Asociace pro mezinárodní otázky
Association for International Affairs

Conference Report

Confronting Cyberterrorism: Tackling Political Aspects of Cybersecurity

–

Prague, 6-7 December 2011

Confronting Cyberterrorism: Tackling Political Aspects of Cybersecurity

–

Prague, 6-7 December 2011

Asociace pro mezinárodní otázky
Association for International Affairs

Conference Report

Confronting Cyberterrorism: Tackling Political Aspects of Cybersecurity

–

Prague, 6-7 December 2011

Introduction

On 6-7th of December 2011, the Association for International Affairs (AMO) in cooperation with the U.S. Office of Naval Research Global, the Estonian Embassy in Prague and NATO Public Diplomacy Division organized an international conference and expert workshop *Confronting Cyberterrorism: Tackling Political Aspects of Cybersecurity*. The conference took place at the European House in Prague.

The event addressed the issue of politically motivated cyberattacks, where IT and other infrastructure serves as the 'first target', a tool to influence the 'second target' which is population and its political representation - in one word, cyberterrorism. The event put under complex scrutiny especially the complex problems of the decision-making process in reaction to politically motivated cyberattacks along different dimensions, namely technical, legal and political, at both domestic and international levels.

The conference lasted for two days and consisted of a public panel discussion and an expert workshop. The speakers included European and U.S. representatives of the IT industry, academia, government and military as well as diplomats and legal. The conference discussions took place under the Chatham House rules.

Conference conclusions

During the panel discussion *Political Aspects of Cybersecurity: Recent Developments and Future Challenges*, the speakers addressed a broad range of issues, including the notion of cyberthreats in general and recent developments in the field, as well as the peculiarities of cyberterrorism. A diverse set of speakers provided for a variety of perspectives on cybersecurity - operational, military, legal, and technical - which made the discussion and the following Q&A session especially fruitful.

Recent developments in cybersecurity

Cyberspace plays an extensive and growing role in our everyday life, from communications through public e-services to leisure. Thus, its protection and security should be among the key priorities of every country in the world.

It is no longer a stretch of imagination to regard cyberattacks as a genuine security threat and an act of terrorism. Economic prosperity of every country nowadays also highly depends on cybersecurity. To illustrate both aspects, it is worth noting two events. In April 2008, Estonia was the first country to experience a massive, politically motivated cyberattack. Recently, Sony has lost 170 mil USD in revenue when its Play Station network was hacked. Cases like this push countries to introduce new laws and other mechanisms to protect their cyberspace. In Estonia the attacks were followed by an establishment of a set of new laws and protection mechanisms, concentrating on national capability building and developing preventive measures, e.g. the National Cybersecurity Strategy, amendments to the penal code, Emergency Act and a new system of Critical Information Infrastructure Protection. In May

2011, the first ever U.S. International Strategy for Cyberspace was introduced, according to which 'active defence' (employment of limited offensive actions and counterattacks) can now be used as a response to a cyberattack.

Thirty international organizations have already put cybersecurity on the list of their top priorities. NATO has taken steps to address the issue (2010 Lisbon Summit's decision to develop and implement a New Cyber Strategy). NATO Cooperative Cyber Defence Centre of Excellence (CCD COE) was established in Tallinn in 2008, with 10 sponsoring nations at the moment. EU has also laid ground to a common cybersecurity policy with moves towards common standards and compatibility of software. In 2004, the European Network and Information Security Agency (ENISA) was established to deal expertly with issues of cybersecurity, with the main focus on the improvement of cooperation, competence in security technology, as well as privacy, trust and awareness. Still, no international treaties on cybersecurity have been signed so far, and national cyberdefence programmes are underfunded and not paid enough attention to. As usual, only countries which have suffered a cyberattack realize the seriousness of the threat and try to promote cooperation in this area.

According to the conference speakers, there are two main lessons to remember. Firstly, cyberattacks happen every day. Secondly, no matter what, one's information security is never strong enough: nobody is invulnerable and organizations are not prepared well, despite the fact that even major attacks are usually not too sophisticated. Generally speaking, we have all the resources to effectively fight cyberattacks, but we lack sufficient awareness and resolve.

Peculiarities of cyberterrorism

The complexity of cyberthreats was stressed repeatedly throughout the conference. Cybersecurity was described with the acronym CHEW – Crime, Hacktivism, Espionage, Warfare. This indicates that there is no single typical feature of cyberattacks. One has to deal with diffused, transnational network groups which often have no clear connection to states or their armies. What makes them strong and relevant is information.

