Chapter 4

A Comprehensive Approach to Cyber Security – Trends, Challenges and the Way Forward

Raphael Perl and Nemanja Malisevic [1]

Growing dependence on information technology (IT) and increasing interconnection of critical (information) infrastructures have made a secure cyberspace vital to the functioning of a modern state. Consequently, cyber threats or "cyber terrorism" remain one of the crucial concerns to be addressed by decision makers – not just political decision makers, but those from industry and civil society as well. This chapter will showcase how dependency on cyberspace is increasing and outline cyber security threats not only to governments and industry but also to the individual Internet user. Specific challenges to cyber security will be highlighted and concrete options offered on how such challenges can best be addressed by implementing an OSCE-type comprehensive approach to cyber security.[2]

Dependency on Cyberspace is Increasing

Exactly how dependent on cyberspace are we, really? In June 2008, the numbers of personal computers in use worldwide hit one billion, while another one billion are expected to be in use by 2014.[3] These computers are operated by more than a billion and a half users worldwide.[4] Much of what most people—at least in the developed world—would describe as "normal everyday life" is to-

[1] Raphael Perl was previously the Head on Anti-Terrorism Issues at the Secretariat of the Organization for Security and Co-operation in Europe (OSCE), and is currently the Director of the Partnership for Peace Consortium. Nemanja Malisevic is the action officer for combating terrorist use of the Internet/enhancing cyber security of the OSCE Secretariat's Action against Terrorism Unit (ATU). This article considers the threat posed by cyber terrorism.

[2] Note that this chapter addresses cyber threats emanating from terrorists and other criminals only. It will not cover cyber-espionage and cyber-war – namely conflict in and for control of cyberspace among nation states. These issues are beyond the OSCE Action against Terrorism Unit's present mandate.

[3] www.gartner.com/it/page.jsp?id=703807.

[4] *Internet World Stats*, www.internetworldstats.com (December 2008).

day based on information technology and cyberspace running smoothly in the background – be it in the home, the car or the office.

But not everybody is convinced that they are directly dependent on the Internet: According to a recent EU study, one third of all Europeans have never used the net. The same study showed that one in four has never even used a PC. Some claimed that they had no need for an Internet connection while others said they simply could not afford one. Europeans above the age of 65 and the unemployed were least active online.[5]

However, that same EU study also noted that in 2008 56% of EU citizens had become regular Internet users – up one third since 2004. Importantly, more than 80% of those users had installed a high-speed Internet connection, compared to some 30% in 2004. According to the study, nearly 70% of EU citizens under the age of 24 used the Internet every day, compared to the EU average of 43%.

While the above represents only a small sample, the trend is clear: Use of the Internet and dependency on cyberspace is increasing. It is unrealistic to expect modern society to overcome its reliance on information technology and cyberspace. Clearly, for the current generation and the next ones, at least those in the developed world, their way of life, both in terms of work and leisure is *intrinsically* linked to cyberspace. Their dependency on cyberspace is increasing continuously and exponentially!

Ironically, as with anything one takes for granted, modern societies may only realise just how dependent they have become on the cyber infrastructures and related services—such as the Global Positioning System or digital communication—when they crash.[6]

Try and think of any infrastructure, service or commodity that could function without it. Saying one could live a modern life without cyberspace is akin to saying: "There was a time before electricity, and we were fine then, too." Or a time without running water. Imagine one actually had to live without running water and electricity. Sure, one would survive, but one's priorities and daily routines would change. Life, as one knows it, would change. And that is exactly what would happen, if cyberspace were to be disrupted in a meaningful way.

Modern societies simply can no longer function, in the way we are used to, without a functioning cyberspace. Terrorists and other criminals are increasingly grasping this, too. As a result, the main challenge for cyber security practitioners is to raise awareness of decision makers and create sufficient will to address cyber security in a comprehensive manner.

And to do it *before* a large-scale cyber attack occurs.

---

5 http://ec.europa.eu/information_society/eeurope/i2010/docs/annual_report/2009/com_2009_390_en.pdf.

