BACKGROUND REPORT

PRAGUE**PRAŽSKÝ**
STUDENT**STUDENTSKÝ**
SUMMIT

NATO

Threat of Cyberterrorism

1. Introduction

The term "cyber-terrorism" has become quite clear in general understanding during last century. It denotes the use of internet for terrorist purposes, mostly tinged by political or ideological background. The cyber-terrorism itself is the most important driver in the matter of changing the face of today's terrorism as we know it.

It takes place at the cross point of two different worlds, the physical world and the virtual world. Everything important is situated within the convergence of these two dimensions. These can be simple home devices, like microwave oven, vacuum cleaner, automatic door gate or mobile phone. But looking at the big picture, these can also apply for big industrial systems like power plants, water dams or factories, where almost everything is controlled by information technology, which were proved to be more effective and efficient. These big systems are not only where the virtual world of controlling meets the physical reality, but also places providing a single point of failure and thus influencing thousands of people in their daily lives. Therefore any real chance of a cyber-attack happening in these institutions gives the impression of vulnerability to the humanity.

As people may get very easily affected by mass media and stories made up by the industry of entertainment, the distinction between reality and fiction becomes much more difficult. But first of all, let's review the hard facts concerning the topic of cyber criminality.

2. The cyber-terrorist's options

The methods of a cyber-terrorist will become clearer when one will understand the general behaviour aspects of such person. There are three main motives for having physical systems driven by something virtual. First one is the **access**, creating ubiquitous interface to data and information. Second one is the **control**, providing (not only) administrators with tools to manage systems remotely. Last but not least it is about the **data mining**, which means knowledge acquisition from the network. These are achieved using four ways. Firstly, it is the **transmission**, specifying longer lines across land and through space, **connections**, resulting in more links of more points, **aggregation**, which is about centralization of more information, and **retrieval**, in order to have more ways of access to data.

Resulting from this information, the cyber-terrorist has to exploit the functions contained within above mentioned areas of the target group and do one of the three general actions. The first one is to **destroy** some data, information, system etc., the second one is to **alter** anything of the previously mentioned, and the last one concerns **acquisition and retransmission** of data or information.

There are two very important aspects of a successful cyber-attack, which cannot be missing when attempting to have a great impact. It is the **scale** of the attack, and the accompanying **publicity**. It is quite certain that the successful destruction of for example one's mobile phone will not be of enough scale, but can be of big publicity if it concerns politically important person.

3. Do you know your cyber-terrorist?

The motivation of the potential attacker is considered a very important aspect, which generally determines the level of danger he is able to generate. There are basically two types of the aims the person wants to achieve. The cyber-terrorist either has **a specific goal**, for example a promotion of a political ideology or making money, or the aim can be purely **enjoyment and enthusiasm caused by potential success**. The second case is considered very threatening as the future actions are difficult to predict, and thus the searching for the weakest part of the chain and vulnerable spots in security precautions might be really hard to perform. One of the important factors is also the inner thoughts of a hack-for-fun hacker, who usually feels innocent of the actions he is performing, believes to be doing a righteous thing and afterwards may even feel persecuted. However, it must be kept-in mind that illegal behaviour cannot be considered a righteous act.

It is important to correctly differentiate between the types of internet subjects with interest in influencing other people's mind, as not every hacker or cracker[1] is a cyber-terrorist. There are three types of internet action. The first one is **activism**, non-disruptive use of internet for the purpose of supporting an agenda or cause. These mostly innocent actions consist in creating websites, posting materials for propagation or any dissemination of certain thoughts within the ethical borders. Second type is called **hacktivism**. This is somewhere between illegal hacking behaviour and the activism. Hactivism includes breaking into someone's computer or sending unsolicited e-mails covered in this area. The last one is **cyber-terrorism** itself. Cyber-terrorists are usually politically motivated and inflict severe harms to people's health, lives or economy.

4. The threats are real

In order to recognize and determine the possible damage caused by potential cyber-attacks, different case scenarios must be specified for drafting back-up plans and recovery scenarios. By the year 1996, the USA has taken a step towards improving the protection of the infrastructure vulnerability, when President Clinton established the President's Commission on Critical Infrastructure Protection (PCCIP) to perform deep-through analysis. The result was an identification of eight basic infrastructure systems: telecommunications, banking and finances, electrical power, oil and gas distribution and storage, water supply, transportation, emergency services and government services. Let's make some of the possible real life examples.

- A cyber-attack will get in control of a food manufacturer factory altering the levels of additives in order to poison the consumers. The food may be delivered to a big number of countries and internationally, thus causing global problems.

