



Organization for Security and
Co-operation in Europe

Reflections on Emerging Cyber Threats and International Co-operative Responses

**Keynote Address by Raphael Perl
Head / OSCE Action against Terrorism Unit**

4th Annual Symposium on Information Assurance (ASIA '09)

June 3-4, 2009 Empire State Plaza, Albany, NY

Sponsored by the School of Business, State University of New York at Albany

Ladies and gentlemen, dear colleagues and friends,

It is a pleasure for me to address this distinguished forum. I thank the organizers for the opportunity to share with you the Organization for Security and Co-operation's (OSCE) experience in combating terrorist use of the Internet and enhancing cyber security. The fact that you have invited an OSCE representative to speak about cyber security illustrates just how much the world has changed since the inception of my organization in the 1970s. It also confirms how the OSCE has remained in step with the times.

The global landscape around us is changing and it is changing rapidly, especially when it comes to the impact of technology on our daily lives. Cyber security is and will remain one of the central security challenges in the years to come – and it will be a true global challenge. This is a challenge that the International community must meet head on. International and regional organizations, such as the OSCE, have a key role to play in this regard.

The OSCE's comprehensive approach to security

As you may know, the OSCE's efforts to counter terrorism reflect the Organization's comprehensive approach to security. This approach encompasses the (1) political-military sphere, (2) the economic and environmental sphere, and the (3) human dimensions of security. Cyber security is a core issue of clear and vital importance to all three of these dimensions.

For our efforts to enhance cyber security to be effective, they must be preventive and must not only focus on improving security, but also on and capacity building in a broad range of sectors. In short, they must be comprehensive. With this in mind, my Unit – the OSCE's Action against Terrorism Unit (ATU) – is increasingly focusing its efforts on comprehensively enhancing cyber security and I will argue that such an approach is our best option in achieving the long-term goal of making cyberspace as safe and secure as possible.

Dependency on cyberspace is increasing

Let us step back for a moment and look at a few figures: Last June the number of personal computers in use worldwide hit one billion, while another billion are expected to be added by 2014.¹ More than a billion and a half computer users exist worldwide today.² These are impressive figures. And I think we agree that they are only likely to continue to grow. These data illustrate our dependency on information technologies. They also show that we as individual users are not alone in our dependence on such technologies. Nation states and industry depend on computer technologies as well.

Computer users worldwide are dependent on their systems' confidentiality, integrity and their availability. Confidentiality, Integrity and Availability – CIA – all of which are under constant virtual attack. Just imagine, one day you wake up. You cannot check your emails, your mobile phone is not working, the TV does not work, the underground is not

¹ <http://www.gartner.com/it/page.jsp?id=703807>

² internetworldstats (Dec 2008)

functioning and you cannot withdraw money from the cash machine. You get the idea. Cisco recently estimated that almost 200 billion messages per day, or approximately 90 percent of all electronic mail sent worldwide, can be defined as spam.³ And, we all know, many of these emails contain malicious code or are sent with malicious intent.

A functioning cyberspace is the glue that holds modern societies and our global economy together. But dependency on cyberspace, unlike many other forms of dependency, is not something one can overcome by sheer willpower alone. To the contrary, I would argue that it be cannot overcome and terrorists and other criminals will do their utmost to exploit our dependency. Hence, what we need to do is ensure that cyberspace remains functional, safe and secure.

Let me give you two very recent examples of abuse of cyberspace we experienced at the OSCE: Not too long ago, a member of my staff was the target of a specifically tailored phishing attempt – so called *spear phishing*. The email he received was designed to look like an update of our Webmail accounts. It just so happened that the staff member in question is Mr. Nemanja Malisevic, our Action Officer for Terrorist Use of the Internet and Cyber Security. He did not fall for this scam and alerted our IT security people who proceeded to warn other staff members.

In other recent attempts, some OSCE staff members received e-mails claiming to originate from the Organisation for Economic Co-operation and Development (OECD) --- offering a financial award. Again, these were phishing attempts targeted at people who work with and trust organizations such as the OECD --- people who might let their guard down when receiving emails which appear to be originating from such trusted sources.

I am sure that many of you have been the target of similar phishing attempts and have similar stories to relate, but let me now move on from the issues of criminal and malicious use of the Internet to the issue of terrorist use of the Internet.

³ Cisco spam report (Dec 2008)

The threat of terrorist use of the Internet

How do terrorists use the opportunities provided to them by this medium?

