTRODUCTION, MOTIVATION AND VISION

The quantity and seriousness of cyber attacks have been clearly growing over the past six years and have surged over the last three months. Although there have been real improvements in enterprise cyber defences, threats have been outpacing them. Recent attacks have ranged from spear phishing email accounts to gain footholds into organizations, infiltration of international economic institutions (possibly with insider advantage), and other neo-mercantilist industrial espionage. Added to these are growing ideological hacktivism and a potential threat of cyber terrorism against critical services and infrastructures as terrorist continue to use the Internet to recruit and coordinate.

Cybersecurity is now receiving high priority for international collaboration. Some recent examples are highlighted here:

- EU–US INCO-Trust workshop of May 2010 [3],
- Munich Security Conference, 4-6th February, 2011 [4]
- US-UK Cyber Communiqué of 25th May 2011[5],
- Recent accession to the Budapest Convention on Cybercrime [6],
- 28th Annual International Workshop on Global Security on June 16, 2011 [7], and
- Vienna Security conference, 1st July 2011 [8].

A key message throughout all of these events 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 network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.

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. The anticipated benefits of an international data exchange system include:

- **Data exchange and sharing capabilities** for monitoring of trends with availability of retrodictive cyber statistics across the OECD; enhanced anti-crime counter-measures better identifying cyber crime targets, vectors, methods, and counter-measures; closing defensive gaps with better defensive coordination and best practices; and enhancement of IP protection with the detection and prevention of industrial espionage.
- **Expertise integration** to focus collective expertise on important cyber data and analysis tasks.
- **Collaboration and coordination** reducing defensive gaps across the OECD

and better crisis response.

- **Research and development coordination** to leverage and combine national expertise.

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.

	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

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

The session speakers were selected based upon their expertise and previous experience in elaborating a comprehensive set of topics related to International cooperation in trust and security. The organizers felt it was very important to also continue the development of cooperation topics from previous interactions so it was decided to use the development of an International Data Exchange Architecture as a clear example of how international cooperation could benefit the trust and security research communities.

On this basis, the final speakers were chosen to introduce the following topics and they were asked to answer the following questions in their talks.

Topic 1. Motivation and Vision: What are we doing and why? What are the expected impacts? What kind of data should we share? What kind of collaborations do we need? What kind of analysis do we need? What are the incentives to participate? What are the risks?

Topic 2. Threat Actors: Who are the threat actors and what are their capabilities? What threat models follow from the actors' business models and capabilities? How are consequences of breach or disruption assessed and their criticality determined?

Topic 3. Technologies to support International Data exchange architecture: Review of the straw man architecture in more detail? What are the enablers eg. Cryptography based obfuscation, sensors on the network, monitoring traffic capabilities? Basics of how we share recognizable data, especially on critical infrastructures and across different countries. eg. share patterns for recognizing advanced persistent threats without losing efficacy if they are exposed? What obfuscation and security measures would make patterns easier to share? Architecting for leakage and resilience under compromise.

Topic 4. Legal, Regulatory, political environment challenges: What challenges arise when dealing across multiple sectors and countries? How are these best addressed at a transnational level? How are legal and regulatory issues including privacy, corporate responsibility best managed in order to improve coordinated defence?

Topic 5. Next steps for planning: What are the concrete next steps until the next event (expected Q4 2011)? How can we motivate countries to contribute and support the effort? More details appear in the agenda (next section).

AGENDA AND SPEAKERS SUMMARIES

Time	Description	Speakers
13:30 – 13:35	Overview / Purpose of Session	Jim Clarke, Waterford Institute of Technology -TSSG
13:35 – 13:55	Part 1. Motivation and Vision: Opening remarks US perspective EU perspective	 Samuel Weber, National Science Foundation, USA Karl Levitt, Univ. of California Davis Barbara Daskala, ENISA
13:55 – 14:05	Part 2. Threats and Actors	Sotiris Ioannidis, FORTH
14:05 – 14:50	Part 3. **Straw man architecture for International data exchange and collaborative analysis** Data exchange architecture used in a financial application in South Africa. Identity related issues for data handling and aggregation	John C. Mallery, Massachusetts Institute of Technology; Barend Taute, The Council for Scientific and Industrial Research (CSIR), South Africa; Glenn Gran, IKED. GINI SA project
14:50 – 15:05	Part 4. Legal, Regulatory, Privacy, and Political Challenges	Jody Westby, Global Cyber Risk LLC, Carnegie Mellon CYLAB
15:05 – 15:30	Part 5. Next steps for planning of workshop in Q4 2011 • Determining a comprehensive coverage of topics required; any gaps? • Identifying key topics for a workshop to be held in the Fall ’11 (see next pages for initial draft terms of reference); • Identify Organising and Program committee; • Identifying the necessary participants; • Identify how to best collaborate between now and then (eg. establishment of working groups, electronic, ….)	BIC partners, interactive

Building a long term strategy for International cooperation in Trustworthy ICT [9]

Speaker: James Clarke, Waterford Institute of Technology, TSSG, Ireland

Since January 2011, James Clarke is Project Coordinator of a European Framework Program 7 Co-ordination action entitled BIC, which stands for Building International Cooperation for Trustworthy ICT: Security, Privacy and Trust in Global Networks & Services. BIC will engage the European Union trust and program management (funding organizations) and research communities with their peers in Brazil, India and South Africa and enable the collaboration with research communities in trust and security already established in the US, Australia, Japan, Korea and Canada established in the recently concluded INCO-Trust project that Mr. Clarke also coordinated from 2008 - 2010. In addition, Mr. Clarke is actively involved in the research community, having served in various international conference committees as organizing, technical and program committee member.

