



GENEVA SECURITY FORUM

FINAL REPORT

Wednesday, Thursday June 20th-21st 2007

Palexpo and Villa Sarasin, Geneva, Switzerland

TABLE OF CONTENTS

INTRODUCTION	4
REPORT	5
The interconnectedness of today's security threats: can we rise to the challenge?	6
Crisis management and post-conflict reconstruction and investment: the challenges and opportunities	7
Internet Surveillance for Criminal Intelligence: tracking the enemy	8
International organized online crime: from hobbyists to professionals - the morphing enemy	8
Securing corporate buildings through the use of biometrics and avant-garde access control mechanisms	9
Cyber-security and cryptology	9
Controlling risk: staying one step ahead of the hackers and cyber-terrorists?	10
Trust and Security	10
Human security, organized crime and conflict	11
Laying the groundwork for security: Arab Islamic renaissance	12
The Secret History of Codes and Code Breaking- Cracking the Cipher Challenge	12
LIST OF SPEAKERS	13

INTRODUCTION

Security in its broadest sense has become one of the most central issues facing the world today, from terrorism to protection of infrastructure to personal security issues. The age of globalization has witnessed not only increasing interdependence and mobility of capital, goods and people but also the growing interconnectedness of global challenges and their diverse effects on citizens everywhere. This interdependence, highlighted by technological advances resulting in a web of interrelated networks, has increased vulnerability to security threats. New security challenges including increasingly sophisticated hackers, computer viruses, the move to network-centric warfare, water shortages, the risk of pandemics, migration, the potential impact of rising number of discontented youth among others, have made it clear that a new multi-stakeholder, interconnected and IT savvy approach to developing and implementing security solutions is urgently required.

Although valuable to look at one element of the security puzzle, it is of vital importance to examine the linkages between security issues. The Geneva Security Forum is focusing on this interconnectedness bringing together the key actors at the forefront of thinking in creating and advancing innovative solutions to security threats. Advancing a comprehensive approach to security and building on Geneva's expertise in humanitarian issues, human rights, environment and international diplomacy, the Forum aims to cultivate the groundwork for new networks and develop dynamic solutions to security challenges. Launched by the Canton of Geneva, the Geneva Security Forum will provide an opportunity for business and policy-makers to learn about, and prepare for, the security threats we will face in 3-5 years, evaluate key issues, share expertise and drive knowledge growth on best responses.



Daniel Stauffacher

*Former Ambassador of Switzerland
Chief Executive Officer, Geneva Security Forum*



The inaugural Geneva Security Forum broached many pressing security concerns including the challenge of accurately assessing new threats and the effectiveness of new security strategies; the need to modernize threat assessment procedures; the importance of prioritizing security issues and the allocation of resources for security measures in both the private and public sectors; the growing interconnectedness of security threats including human security, health, environment, poverty, social exclusion, migration and human trafficking; the management of rising levels of public fear; the proliferation of defensive borders despite the need for more international cooperation to fight global threats; and the importance of networks and collaborative partnerships.

The Geneva Security Forum announced at its inaugural meeting that it will launch a process to discuss the development of a security audit methodology procedure to assess companies and provide a matrix against which IT security can be measured. **A group of high-level experts also called for increased education as a means to improve global security. Education is critical both for the growing number of marginalized youth in developing countries and for IT users to protect themselves against new cyber threats such as banking Trojans and highly sophisticated hackers. The Forum called for increased cooperation between the public, private and non-governmental sectors to respond effectively to new threats and highlighted the critical need for information sharing between countries even in highly sensitive sectors.** Stakeholders also recommended that the global community needs to find ways to address the legal problem of how, in the case of terrorism, we can intervene at the stage of “intention” rather than at the stage of “action”. The Geneva Security Forum is committed to furthering the debate about the move to new technologies, e-government, privacy issues and their relation to personal security.