6 Kenneth Geers, "The Cyber Threat to National Critical Infrastructures: Beyond Theory," *Information Security Journal: A Global Perspective* 18:1 (2009): 1-7.

Recent Trends and Developments

Looking at cyber threats, what are some recent trends and developments? To cite but a few:

1. Cyber criminals are increasingly operating akin to successful businesses.
2. Command-and-control systems remain vulnerable.
3. New technologies create innovative attack vectors.
4. Threats to mobile devices are increasing.
5. Attacks on legitimate websites are increasing.
6. Volume of SPAM is increasing.
7. Attacks on social networking sites are increasing.
8. Volume of *spear phishing* is increasing.
9. Lack of user awareness combined with negligence leads to loss of sensitive data.
10. Cyber infrastructures may be more vulnerable than is traditionally believed.

1. Cyber criminals are increasingly operating akin to successful businesses

Cyber criminals are increasingly operating akin to successful businesses—incorporating practices used by the private sector, including resource sharing, specialisation, co-operation and co-ordination—with the overall aim of maximising profits.[7]

2. Command-and-control systems remain vulnerable

Attacks on command-and-control systems of critical infrastructures remain a concern. For example, a recent Federal Aviation Administration (FAA) report warns that unless "effective action is taken quickly, it is likely to be a matter of when, not if, ATC (air traffic control) systems encounter attacks that do serious harm to ATC operations." Among other cases it outlines a cyber attack on FAA computers in Alaska in August 2008. Hackers seized control and by exploiting the network's interconnection stole an administrator's password and took control of a domain controller in the Western Pacific region, thereby gaining access

[7] *Cisco 2009 Midyear Security Report*, http://cisco.com/web/about/security/intelligence/midyear_security_review09.pdf.

to more than 40,000 login credentials used to control part of the FAA's mission support network.[8]

3. New technologies create innovative attack vectors

The number of instances is rising where in addition to using *key loggers* to record the victims' keystrokes, cyber criminals take control of webcams – sound included. Many computers today already contain built-in webcams and such cameras will likely be a standard feature in all computers of the future. Therefore, these recent cases may well only represent the tip of the iceberg.[9] Moreover, the thirst for and the availability of instant news in cyberspace is another attack vector exploited by cyber criminals. For example, hiding malicious software in emails that appear to be linked to major news stories is becoming increasingly popular among cyber evildoers. Recent examples include malicious code hidden in emails posing as news on the swine flu or President Obama's inauguration speech.

4. Threats to mobile devices are increasing

Mobile device threats such as *smishing* are another threat vector that is expected to become more prevalent. This is hardly surprising, given the fact that several billion handsets are already in use worldwide.[10]

5. Attacks on legitimate websites are increasing

A recent report by Cisco predicted a surge in attacks on legitimate websites. In fact, their data showed that, already, exploited websites are responsible for nearly 90 % of web-based threats.[11]

6. Volume of SPAM is increasing

Cisco estimates that, currently, almost 200 billion messages per day—or approximately 90 percent of all electronic mail sent worldwide—can be defined as spam.[12] According to a recent Microsoft security report more than 97 % of all e-mails sent over the net are unwanted.[13] Many of these emails contain mali-

---

8 *Review of Web Applications Security and Intrusion Detection in Air Traffic Control Systems*, Report No. FI-2009-049 (U.S. Department of Transportation, Federal Aviation Administration, 4 May 2009), http://www.oig.dot.gov/sites/dot/files/pdfdocs/ATC_Web_Report.pdf.

9 "Webcam under hacker's control," *BBC News*, 18 May 2009; http://news.bbc.co.uk/2/hi/technology/8039207.stm.

10 *Cisco 2009 Midyear Security Report*.

11 Ibid.

12 *Cisco Cyber Risk Report* (December 2008), http://www.cisco.com/web/about/security/intelligence/CRR_dec1-7.html.

13 Darren Waters, "Spam overwhelms e-mail messages," *BBC News*, 8 April 2009, http://news.bbc.co.uk/2/hi/technology/7988579.stm.

cious code or are sent with malicious intent. And even though most never reach our inboxes, the sheer volume guarantees that many still get through.