Mr. Clarke opened the session by describing the overall purpose of the BIC session, which was to generate discussions with the systems and network security attendees at the SysSec workshop [10] on addressing the general question of the scope and priorities, and initial planning considerations for international collaboration on R&D towards trustworthy ICT and continue the work started at the May 2010 INCO-Trust workshop [11] on exploring *Frameworks for Data Sharing*, as a specific enabler for collective defence and response to proliferating cyber-attacks.

Mr. Clarke further elaborated the main goals of the session, which are to prepare the ground for the extended BIC workshop being planned for 2011, Q4, discuss with the main stakeholders in attendance to clarify scope for international collaboration on cybersecurity, and continue the good work already started by some of the researchers and to invite others to contribute on the development of a secure International Data Exchange Architecture for Cybersecurity and to further explore the technical and organisational requirements and constraints.

Mr. Clarke described the agenda, which was broken down under a variety of connecting topics, including motivation and vision, threats and actors, technical issues related to the international data exchange architecture for cybersecurity including a strawman architecture, a real life example of a data sharing case for the finance sector and enabling technologies required including privacy protecting identity management, legal, regulatory, privacy and political challenges involved with data exchange and sharing and next steps and planning.

Mr. Clarke concluded by thanking the SysSec workshop organisers for providing the venue for the session and to all of the BIC session organising committee members for the hard work in pulling together the contents of the session. These included John C. Mallery, MIT, USA; Aljosa Pasic, ATOS, Spain; Karl Levitt, The University of California, Davis, USA; Evangelos Markatos, FORTH, Greece; Neeraj Suri, TUD, Germany; Michel Riguidel, Telecom Paris-Tech, France; and Rebecca Wright, Rutgers University, USA.

Opening remarks: International cooperation in Trustworthy ICT [12]

Speaker: Samuel Weber, National Science Foundation, USA

Samuel Weber is in the Directorate for Computer and Information Science and Engineering (CISE) of the National Science Foundation (NSF). Specifically, he is a Program Director in the CISE cross cutting program in Trustworthy Computing.

Dr. Weber presented the National Science Foundation's strategy for international cooperation. Dr. Weber stressed that in addition to NSF, there are other agencies where researchers can look for funding. He emphasised that NSF is not the only funding agency out there. There are many involved in research funding with different missions and priorities and these were highlighted during the presentation. All have different missions but they all coordinated together on a joint strategy in the US research landscape on trustworthy computing. The coordination is carried out by the NCO/NITRD = National Coordination Office for Networking and Information Technology Research and Development (see also the document "Trustworthy Cyberspace: Strategic Plan for the Federal Cybersecurity Research and Development Program").

Dr. Weber described the four main thrusts to the NCO-NITRD* Game-Change Strategy: 1. Inducing Change: within 3 themes

i. Tailored Trustworthy Spaces;
ii. Moving targets; and
iii. Cyber Economic Incentives.

2. Developing scientific foundations.
3. Maximizing research impact.
4. Accelerating transition to practice.

The NSF focuses on long term research and is able and willing to partner with other agencies, who may be looking at more short term research. The NSF is more a bottom up agency where there are broad solicitations from a wide range of topics. For example, these could range from cryptography, operating systems, economics of cybersecurity, and human computer interaction in one big solicitation. The NSF FY 11 funding level is $55M dollars. The ethos of the NSF is to see what people want to research and decide which areas of research need help. They try to spread things out fairly and evolve funding decisions that way.

International cooperation is seen as very important in the NSF, especially from the trustworthy computing perspective. Clearly, different countries have different focuses in which centers of expertise are isolated geographically, hindering everyone. For example, there was a recent RFID security workshop in the US that had many EU people there while other EU based workshops have many US people there. The NSF want to improve the balance by giving more opportunities to those not located in the correct geographical location for their research. For International collaboration, there are different opportunities: *Individual supplements*, support for collaboration: travel, visitors, workshops; *Ad-hoc supplements* in which international proposals can get co-reviews with NSF-equivalents thus avoiding "double-jeopardy" when involving a one review process; and lastly, the harder to obtain *Coordinated solicitations*, which are more focused on solicitation involving multiple agencies on single topics. This is quite difficult to obtain as every agency has different procedures, mechanisms, timing restrictions, but it is possible.

Towards Collaborative Data Sharing – "US perspective" [13]

Speaker: Karl Levitt, University of California Davis, USA

Karl Levitt is a Professor at the University of California Davis. He conducts research in the areas of computer security, automated verification and software engineering. Prof. Levitt is a co-Director of the Computer Security Lab at UC Davis.

Prior to returning to UC Davis, Professor Levitt spent four years at the National Science Foundation during the INCO-Trust project and was involved in the build up of the EU – US collaborations in ICT Trust and Security from the very start.

Professor Levitt's presentation focussed on the motivation from the "U.S. Perspective" to foster international cooperation on security, with a main focus on collaborative data sharing – how to share, what data to share, what guarantees can be made about legal, regulatory, privacy issues, etc.

The many agencies within the US that are involved in cybersecurity were presented and Professor Levitt stressed the point made earlier by Sam Weber of the NSF that a tight integration and harmonization of the agencies involved both on a national and international scale is required. The point was also made that the other stakeholders should also be involved in these efforts, including the companies, research institutions, consultants, and others. The talk focused the two motivational focal points:

1. **A need for highlighting the needs for** a collaborative data sharing framework or architecture to deal with ongoing incidents. This should also not only focus on the technical aspects but should also deal with legal and regulatory challenges. A number of examples were given to show how the attacks don't respect international boundaries and we need to deal with them on a global scale. The systems must be able to monitor data for systems, routers, application logs in which different detailed levels of semantics are needed. There is also the issue of standardization when sharing data in order to ensure protection of data and that policies regarding the protection of data needs are being addressed. Prof. Levitt asserts that these discussions would leads to an architecture and presented some examples (medical data) of how we need to cooperate on an international basis, which is at a very low bandwidth today and this will have to change if we are to get a more favorable balance against the attackers.