There was general agreement that the threats we face today do not match the organizational structures of our nations and societies. These threats do not respect borders and are international in their nature. As per **Brian Jenkins, Rand Corporation, there is a tendency in some areas to**



move toward walled centers and security-driven protection at national frontiers. Instead we should be moving toward seamless and transborder cooperation. There is a growing realization that national security cannot be maintained through a purely national approach which in turn raises serious questions about the potential loss of sovereignty. Transparency will have to become a policy of choice and the prestige of the nation will lie in **not** hiding information. This is a radical shift in security thinking and was recently reflected in the global response to SARS, which was characterized by information-sharing, new international health regulations and real-time communication. The

most critical tools needed as we move forward include the dissemination of information, the understanding of which pieces of information are relevant and the ability to turn data into knowledge.

The interconnectedness of today's security threats: can we rise to the challenge?

The World Trade Centre attack on 9/11 changed the way the US perceives risk, blurring the line between risk to the community and risk to the individual. According to **Brian Jenkins, Rand Corporation**, there has been an important change in the way the US analyzes threats. Traditional analysis is based on an assessment of your enemy's capabilities, which are easily quantifiable. With terrorist networks, there is a great deal of uncertainty, which results in a *vulnerability analysis* (how vulnerable are our energy systems, airports, ports, etc). This analysis involves postulating an attack and evaluating worst-case scenarios. Due to the fact that these analyses are part of the public discussion and debate, it not only encourages US politicians to be champions of specific threats but also leads to a sense of alarm, complicating intelligence and possibly inspiring terrorists. Over time this encourages irrational levels of fear in society and also leads to a bizarre allocation of security resources. Today's threats do not correspond to how we have organized our societies politically and economically. Cyber-terrorism and epidemics do not recognize borders. **Brian Jenkins, Rand Corporation** recommends moving from the traditional reactive law enforcement approach to a proactive response. A serious hurdle in this transition is that democracies do not have well developed laws for dealing with intent. At what point does intent to kill or to terrorize, move out of the realm of free speech and become a crime?



"The average American has 1/7000 chances of dying in a car accident; 1/18000 of being a victim of a homicide; 1/650000 of being involved in a terrorist attack; we are not living in peril as a consequence of terrorism although we can justify significant expenditure to protect the community".

Brian Jenkins

Brian Jenkins with Forum participants

Tim Bloechl, Microsoft, focused his remarks on the very real threat of cyber-terrorism and heightened security risks due to improved technological capabilities. He reminded us that many of us are cyber terrorists through negligence; i.e. leaving computers connected to the internet, making it easy for "bad guys" to use the computer for other purposes. This was likely the case in Estonia with the use of Botnets. The techno threat is real and its impact could be huge on banking, finance, air traffic control, power and our personal privacy. The good news is that the international community, governments and corporations are focusing on this threat and that individuals are also becoming more aware. The establishment of computer emergency response teams around the world is flourishing. The importance of collaboration and cooperative partnerships, government to government and business to business, is critical.

Mike Ryan, WHO, stressed the important links between health and security issues; the risks of bioterrorism; new diseases and how epidemics and pandemics have shaped our history. Our interconnectedness is simultaneously a major weakness and also a strength. The real impact of a pandemic will be on the broader society unlike most wars which are local events that can be contained. Imagine the economic impact if 25-30 percent of people could not go to work. Societal preparedness and how we process information and understand risk is of critical importance. SARS was global within 48 hours which means there will be very little time to prepare and respond to any future pandemic. Current medical strategies call for international response and prompt intervention. This could mean a quarantine process, which will further affect the functioning of the world economy. In 1998 a Global Public Health system was developed by WHO in cooperation with Health Canada, which has now been using data-mining for 10 years. The real issue is not just about gathering more information, it is about real-time decisions and processing information.

Alyson Bailes, Stockholm International Peace Research Institute, noted the benefits of finding solutions to security threats that hit 4-5 risks simultaneously and the importance of people in the security response. For example, if you can train a lab assistant to be aware of risks then you are more likely to succeed in your overall security policy. The importance of a good personal security culture cannot be underestimated in the battle against new threats. It would also be very helpful to have **universal rules to manage threats collectively**. **The global community needs to discuss this and to assess how much national sovereignty can be relinquished.**



"People are the answer. A good personal security culture is going to stop a lot of natural and casual risks, and give us a stronger position to deal with man-made ones. Integrated solutions: we should cyber-defend Estonia, but also my personal computer against spam and viruses - that would make the whole system more secure".