7. Attacks on social networking sites are increasing

As a general rule, cyber criminals follow the user. They commonly target software that is used by the majority of users and routinely target those websites attracting the most people. As a consequence, one can expect a continuous increase in attacks on social networking sites. The Kaspersky Lab Research Centre found that cyber criminals who used sites like Facebook, MySpace and Twitter to spread viruses and worms were *ten times* more successful in their attacks than if they had used email.[14]

8. Volume of *(spear) phishing* is increasing

According to an April 2009 study from Gartner Research, more than 5 million Americans alone lost money to phishing schemes in 2008, a 40% increase from the year before, although the average amount lost in each scam decreased, largely due to strengthened bank safeguards.[15] Highly targeted phishing attacks—so called "spear phishing"—continue to be particularly effective even against users who have previously participated in user-awareness training. Moreover, cyber criminals are, it seems, using spear phishing to increasingly target small business accounts.[16]

9. Lack of user awareness combined with negligence leads to loss of sensitive data

Many users still have not grasped the concept that pressing "delete" does not permanently remove data from their machines. In one recent study, of 300 hard disks bought randomly at computer fairs and an online auction site, 34% still held personal data. Shockingly, this data included sensitive information for shooting down intercontinental missiles, bank details and the UK's National Health Service (NHS).[17] Combined with all the USB-sticks and laptops lost worldwide, the amount of sensitive information that is lost every year is concerning, indeed.

---

[14] Maggie Shiels, "Cyber crooks get business savvy," *BBC News*, 14 July 2009, http://news.bbc.co.uk/2/hi/technology/8149034.stm.

[15] Andy Greenberg, "Cybercops Without Borders," *Forbes.com*, 6 January 2009, www.forbes.com/2009/06/01/cyberbusts-security-internet-technology-security-cyberbusts.html.

[16] Brian Krebs, "European Cyber-Gangs Target Small U.S. Firms, Group Says," *Washington Post*, 25 August 2009, www.washingtonpost.com/wp-dyn/content/article/2009/08/24/AR2009082402272.html.

[17] "Missile data found on hard drives," *BBC News*, 7 May 2009, http://news.bbc.co.uk/2/hi/uk_news/wales/8036324.stm.

10. Cyber infrastructures may be more vulnerable than is traditionally believed

Events which unfolded after the death of Michael Jackson provided insight into just how fragile the cyber infrastructure can be – at least in certain circumstances: When the news broke such large amounts of people rushed online to double-check, contact their friends or just express their feelings that many sites and services slowed down significantly. Some even crashed. Examples include Google News, Twitter, Wikipedia and AOL's instant messenger service. Clearly, the cyber infrastructure is vulnerable, if not fragile – under certain circumstances. This did not go unnoticed among cyber criminals and terrorists.

Challenges

With the above in mind, what are some of the challenges when responding to the aforementioned developments and trends?

1. Security was not a priority when the cyber infrastructure was created.
2. Research on key cyber security questions is lacking.
3. Cyberspace favours the aggressor and not the defender.
4. High-level expertise on cyber attacks is likely spreading.
5. Skill required to conduct cyber attacks is decreasing.
6. Likelihood of cyber attacks by terrorist groups is increasing.
7. Classification of cyber attacks as "weapons of mass disruption" is confusing.
8. Threat of a combined cyber- and physical attack is increasing.
9. No universally accepted legal framework for dealing with cyber threats exists.
10. Public-Private Partnerships (PPP) are still lacking.

1. Security was not a priority when the cyber infrastructure was created

Much of the challenge in keeping cyberspace safe, secure and functional derives from the fact that security was not a priority when the Internet was created. Instead, the focus was on redundancy, efficiency and interoperability.

2. Research on key cyber security questions is lacking

Another challenge lies in the fact that societies, in general, are uncomfortable dealing with issues they do not clearly understand or cannot control. Unfortunately, in terms of cyber security, there is actually quite a lot we do not understand.

- We do not know exactly how dependent we are on IT infrastructures.
- We do not know exactly how robust our Internet infrastructure is.