2. **The extension of the GENI system to include international components in the future**. GENI is a large testbed in networking including security, which has been in operation for the last 5-6 years, has a primary objective of examining what the future networks will look like at scale. Experiments have been going live across the US to look at this. However, there are plans to have GENI sites internationally and they are looking for participation.

In summary, Professor Levitt said it is viewed as very important from the US perspective to build a framework and architecture for data sharing with collaborative parties from both the EU and further. The incentives are plentiful for this and are highlighted in the presentation materials as the big questions being addressed during the session.

Towards Collaborative Data Sharing – "EU perspective" [14]

Speaker: Barbara Daskala, ENISA, Greece

Barbara Daskala is employed in the European Network and Information Security Agency (ENISA), where she currently works on risk management practices and identifying emerging security and privacy risks posed by new technologies and ways to address them. Before that she was employed in the Institute for Prospective Technological Studies (IPTS) of European Commission's Joint Research Centre, where she was involved in research on the social implications of emerging and future technologies.

Ms. Daskala opened the talk by outlining the role of ENISA. ENISA is an EU agency established in 2004 and is located in Heraklion, Crete in Greece. There are around 65 experts at ENISA and it is an *EU Centre of Expertise specifically* involved in information security that facilitates information exchange across EU institutions, public and private sectors. Therefore, it is quite challenging for ENISA to provide the whole EU perspective on international data exchange needs.

Regarding the motivation for collaboration on data sharing for cybersecurity, ENISA have been involved within INCO-Trust and BIC activities and following the news of all of the recent security breaches, it is quite clear that it is a global challenge and motivation for us to work together to increase levels of security. Furthermore, the different approaches taken in various countries can also complement each other and result in a better methodology for improved security solutions and more effective mitigation.

The challenges we must face together are:

- Different views and mentalities in various countries;
- Different ICT maturity levels in various countries;
- Legal cross-border issues especially when talking about data exchange and sharing;
- For ENISA and EU: different approaches among EU Member States – it is therefore *difficult to have one point of reference!*

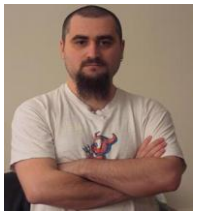
Some of the areas that ENISA are engaged in regarding International cooperation include the following:

a) **CERT work.** FIRST is a global initiative for CERTs setting up & incident handling guide, exercise material. Another initiative has been involved in supporting and facilitation of setting up CERTs in eastern African countries, e.g. Kenya, Tanzania.

b) **EU-US Working Group on cyber-security has been recently established in April 2011.** The role is to enhance collaboration between CERTs and facilitate a 1st EU-US cyber security exercise.

Ms. Daskala stressed that this is not an exhaustive list of EU initiatives. Other initiatives undertaken by ENISA include the setting up and running of expert groups of international experts, e.g. in cloud computing, smart phones, life-logging and engagement in "Information exchange" visits: e.g. Japan, Korea, China.

Threats and Actors [15]



Speaker: Sotiris Ioannidis, FORTH, Greece
Sotiris Ioannidis is a researcher with the Institute of Computer Science at the Foundation for Research and Technology (FORTH) in Crete, Greece.

Drawing upon his work in the FP7 projects WOMBAT [16] and SYSSEC [2], Sotiris Ioannidis presented the current situation on threat actors and provided an overview of their capabilities, threat models and assessment of the consequences of breaches or disruptions and their criticality. He stressed that in order to improve our knowledge about malicious code, we must work together on international data exchange especially on malware and to enable increased and better analysis results for context consolidation. This would enable the community to understand malware activities and trends. In order to improve our posture against these threat actors, this work can be supported by technologies and tools developed within these projects including new sensors for data acquisition (wireless, …) and new analysis techniques (code, context, …). The speaker highlighted a number of proposals for new technologies for enterprise and home-use and for new practices (CERTs, ISPs) and regulations.

The speaker focussed on the approach taken by the WOMBAT project, whose goal was the collection of information and alert data from multiple sources to learn something about the attacks. The motivation behind this was to understand the attackers and the enemy as cybercrime has become a huge business. Needed to understand what they were doing by collecting, sharing, manipulating and analysing the collected data. However, it is recognised there are a number of issues when collecting data, including monetary disincentives of sharing data (someone could be looking to make money with it); and of course, privacy issues. WOMBAT pushed for the sharing of this data to give the ability to investigate malware and how the threat actors operate. The first step in the WOMBAT process is data acquisition and collection of the data. The next step was the enhancement of the data to better visualise and contextualise of the data. This enabled more intensive data mining to understand the threats better and allowed the project to then build better tools in a feedback loop. The tools must be dynamic with the services being developed further with more enhancements. The project was able to promote the tools to industry, who were very supportive of the ideas and algorithms and have utilised them into new services. The project strived for a common API that could be adapted by others with different data sources and an interest in examining the data. There has been significant knowledge transfer to the security industry into their security projects and the project has made a great deal of impact and improved the knowledge of malware and threats by looking at the raw data and harvesting of this data via the new tools developed including new sensors used to collect the data.

The speaker concluded with lessons learned within the WOMBAT project. The TRIAGE framework enables multi dimensional analysis of security events. It has been applied to several data sources and led to interesting findings that will improve our ability to counter the many threat actors that are out there. The framework has been used and is being transferred within Symantec. Publications of these lessons contributed significantly to the visibility of WOMBAT, which concluded a few weeks ago.

Straw man architecture for International data exchange and collaborative analysis [17]

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.

John C. Mallery explained that the purpose of this technical part of the session was continuation of the work that was started during an earlier INCO-Trust workshop in May 2010, in New York City, specifically on jointly developing a Secure International Data Exchange Architecture for Cybersecurity outlined by the *Technical Challenges for Transnational Repositories* session[1]. Such a capability would reduce defensive gaps across the contributing states, and build crisis-response capacity and an international system for data exchange related to cyber crime. This would include attack patterns and '*signatures*', best defence practices, and response and recovery – individual and collective. This would greatly improve defensive understanding and coordination resulting in biasing the successful work factors for cyber attack and defense in favor of defenders.