- A cyber-attack will get in control of an air traffic control system of an international airport. The system may be either brought down or provide altered information to airplanes, which may result in possible crash and loss of lives. The intrusion may also be extended to altering the data the pilots are getting from in-

[1] Hacker is a computer professional at an elite level knowing technical information and inner processes of a computer system without illegality involved. Cracker is a hacker using his skills for illegal purposes.

cockpit sensors, which may cause their severe confusion.

- The cyber-attack will bring down stock exchanges and get in control of thousands of bank accounts for the purpose of undermining the confidence in the financial system. Failure of the economic system follows as people are trying to run the banks in order to save their money.

All of these three examples have one very important aspect in common. To perform the attack the intruder does not have to be actually present at the point of the damage caused, neither has to have too many human resources. Therefore, the real danger caused is the transformation of terrorism into cyber-terrorism. Terrorism has been a privilege of big political movements with great financial donors, whilst cyber-terrorist can be a single person sitting in the comfort of his couch.

5. Point of objection – historic analogy

However, cyber-terrorism is not the only way of infrastructure disruption. After the First World War, European strategists considered potential attacks against infrastructure important to cripple the enemy's operational capacity. Those theories have been turned in practice during World War II by Royal Air Forces and United States Army during operations aimed at destroying war facilities, disabling the transportation system and interrupting electricity. When compared to the use case scenarios mentioned in previous chapter, those have similar effects to cyber-terrorism.

This practical experience provides us with learning material. During the war, Great Britain and United States dropped thousands of bombs at the territory of the Third Reich. However, the desired effect was different than expected. Whereas the attackers considered destroyed infrastructure as disabled and unable to operate, the real time for the Germans to restore it was not unbearably long. A document called Strategic Bombing Survey, conducted by Unites States, shows that whatever the target system was, no indispensable industry was permanently put out of commission by a single attack and that persistent re-attacks were necessary[2].

The main point of analogy to cyber terrorism is, that just like the German factories during World War II, today's infrastructure elements are governed by people, who are able to think and decide independently on their own, based on their professional practice. Thus when an attack occurs adequate counter-actions will very likely be done in a short matter of time.

6. Point of objection – routine failure

Cyber-terrorism is not the only factor threatening the infrastructure of today's civilization. Other factors are involved as well. In order to recognize the real risk coming from the impact of cyber-terrorism, it is good to compare it with similar causes of failure.

[2] Lewis, James. Assesing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats. *Center for Strategic & International Studies.* [Online] December 2002. Available at: <http://csis.org/files/media/csis/pubs/021101_risks_of_cyberterror.pdf>.

Services provided by infrastructure are not necessarily needed to be operational in every moment. It is quite common even within the private sector that services and systems are planned to be out of order for some time, based on a service level agreement. The time allowed for the service to be inaccessible is usually negotiated as a percentage of business hours, generally between 95% and 99.99% based on the service criticality[3]. Reaching 100% is considered to be extremely costly and therefore undesirable, as the last several percentages is usually a tolerable boundary of a downtime of one system. The same applies for electrical power or water distribution. Even citizens of the most industrialized countries are familiar with situations of being without access to these resources for a very limited period and are willing to sacrifice these short periods for cheaper prices. In the meantime corporations requiring 24/7 operation tackle these issues using other resources, like battery backups, redundancy etc. In conclusion, these periods of operation, which can be referred to as service downtime, occur even without the participation of cyber-attacks and the end-users do count on them and perform necessary counter-operations.

7. Point of objection – the involvement of nature

Also, there are other risks to infrastructure, for example natural disasters. When the sky turns dark and it starts to rain or even thunder, flights get delayed, cancelled or rerouted to different airport. When the water system is brought down by flooding, the affected populated areas are provided with spare water sources. When the electricity wiring are hit by falling trees, the citizens without power use their own sources to generate energy or may move temporarily to their relatives. In all of these situations, an infrastructure element has been brought down without causing severe damage, casualties or a major paralysis. These situations occur daily, monthly or on an annual basis without being significantly noticed.

8. The real issue

One can get an impression, that the threat is not actually real, but in the same time can see the hysteria of the media concerning this issue. First of all, it is important to realize that people are usually and often only scared of the unknown and things that are beyond their understanding. Not being an IT expert, and in the meantime using the computer daily for common work, is perfect opportunity for hackers for planting the seed of causing fear out of nothing.

What generally causes controversy concerning technology and its abuse is for a good reason a data leak. Initially, the data leak is irreversible. Once this situation occurs, it is impossible to undo the action and fix it. Therefore this is a situation where proactive stance to the problem is necessary. Leaking of private data has occurred several times and is the real threat for the trust of the users of the cyber-space.