- We do not know exactly how much damage cybercrime does annually.
- We do not know exactly how far terrorists are in terms of developing cyber capabilities.

The list goes on.

Much speculation exists, but not enough factual knowledge. Focused research is required to shed light on the above questions.

3. Cyberspace favors the aggressor and not the defender

A key challenge is the immense difficulty in locating the origin of a cyber attack. As a result, attribution remains virtually impossible. 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 – cyberspace presently favours the aggressor and not the defender.

4. High-level expertise on cyber attacks is likely spreading

Another challenge is that the current economic situation has already led to many qualified people losing their jobs in all walks of life – including people with considerable IT skills. Much concern exists that, if the current economic crisis continues, unemployed IT specialists may sell their skills to the highest bidder – potentially even to criminal or terrorist groups.

5. Skill required to conduct cyber attacks is decreasing

Linked to Challenge # 4 is an additional overarching challenge: Evidence clearly suggests that, on the whole, it is constantly becoming easier to conduct cyber attacks. Thousands of websites dedicated to hacking exist. Many of them not only offer the necessary tools of the trade for download, but also contain detailed descriptions and how-to manuals. In short, with the tools that are available today people with little or no IT experience can commit crimes online. It takes about 20 minutes to set up all the necessary programmes to steal music, movies, and games via one's computer. It takes a little longer to set up a botnet but, as was not too long ago even illustrated by the BBC in their show *Click*, it is not all that difficult.

The challenge posed by this trend is very worrisome. More and more people will eventually realise just how easy it is to conduct cyber attacks. These will be people who would never rob a store, a bank or somebody else in the street. But if they could attack from the comfort of their homes without ever having to look their victims in the eyes … who knows?

6. Likelihood of cyber attacks by terrorist groups is increasing

Disagreement exists among experts over the likelihood of a cyber-attack by terrorists. In particular, some argue that terrorist groups have neither the necessary resources nor the skills to conduct large-scale cyber-attacks, namely attacks which would disrupt critical infrastructure or critical information infrastructure in a significant way.

However, terrorist groups—in addition to engaging in activities such as identifying, recruiting and training new members, collecting and transferring funds, organizing terrorist acts, and inciting terrorist violence—have shown their clear intent to study hacking and cyber attacks. Data found on seized hard-drives proves this.

Some 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 on terrorism charges. Tsouli, in addition to his cyber-activities in support of Al-Qaeda, was also engaged in credit card fraud.

To date a major cyber-attack has not been conducted by terrorists. However, cybercrime remains on the rise: Cyber criminals continue to find new and improved ways to abuse information technology and cyberspace. Although most individuals who engage in these types of activities are "ordinary" criminals or, at times, pranksters rather than terrorists, their actions continue to set precedents. Or even "proofs of concept."[18]

What this phenomenon demonstrates is that, as previously mentioned, the relevant expertise to conduct cyber attacks is available and it is growing, both in terms of depth and dissemination. It also means that terrorists can acquire such expertise, through money, violence or the threat of violence, or even their own diligence. Regardless of which path evildoers choose, the technology and the related techniques to do harm cannot be contained and—as with every other type of expertise—eventually those who have it may likely be tempted to use it. At least once!

The challenge countries and individuals alike face is that "at least once" may just be once too many for much of the world's economy. 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.

7. Classification of cyber attacks as "weapons of mass disruption" is confusing

Another challenge is one of definition: Cyber attacks are often classified as "weapons of mass disruption" as opposed to "weapons of mass destruction." What exactly does this mean? What purpose does such a distinction serve? Human casualties aside or whether an IT service or infrastructure is *disrupted* or *destroyed*, the key point is that said infrastructure *cannot be used*. Disrupted or destroyed only refers to the time it may take to rebuild it or to get it going again. If a cyber attack on a critical infrastructure were to be conducted over an ongoing and extended time period the effect would be akin to that infrastructure being destroyed.