Alyson Bailes

Crisis management and post-conflict reconstruction and investment: the challenges and opportunities

Alain Deletroz, International Crisis Group, identified five pillars of post-conflict reconstruction and lasting peace-building:

- 1) a peace agreement that is seen by all parties as accommodating their needs and that can be a real starting point for re-building
- 2) a very good transition mechanism that inspires confidence in all parties and the international community,
- 3) a real truth and reconciliation process without which resentment in the society can remain,
- 4) a real commitment from the international community,
- 5) an ambitious state-rebuilding program (rule of law, security and judiciary reform).

Thomas Tighe, DirectRelief noted that markets work when they can work, where there is money to be made. But approximately one third of humans are in places where market forces will not work, so the expectation that the market will come in and develop is false. The aim of DirectRelief is to get medical supplies and drugs to clinics that are "off the grid".

Scott Weber, Interpeace, spoke of 15 conflict zones in the world, stressing the importance of ownership and justice in peace-building. Using the example of Shell in Nigeria, he noted that if the locals do not feel they own part of the oil pipeline they will not be willing to protect it.

Internet Surveillance for Criminal Intelligence: tracking the enemy

Christian Buchs, HEIG and **Oliver Ribaux, UNIL**, are working on a tool to track and trace the "Nigerian internet scam" e-mails (the messages you get asking you for help in transferring big sums of money out of a developing country, against a commission), online check frauds and other investment frauds. The system will be up and running in October 2007.

International organized online crime: from hobbyists to professionals - the morphing enemy

Mikko H. Hyppönen, F-Secure: Hackers are turning into attackers. They have become more sophisticated and are now doing it for money rather than for fame. "People are still worried that a virus will come and destroy their data. Today that never happens, viruses are not destructive anymore, the last destructive virus we saw was one year ago: there is no money to be made in destroying data". Where are these attackers coming from? In large part from the USA, China, Brazil and the former USSR.



The most likely place for you to be the target of a crime is on the internet.
Mikko H. Hyppönen

Cyber-crime includes cash from phishing, infecting large amounts of home computers with spam, denial-of-service extortion, credit card number/email address/password theft, targeted attacks, industrial espionage, re-selling stolen credit card numbers, stealing passwords to banks, ebay, stockbrokers, poker sites and the list goes on. „**The money is good and nobody is getting caught**“. Spam is like cockroaches- you can try to limit the problem but it will never go away. Phishing will stay at levels we see today and will be replaced by worse problems like banking trojans whereby a user has his/her banking transactions altered and money stolen.

Hyppönen believes that education never works as people will always double click, fall for every phishing spam and give away their passwords. What we should do is take away the responsibility from the end user and give it to the operating managers like Microsoft and firms like F-Secure. We have to move toward the idea of security as a service. From 1986-2003, hackers were hobbyists. As of 2003 they were criminals and as of 2006 they were spies using malware in their attacks.

Securing corporate buildings through the use of biometrics and avant-garde access control mechanisms

Biometric verification such as iris recognition to access corporate buildings is no science fiction but applied science and calculated risk. The Geneva Security Forum saw the presentation of a worldwide premiere: **Banque Pictet & Cie** in Switzerland, uses a cardless, keyless and pinless security system for access into their new corporate headquarters. The bank employs only biometric verification per facial 3D recognition to allow secure access for its some 2000 employees. **Jean-Pierre Therre, Banque Pictet & Cie:** *"Perfect security is just an illusion, therefore we look for the most high-level security solution."* The bank has 50 different security points and 1500 doors which apply the biometric entry system. Therre confirmed that the biometric solutions they use are scalable and reliable enough to tackle the bank's security objectives. "They will become commonplace in many banks in the future." The facial recognition system has a level of precision that can identify identical twins within less than 1/10th of a second (see picture).



The requirements for an ideal biometric system are universality, uniqueness, permanence, collectability and acceptability. On this last point, Pictet has done a lot of explaining to employees to "demystify biometrics". The three most asked questions are: Is there any health risk in the use of biometrics? Can biometrics detect illnesses or addictions? What's the situation as far as individual privacy is concerned? Pictet is working on extending the system to access documents and computers. Clients and visitors have a separate entrance and reception.