The Internet is user blind. It serves good and evil causes alike. Unfortunately, the Internet has become a key instrument for terrorists and other criminals; it is used for a variety of illicit purposes such as fraud; child sexual exploitation; identity and data theft; identifying, recruiting and training new members of a terrorist group; collecting and transferring funds for criminal ends; organizing terrorist acts; inciting to racism, hatred and terrorist violence. Cyber attacks – the use of computer systems and the Internet as weapons – are also a growing concern.

Our time is limited today, and you are all experts, so I will not go into details. But I would like to elaborate on one issue. Experts disagree over the likelihood of cyber attacks by terrorists. In particular, some argue that terrorist groups, at this point in time, have neither the resources nor the skills necessary to conduct large-scale cyber attacks, namely attacks which would disrupt critical infrastructure or critical information infrastructure in a significant way.

Also, there has not *yet* been a major cyber attack conducted by terrorists. But on the other hand, we must never forget that cyber crime is on the rise. Cyber criminals continue to find new and improved ways to abuse information technology and cyberspace. What cyber criminals and terrorists do-- and continue to do-- is to set precedents.

Every precedent, every cyber attack, regardless of its individual background and the motivation of the individual perpetrator is something that can be copied by terrorists. All they need is to acquire the necessary expertise and tools. And both are available to people with sufficient determination or money. At a recent conference organised by my Unit, one of our speakers, put it in the following terms: “Terrorists are getting a free ride from cyber criminals”.

Moreover, terrorists are already abusing cyberspace for profit, akin to “ordinary” cyber criminals. They include people like Younis Tsouli, better known as *Irhabi007*, who was jailed in July 2007 in the UK. As you may know, in addition to his cyber activities in support of Al-Qaeda, Tsouli was also engaged in credit card fraud.

There is another concern here: The current economic downturn has already led to many qualified people losing their jobs in all walks of life. This includes people with considerable IT skills. Not long ago, an expert from one of the world’s leading anti-virus companies told me that there is a great deal of anxiety that, should the current economic crisis persist, will be unemployed IT specialists seeking remuneration for their skills from other sources, potentially even criminal or terrorist ones. We need to keep this in mind.

Linked to this idea is an additional problem: On the whole, cyber crimes are constantly becoming easier to commit. With the tools readily available today, people with little or no IT experience can commit a multiple of crimes online. 20 minutes is approximately about all it takes to set up all the necessary programmes to steal music, movies, and games via your computer. Setting up a botnet takes a little bit longer, but, as was recently illustrated by the BBC in their show *Click*, it is not all that difficult.

This trend towards rising cyber crime is worrisome indeed. More and more people will eventually realise just how easy it is to commit cyber crimes. These will be people who would never rob a store, a bank or rob somebody else in the street. But if they can “make” money from the comfort and safety of their homes without ever having to look their victims in the eyes... who knows?

And what about terrorists or their supporters? It is true that thus far, terrorists have traditionally relied on physical attack such as bombings and assassinations. There is no need to elaborate on the potential reasons for this. I am sure we have all heard many different arguments.

Let us, however, not forget that terrorism is not only about killing. It never was. Terrorism, as a method, is about inflicting harm on any number of people to scare a much larger

audience, including governments, in order to influence them into taking or abstaining from certain policies or actions.

Terrorism is about forcing people to change their way of life. And more and more the strategic goals and targets of terrorist groups are focusing on causing economic damage. Remember my example in the beginning where things we rely on in our daily life don't work? Is that not exactly what large-scale cyber terrorist attacks resulting in substantial economic damage could achieve? Think about damage in both physical and economic terms. What if a series of cyber attacks were coupled with some strategically placed bombs, or with a series of biological, chemical, or radiological attacks?

I would like to underscore that in my view the biggest threat nations face today is a combined real-world/cyber attack. This is in line with the thinking of a large number of cyber security experts with whom my staff and I have spoken over the past 18 months. In the opinion of many, it is only a question of time.

It is only a question of time until cyber terrorists use methods pioneered by cyber criminals and hackers not only to communicate or make a profit. It is only a question of time until they use cyber attacks to either increase the effect of a more traditional terrorist attack – for example a bombing – or cause large scale damage to the information infrastructure or critical infrastructures in general.⁴ The potential for cyber attacks to cause widespread damage-- not only limited to economic damage-- is immeasurable. And as a result, both individuals and nations need to be prepared.