At the workshop in May 2010 and in follow up iterations between the participants, as shown in **Figure 1** [18], a straw-man architecture was generated and this was described in more detail at the BIC session. Due to the duration of the session, it wasn't possible to get into very technical discussions but instead focus on bringing this work to the next level and commitment to the research and development coordination, which will enhance the outcomes through tactical planning, leveraging and combining task-relevant national expertise.

Malicious actors[2] 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.

Mr. Mallery asserted that 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.

Figure 1 illustrates an international cyber data sharing architecture that integrate data from multiple countries and sectors and returns collaboratively produce analytical products and threat mitigation techniques. Country fusion centers integrate country

[1] Mallery, John C. "Straw Man Architecture for an International Cyber Data Sharing System," position piece, INCO-TRUST Workshop On International Cooperation In Security And Privacy: International Data Exchange with Security and Privacy: Applications, Policy, Technology, and Use, New York: New York Academy of Sciences, May 3 - 5, 2010. http://www.cs.rutgers.edu/~rebecca.wright/INCO-TRUST/position.html

[2] cyber criminals, adversarial national intelligence agencies, hacktivists, and cyber terrorists for starters

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.

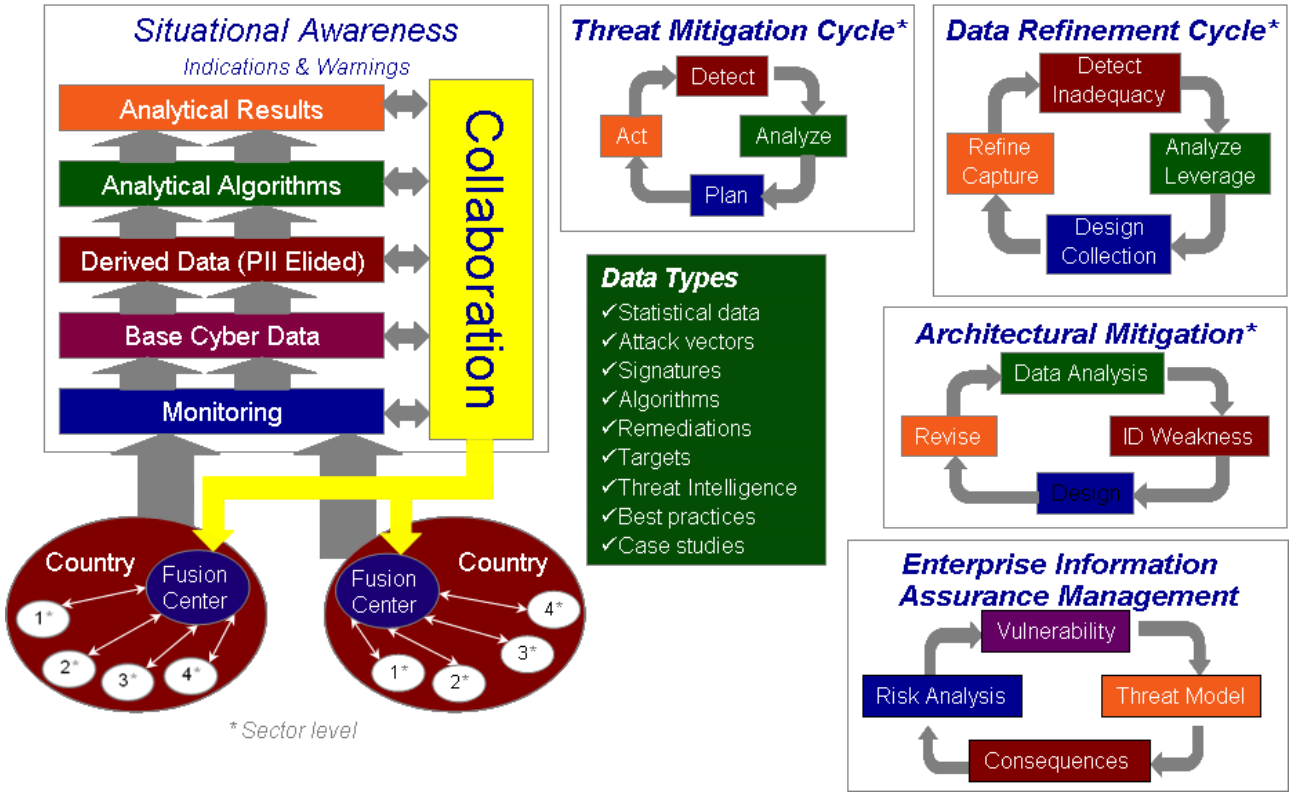


Fig. 1. Straw man architecture for international data sharing and collaboration.

Mr. Mallery explained that 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.

Mr. Mallery concluded by emphasising that as an international community, 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 defense. 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 defenses necessary for effective defense.

