Ladies and Gentlemen,

If I had to give an account of the events of the past few months, inevitably the most important thing was the Cyber Storm II exercise, taking place in early March. Without stealing the merit from the organizers, let me say that cooperation of this kind is what will drive policymakers and all stakeholders ahead in the fight against global cyber threats. I had the chance to take part in the observer program of the exercise, which allowed some insight to the planning stage and the ‘real action’ in the operation room. Cyber Storm II proved to be a great success, and DHS has been kind enough to provide a brief summary of what the exercise was about. And while reading the article, let us not forget that the scenario involved cross-sector and inter-governmental representation from five countries. Cyber Storm III is already on the agenda, where international involvement will be even greater, so it is just a matter of time before a global cyber exercise can take place.

In connection with CSII, another initiative has to be mentioned. Also in March, the first meeting of the International Cyber Center at George Mason University (GMU) took place in Washington, DC. Andy Purdy of former DHS NCSD/US-CERT and Arun Sood of GMU are the masterminds behind the initiative, and leading international figures were present from governments, academia, and the private sector to address some issues related to information and communications technologies, that connect our CII sectors. The article provides a vision of the center.

Let us move over to the this side of the Atlantic, and see how old Europe is doing in ICT and CIIP issues. It is good to see that cooperation seems to be the keyword in the article provided by Switzerland, and from the ENISA as well.

Courtesy of the Swiss MELANI, we can get an insight on a program to raise awareness on the dangers of industrial espionage and proliferation. The article highlights on the overlap and the scope of possible cooperation between internal security, intelligence and critical information infrastructure protection. The beneficiaries of this program are the numerous players of the private sector of the Swiss economy.

ENISA, on the other hand builds on a more regional cooperation. A workshop has taken place early March on resilient eCommunications actions in Europe, and a summary of the workshop provides some insights and visions on the regulatory issues and technologies and standards to create service integrity. You may already know that resilience is a new magic word, so keep we’ll keep you posted on follow ups to this event as well.

Hope these articles will be of interest, and you will once again enjoy the readings!

Sincerely,

Ferenc Suba
Editor-in-Chief, Meridian Newsletter
General Manager, CERT-Hungary
Cyber Storm II Recap

In March, the United States Department of Homeland Security’s National Cyber Security Division hosted the Cyber Storm II National Cyber Exercise. The exercise included participants representing over 18 Federal Department and Agencies, 40 companies, 9 states, and 5 countries. During the exercise, participants from the public and private sectors had the opportunity to exercise their response capabilities and examine their policies, processes, and procedures for handling a cyber attack.

The exercise examined the linkages between public and private sectors, and how their connections play a role in cyber security and incident response capabilities. In addition to government agencies, Cyber Storm II participants included private sector companies from industries dependent upon cyber infrastructure, including communications, information technology, chemical, and transportation (rail/pipeline).

Given the growing sophistication of cyber attacks and the increasing reliance on cyber infrastructure, exercises like Cyber Storm II provide a platform to better understand the existing interdependencies.

Cyber Storm II planners collaborated during an extended planning period to develop a realistic scenario which allowed all participants to assess their individual exercise performance. Throughout the exercise planning process, planners convened during a series of conferences and meetings designed to help establish and strengthen relationships that were critical during Cyber Storm II, as well as in the event of a real cyber incident.

The fictitious adversary in Cyber Storm II executed a scenario to advance a distinct political and economic agenda. Throughout the exercise, players responded to attacks from a variety of sophisticated threat vectors to examine their organization’s ability to prepare for, protect from, and respond to a cyber attack. To ensure that participants gauged the capacity of their crisis response systems, the scenario simulated an attack that was plausible, but not tied to any specific vulnerability.

The scenario progressed as players received “injects” from Exercise Control via e-mail, phone, fax, in person, and exercise web sites. As a distributed exercise, Cyber Storm II players responded to the scenario from their own office locations using their standard means of communications.

To capture and implement the lessons learned from Cyber Storm II, exercise participants are participating in a series of After Action Conferences designed to inform an After Action Report to be released in late summer.