This also affects strategies and tactics which, due to the specific nature of internet networks, are no longer concerned with territorial integrity. Targets have transformed from military and industrial objects to critical infrastructure, a large proportion of which is privately owned.
The effects of an attack are not measured by the number of injured or dead, even though they might be a result of an attack. The attacker is in a much better position than the defender and it is impossible to be completely secure from a cyberattack. Also expectations have a different meaning in cyberdefence: while it is relatively feasible to predict what happens in a case of usual warfare, hardly anyone can predict accurately what would happen in a case of a cyberwar.

Cyberattacks are global by nature and should be approached from a three-dimensional perspective: everyday business (analysis of threats), national point of view, and global perspective. Moreover, cyberattacks present a 'multi-stakeholder puzzle' due to a great number of actors involved. There are a lot of different players and they all need to be included in the process. However, this is complicated as they all have different interests, and communication patterns which lead to a lack of cooperation and interaction. As a result, we

face converging cyber-insecurity drivers, fragmented efforts and reluctance to share intelligence.

Fighting cyberterrorism

Modern threats such as cyberattacks need to be faced in collaboration of the military, public and private sector on national and international levels. To be able to effectively fight cyberterrorism, it is essential to learn from the past, be aware of the present developments and be able to distil the future trends out of experience and current vision. It should start from defining the threat picture, followed by the singling out of every stakeholder that should be brought into the decision-making process. This is one of the most challenging parts, because the government needs to figure out where the help of the private sector is crucial, bring it in and orchestrate coordination among all players.

While it is a widespread belief that there are no effective legal instruments to face cyberthreats, according to the conference speakers this is not the case. There are a lot of laws and specific legal clauses which can be used. It is thus extremely important to connect the existing instruments and the experience of those who have already applied them to the current situation. Cybersecurity touches upon such legal issues as data protection, duty of care, access to information, criminalization, the mandate of international organizations etc. Not the least, it is a great challenge for the governments to fight cybersecurity while not harming the freedom of speech. Proper balance between security and fundamental rights should always be maintained.

It was stressed by the discussants that there are no generally applicable rules, no universal solution for countering a cyberthreat. The peculiarity of each case should be taken into account when fighting an attack. Despite all the developments in the cybersecurity domain, the discussion concluded, there are still more questions than answers: when is a cyber-attack an act of war; can software be regarded as a weapon; how do you inspect it; can critical infrastructure be a protected target; what constitutes ‘excessive force’; what constitutes ‘proportionality’ etc.?

Workshop findings

The expert workshop *Responding to a Politically Motivated Cyberattack: Navigating through the Decision-Making Maze* held during the second day of the conference provided a unique opportunity for invited experts, diplomats and government officials to take part in a complex cyberattack simulation and its evolution towards a ‘disaster scenario’. The workshop aimed at demonstrating the complexity of a cyberthreats and the reactions thereto. Due to the exclusive character of the seminar, the contents of the scenario are not revealed here. What follows are the ‘lessons learned’ based on the discussion among workshop participants.

- First of all, it was pointed out during the discussion that there is a **legal obligation to share security-related information** among NATO members, but cyber attacks of low intensity are often considered a ‘background noise’ and rarely paid enough

attention to. They tend to be considered a 'non-event', because they happen every day and usually do not trigger high-level political attention. However, it is still worth considering that a mere 'probe' can be a preliminary check of the strength of a network, the point being that technically insignificant events can have potentially enormous effects politically.

- One of the key issues is **what constitutes an 'attack'**. From a political point of view, a cyberattack comes to exist once an action is officially denoted as such. It therefore completely depends on the intentions of the countries or organizations involved: after all, if actors want to escalate the situation, they do not need to know who initiated the attack, only who they want to blame for it.

- Thirdly, even politically trivial attacks, such as defacing the website of a country's official, require the act of hacking - thus **constituting a criminal act**. The problem is to point to the original source of access to the website and define the perpetrator. Generally, there are three possible reactions to such attacks: ignore them, complain to the suspected perpetrator or his backer, or hack back.

- Another important issue concerns the **decision-making authority**: For example, in case of a request, who is responsible to make a decision on whether to host a foreign government's websites? And, can the government do anything to prevent actions of private providers within its jurisdiction, if they threaten to politically implicate the country as such? Workshop discussants voiced an opinion that a government is not legally responsible or the private companies' behaviour as it is their private business issue. Yet, there have been precedents of governments forbidding the private sector to get involved, since it was perceived as a question of national security. After all, in cyberwarfare, even an action by a nominally private party can make the country of its origin a potential target for retaliatory action.