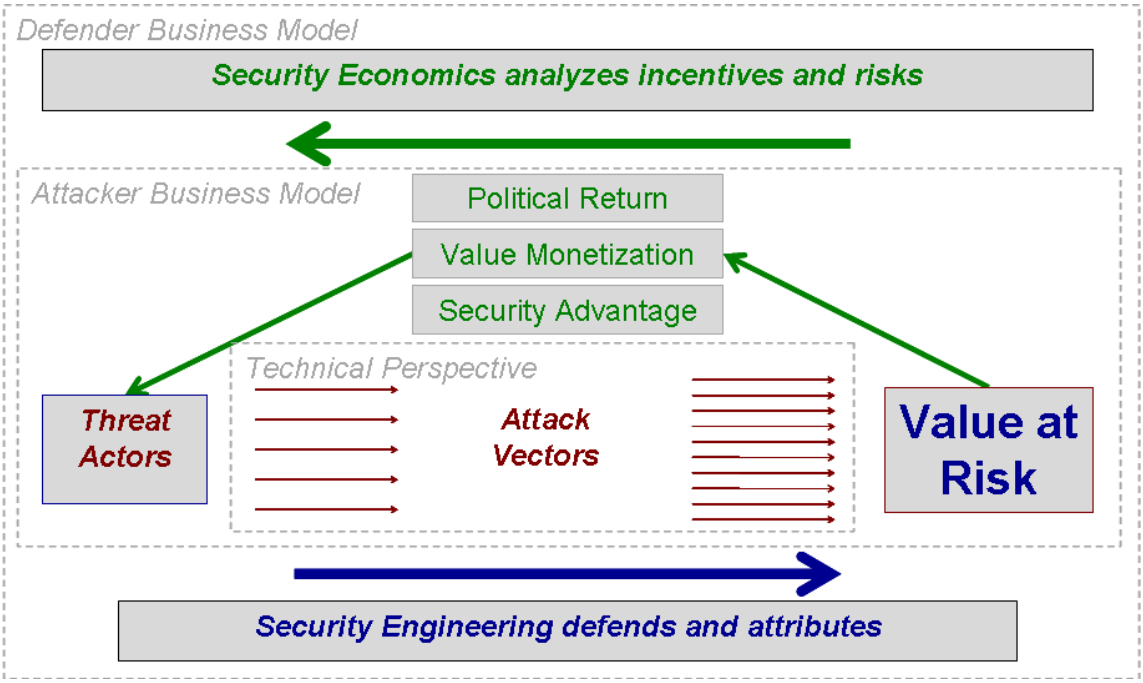


Fig. 2. Optimising integration of technical and economic perspectives for cyber-security.

Data exchange architecture used in a financial application in South Africa [19]

Speaker: Dr Barend Taute, CSIR Meraka Institute, South Africa
Barend Taute is an electrical engineer with a PhD in Electromagnetics. He is employed by the Council for Scientific and Industrial Research in Pretoria, South Africa and his current role is Manager: Contract R&D in their ICT unit. Barend is also FP7 Security NCP for South Africa and involved in various projects that promote Euro-Africa research collaboration.

Dr. Barend Taute set the scene for his talk describing the typical timeline for phishing incidents that have occurred in South Africa as shown in Figure 3. The phisher, the exploited website, the phishing website, the email harvesting activity and the banking victim could all be in different countries, creating various challenges for banks and forensic investigations. The whole process can be conducted with relative ease in a short time-frame using commercially available software.

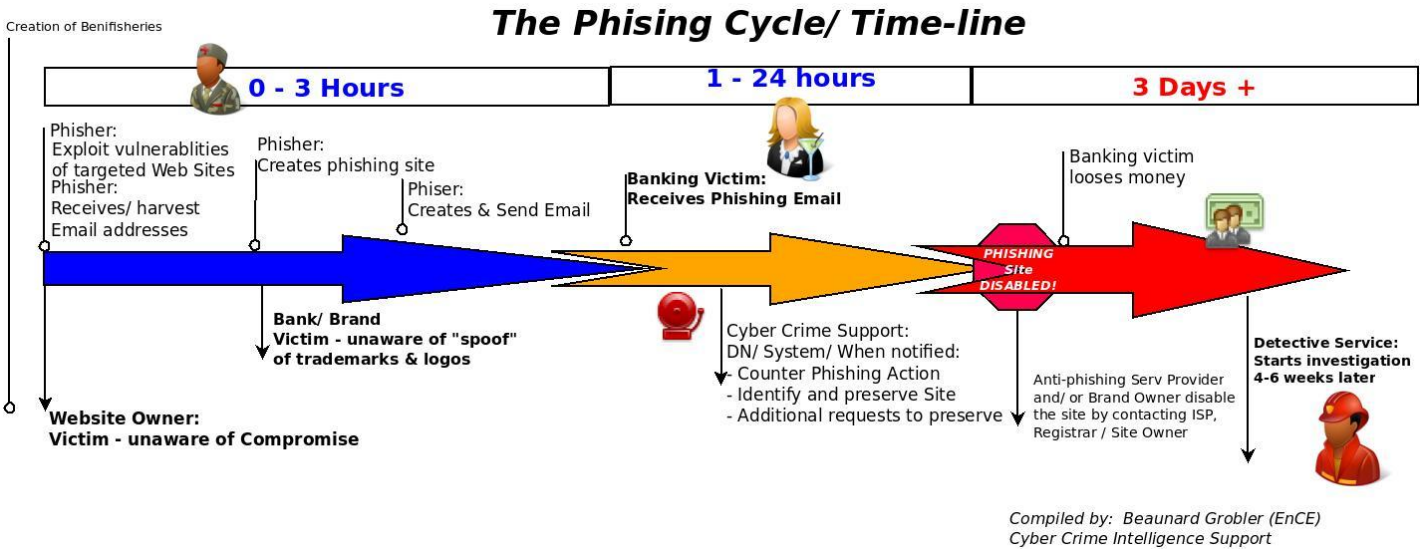


Figure 3. The phishing cycle/time-line.

The challenges for South African researches and investigators include:

- South Africa is getting about 4 % of the world's phishing volume and is currently 4th in the world (down from 18%, 3rd) after USA, UK, India;
- There are still new victims and an increase in local phishers;
- National Computer Security Incident Response Team (CSIRT) is not in place yet.

In addition, a new era of phishing is taking place with the use of malware and spyware, which enables the criminals to be more creative in their targeting of victims while remaining less visible. The steps to combat phishing are different for police and banks: Banks want to close down the phishing activities (via service providers) as soon as possible, while the Police need to investigate and find forensic evidence on active sites. This requires mutual legal assistance with the countries in question (not always in place) and gets complicated due to privacy issues and/or the lack of a local victim or complainant.