Imagine a bombing attack on a pipeline or a container shipment. It would disrupt the supply chain. Now imagine a cyber attack on the computers of the port handling the container or on the command-and-control centre that regu-

[18] Geers, "The Cyber Threat to National Critical Infrastructures."

lates how much oil or gas is pumped through the pipeline. Again, the supply chain would be disrupted. A cyber attack, in this example, achieves the same effect as a conventional attack, just by different means.

Obviously, a pure cyber attack—at least for the time being—still does not have the same potential for human casualties as the detonation of a bomb. However, it needs to be understood 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. Clearly, dealing with the effects of a large-scale cyber attack would force many people to change their way of life – at least temporarily.

8. Threat of a combined cyber- and physical attack is increasing

Another potential challenge is posed by a combined cyber- and physical attack. Think about damage caused by cyber attacks in both physical and economic terms. What if a series of cyber attacks were coupled with strategically placed bombs, or with a series of biological, chemical, or radiological attacks? Such attacks, in particular on critical infrastructure would have devastating effects on large parts of the population – also in terms of psychological effects.

A cyber attack, coupled with strategically placed bombs. Such a combined real-world/cyber attack remains the biggest threat. And it may only be a question of time.

The fact that cyber-terrorists currently use methods pioneered by cyber-criminals and hackers to communicate or make a profit does not limit their potential activities to these fields. It may only be 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.[19] The potential for economic and possibly even human damage is immense.

Some argue that a terrorist attack on critical information infrastructure or the Internet itself is unlikely because terrorists themselves depend on it. We would counter that relying on terrorists *not* attacking an infrastructure they themselves depend on is very risky – one just needs to look at civil aviation or public transport.

9. No universally accepted legal framework for dealing with cyber threats exists

On a multilateral level, no agreement exists on how to effectively enhance cyber

[19] 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. See Marco Gercke, "*Cyberterrorism: How Terrorists Use the Internet*," *Computer und Recht* (2008).

security. The OSCE has been promoting, among other issues, the ratification and implementation of various anti-terrorism instruments – among them the Council of Europe's (CoE) Convention on Cybercrime (2001) and the Council of Europe Convention on the Prevention of Terrorism (2005). Both instruments are open for accession by non-members of the CoE.

However, some OSCE participating States have been calling for the creation of another international instrument dealing specifically with terrorist use of the Internet. This is of particular importance in relation to a much overlooked issue, namely Article 27 Paragraph 4a of Council of Europe's Convention on Cybercrime (2001) which allows for a requested party to refuse assistance if "the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence." Such a "political exception clause" is always problematic for those who seek to bring terrorists to justice.

Importantly, the Council of Europe Convention on the Prevention of Terrorism (2005) does not allow for such a political exception (Article 20, paragraph 1) for terror motivated cybercrimes. Moreover, it criminalizes public provocation to commit a terrorist offence (Article 5) as well as recruitment (Article 6) and training for terrorism (Article 7), which are, of course, some of the key reasons why terrorists use the Internet.

In theory, therefore, both instruments together—and only together—provide a good framework for countering terrorist use of the Internet. In reality, however, many states face certain challenges in becoming parties to these conventions. Today only about a dozen countries worldwide are party to both instruments.

10. Public-Private Partnerships are still lacking

Systematic consultation and co-ordination with private sector experts, academia and civil society is still lacking. Industry expertise and academic research, in particular, could bring large benefits during the drafting of national cyber security strategies and during the elaboration of any new law aimed at tackling cyber threats. For example, some countries' inadequate laws on dealing with encryption could have been significantly improved had the private sector and academia been consulted beforehand.

The bottom line is that many challenges exist and that individuals, businesses and countries need to be better prepared.

Need for a Comprehensive Approach to Cyber Security

Why is a comprehensive approach to cyber security needed and how can it be accomplished?

Arguably, the best option to address the challenges to our cyber security by terrorists and other criminals is to implement a comprehensive approach to cyber security – an approach (a) that strengthens national security; (b) that tackles cybercrime, and (c) terrorist use of the Internet; (d) that is responsive

to a wide variety of risks and threats; and (e) that enables countries to protect a wide spectrum of targets ranging from the individual Internet user to critical infrastructures.