[3] Greiner, Lynn and Paul, Lauren Gibbons. SLA Definitions and Solutions. *CIO.* [Online] August 8, 2007. Available at: <http://www.cio.com/article/print/128900>.

9. The matter of protection

Defence against cyber-terrorism is becoming one of the top priorities of NATO in recent past. However, the main focus is concentrated on the cyber strength of nation states, as the Assistant Secretary General for emerging security challenges at NATO claims[4].

First of all, counter cyber-terrorism must keep changing. As technologies improve continuously, so do the cyber-terroristic tools and methods. Therefore, in order to keep up with the advance, the protection must develop, proceed and change continuously.

Secondly, the need to share intelligence and cooperate between participants of the anti-cyber-terroristic group is invaluable. As the hackers develop more modern ways of intrusion every day, keeping your country up-to-date with the latest security matters is the best method not to get attacked. The benefits of cooperation are always mutual, as the field of abusing options is really wide and difficult to cover with adequate defence.

In order to recognize the true aims and methods of cyber-terrorists, it is very important to get to know them and to get access to their know-how. Therefore connections or even double-agents among cyber-terrorists become an invaluable source of information and should be consulted either way.

There are two important terms to describe the best aspect of security protection. Firstly, it is the **diversity**. For example as of December 2002, there were 54 064 separate water systems in the United States. It is understandable that the diversity in the technology used in this amount is enormous, and with free market in operation, there would very likely be many suppliers of the technological elements for these, including the software matters. The U. S. electrical grid consists of more than 3 000 electrical providers who naturally use a great variety of information technology[5]. For the potential cyber-attacker it would be extremely difficult, if not even impossible, to cover the entire diversity of hundreds and thousands of different technology and software of these complex infrastructure systems.

The other very important term is **failover**. When one becomes a chief of operations in the field of information technology, one must count on the possible failure. The technical equipment is never perfect and always suffers from several effects – like ageing and becoming obsolete and other outer influences. It is absolutely certain, that a technical device will eventually fail in the future. Therefore there must be back-up and strategy plans set and redundancy involved, so in the case of technical failure devices may be replaced. The same applies for the big picture, where there is probability of failure. For example, when electricity wiring is cut off, there may be a back-up plan to use a spare provider with his own wiring and infrastructure to cover the outage. When the airport air traffic control system is brought down for any reason, the back-up plan will state that the airport is temporarily closed for operation and that nearby airports will be used instead. In all these situations the human

---

4 Brewster, Tom. NATO: Cyber Terrorism Not Yet A Real Threat. *TechWeek Europe.* [Online] July 4, 2012. Available at: <http://www.techweekeurope.co.uk/news/nato-cyber-terrorism-84942>.

5 Lewis, James. Assesing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats. *Center for Strategic & International Studies.* [Online] December 2002. Available at: <http://csis.org/files/media/csis/pubs/021101_risks_of_cyberterror.pdf>.

factor is involved, and so is the human factor important, because the people are the ones making the decisions and being in control, not the technology.

10. Kosovo – first war on the internet

Along with the development of information technology, one of the commodities has gradually gained great value and power. Information drives today's businesses, decisions of billions of people and makes some people rich and some poor. But information is a commodity, which easily gets subjected to the influence of a distortion. Information has the power to change people's minds, along with their political opinions, to start a war while making it justified no matter the real reason, or turn two groups of people against each other without any previous mutual hatred.

During the war in Kosovo, the governments and non-governmental institutions started to use the internet to spread information and propaganda, to slander their political and war enemies and to solicit support for their own positions. Hackers, too, used a technique for disrupting services of governments to prevent them from spreading their information, known as distributed denial of service.

Based on previous experience, some would expect war opponents to try to shut down the internet as one of the first communication channels, so the opposing parties would not have such opportunities to organize. But it was official NATO policy to keep the internet open[6], so the influencing information could be appropriately spread among citizens. It is reported that hundreds of e-mails have been delivered to the mailboxes of United States institutions, potentially originating from the citizens of Serbia for NATO to stop the bombing. However, the credibility of these letters is threatened by the possibility of being faked by the government.

Los Angeles Times have published an article stating that: "The Kosovo conflict has begun to spread to the Internet, turning cyberspace into an ethereal war zone where the battle for hearts and minds is being waged through the use of electronic images, online discussion group postings and hacking attacks."[7]

11. Several examples for all

By the year 2003 the U. S. government computers suffered from data theft, including the ones belonging to NASA or U. S. Army technological supplier Lockheed Martin. This action, known as "Titan Rain", is thought to be one of the biggest attacks in cybernetic history and is thought to have been perpetrated by Chinese military.