Abdulaziz Sager, Bruno Giussani and Simon Singh

Cyber-security and cryptology

Information technology is becoming pervasive and increasingly connected to, and managed via, networks. **Patrick Amon, EPFL**, argues that no-one really understands the complexity of the system which makes it very hard to secure. The weakest points are often not technical but rather societal: the poor implementation of algorithms, the behaviour of employees, human error and faulty business processes.



The existing encryption techniques are based on mathematics, code that is "unbreakable" because it takes too much computational power to break it. But theoretically an algorithm to factorize efficiently large numbers could exist in the future. If someone publishes such an algorithm tomorrow, it would stop the whole world economy immediately because all data would be completely transparent and accessible.

Nicolas Gisin, University of Geneva

Quantum cryptography could be a solution but quantum computers are also a threat. If a quantum computer is developed (order of magnitudes more powerful than current computers) it would be easy to crack current codes. What kind of security do we want for the future? How long do you want your data remain secret? Imagine in 10 years that big banks could see the names of all their clients published on the internet because people are now using security measures that will be accessible if a quantum computer is developed.

Controlling risk: staying one step ahead of the hackers and cyber-terrorists?

Cédric Renouard, Ilion Security: "Hackers can break in anywhere with time and money". The attack on the public and private e-infrastructure of Estonia in Spring 2007 may have been led by a government but it was a very simple attack. It was massive and non-destructive, more a demonstration than an attack from a technical point of view. Ilion performs "ethical hacking" and "pragmatic risk assessment". Ilion tries to penetrate sensitive systems such as power plants, financial networks to identify weaknesses. Most systems are not well protected and security holes are often underestimated.

Trust and Security



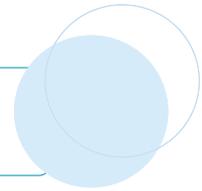
*"There is an **emerging digital identification divide**, which is much more serious than just the digital divide. The digital divide was about connectivity. But if you want to participate in the network economy in an active way, you need identification and trust".*

Carlos Moreira, WiseKey SA

Technological developments are not just about smart cards, USBs, root keys and secure processes but rather part of a larger movement. Trust is an emerging concept in technology. **Carlos Moreira, WiseKey SA**, pointed out that of the top ten companies who have made money on the internet none are European because Europeans do not own the critical piece of the infrastructure. To promote trust, Moreira recommends developing and applying international standards. Geneva is ideally placed to bring together the private sector actors to develop such standards.

In order for the internet to become transactional, countries have started developing their own DNS capability. **Ram Mohan, Afiliis**, pointed out that the next generation already trusts the web as witnessed through the use of Facebook, MySpace etc. Therefore we need to secure what we already have. The internet does not know geographic boundaries so introducing national IDs is counter to the revolution we are faced with. Think global- secure local!

Robert Hensler, State Chancellor of the Republic and Canton of Geneva presented the innovative Geneva internet voting project. "We extend the security of the voting process far beyond what is achieved with postal voting. We control the integrity of your vote and can see when your vote was manipulated or altered, e.g. by hostile software located in your computer." He underlined that citizen participation in elections has been increased with the use of e-Voting.



Brian Jenkins, Rand Corporation: The global community needs to focus increasingly on building networks that can come together on short notice to respond to threats and attacks. There is also a need to restructure and re-think the way we gather and process intelligence information. There has been a radical transformation since the Cold War where adversaries were hierarchical, enemies well-defined and things moved at a very slow pace. We are now in the opposite situation with a very fluid situation and ill-defined enemies. Terrorism is too readily consigned as an empire of evil with very little serious effort to look at where they are coming from. There is a need to bring people from outside the intelligence community to analyze situations and threats. There are too many challenges worldwide to have in-house expertise to match our morphing enemies.