Why is such a comprehensive approach so important?

- ✓ Because there is only one cyberspace

The cyberspace we use at work and during our free time is the same our children use to play videogames or chat with friends. It is also the very same cyberspace abused by cyber criminals and terrorists.

Cyber evildoers share common methods of cyber attack even if their goals and motivations differ. They learn from each other and, as mentioned above, often work together. Unfortunately, as previously mentioned, the international community lacks a shared and common response. All too often it is divided and firewalled in the use of resources, expertise, functional jurisdictions and legal frameworks.

It is therefore crucial for the international community to implement a comprehensive approach to cyber security as soon as possible. Cyber security needs to be an intrinsic part of any state's national security considerations and planning – and a comprehensive approach is the only viable option for national authorities and the international community to ensure long-term and sustainable cyber security.

Options for Consideration

How can the aforementioned cyber security challenges potentially be tackled?

Participants at OSCE expert workshops on the topic have identified a series of policy options for decision makers, some of which include:

1. International co-operation should be improved & the role of RO/IOs strengthened.
2. The international legal framework should be strengthened.
3. Computer Emergency Response Teams should be established.
4. Critical Infrastructure protection should be improved.
5. Baseline questions for critical infrastructure protection should be established.
6. Public-Private Partnerships (PPP) should be improved.
7. The role of Internet Service Providers (ISPs) should to be clarified.
8. Research on cyber security threats should be conducted.
9. Traditional law-enforcement practices should also be used against cyber-threats.
10. End-user education should be improved.

1. International co-operation should be improved and the role of RO/IOs strengthened

International co-operation remains crucial. As cyber-threats are truly global threats, effective responses need global co-ordination. Countries should establish and maintain reliable and knowledgeable contacts, in particular as many investigations into cyber crimes and cyber threats are highly time sensitive. 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.

2. The international legal framework should be strengthened

Existing laws pertaining to cyber security should be harmonised and universally implemented. No agreement exists whether present international and regional legal instruments, including the CoE's Convention on Cybercrime (2001) and the CoE Convention on the Prevention of Terrorism (2005), provide a legal framework adequate for dealing with modern threats to cyber security or whether new specific instruments may need to be adopted for this purpose. Focussed discussion on this topic should be promoted.

3. Computer Emergency Response Teams should be established

All countries should establish specialised Computer Emergency Response Teams (CERTs) or Computer Security Incident Response Teams (CSIRTs) 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 investigation of serious criminal offenses committed through the Internet. Law-enforcement agencies should also establish mechanisms to systematically share information, best practices and lessons learned.

4. Critical Infrastructure protection should be improved

Critical infrastructure protection should take into account physical threats as well as cyber threats. Vital command-and-control systems need to be protected through appropriate technical measures and maintained by adequately trained staff. For the most critical infrastructures, "air-gapping" of at least the backup systems should be considered. Staff should be trained in password protection and, if necessary, other means of authentication should be installed. Particular focus should be placed on countering the threat posed by "insiders" – cyber-measures may not be enough to counter this particular threat. Thorough background checks, vetting and individual accountability procedures should be established. Overall, stricter regulation of cyberspace may be necessary with regard to critical infrastructure protection.

5. Baseline questions for critical infrastructure protection should be established

The majority of critical infrastructures are very resilient and strong, having been designed not only to allow for human error but to withstand natural disasters as well. Nonetheless, some experts argue that national security planners should aim to answer, at a minimum the three following questions and follow-up as necessary: (1) How dependent is the country's critical infrastructure on IT? (2) To what degree is said critical infrastructure connected to (and dependent upon) the Internet? (3) In theory, what would the most successful cyber attack against this infrastructure look like, and would it rise to the level of a national security threat.[20]

6. Public-Private Partnerships (PPP) should be improved

PPPs are critically important – not only because the private sector researches, designs, develops, builds and maintains many of the most commonly used information technologies, but also because many of the world's critical infrastructures are, in fact, owned by industry, often with the main goal of turning a profit and being cost efficient rather than being as secure as possible. As a result, incentives may have to be provided to the private sector to address this issue.[21] Moreover, expertise as well as technical knowledge available from the private sector and academia should be sought and utilised in a systematic manner, in particular when new legislation is drafted in this area. This would ensure that such laws are adequate and useful. Similarly, civil society representatives should be involved in initiatives which foster end-user education and in efforts to counter terrorist messages online.