In order to address these challenges, Dr. Taute explained that trust must form the basis for international intelligence sharing and quick International Cyber Legal Assistance when it is needed. In addition, cyber security awareness is needed for users at all levels. This level of awareness is quite difficult in the developing world due to the lower levels of ICT literacy, and moving in a short time from very low levels of communications to full broadband connectivity. This makes them both more vulnerable and potentially becoming the hosts for cyber attacks. We need to look at creative ways to raise awareness so that the message is retained, e.g. using games and videos.

Dr. Taute pointed out there is a research project on network attack prediction and visualization using network telescopes to examine attack taxonomy and provision of alerts and data sharing.

Dr. Taute concluded by referring to a sector level data sharing architecture for the financial sector in South Africa, involving 6 major banks with internet banking that use techniques such as one-time passwords to cellphones. This is coordinated by the SA Banking Risk Information Centre. They are already gathering and sharing crime related information for the banks. There is a banking CSIRT in the planning phase and the data sharing architecture has some challenges concerning privacy and reputational risk that must be addressed firstly within the sector and then it will be addressed with local internet service providers and eventually international banks.

Identity related issues for data handling and aggregation [20]

Speaker: Glenn Gran, International Organisation for Knowledge Economy and Enterprise Development (IKED) –Sweden. Glenn Gran is a programme manager at IKED, the coordinator of the FP7 GINI Support action Project. Glenn Gran is an expert on innovation and ICT policies. Prior to this, he was the Research Director in an organisation affiliated with IKED, the Global Trust Center. Here he developed special competences in outstanding issues in the development and implementation of radical new solutions to improved ICT and cloud computing governance.

In his presentation, Mr Gran provided an overview of the GINI-SA project, which aims to investigate and establish the foundations for the architectural, legal, regulatory requirements, as well as the provisioning and privacy enhancing aspects, of an environment of user-centric identity management services. GINI-SA is based on the assumption that individuals, i.e. citizens, consumers, users of any related services, should be able to manage their own identity data and provide it in an open and flexible manner.

On this basis, the user can create and manage its own Individual Digital Identity (INDI) throughout its lifecycle (creation, change, management, revocation etc.). To enable trust between the actors in the INDI environment (INDI Users, Operators, Data Sources and Relying Parties), GINI envisions an operator-based trust model (i.e. 'brokered' trust relationship), where multiple INDI Operators mediate trust among the different actors involved. One of the underlying objectives of the GINI conceptual model is to remove (or at least minimize) the need for bilateral negotiation and/or communication among the different actors when making use of INDI Services. The INDI Operator with whom the INDI User has a direct contractual relationship serves as the main point of entry to the INDI environment for that User. One of the key benefits of the Operator Network model is that it can be standardised and regulated easier than a model, which is based on very heterogeneous and uneven entities, and this can greatly enhance the user's ability to build trust relationships with Operators.

Mr. Gran highlighted the fact that the INDI is verifiable against authoritative registers or data sources that the user selects. In principle, the INDI can be verified in two different ways: the user submits data to the Operator and these are verified against data sources of the users choice or the user does not submit data to the Operator but points to the data source where the data is located, and registers verified (and verifiable) links to those data. Obviously the latter is preferable from a privacy point of view since it removes the need to disclose the identity and send new data to the operator.

Mr. Gran also emphasized that using authoritative registers or data sources for verification will allow developers to leverage existing infrastructures, and offers the advantage of having single points of contact to update and manage information. This may help reduce the amount of copies of the same information in different databases, among which discrepancies may start to develop over time. From a privacy point of view, reliance upon distributed information repositories may additionally help minimize the amount of data stored centrally, which may in turn reduce the potential gain for attackers and as a result reduce cyber crime. However, the actual benefits for data

protection and privacy will depend largely on the implementation model and the safeguards that are put in place.

The GINI-SA recently finished the first year of the project, and will in the coming year put strong attention on the issue of the business model and what is required for developing viable operator solutions based on paying customers.

Legal Issues Associated With Data Collection & Sharing [21]

Speaker: Jody R. Westby, Esq., Global Cyber Risk LLC
Jody R. Westby is CEO of Global Cyber Risk LLC, located in Washington, DC. Ms. Westby also serves as Adjunct Distinguished Fellow to Carnegie Mellon CyLab. She chairs the American Bar Association's Privacy & Computer Crime Committee (Section of Science & Technology Law) and co-chairs the World Federation of Scientists' Permanent Monitoring Panel on Information Security. She is the author of the *Legal & Policy Tool Chest for Cyber Security R&D* and the *Legal Guide to Cyber Security Research on Botnets.* She has published four books on international issues pertaining to privacy, cybercrime, cyber security and enterprise security programs, as well as numerous articles and papers. She speaks globally on these topics.

Ms. Westby described the problem areas that arise from the complex legal and regulatory situations when dealing with data collection and the sharing of this data for for the purposes of cybersecurity research and development (R&D). As cyber attacks become more complex, organizations also are becoming more concerned about the legal and policy considerations associated with R&D projects, particularly those involving botnets or sophisticated attack structures, because they can raise a number of legal issues. Guidance on the legal, regulatory and privacy issues, however, is scarce and highly complicated. This complexity is compounded by a highly inconsistent global legal framework that makes an analysis of the legality of a research approach even more difficult.

