Organization for Security and Co-operation in Europe

Combating Terrorist Use of the Internet / Comprehensively Enhancing Cyber Security

2010 Counter Terror Expo: "Countering Terrorism in a Changed World"

(14-15 April 2010, London, UK)

Remarks by: Raphael Perl
Head on Anti-Terrorism Issues of the Organization for Security and Co-operation in Europe (OSCE)

Ladies and gentlemen,

On behalf of the Organization for Security and Co-operation in Europe (OSCE) it is a pleasure for me to address this distinguished audience at this prestigious event.

Is exploitation of the Internet the most imminent global challenge from terrorists and extremists? Probably not! But can and should we exploit the Internet for national security and anti-terrorist purposes? Absolutely!

For terrorists and other criminals the Internet is a vehicle. It is a real-time, widely accessible, transnational and multi-lingual vehicle. The Internet is a communication system, a networking system, a fund-raising and logistical support system – and it can also be a delivery system for real-life, physical attacks on infrastructures that rely on cyber components. Clearly, the bad guys use this vehicle. We – the good guys – need to better use it for our purposes, as well!

For those not familiar with my organization, let me briefly note that the OSCE is the world's largest regional security organization under the UN Charter. It brings together 56

countries from North America to Central Asia, including all member states of NATO, the EU and the Commonwealth of Independent States (CIS).

My Unit, the Action against Terrorism Unit – or ATU, is the organization's focal point for counter-terrorism activities.

Cyber security is one of the thematic areas where we have been particularly active in recent years. In particular, we have increasingly focused on promoting a comprehensive approach to cyber security.

I take note of the four sub-topics included in the agenda relating to my talk. However, I would like to focus specifically on two related issues, which I believe encompass all four sub-topics, namely:

(1) How can we enhance our efforts to use the Internet as an instrument to counter criminal and terrorist activity without improperly impacting on human rights?

(2) How can we better mitigate the threat posed by anonymity and the resulting complexities of identity verification in cyberspace?

First of all, however, I would like to share with you some underlying assumptions we hopefully are in agreement upon.

(1) Growing reliance on information technology (IT) and the interconnection of critical infrastructure have increased economic productivity, enhanced global trade and, in many ways, have made a secure cyberspace central to the functioning of a modern state. Effective IT is a strength!

(2) The flipside is that IT can also be a vulnerability. Advances in the IT sector also present terrorists and

other criminals with new opportunities and attack vectors, which they are increasingly exploiting.

(3) Perpetrators of cyber crimes share common methods, even if their goals and motivations differ. They learn from each other and frequently work together – the so called copy-cat phenomenon.

(4) The international community lacks shared and common responses. All too often it is divided and firewalled in the way in which it utilises resources, expertise, functional jurisdictions and legal frameworks.

(1) How can we enhance efforts to use the Internet as an instrument to counter criminal and terrorist activity without improperly impacting on human rights?

Clearly, the Internet has become a strategic device and a tactical facilitator for terrorists. Terrorists and other criminals have, over the years, become increasingly adept at using or abusing the Internet for their purposes.

So how can we enhance efforts to use the Internet as an instrument to counter criminal and terrorist activity without improperly impacting on human rights?

In answering, let me center my remarks on the need for law enforcement authorities to improve their capacities to use the Internet for countermeasures and for information and intelligence gathering.

At a recent cyber security event organised by the OSCE in Croatia, one of the key conclusions of our expert panel was that it is unrealistic to control terrorist and criminal materials online. It is simply too easy for terrorists and other criminals to set-up, copy and move websites. Any takedown-measure

can only be effective in the very short term and is often costly in terms of restricting human rights.

Rather than attempting to shut down websites our panellists recommended efforts be focused generally on gathering sufficient evidence to prosecute webmasters. In the long term, exploiting information obtained from these sites was deemed more productive than shutting them down.

Policy options

So what can be done?