Ulrich Schneckener, German Institute for International and Security Affairs: Intelligence cooperation requires trust and transparency, both of which are very difficult to achieve. Often threat perception is more important than the threats themselves. What is a risk? How do we measure risk? How probable is the risk? What is its destruction potential? These variables are difficult to measure making it impossible to have clear answers which in turn has consequences for the development of government policy. The German government has launched a 120 million Euro project in security research, largely in security technology and security technology innovation. This is worthwhile but only half of the story. We should not neglect the fact that most crime is linked to low tech, low budget conflict zones

Stefan Wolff, University of Nottingham: Major new security threats, not just terrorism, crime and conflict, but also the increasing convergence of these types of security problems exposes our inability to think more comprehensively about security. The incapacity to contain ethnic conflicts creates enabling environments for organized crime, which in turn provides incentives as well as resources for many of the conflicts we see around the world today. The real problem the global community faces is in terms of its response to security challenges and the inability to network and share knowledge.



Sundeep Waslekar and Forum participants

Laying the groundwork for security: Arab Islamic renaissance

There is a crisis of vision in the region. **Abdulaziz Sager, Gulf Research Center**, discussed the groundwork for security in the Arab Islamic region. He pointed out that the 3 key current risks are “the situation in Iraq, the possible nuclear rise of the Iranian military program and the continuous terrorist operations in the region.” However, on the positive side, these three issues have prompted the mobilization of global cooperation in the world community.



Maria Cattai and Abdulaziz Sager

Pär Stenbäck, International Crisis Group, highlighted the importance of education as the key to future stability and human dignity. According to PISA, Finland has the best educational system which some believe can be replicated through “technical” changes to existing systems. However, any reputable educational system also requires a culture that is favourable to educational values. This is lacking in many countries, including the Middle East.

Jihad el-Khazen, former Editor-in-Chief, Al Hayat, pointed out that there is education in the Arab world but it is not progressive or forward looking. With 25 % of population under the age of 14 there are also massive demographic pressures on services and education reform. Qatar is starting an interesting education foundation and Saudi Arabia has 25 000 students studying outside the country. In the Middle East, the youth problem is reaching critical proportions and what could be a huge competitive advantage for the region is turning into a massive liability. In Iran alone the number of young people under 20 years of age is 28 million. The Arab world will need 80 million new jobs in 10 years. A revolution of reform is needed.

The Secret History of Codes and Code Breaking- Cracking the CIPHER Challenge

Simon Singh, Author, Journalist, TV Producer, UK: Ever since humans began writing, they have been communicating in code. This obsession with secrecy has had dramatic effects on the outcome of wars, monarchies and individual lives. With clear mathematical, linguistic and technological demonstrations of many of the codes, as well as illustrations of some of the remarkable personalities behind them - many courageous, some villainous – Simon Singh traced the development of codes and code-breaking from military espionage in Ancient Greece to modern computer ciphers, to reveal how the remarkable science of cryptography has often changed the course of history. Now, with the Information Age bringing the possibility of a truly unbreakable code ever nearer, and cryptography one of the major debates of our times, Singh investigated the challenge that technology has brought to personal privacy today.