In order to improve the situation, the Department of Homeland Security's Cyber Security R&D Division funded a project entitled "New Frameworks for Detecting and Minimizing Information Leakage in Anonymized Network Data." Within this project, a publication was developed by Ms. Westby entitled The *Legal & Policy Tool Chest for Cyber Security R&D* (*Tool Chest*). Ms. Westby described the Legal & Policy Analysis Tool Chest, which is a comprehensive set of three tools that may be used both to help analyze the legal and policy implications associated with the use of traffic data in cyber security R&D and to mitigate identified risks. The tools are:

1. Legal Analysis Tool on Obtaining & Using Network Communications Data (Legal Analysis Tool), which focuses on obtaining, using, and disclosing intercepted and stored communications data.
2. Privacy Tool on Using Network Communications Data (Privacy Tool), which focuses on the relevant privacy legal considerations with this data.
3. Protection Measures Tool, which contains sample contract clauses and memoranda of agreement that can be used by researchers and their organizations to mitigate legal risk.

While the Tool Chest is based on U.S. laws, Ms. Westby stressed that it also takes into account foreign legal issues, such as disparities in privacy laws, especially with respect to the EU. The Privacy Analysis Tool explains these legal and policy privacy considerations and provides a decisional framework to guide researchers and institutional review boards (IRBs) through the process of determining (1) whether a dataset has legal or privacy issues associated with it, (2) whether these issues are fatal and may preclude the use of the data, and (3) whether certain legal issues may be mitigated or eliminated through anonymization or other de-identification techniques.

Ms. Westby presented the *Legal Guide on Cyber Security Research on Botnets (Botnet Legal Guide),* which was developed in order to extend the *Tool Chest's* analysis and examine the myriad of legal issues associated with this particular type of research. The *Botnet Legal Guide* also was funded by DHS's Cyber Security R&D Division and developed by Ms. Westby as a component of a technical research project led by Georgia Institute of Technology on "Countering Botnets: Anomaly-Based Detection, Comprehensive Analysis, and Efficient Mitigation."

In conclusion, the *Tool Chest* and *Botnet Legal Guide* are companion publications that provide the cyber security research community with a central repository of definitions, descriptions of the laws, worksheets, decisional frameworks, tables simplifying privacy provisions and penalties, and conclusions regarding how U.S. laws apply to datasets to be used in research projects and impact research activities. International considerations, especially with respect to privacy and cybercrime laws, present challenges for researchers that require careful and joint analysis. The *Tool Chest* and *Botnet Legal Guide* offer a positive step toward helping researchers, IRBs, legal counsel and management better understand the legal issues associated with research projects and the data used in them. Both publications are being published by the American Bar Association in the fall of 2011.

Ms. Westby stressed the need for international collaboration between the legal and technical communities, particularly with respect to exploring the extraterritorial reach of laws and inconsistencies in legal frameworks. Researchers particularly need to better understand critical jurisdictional differences in the global legal framework for interception, privacy, and cybercrime. Programs such as PREDICT[3] that include the legal analysis of datasets that are offered to researchers help build confidence that data used in research efforts will not run afoul of the law, but they do not address the legality of the activities undertaken by researchers when using the data. The development of best practices with respect to certain research activities would make a significant difference toward encouraging legal conduct in R&D projects.

More information on this work can be found in a recently published paper by Ms. Westby in the proceedings of the Building Analysis Datasets and Gathering Experience Returns for Security (BADGERS) 2011 Workshop, Apr. 10, 2011, Salzburg, Austria (part of EuroSys 2011), http://iseclab.org/badgers2011/.

[3] PREDICT is an acronym for the Protected Repository for the Defense of Infrastructure Against Cyber Threats sponsored by the U.S. Department of Homeland Security (DHS) Science & Technology Directorate's Cyber Security R&D division,

SUMMARY AND CONCLUSIONS

The goals of the BIC session were the following:

- *Planning matters:* to prepare the ground for the extended BIC Annual forum workshop currently scheduled for late 2011;
- *Scope and topics for collaboration:* to clarify scope and possibilities for international collaboration on ICT trust and security; as an example of identified topics, to continue the work on the development of a *straw-man* architecture for secure international data exchange for cybersecurity, introduced at an earlier (May, 2010) INCO-Trust workshop, and to explore the technical and organisational challenges and constraints that arise from this.

A further goal was to benefit from co-locating this meeting as part of the SysSec Workshop to allow contribution by a wide representation from security research communities.

The results of the meeting are summarised against these headings.

Planning matters

The precise date and location for the BIC annual forum in Q4 2011 is still under discussion as many of the stakeholders need to be included in the discussions. Among the options considered is to relate it to another large scale event being held in the EU during Q4 2011.

The mission of the BIC annual forum is discussion and agreement on technological challenges/gaps of common interest amongst the countries, agree on what can and needs to be done internationally (who can contribute to what), and then work at an international level towards delivering on cooperation towards solving these joint technological challenges. The forum will enable the working towards the definition of tangible international activities, including establishing success metrics and setting up global projects.

The objectives of the BIC annual forum are the following:

- Identification of the technological challenges that really need and could be tackled in common between the countries so they can be elaborated clearly with the policy makers in the respective countries as a way forward;
- highlighting the current bi-lateral (and potentially overlapping) country to country cooperation(s) into a more comprehensive unified global cooperation eg. US-India, EU- US, etc.
- Identification of the responsible agency(ies) per country and points of contacts to participate in the global cooperation on ICT trust and security.

In the BIC session on 6th July 2011, during discussions and presentations, a number of topics were already identified for further planning consideration that can be carried forward to a longer, more detailed session at the BIC annual forum. Contributions were invited on these in preparation for the larger event. These include:

- What kind of data sharing and collaborative analysis architecture could be built

with today's technologies and operational knowledge?

- Who are the current actors around the globe and what are their approaches and can these be leveraged and harmonized together?
- What are the gaps?
- What research would be needed to build a better data exchange architecture for cyber security in the 5-10 year time frame?
- Who are the actors needed to carry out this research and where are they from?
- What organizational modes are necessary for this research to proceed most expeditiously?
- What funding sources and mechanisms can be mobilized to support the joint international efforts required in research and adoption?
- In order to better motivate countries to contribute and support the effort, we should highlight the rationale and motivation for designing and building sophisticated architectures for international cyber data sharing, collaborative analysis, and collective defence. For example,
  - Dramatically improve defensive coordination to move the economic advantage away from offence in favour of defence;
  - Create shared real-time situational awareness;
  - Identify cyber data for sharing together with leverage scenarios and collection issues;
  - Motivate targeted research to enable effective collection, sharing, analysis and response.