Exercises such as Cyber Storm II are critical for maintaining and strengthening cross-sector, inter-governmental and international relationships; enhancing processes and communications linkages; and ensuring continued improvement to cyber security procedures and processes.
Prophylax
-A program to prevent from industrial espionage and proliferation

In 2004, Switzerland set up a prevention and awareness campaign known as “Prophylax”. The objective of this campaign is to inform private enterprises and public institutions about the dangers of industrial espionage and proliferation. MELANI, the Reporting and Analysis Centre for Information Assurance is involved in this program since 2007.

Prophylax was set up as part of the Federal Act on Measures to Safeguard Internal Security. According to this act, the Service for Analysis and Prevention (belonging to the Federal Office of Police) has amongst others the task of taking preventive measures in order to early recognize the risks relating to illegal intelligence activities, illegal traffic in weapons and illegal dealings with radioactive materials and sensitive technology (falling under the heading of “non-proliferation”). Prophylax was initiated by the Service for Analysis and Prevention in cooperation with the local police authorities.

The fight against espionage and proliferation in Switzerland is first of all based on prevention and awareness raising. Prophylax is mainly based on personal visits to private enterprises and public institutions that operate in sensitive areas and are vulnerable to espionage or proliferation.

In our modern information society, companies and institutions are increasingly dependent on modern systems of information and communication. Security issues concerning information infrastructures have thus become a vital concern due to the growing number of communication networks. The infiltration of networks, or the theft, manipulation or loss of data, can seriously threaten the economy, society and the state. It has therefore become essential to protect against these risks. Even small and medium-sized businesses can be targeted due to their research and development projects and the know-how they possess.

This is where MELANI plays a role; bringing to the Prophylax campaign its know-how concerning information assurance and espionage by means of information technology. MELANI participates by visiting institutions and enterprises for which information and communication infrastructure has a strategic role. Furthermore, Information security must not stop at the gates of a company or at the borders of a state. International companies must be aware that information can go astray at the level of their subsidiaries, consortiums or commercial partners.

Prophylax is an example of cooperation in raising awareness between different partners on a local and state level with the private industry or public institutions. Furthermore, Prophylax also sheds light on the overlap and the scope of possible cooperation between internal security, intelligence and critical information infrastructure protection.
Reliable communications networks and services are now critical to public welfare and economic stability. Attacks on Internet services, disruptions due to physical phenomena, software and hardware failures, and human mistakes all affect the proper functioning of public electronic communications (eCommunications). Such disruptions reveal the increased dependency of our society to these networks and their services.

The experience shows that neither single providers nor a country alone could effectively detect, prevent, and effectively respond to such threats. Today, the effort to secure businesses, countries and personal identities requires a greater level of coordination among parties that have not traditionally worked together as closely as they will need to. National Regulatory Authorities, public e-Communication Network and Service Providers, Software and Hardware Vendors, IT security teams, Consumers, Research Entities and Standardization Bodies, they are all possible targets, yet they’re also allies.

Recent European Commission’s Communications\(^1\) highlighted the importance of network and information security and resilience for the creation of a single European Information Space. They stressed the importance of dialogue, partnership and empowerment of all stakeholders to properly address these threats. The existing and recently proposed updates of Regulatory Framework Directives include certain regulatory provisions for the improvement of the security and resiliency of public eCommunications.

The European Network and Information Security Agency (ENISA), fully recognising this problem, devised a Multi-annual Thematic Program (MTP) with the ultimate objective to collectively evaluate and improve the resiliency of public eCommunications in Europe\(^2\).

The Agency intends to reach this goal, among others, by taking stock in every Member State of the existing security regulatory frameworks related to the resilience of public eCommunications. The stock taking will help the Agency to identify common measures and good practices but also gaps and inconsistencies. The Agency intends to compare its findings against trends, recommendations, and guidelines proposed by other national, European and global initiatives. After extensive consultation with all relevant stakeholders ENISA plans to suggest guidelines that could improve the resiliency of public eCommunications in Europe.

On the 7\(^{th}\) of March ENISA organised its first consultation workshop on the resiliency of eCommunications. The workshop attracted the interest of leading pan European experts, policy makers, national regulators, eCommunications providers and sector associations (EICTA, ETNO, ECTA). The participants discussed about regulatory issues, as well as, technologies and standards.