Past and recent activities

What has my unit, the OSCE's Action against Terrorism Unit (ATU,) done to combat this threat? What have we done to help our 56 OSCE participating States and 11 affiliate cooperating states prepare? We have organized workshops and national training events

⁴ This concerns in particular electrical power systems, telecommunication systems, gas and oil storage and transportation, banking and finance, transportation, water supply systems and emergency services. (M. Gercke (2008), *Cyberterrorism: how terrorists use the Internet*.)

that have brought together in excess of 600 experts from more than 50 countries. In February 2009, at the request of Serbia, we organized a *National Expert Workshop on Combating Terrorist Use of the Internet / Comprehensively Enhancing Cyber Security*, in Belgrade, Serbia. This workshop sought to raise awareness on concrete steps to strengthen cyber security, the impact – including the economic impact – of potential attacks and to showcase pertinent defensive measures, lessons-learned and relevant best-practices. Dr. Sanjay Goel, the driving force behind this conference today, was one of our star presenters in Belgrade and we thank him for his contribution there.

Subsequently, in March 2009, we facilitated an *OSCE Workshop on a Comprehensive OSCE Approach to Enhancing Cyber Security*. The overall aim was to increase awareness of OSCE participating States of cutting edge threats to cyber security and to highlight concrete steps that can be taken to comprehensively strengthen cyber security.

A comprehensive approach to cyber security

Why is a comprehensive approach to cyber security so important? Because there is only one cyberspace and it encompasses many dimensions. The good guys use cyberspace and the bad guys use it. The perpetrators are united in their methods and different cyber perpetrators use the same or similar types of cyber attacks, even if their own backgrounds, aims and motivations may differ. But when it comes to countering such tactics, we are often divided and firewalled in use of resources, expertise, functional jurisdictions and legal frameworks.

Growing dependence on information technology and increasing interconnection of critical (information) infrastructures has made a secure cyberspace vital to the functioning of a modern state. Hence, cyber security needs to be an intrinsic part of any state's national security considerations and planning and the international community needs to systematically address this issue as well. I suggest to you that a comprehensive approach—an internationally integrated and harmonized approach-- is the only viable option for national authorities and the international community to ensure long-term and sustainable cyber security. This is the kind of approach that we take with the OSCE

Counter-Terrorism Network (CTN) – a web based network linking some 350 counter-terrorism practitioners – to distribute relevant information, lessons learned and best practices.

Some concrete policy options we may want to consider

So what should we do, what can we do to contain the rising challenge to cyber security?

What I might normally do at this point is to share my own views with you here. But today, I would like to take advantage of our recent Belgrade workshop and share with you nine suggestions and policy recommendations made by experts there:

1. **International co-operation** is crucial. Cyber threats are global threats and therefore are the best to be addressed, where practical, in a global context. Countries should establish and maintain networks of reliable and knowledgeable contacts, in the field to include contacts in government, industry, academia, and society at large. Reliable frameworks should be established to facilitate co-operation in cyber investigations to allow for the timely seizing of evidence. Better co-ordination is needed in the field of defining cyber security terms and concepts.
2. Countries should establish specialised **Computer Emergency Response Teams (CERTs)** or **Computer Security Incident Response Teams (CSIRTs)**. Staff should be regularly trained in latest trends and developments pertaining to cyber security. Additionally, specialized Units within law enforcement agencies should be established and provided with the necessary means and standardized training to investigate serious criminal offenses committed through the Internet. Law-enforcement agencies should seek to establish enhanced mechanisms to facilitate systematically sharing of information, best practices and lessons learned.
3. **Critical infrastructure protection** should increasingly take into account potential cyber threats. In addition, states should be very careful in what they designate to be a “critical infrastructure”. Overall, stricter regulation of cyberspace may be necessary with regard to critical infrastructure protection. Particular focus should

be placed on countering the threat posed by “**insiders**” – cyber measures alone, may not be enough to counter this particular threat.