Scope and topics for collaboration

During the session on 6th July 2011, although there wasn't sufficient time to allow for more in-depth exploration or further detailing of the proposal for a data-sharing framework, it was clear that this provided a powerful example of where well-organised and motivated international collaboration could provide the leverage to address high-priority issues: in this case, rapid, collective response to attack or failure in cyberspace, through the sharing of intelligence and the design and development of shared defence strategies. As with all defences, penetration by an attacker would have drastic consequences, so the protection of the system itself and of its contents leads to further challenges.

A number of technical aspects were highlighted when going through the straw-man architecture for coverage at the larger workshop being planned for Q4 2011. These included:

- ***Research required on technical enablers:*** The enablers for a secure international data exchange architecture eg. cryptography based obfuscation, sensors on the network, monitoring traffic capabilities, privacy protecting identity management, amongst others.
- ***Integration of technical and economic perspectives:*** *to* optimize defensive interventions for the disruption of malicious business models.

- ***Sharing Incentives:*** Research is needed on incentivizing data sharing and collaboration across entities, sectors and countries. Basics of how we share recognizable data, especially on critical infrastructures and across different countries. eg. share patterns for recognizing advanced persistent threats without losing efficacy if they are exposed. What obfuscation and security measures would make patterns easier to share?
- ***Collection Prioritization:*** Methodologies are needed for identifying and prioritizing data for collection in order to yield high leverage against cyber threats across different time.
- ***Learning and Agility:*** Data sharing and collaboration needs to evolve rapidly to keep pace with emerging threats.
- ***Resilient Sharing Architecture:*** Research needs to produce a defensible architecture for sharing and collaboration.
- ***Integration of technical and legal requirements:*** The need for international collaboration between the legal and technical communities, particularly with respect to exploring the extraterritorial agreements, including Safe Harbor agreements, pertaining to reach of laws and inconsistencies in legal frameworks.
- ***Trust:*** Data sharing and collaboration will only be a good as the confidence participants have in the ability of the architecture to enforce access control and dissemination policies.

Acknowledgments

The BIC project is funded under Call 5 of FP7 ICT and began on 1st January 2011 with a duration of three years. The project is supported by the European Commission DG INFSO, Unit F5 ICT Trust and Security Research [22].

The BIC project would like to acknowledge the support of the organizing committee members and to the SysSec project workshop organizers.

A number of additional positions were submitted to the organisers prior to the session and there wasn't enough time to include during the session. Please see [23], [24], [25], [26] for more details. The presentations are available at http://www.bic-trust.eu/events/event/bic-session-syssec-workshop/.

REFERENCES

[1] BiC project web site http://www.bic-trust.eu/

[2] SysSec project web site http://www.syssec-project.eu/

[3] http://www.cs.rutgers.edu/~rebecca.wright/INCO-TRUST

[4] http://www.securityconference.de/Home.4.0.html?&L=1

[5] https://update.cabinetoffice.gov.uk/sites/default/files/resources/CyberCommunique-Final.pdf

[6] http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CL=ENG

[7] Remarks at the 28th Annual International Workshop on Global Security, Paris, France 16th June 2011 http://www.defense.gov/speeches/speech.aspx?speechid=1586

[8] International cooperation "at nascent stage" - U.S. Secretary of Homeland Security Janet Napolitano, Vienna, 1st July 2011. http://www.reuters.com/article/2011/07/01/us-cybercrime-idUKLDE75T1CC20110701

[9] http://www.syssec-project.eu/media/page-media/23/bic2011-01-clarke.pdf

[10] SysSec workshop http://www.syssec-project.eu/events/1st-syssec-workshop-program/

[11] Clarke, James, Wright, Rebecca, et al., "D4.2 INCO-Trust 2nd Workshop report", available at http://www.inco-trust.eu/incotrust/general/project-impact.html

[12] http://www.syssec-project.eu/media/page-media/23/bic2011-02-weber.pdf

[13] http://www.syssec-project.eu/media/page-media/23/bic2011-03-levitt.pdf

[14] http://www.syssec-project.eu/media/page-media/23/bic2011-04-daskala.pdf

[15] http://www.syssec-project.eu/media/page-media/23/bic2011-05-ioannidis.pdf

[16] WOMBAT project web site http://www.wombat-project.eu/

[17] http://www.syssec-project.eu/media/page-media/23/bic2011-06-mallery.pdf

[18] Mallery, John C. "Straw Man Architecture for an International Cyber Data Sharing System," position piece, *INCO-TRUST Workshop On International Cooperation In Security And Privacy: International Data Exchange with Security and Privacy: Applications, Policy, Technology, and Use*, New York: New York Academy of Sciences, May 3 - 5, 2010. http://www.cs.rutgers.edu/~rebecca.wright/INCO-TRUST/position.html

[19] http://www.syssec-project.eu/media/page-media/23/bic2011-07-taute.pdf

[20] http://www.syssec-project.eu/media/page-media/23/bic2011-08-grann.pdf

[21] http://www.syssec-project.eu/media/page-media/23/bic2011-09-westby.pdf

[22] DG INFSO Unit F5 web site http://cordis.europa.eu/fp7/ict/security/

[23] Challenges in streaming temporal and spatial network data (78.1 KB) Chalmers University

[24] Multi-party computation approach as a privacy solution developed in the SEPIA project (314.5 KB) ETH Zurich

[25] Different approaches for data sharing (78.0 KB) Moscow State University

[26] Joint collaboration to guarantee an optimal incident response and post incident data analysis in mobile scenarios (148.2 KB) JRC & KTH