The year 2007 is significant for NATO in the area of cyber-security. Massive attacks have occurred at the state organizations' websites of Estonia, resulting in their unavailability. This led NATO to establish its own cyber-security task force. The organization is known as the "Cooperative Cyber Defence Centre of Excellence" (CCD CoE) and is located in Estonian

---

6 Denning, Dorothy. Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy. *totse.com.* [Online] 2000. Available at: <http://www.totse2.com/totse/en/technology/cyberspace_the_new_frontier/cyberspc.html>.

7 Dunn, Ashley. Battle Spilling Over Onto the Internet. *Los Angeles Times.* April 3, 1999.

capital, Tallinn. As of today (August 2012), 11 countries are participating: Estonia, Germany, Hungary, Italy, Latvia, Lithuania, Netherlands, Poland, Slovakia, Spain, and United States.

In April 2010, 15% of the world internet traffic was being redirected through Chinese state-owned telecommunications company for a 20 minute period. Despite the sensitive content, likely to be encrypted, the redirection might have caused a leak of U. S. military data.

Between the years 2008 and 2012 the concept of Anonymous has gotten to public attention. Anonymous is a decentralized and anarchistic network aiming at controlling state institutions through hacktivistic actions.

12. The NATO cooperation

The war in Kosovo in 1999 and Estonian cyber-attacks in 2007 have shown NATO the true risk of cyberspace. Despite the relatively short history of the virtual world, as is widely known, the Alliance has managed to set several organizational units to protect the members against the threats coming from the digital world. The main impulse was the sudden realization of the lack of preparedness and formal background covering this issue following the two mentioned events. As of today, there are three NATO units in operation.

The first one is called NATO's Computer Incident Response Capability Technical Centre (NCIRC TC), set up after the Kosovo war. It is responsible for monitoring NATO-related websites and providing 24/7 support and technical response to cyber threats. This unit is expected to be strengthened in the future to cover more types of incidents.

The second one is the Cyber Defence Management Authority (CDMA), set up in 2008 to centralize, manage and coordinate cyber defence operational readiness across the Alliance. The future plans see this unit as a war-room operation centre to fight cyber-terrorism and cyber-threats in general.

The last one is the Cooperative Cyber Defence Centre of Excellence (CCD CoE), set up after the Estonian 2007 cyber-attacks. The responsibility covers development of long-term doctrines and strategy to be accepted by NATO members.

Although these organizational units may seem as a professional and adequate basis for the cyberspace protection within NATO, the truth is the entire section of counter cyber-crime is in its infancy and has to be further developed.

13. Conclusion

The danger, resulting from transformation of terrorism performed as aggressive and lethal actions in physical world to cyber-terrorism taking place in the virtual world causing political or economic consequences, must in no way be underestimated. On the other side, overestimation and media hysteria is not in place either. It is the countries' responsibility to negotiate and deliver appropriate security measures, whilst considering the right balance of limiting one's freedom and individualism and protecting against cyber-terrorism using the boundaries set by laws and agreements.

It is the responsibility of NATO Council members to agree upon adequate financial and military support of cyber-space defence and operations in order to maintain abilities and capacity of ensuring mutual security.

14. Timeline

2003	*U. S. government network suffered from data leak, known as the "Titan Rain".*
2007	*The cyber-attacks originating from Russia have taken down many state organizations' websites. Firstly, Estonian foreign minister Urmas Paet accused the Russian Federation, but later acknowledged no real evidence led to this proclaim. The responsibility for the attack has been acknowledged by Kremlin-backed youth group Nashi in 2009.*
June 27, 2007	The website of private corporation, Microsoft, in United Kingdom has been defaced and replaced by a Saudi Arabian flag.
September, 2007	Israeli army performed an airstrike on Syria under the head of Operation Orchard. Speculations say that the cyber-attacks might have been used for the Israeli airplanes fly undetected by Syrian radars[8].
2008	Popularization of the Anonymous concept after taking down the Church of Scientology websites during operation called "Project Chanology". As a possible revenge, the website of Epilepsy foundation has been defaced and replaced by a blinking screen causing potential epilepsy seizure to certain visitors, for which the Anonymous have been blamed, despite the unconfirmed origin of the attacker.
2008	The NATO CCD CoE in Tallin has been established in response to the Estonian cyber-attacks.
2008	Websites of Russian Federation, South Ossetia, Georgia and Azerbaijan suffered from attacks during the 2008 South Ossetia War.
2010	Computer virus Stuxnet is spread among 45 000 computers. This is the first occurrence of a virus targeting exclusively industrial systems. Bushehr nuclear power plant and Natanz nuclear enrichment site, both situated in Iran, have been affected[9].
April 2010	*15% of the world's internet traffic redirected through Chinese Telecommunications Company owned by state.*

[8] Markoff, John. A Silent Attack, but Not a Subtle One. *New York Times.* September 26, 2010.