LIST OF SPEAKERS

Antonio Acin	Assistant Professor, The Institute of Photonic Sciences, Spain
Anne Aldis	Head of the Conflict Studies Research Centre at the Defence Academy of the UK
Patrick Amon	Research Scientist, EPFL, Switzerland
Ian Anthony	Research Coordinator & Leader, Project on Nonproliferation and Export Control, Stockholm International Peace Research Institute, Sweden
Alyson J. K. Bailes	Director, Stockholm International Peace Research Institute, Sweden
Timothy D. Bloechl	Executive Director, Worldwide Public Safety and National Security, Microsoft; former Director, International Information Assurance, US DoD
Blaise Bonvin	TC Team Consult SA, Switzerland
Christian Buchs	Professor, Département des Technologies de l'Information et de la Communication, HEIG-VD, Switzerland
Victor Canivell	CEO, WISEKey SA, Spain
Maria Livanos Cattai	Member of the Board of Directors, Petroplus, Switzerland; Vice-Chairman, International Crisis Group and Chairman of the Strategic Advisory Board, Geneva Security Forum
Arnold Chrste	Chief Operating Officer, Member of the Executive Board, Trüb AG, Switzerland
Victor-Emmanuel de Sa	Co-Founder of Geneva Solutions, Geneva
Alain Deletroz	Vice President (Europe), International Crisis Group, Brussels
Nitin Desai	Former UN Under Secretary General for Social and Economic Affairs and Chairman of the Internet Governance Group
Peter Foot	Head of Training and Education, Geneva Centre for Security Policy, Switzerland
Eva Frölich	Interim Chair & President of the Public Interest Registry, PIR, Sweden
Patrick Gannon	President & CEO, OASIS
Nicolas Gisin	Professor and Leader, Group of Applied Physics, University of Geneva, Switzerland
Ed Girardet	Author and Journalist, Media 21, Switzerland
Bruno Giussani	European Director, TED and Co-founder, Tinex, Switzerland
Robert Hensler	State Chancellor of the Republic and Canton of Geneva
Mikko H. Hyppönen	Chief Research Officer, F-Secure, Helsinki
Brian Michael Jenkins	Senior Advisor, Rand Corporation, USA
George Joffé	Independent Consultant and former Deputy Director of the Royal Institute of International Affairs (Chatham House), London
Jürgen Junghanns	Product Manager Biometrics and Recognition, Interflex Datensysteme GmbH, Germany
Jihad el-Khazen	Columnist and former Editor-in-Chief, Al Hayat, London, UK
Keith Krause	Executive Director, Small Arms Survey, HEI, Geneva
Lucy P. Marcus	CEO, Marcus Venture Consulting, UK
Ram Mohan	Vice President of Business Operations, Afilias & Member of the Security and Stability Advisory Committee (SSAC)

Carlos Moreira	Co-Founder, Chairman/President, WISEKey SA, Switzerland
David Morrison	Director of Communications, UNDP, New York, USA
Philippe Mottaz	Director, World Radio Geneva, Switzerland
Philippe Niederhauser	Sales Director, Fastcom Technology SA, Switzerland
Peter Purdue	Dean, Graduate School of Operational and Information Sciences, Naval Postgraduate School
Cedric Renouard	Cofounder-Director, ilion Security S.A., Network Audit by Ethical Hacking, Switzerland
Olivier Ribaux	Forensic Science Institute, University of Lausanne, Switzerland
Grégoire Ribordy	Co-Founder and Chief Executive Officer, id Quantique, Switzerland
Kelly Richdale	Vice Presidents Internationals Sales , & Managing Director International Operations, BIOSCRYPT
Frank-Jürgen Richter	President, HORASIS, Switzerland
Rodolfo Rosini	Chief Executive Officer, Cellcrypt, London, UK
Mike Ryan	Director, Department of Epidemic and Pandemic Alert and Response (EPR), WHO, Geneva
Abdulaziz Sager	Chairman, Gulf Research Centre, Dubai, UAE
Ulrich Schneckener	Head, Global Issues Group, German Institute for International and Security Affairs, Germany
Simon Singh	Author, Journalist, TV Producer, UK
Daniel Stauffacher	CEO, Geneva Security Forum & Former Ambassador of Switzerland
Pär Stenbäck	Chairman of the Swedish-Finnish Cultural Foundation and Executive Board Member of the International Crisis Group (ICG)
Francois Stieger	President and Founder, Securitytech SA, Switzerland
Jean-Pierre Therre	Chief Security Officer, Banque Pictet & CIE, Switzerland
Thomas Tighe	CEO, Direct Relief International
Michels Warynski	Technical Head of Geneva eVoting sProject, Chancellerie d'Etat, Geneva
Sundeep Waslekar	President, Strategic Foresight Group, India
Scott Weber	Director General, Interpeace - International Peacebuilding Alliance, Geneva
Gerold H. Werner	Max-Consult AG, Switzerland
Stefan Wolff	Professor of Political Science School of Politics and International Relations University of Nottingham, UK
Houlin Zhao	Deputy Secretary-General, ITU, Geneva
Randall Zindler	Chief Executive Officer, Medair, Switzerland

Written by:

*Barbara Weekes, Director, Strategy and Content,
Geneva Security Forum*

Contributions from:

*Bruno Giussani, European Director, TED and Co-founder, Tinex, Switzerland,
<http://www.LunchOverIP.com>*





GENEVA
SECURITY FORUM

www.genevasecurityforum.org