A number of options exist for enhancing efforts to use the Internet as an instrument to counter criminal and terrorist activity without improperly impacting on Human Rights. Consequently, just to list six of them:

(1) *Strengthening the legal framework for cyber countermeasures.* Without laws that authorise countermeasures in cyberspace criminals can almost operate with impunity online. States must, therefore, establish legal frameworks which enable them to conduct appropriate online countermeasures against terrorists and other criminals. For example, states may have technologies in place to attack criminal botnets once they are identified. However, in most, if not all cases, these states do not have the legal framework in place that would allow or adequately regulate the timely use of such measures.

(2) *Exploiting rather than shutting down criminal and terrorist websites.* Websites are a treasure trove of information about terrorist and other criminal groups. You do not want to kill the goose that lays the golden eggs.

(3) *Defining the exact purpose of data collection in order to more effectively target its use.* Only if you know what you want to accomplish can you gather the information to support reaching this aim. Before ordering the collection of any data states must first clearly define the *exact purpose* behind any such collection. This involves coming to an agreement on the following issues: (a) Is the data going to be used for intelligence purposes only? (b) Is the data going to influence the planning of specific countermeasures? (c) Is the data meant to be used in court and if so, would it be admissible in another country, too? All too often data is gathered without a clearly defined purpose resulting in waste of resources and insufficient actionable information.

(4) *Deciding who exactly will be tasked with collecting the data.* Deciding in advance exactly who will be tasked with the collection of data is crucial because it enables countries to adequately allocate human and financial resources. Without the appropriate human and financial resources any data collection effort is doomed to failure.

(5) *Making the collected data available to those who need it.* Making the collected data available to a majority of those who could put it to good use is essential. Otherwise vital data can easily slip through the cracks – as the recent Christmas bomber case illustrated.

(6) *Prioritising the collected data in terms of time sensitivity and relevance/importance*. Within such a framework, prioritising the collected data is a prerequisite for effective analysis. An obvious problem, of course, is what to do with all the collected data? Already, we may have a situation where the amount of data collected is beyond the capabilities of available analysts. Let us not forget that data without analysis is

nothing but zeros and ones rotting away on a hard-drive. This is not lost on contemporary terrorist groups. We know that groups like Al-Qaeda are trying to overwhelm and distract us with information and background noise.

(2) How can we better mitigate the threat posed by anonymity and the resulting complexities of identity verification in cyberspace?

Let me now move to the question of how to better mitigate the threat posed by anonymity and the resulting complexities of identity verification in cyberspace.

The inherent anonymity of cyberspace poses ongoing and perplexing challenges to law enforcement authorities.

As long as law-enforcement authorities cannot locate *with certainty* the origin of a cyber attack, cyber terrorists and all other cyber criminals have a decisive advantage.

For every technology designed to make cyberspace more transparent new technologies are developed to obscure one's identity online. Anonymity online makes attribution of cyber attacks a major challenge if not a virtual impossibility

But let us ask ourselves: How anonymous is cyberspace, really?

Technical experts who deal with this question on a daily basis often contend that on the whole, those who really wish to remain anonymous while online – and are willing to take the necessary precautions – can do so.

Indeed, many ways exist for perpetrators of cyber crimes to disguise their location in the physical world and the exact nature of their online activities.

In fact, many, if not most, of the technologies which enable users to hide or mask their identities and intentions online are not developed by criminals. They are developed by people who have embraced the idea of the Internet as a free and ungoverned space. Such applications can be downloaded for free and are easy to use.

Make no mistake, in terms of anonymity in cyberspace the responsible elements of society are in an ongoing arms-type race for the competitive technological edge with terrorists and other criminals. And unfortunately, at this point in time, the good guys are not winning. Ever increasing instances of cybercrime clearly illustrate this phenomenon.

Moreover, the growing prevalence of Internet-enabled mobile devices is likely to further tip the scale in favour of those who wish to remain anonymous online. They will be able to access the Internet from literally anywhere and hide inside a growing pool of Internet users.

As internet-enabled mobile devices become more powerful, the trend of using them for criminal purposes will likely accelerate – especially as it is easy to discard or destroy such devices after use. If the device is gone, any further investigation is exceedingly difficult as even the best cyber trace can only ever lead law enforcement officials to the IP address that was used, i.e. to the machine – rather than the person.