The workshop revealed differences in the regulatory approaches, practices and measures of Member States. Differences include the mandate of “NIS regulators” (e.g. mandate is assumed by the NRA, or other organisations and/or ministries), the regulatory compliance tasks (e.g. audits, issuing of regulations and recommendations), or even the regulated topics. The workshop also revealed different levels of maturity regarding NIS regulatory experience, i.e. some countries have long experience with regulatory measures on the resilience of eCommunications, while others are developing their capabilities. Finally, the participants discussed co-operation models among providers and regulators and highlighted the importance of co-operation, exchange of knowledge and the development of best practices.

\(^1\) “2010 – A European Information Society for growth and employment” & “A strategy for a Secure Information Society”.

The workshop also addressed technologies and standards in the area of network availability, network integrity, preparedness measures and infrastructure service integrity. More specifically, in the area of network availability participants debated about resilient design, resilient equipment, diverse transmission routing, priority communications, emergency calls, securing power supply, etc. In the area of network integrity participants debated about fault/incident management and response plans, configuration, performance and real-time traffic management, access control management, etc. Regarding preparedness measures participants discussed about provocative testing of networks and equipment, identification of failure scenarios, contingency plans for service restoration, repair and recovery, systemic analysis of faults, etc. Finally, regarding infrastructure service integrity participants debated about IPv6, DNSSec, security in BGP, etc.

The workshop and its results will help the agency to better focus its efforts by identifying the topics that mostly affect the resilience of public eCommunications. It’s a great opportunity to build trustful working relationships with identified stakeholders and engage them at the different steps of the initiative, namely in the identification of issues, participation in targeted interviews, validation of findings and assessment of results, exchange of experiences, identification and validation of gaps and good practices, and contribution to the preparation of ENISA’s guidelines.

The effectiveness of such an initiative heavily depends on the collaboration and communication among constituencies that have not traditionally worked together as closely as they will need to.

For that reason ENISA issued an open Call for Expression of Interest addressed to all relevant stakeholders. Interested stakeholders that would like to contribute to this initiative are kindly asked to visit our web site http://www.enisa.europa.eu/pages/resilience.htm.

The International CIIP Handbook 2008
-A forthcoming publication

This summer, the Center for Security Studies (CSS) at the ETH Zurich launches the 4th edition of the International Critical Information Infrastructure Protection (CIIP) Handbook. The 2006 edition contained surveys of 20 national and 6 international critical information infrastructure protection policies. The new edition includes an update of the existing surveys and covers five additional countries (Brazil, Estonia, Hungary, Poland, and Spain). For each country survey, five focal points of high importance covering conceptual and organizational aspects of CIIP are considered: the definition of critical sectors; past and present CIIP initiatives and policies; organizational structures; early warning approaches and public outreach; and law and legislation in the field of CIIP.

Like the previous editions, the Handbook will be available both in electronic form on the internet (http://www.cm.ethz.ch/projects/current/detail.cfm?id=15165) and in hardcopy. It can be used either as a reference work for an overview of CIIP policy formulation and commonly used CIIP methods and models or as a starting point for further in-depth research.
The Center’s goal is to better drive measurable progress on national and international priorities and issues related to information and communications technologies (ICT) – not the least of which is security, business continuity, resilience, and research and development. We believe it is essential for governments and private companies, academic institutions, and other organizations to increase collaboration and information sharing – within nations and internationally – to more effectively identify, resource, address, and track progress related to important issues.

To achieve measurable and efficient progress, we will work collaboratively with key stakeholders to facilitate creation of a strategic vision, framework and plans on issues and priorities where it is lacking, and strengthen and implement strategies that do exist, we are forming an International Cyber Center at George Mason University (GMU) near Washington, DC.

Among the issues we tentatively have in our sights that we believe need greater collaboration and information sharing, are several we have identified as priorities:

• ICT to the developing world, including CERT capacity building;
• Risk to the global information infrastructure and preparedness for incident response and recovery;
• Greater coordination on the collection, analysis, and sharing of data regarding – and pursuit of – the most significant malicious actors in cyberspace and those who enable them;
• Research and development – how to better assess and mitigate risk to the global information infrastructure (and ICT within nations), and to address the long-term hard problems facing the evolution of cyberspace.