7. The role of Internet Service Providers (ISPs) should be clarified

The international community also needs to reach agreement on the roles and responsibilities of ISPs in efforts to comprehensively enhance cyber security. Governments need to give clear guidance to ISPs so that they can contribute to national and international cyber security efforts. In particular, guidelines are required regulating the data ISP's should store, for how long and who should have access to such data.

8. More research on cyber security threats should be conducted

A need exists for the promotion of more focused research on cyber security threats. One long-term priority should be development of technologies to enable law enforcement to locate the origin of a cyber attack – in line with clear legal frameworks that provide guidance when and by whom these technologies

---

[20] Geers, "The Cyber Threat to National Critical Infrastructures."

[21] *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure* (U.S.: The White House); www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf.

can lawfully be used. The international community needs to ensure that cyber evildoers know and fear that negative consequences exist for their actions online.

9. Traditional law-enforcement practices should also be used against cyber-threats

Online problems may not always have online solutions. Moreover, the experience of well trained people 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 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. Consequently, traditional law-enforcement cooperation also needs to be continuously strengthened.

10. End-user education should be improved

Enhancing end-user education is critically important as well and should be significantly improved (see below). Many forms of cybercrime take advantage of—and frequently even depend on—the fact that most Internet users do not take all possible precautions to make their machines and accounts as secure and as impenetrable as possible.

Need for Improved End-user Education

Investing into new technologies, setting up CERT's, training specialised staff – these are all very necessary steps. But for most cyber threats, the key step that all countries need to take is to significantly raise awareness and improve end-user education. Educational efforts should emphasise that many easy steps exist which each and every user can take to stop their computers and accounts from being hacked or hijacked, or at least make it much more difficult for all criminals, whatever their motivation, to do so.

Cyber criminals are taking advantage of a growing pool of users who do not keep their machines and accounts as secure as possible – the "Conficker" worm, which infected millions of PCs in mere days, is a case in point.

Too often security measures are only implemented after the user has become a victim. However, neither industry nor the international community can afford to wait until everybody has a bad experience before they become more vigilant against cyber threats.

Clearly, central here is raising awareness of political decision-makers about the need for end-user education – and it is here that regional organizations such as the OSCE can be of particular value by providing a platform for networking and information exchange.

Every uneducated user, every unprotected computer, every unsecure network is a weak link begging to be exploited. In the real world, we tend to look

out for ourselves. Online, we need not only to better protect ourselves, but also our cyber neighbours. In this way all of us can contribute to making the Internet more secure. Because in a cyberspace where users are not security aware and their machines not secure, nobody is safe!

Summary and Conclusion

In conclusion, it is clear that along with contemporary society's dependency on information technology and cyberspace, the threat posed by terrorist and criminal use of the Internet is growing. In particular, increasing concern exists over the potential threat posed by combined real-world and cyber attacks. Continued and enhanced international co-operation is crucial in addressing this threat and international and regional organizations can play a key role to establish, foster and strengthen such co-operation.

There is *only one cyberspace*. No matter from where we access the world-wide-web, the cyberspace we navigate is *one and the same*. An attack on this cyberspace, any attack, whatever its background or motivation is *an attack on all of us* as it affects us collectively as Internet users in an increasingly IT dependent world. A *comprehensive approach* to cyber security is therefore the only reasonable way forward – an approach (a) that strengthens national security; (b) that tackles cybercrime, and (c) terrorist use of the Internet; (d) that is responsive to a wide variety of risks and threats; and (e) that enables countries to protect a wide spectrum of targets ranging from the individual Internet user to critical infrastructures.

Such a comprehensive approach to cyber security is the only way to achieve the long-term goal of making cyberspace as *safe and secure* as possible – and to ensure that it remains that way.