Policy options

So what can be done to enable us to better mitigate the threat posed by anonymity and the resulting complexities of identity verification in cyberspace?

Participants at OSCE expert workshops on the topic have identified a series of policy options for decision makers to

mitigate the current inability to reliably trace perpetrators of cyber attacks. These options presently center on offline efforts. In the absence of better tracking-technologies such efforts can be time-consuming and even cumbersome. But until we develop the required technologies seven of the arguably best offline options include:

(1) *Conducting more focused research on cyber security threats with a strong emphasis on locating the origin of cyber attacks.* A clear need exists for the promotion of more focused research on cyber security threats. Arguably, our top priority should be to develop technologies enabling law enforcement to locate with certainty the origin of a cyber attack – in line with clear legal frameworks that provide guidance when and by whom these technologies can lawfully be used.

(2) *Using traditional law-enforcement practices against cyber-threats.* Traditional law-enforcement practices are in place and well established. Until we have the technologies to reliably trace the origin of cyber attacks we have to accept that online problems may not always have online solutions. The experience of well trained people is crucial and cannot be replaced by technology. While attempting to stay ahead of the technology-vulnerability curve, countries should not disregard tools which were used prior to the IT-revolution. Even if e.g. terrorists do not make technical mistakes in cyberspace, they can still make mistakes in the real world. For example, the infamous *Irhabi007* was apprehended through traditional detective work and not through a trace in cyberspace.

(3) *Establishing Computer Emergency Response Teams (CERTs).* Countries should consider establishing specialised Computer Emergency Response Teams (CERTs) and continuously train their staff in the latest

trends and developments pertaining to cyber security. Moreover, specialized Units within law enforcement agencies should be established and provided with the necessary means and standardized training for the tracking and investigation of serious criminal offenses committed through the Internet. Without such specialists countries are at a severe disadvantage in identifying perpetrators of cyber attacks and when fighting against the highly specialised cyber criminals of today.

(4) *Strengthening Public-Private Partnerships (PPP) in particular when devising methods to track the origin of cyber attacks and mitigate the threat posed by anonymity in cyberspace.* Many stakeholders are involved in enhancing cyber security, including state authorities, the private sector and civil society. Partnerships between and among all these stakeholders are critically important for effective and sustainable cyber security efforts. After all, the private sector develops, builds and maintains many of the most commonly used information technologies. Expertise and technical knowledge available from the private sector and academia should be sought and utilised in a systematic manner when combating cyber threats.

(5) *Clarifying the role of Internet Service Providers (ISPs).* Internet Service Providers are in a unique position in terms of access to data which could potentially be used for tracking and subsequently prosecuting cyber criminals and terrorists. For example, ISP co-operation is often crucial for the timely securing of evidence. As a prerequisite, governments need to give clear guidance to ISPs so that they can contribute within appropriate legal frameworks to national and international cyber security efforts. In particular, guidance is required as to (a) which data to store, (b) for how long and (c) who should have access to such data.

(6) *Improving end-user education.* In cyberspace, an educated user is often the first and arguably best line of defence against cyber attacks. Well educated end-users are able to better protect their machines and accounts from being hacked, hijacked and exploited by terrorists and other criminals who can use said accounts to remain anonymous in cyberspace. Clearly, many forms of cybercrime take advantage of – and frequently even depend on – Internet users not taking reasonable precautions to make their machines and accounts as secure and as impenetrable as possible. Educational campaigns, starting at the primary school level and continuing all the way through a person's career could significantly improve this situation.

Finally,

(7) *Improving international co-operation and strengthening the role of Regional and International Organizations.* When attempting to track terrorists and other criminals in cyberspace international co-operation is a critically important component of cyber security efforts. As cyber-threats are truly global threats, effective responses need global co-ordination. To enhance international co-operation a constructive dialogue on a multi-lateral level and using all available and appropriate fora, including International and Regional Organizations should be sought.

To conclude, it is my belief that an enlightened way to implement the above recommendations is through the framework of a comprehensive approach to cyber security. I look forward to hearing your views on these issues and to collaborating with you.

Thank you for your attention.