We believe that priorities and issues can best be addressed when interested individuals and organizations within and across governments and the private sector, can be encouraged to come together to collaborate and leverage their efforts, identify and fund resource requirements, and track progress toward common goals. If we do not try to work together to identify what we need and want to do, and track our progress along the way, we significantly lessen chances of success, and increase the costs of our efforts.

In forming our Center at GMU, it will not be our intent to replace or otherwise supplant the efforts of others currently engaged in the issues we will work on. On the contrary, we want to serve as a sort of clearinghouse about the priority or issue, and the efforts being taken to address it. We want to help make sure that key players, other stakeholders, and those who care about or might be impacted by efforts in a subject area, are informed about past, current, and future efforts, and are encouraged to work together at the strategic level to identify and collaborate on goals, resource requirements, milestones, and deliverables. We want to increase the visibility of such efforts to those who can affect the actions and expenditure of resources of government, academia, and private organizations. We want to make it much clearer and easier for those in positions of authority to know why an issue or priority is important, and what they can do to help.

We want to help encourage collaboration and information sharing so that conflicting, parallel, and overlapping efforts can be coordinated and leveraged where possible. We hope individuals and entities with similar interests will at least share information on the nature of the problem or priority they are working to address, and the work that has been and is being done, and that opportunities are created to bring work together.

1 Donald A. (Andy) Purdy, Jr., Esq., was former Acting Director, National Cyber Security Division (NCSD)/US-CERT, of the U.S. Department of Homeland Security, and currently is President of DRA Enterprises, Inc. (www.andypurdy.com), member of the Executive Advisory Board of BigFix, Inc., and a partner in the law firm of Allenbaugh Samini LLP (www.alsalaw.com).
2 Dr. Arun Sood is from the Computer Science Department of George Mason University.
To provide a better idea of what we will be looking at and how we hope to partner and seek funding for our efforts, here is additional detail on the subject areas we have identified as priorities so far.

1. **ICT to the Developing World.**

We would like to help promote the proliferation of information technology capability and infrastructure, and internet connectivity to the citizens in the developing world, in a manner that strives to be consistent with ever-improving security best practices and standards, and is demonstrably sensitive to privacy concerns, and the need to have a decreasing impact on the environment.

To achieve this we want to partner with government, academic institutions, and private companies to help to bring (or enhance) information and communications technologies to the developing world, and to build or strengthen the security and resilience of those infrastructures, including the formation of robust CERTs/CSIRTS (Computer Emergency Response Teams/Computer Security Incident Response Teams).

We want to build on efforts of the Organization of American States (OAS) the International Telecommunications Union (ITU), in partnership with the governments of individual nations, multi-nation organizations, associations, academic institutions, and private companies, to identify and fund progress, and promote the information sharing and collaborative efforts within nations, regionally, and globally that are necessary to create or strengthen existing efforts. We want to develop approaches that can be customized for each nation’s circumstances and culture, and which leverage the resources, capabilities, and resources that exist there, and that can be sustained by the resources and funding of that nation’s government and private sector.

2. **Risk to the global information infrastructure and preparedness for incident response and recovery**

Our center envisions the creation of an international collaboration framework involving key government, academic, and private sector partners to address the cyber risk to the global information infrastructure.

Although there have been important efforts at multi-lateral collaboration, such as, the IWNN (International Watch and Warning Network), there has been insufficient coordinated, collaborative efforts among governments – much less governments and the private sector –

- to assess and to identify priority measures to mitigate the risk to the global information infrastructure, and
- to identify and implement the requirements for a robust international capability to detect, analyze, respond to, and recover from major cyber incidents.

We want to help interested persons in government and the private sector in Europe, the U.S., and globally come together to identify requirements, necessary resources, and begin the progress of implementing those requirements and tracking progress along the way.