- Once the conflict presented in the scenario intensified, it reached the level when websites across all government's services were attacked. The discussants agreed that this amounted to targeting **essential components of government infrastructure**, which later might lead to a collapse of the whole system. According to the prevailing opinion, at such a moment it would be essential to inform and get on board the IT industry, including producers of the equipment used in the infrastructure.

- The question was asked repeatedly throughout the workshop when should a situation be regarded as a **state of emergency**. Based on the discussion, it seems two different opinions usually exist: those who are in favour of declaring the state of emergency as soon as possible, hence opening way for extraordinary measures, and those who resist this step and tend to rely on regular, legal provisions. Among other things, this dilemma raises numerous legal and human rights challenges. The discussants agreed that some decision must be taken, and in the end it is better to make a wrong decision than to vacillate.

- The discussants experienced firsthand that there are **no definitive (and sometimes no good) answers** to many of the questions asked. Legal, military, political and technical dimensions intertwine and complicate the situation to extremely high

levels, and people in a position of power often do not know what to do. The workshop plainly demonstrated how complicated and multifaceted the issue of cybersecurity is. It was therefore stressed that countries urgently need – but at the moment do not have - ready-to-use **contingency plans**. While the EU and NATO are perfect platforms to develop such plans, they have not seized the opportunity yet.

Recommendations

The conference underlined the significance and complexity of cybersecurity, and hinted at the unpreparedness of governments to respond to cyberattacks. Following recommendations were formulated on the basis of panel and workshop discussions:

Readiness and cooperation

- We should not wait for a tragic event to improve our cybersecurity. The danger is real and imminent.
- It is time to develop a body of **international law** on cybersecurity, based on the example of the fight against terrorism and maritime threats. Rules of engagement, cyberspace, cyberattack, cyberwar and other crucial terms need to be defined.
- **Synergy** between the public and private sectors is crucial, and so is timely **international cooperation**, as no country is able to face cyberattacks on its own.
- On the other hand, executive decisions need to be taken fast, which is typically beyond the capacity of international organizations such as NATO or the EU.
- Since many countries have misguided strategies of dealing with cyberthreats, or none at all, conducting **simulations** based on scenarios similar to the one presented at the workshop could be extremely helpful.

Human factor versus technical issues

- Human factor remains the weakest link in the chain. **Education** of the public as well as officials is therefore of crucial importance.
- Experts (technicians) and politicians speak a different ‘language’. More effort should be invested in ‘getting the message through’. Ways of simplifying **communication** are essential, so that non-professionals (politicians) can grasp the essence of the problem and act on it. People who know what is going on should be able to communicate efficiently with the people who need to make decisions.
- The problems of **technical and legal attributions** of cyberattacks need to be handled separately. The problem is that technical attribution is almost impossible to achieve.
- More attention should be paid to the **control of software and data**, not just viruses and access denial, since a lot of products become infected already at the factory.

Prepared by Tomáš Karásek and Lilia Revak

Conference organizers

- Association for International Affairs (AMO)
- U.S. Office of Naval Research Global
- Estonian Embassy in Prague
- NATO Public Diplomacy Division

Conference partners

- European House in Prague

Conference Report

Confronting Cyberterrorism: Tackling Political Aspects of Cybersecurity

–

Prague, 6-7 December 2011

About AMO

Association for International Affairs (AMO) is a preeminent, Prague-based independent think-tank in the field of international affairs and foreign policy. The mission of AMO is to contribute to a deeper understanding of international affairs through a broad range of educational and research activities. Today, AMO represents a unique and transparent platform in which academics, policy makers, diplomats, business people, the media and NGOs can interact in an open and impartial environment.

In order to achieve its goals, AMO strives to

- formulate and publish briefings, research and policy papers
- arrange international conferences, expert seminars, roundtables and public debates
- organize educational projects
- present critical assessment and comments on current events for local and international press
- create vital conditions for the growth of a new expert generation
- support the interest in international relations among broad public
- cooperate with like-minded local and international institutions

Founded in October 2003, the AMO‘s **Research Center** has been dedicated to carrying out research and raising public awareness of international affairs, security and foreign policy. The Research Center strives to identify and analyze issues important to Czech foreign policy and the country‘s position in the world. To this end, the Research Center produces independent analyses; encourages expert and public debate on international affairs; and suggests solutions to tackle problems in today‘s world. The Center‘s activities can be divided into two main areas: First, the Center undertakes research and analysis of foreign policy issues. Second, the Center fosters dialogue with the policy-makers, expert community and broad public.

Asociace
pro mezinárodní
otázky
Association
for International
Affairs