4. The importance of **Public-Private Partnerships (PPP)**, i.e. partnerships that include government, industry, and civil society, was underscored. The expertise as well as technical knowledge available from the private sector should be sought and utilised in a systematic manner, especially when drafting new legislation in this area. Otherwise there is a risk of legislation being overtaken by technology from day one. Additionally, Internet Service Providers (ISPs) should designate **one contact point** for interaction with law-enforcement agencies. Clear and direct reporting lines for security responsibilities should be established everywhere.
5. Discussions about technology should be separated from discussions about the crimes themselves. For example, disseminating propaganda that incites to murder may constitute a crime, but not necessarily the technology used to disseminate this propaganda. We must also be mindful of the danger of over-reliance on technology. Technology cannot replace well trained people. **Online problems may not always have online solutions.** While attempting to stay ahead of the technology-vulnerability curve, countries should not disregard tools which were used prior to the IT-revolution.
6. Raising awareness and **educating the individual Internet user** is essential. Security is everyone’s business and the human user remains the weakest link in terms of cyber security. More debate is needed with regard to **user liability** in cases of extreme negligence. Contemporary IT systems are so powerful that a certain degree of responsibility should be expected from their users. Moreover, it is crucial to educate and **raise awareness of judges and juries charged with trying cyber perpetrators.** More information and training should be made available in this regard.
7. **Online terrorist threats should be better prioritised,** particularly in terms of monitoring terrorist online presence. Although there are many websites related to

terrorist groups, the number of significant ones – namely those which warrant to be monitoring on a daily basis – remains small. Moreover, the threat from terrorist **online training materials** may be given too high a priority. Focus should instead be placed on countering the use of the Internet to radicalise or finance terrorism. Additionally, the Internet should be used to encourage and **promote disruptive arguments within terrorist organizations**, thereby drawing their energy and resources away from offensive activity.

8. Existing laws pertaining to cyber security should be harmonised and implemented. However, in our recent Belgrade workshop, participants failed to agree on whether **existing international and regional legal instruments**, including the Convention on Cybercrime (2001) and the Council of Europe Convention on the Prevention of Terrorism (2005), provide an adequate legal framework adequate for dealing with modern threats to cyber security, or whether **new specific instruments** may need to be adopted for this purpose.
9. States should strive to **reign in the use of anonymous means of payment** over the Internet by reinforcing the identification requirements of individuals using these means.

All these suggestions made by experts at our Belgrade workshop are relevant, but I would like to pick out and underscore one point: All of the above will mean little without the support and understanding of the general public. It is here that the fight against cyber terrorism, cyber crime, or any other kind of cyber threat for that matter, will be decided.

Let us not forget that many forms of cyber crime take advantage of – and often even depend on – the fact that many Internet users do not take all possible precautions to make their machines and accounts as secure and as impenetrable as possible.

The recent “Conficker” worm, which infected 10Million PCs in 4 days, is a case in point. It was able to spread so rapidly because users had not installed a security update, which

had been readily available. One response option, not without potential downsides, might be for nations to require that a new computer offered for sale include anti-virus protection. Moreover, contrary to popular belief, end-user education needs to target all Internet users, old and young. It is true that contemporary generations, as a whole, are more skilled in terms of using information technology than previous ones. However, being able to use a technology does not miraculously create a security conscious user.

Today's youth may be very skilled using Facebook or MySpace, but that does not mean that they necessarily know how to optimise their computers' security settings. Nor does it prevent them from disclosing personal information online, the use of which is arguably more restricted. Every uneducated user and every unprotected computer is a weak link, essentially begging to be exploited. A logical conclusion here is that end-user education is essential. In particular because there are many easy steps that each and every user can take to harden their computers and accounts from being hacked or hijacked.

We tend to look out for ourselves and our neighbours in the real world. But shouldn't we be doing this more for our cyber neighbours – the other Internet users. In whatever small way, this is a contribution each and every one of us can make to the global struggle against criminal and terrorist use of the Internet. Important here, as well, is to do a better job “selling” this idea to the public and it is here that regional organizations such as the OSCE can be of use in this regard.

Summary and concluding remarks

Growing dependence on information and communication technology and increasing interconnection of critical infrastructures has made a secure cyberspace essential to the very functioning of a modern society. This dependence extends from our professional to our private lives. Looking around this room I see an impressive number of ethnicities, nationalities and backgrounds represented. Irrespective of where one is based and what the specifics of one's respective jobs are, during working hours you will take care of business relying heavily on emails and Internet research. After hours, you will likely rely on the

very same infrastructure to communicate with friends and families, back home or wherever they happen to be located in today's global village.

We all need to do our utmost to protect this infrastructure, so critical to many different spheres of our lives. A **comprehensive OSCE-type approach** to enhancing cyber security with the long-term goal of making cyberspace as **safe and secure** as possible – and to ensure that it remains that way, I suggest to you, is the only reasonable way forward.

Thank you for your attention.