One early step might be to have a meeting at which key government and private sector representatives discuss the results of key exercises (like Cyber Storm in the U.S.) and real-world experiences (such as impacted networks in Estonia). This meeting would include a “table top” exercise to talk through how future incidents might be addressed - what information would be necessary, who should it be given to and shared with, how would it be analyzed, how would alerts go to users, and how would recovery be coordinated and effectuated.

3. **Cyber Crime/Malicious actors -- Greater coordination in the collection, analysis, and sharing of data regarding -- and pursuit of -- the most significant malicious actors in cyberspace and those who enable them.**

It is not without some hesitation that we raise this issue, because we value so highly the efforts of law enforcement in this area, and do not want to appear to be criticizing the quality or success of their efforts, particularly accomplished as it usually is with such scant resources and sometimes at great personal risk.

We believe the efforts of law enforcement must be complemented and supplemented by a strategically coordinated collaboration at the national and international levels, between law enforcement, others in government, private associations, and private companies.
The traditional efforts of law enforcement to detect/investigate wrongdoing in the United States have included some notable efforts to reach out to, and partner with the private sector – FBI/InfraGard, the Secret Service/Electronic Crimes Task Forces and the Department of Justice (Computer Crime and Intellectual Property efforts), and to raise public awareness of the threats in cyberspace. There have been some significant efforts by the U.S. Department of Justice to collaborate with European and other nations on the European Convention on Cybercrime and the G-8 High Tech Crime initiative.

Our center will promote an enhanced national and international strategic level of collaboration and information sharing by law enforcement, others in government, private companies and organizations, and business, consumer, and user groups, to help reduce the frequency and impact of malicious activity in cyberspace and the black market in malicious cyber tools, and help to cut off the payment processes that are the life blood of the criminality.

Collaboration on the collection, analysis, and sharing of data on malicious activity should help build a common understanding of (i) the most significant players and those who enable them, whether it be uncooperative governments, unscrupulous merchants or businesses, credit card companies (or other payment processors), (ii) the exploits they are using and vulnerabilities they are exploiting, (iii) the nations that lack the resources and/or will to cooperate against the malicious actors, (iv) the technology requirements and processes that can reduce vulnerabilities and the impact of exploitation, and (v) practices and policies of internet service providers and others that can help reduce the malicious activity and its impact.

Non-law enforcement government entities and international organizations must work more actively to help to facilitate the creation and enhancement of international collaboration to remove obstacles to successful investigation, prosecution, and punishment of malicious actors, and help law enforcement and private entities tackle the issues that contribute to the magnitude and success of the malicious activity.

Private sector organizations must play their part in working with government to support law enforcement, to work collaboratively to reduce the magnitude and severity of malicious activity, and to pool their resources to bring civil legal actions against malicious actors and those who enable them. The full complement of actions must be brought to bear in a strategic approach to address these issues: law enforcement, diplomatic and political, technological, and nongovernmental lawsuits. Once identified, the key stakeholder groups must meet regularly to track the progress their efforts are making in reducing the magnitude and severity of malicious activity in cyberspace.

4. Research and development

Research and development is being undertaken by governments and private sector entities around the world. The Center will help to create and enhance strategic and tactical collaboration and information sharing on how to better assess and mitigate risk to, and increase the resiliency of, the information and communications infrastructure and technologies (and ICT within nations), and to address the long-term hard problems facing the evolution of cyberspace.

On March 14th of this year at George Mason University, we helped to organize and conduct an R&D event involving representatives of the European Commission, the United States Government, the Internet Security Alliance, and major private companies. Building on that collaboration, we are planning to hold a larger Forum on information and communications technologies in December of this year in Europe to bring together representatives of the U.S. Government, the European Union, other interested nations, and academic institutions and corporations from around the globe.

We are seeking representatives of these organizations to help us plan the forum and find sponsors and other funding sources to bring it to reality.

Conclusion

The vision of the center is one founded on the importance of collaboration and partnerships. We invite expressions of interest in helping us form, inform, fund, plan, and implement the priorities of the center. We are particularly interested in finding organizations with which we can collaborate, funding sources for the center and its priorities, information about work that has been done and/or is ongoing, and individuals who would like to help us refine and implement this vision.
Appendix

The following are the proposed issues and actions for the center to consider focusing on, with the timing/prioritization to depend on the interests of key partners and stakeholders, and opportunities presented by available funding:

1. Promotion of information technology capability and infrastructure, and internet connectivity to the citizens in the emerging world, in a manner that strives to be consistent with ever-improving security best practices and standards, and is demonstrably sensitive to privacy concerns, and the need to have a decreasing impact on the environment;
2. Creation of an international collaboration framework involving key government, academic, and private sector partners to address the cyber risk to the global information infrastructure;
3. Promotion of information security and assurance awareness by users, security professionals, and providers;
4. Promotion of cyber defense “best practices” by sharing information on tools, procedures, and policies;
5. Beginning with a pilot in Virginia, development and promotion of state cyber best practices and creation of infrastructure that is integrated into state all-hazards capabilities for collaboration and information sharing regarding cyber risk, and coordinated response to cyber incidents.
6. Facilitate development of policy frameworks for privacy and security keeping in view the local conditions in emerging countries;
7. Promotion of capacity building of national computer emergency response/readiness teams and incident response teams (CERT and CSIRT) and infrastructures, and information sharing and collaboration among them, to assess and mitigate the risk to the global and regional information infrastructure;
8. An initiative to reduce the amount, seriousness, and impact of malicious cyber activity and cyber crime by promotion of information sharing and collaboration (and status/progress reporting) among law enforcement, the private sector, and other government organizations;
9. Promotion of IT and IT security-related research and development on issues related to these goals, by facilitating information sharing and collaboration among private sector and government (and government-financed) entities, and academic institutions.
10. Promote collaboration and information sharing about existing and developing compliance and regulatory frameworks designed to strengthen data privacy and computer security in the emerging world, building on and integrating with, the available international cyber infrastructure, and the international cyber crime prevention efforts.

It is anticipated that the first full-time and part-time staff members will be individuals with experience working with international or national IT or cyber security entities or other IT stakeholders. We anticipate forming an advisory board for the center that will include prominent persons from the global ICT community.

We also anticipate that faculty from GMU and perhaps other universities will serve actively in one or more affiliate-type capacities, and benefit from center funding sources for research, writing papers, working group and special project participation, and travel to conferences and training sessions.
News and Events

**AusCERT2008**
An international conference focusing on Information Security for CFOs, CIOs, CTOs and technical staff from government agencies, universities and industry. Featuring local and international Information Security experts.

19-23 May 2008
conference.auscert.org.au/conf2008/
Gold Coast, Australia

**Process Control Security Event**
The goal of this event is to share knowledge and exchange information about security in the area of process automation.

21 May 2008
Utrecht, The Netherlands
www.samenteagencycybercrime.nl
www.hetinstrument.nl

**2nd Annual Counter-eCrime Operations Summit 2008**
The event will engage questions of operational challenges and the development of common resources for the first responders and forensic professionals who protect consumers and enterprises from the ecrime threat every day.

26-27 May 2008
Tokyo, Japan
www.antiphishing.org/events/2008_operationsSummit.html

**IDC's Asia/Pacific SecurityVision 2008 Conference**
**Next-Gen Security: Defending Against Enterprise Threats From a New Era**
This event will address how the convergence of business and personal devices has implications for data protection and security that can’t be ignored by enterprises.

29 May 2008
Kuala Lumpur, Malaysia
Annual WARP Forum 2008
The event offers delegates a unique opportunity to network with other people active in the area, and to share advice and experiences.

7th Annual National SCADA Conference
Australia's premier gathering for SCADA specialists. The National SCADA Conference is the premier event, and the only event, specialising in the unique attributes of SCADA for the utilities sector.

3 June 2008
London, UK
www.warp.gov.uk/Index/Forum/indexannualforum.htm

16-17 June 2008
Brisbane, Australia

CIIP Matters is the quarterly newsletter compiled by the Theodore Puskas Foundation of Hungary, supervised by an editorial committee on behalf of the Meridian presidency.

The editors wish to thank all contributions, and would like to provide the opportunity for submitting materials of CIIP interest to be published in future editions.

Contact information:
Editor-in-Chief: Ferenc Suba
newsletter@meridianconference.org