[9] Beaumont, Peter. Stuxnet worm heralds new era of global cyberwar. *The Guardian.* September 30, 2010.

2010	Data leak from U. S. Army computer network started the WikiLeaks affair. Private Bradley Manning downloaded sensitive data and provided these to Julian Assange. Because of Manning's military ranking the access to such secreted information remains questionable at the very time. The leaked information included two videos proving the killing of two Reuters' journalists by the U. S. Army, documents concerning torturing of Iranians held captive, faking information about amount of killed civilians and American internal diplomatic messages. WikiLeaks is considered to be the national security threat by Pentagon and is currently (September 2012) attempting to shut it down and get Julian Assange to the court.
2011	China sets up so-called "cyber blue team" to defend the country against cyber-terrorism. The team consists of 30 men. The Defence Ministry of China emphasizes, that the unit does not consist of hackers and that the unit purpose must not be misunderstood.
July, 2011	The South Korean company SK Communications suffered from data leak of up to 35 million people's personal details.
October, 2011	U. S. Air Force announced the fleet and command centre for Creech AFB's drone and Predators, the technological aerial weapons actively operating in current US foreign military missions, has been keylogged (obtaining data about pressed keys on computer keyboard). Statement later issued, that the virus was not a threat to the operational state of the mission.
August, 2012	The so-called Shamoon virus is discovered in an oil infrastructure facility in Saudi Arabia. The intrusion has resulted in outage of the company network, but not affecting the facility operation[10].

15. Tips for further study

NATO list of useful links about cyberterrorism. Available at: <http://www.nato.int/structur/library/bibref/cyberterrorism.pdf>

[10] Shamoon virus targets energy sector infrastructure. *BBC News.* August 17, 2012.

16. Bibliography

1. Lewis, James. Assesing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats. *Center for Strategic & International Studies.* [Online] December 2002. Available at: <http://csis.org/files/media/csis/pubs/021101_risks_of_cyberterror.pdf>.

2. Greiner, Lynn and Paul, Lauren Gibbons. SLA Definitions and Solutions. *CIO.* [Online] August 8, 2007. Available at: <http://www.cio.com/article/print/128900>.

3. Brewster, Tom. NATO: Cyber Terrorism Not Yet A Real Threat. *TechWeek Europe.* [Online] July 4, 2012. Available at: <http://www.techweekeurope.co.uk/news/nato-cyber-terrorism-84942>.

4. Denning, Dorothy. Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy. *totse.com.* [Online] 2000. Available at: <http://www.totse2.com/totse/en/technology/cyberspace_the_new_frontier/cyberspc.html>.

5. Dunn, Ashley. Battle Spilling Over Onto the Internet. *Los Angeles Times.* April 3, 1999.

6. Markoff, John. A Silent Attack, but Not a Subtle One. *New York Times.* September 26, 2010.

7. Beaumont, Peter. Stuxnet worm heralds new era of global cyberwar. *The Guardian.* September 30, 2010.

8. Shamoon virus targets energy sector infrastructure. *BBC News.* August 17, 2012.

9. Havlíček, Jiří. NATO in 21st century. *Pražský studentský summit.* [Online] 2011. Available at: <http://www.studentsummit.cz/data/1321994983703NATO_N21ST.pdf>.

10. *CCD CoE.* [Online] Available at: <http://www.ccdcoe.org/>.

11. Cyberterrorism. *NATO.* [Online] Available at: <http://www.nato.int/structur/library/bibref/cyberterrorism.pdf>.

12. Hackmageddon. *Hackmageddon.* [Online] Available at: <http://hackmageddon.com/>.

13. NATO's role in relation to the conflict in Kosovo. *NATO.* [Online] July 15, 1999. Available at: <http://www.nato.int/kosovo/history.htm>.

14. Specialised cybercrime units. *Council of Europe.* [Online] November 9, 2011. Available at: <http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/Octopus2011/2467_HTCU_study_V30_9Nov11.pdf>.

15. Cavelty, Myriam Dunn. Cyber-Allies - Strengths and weaknesses of NATO's cyberdefense posture. *academia.edu.* [Online] March 2011. Available at: <http://ethz.academia.edu/MyriamCavelty/Papers/563353/Cyber-Allies_Strengths_and_weaknesses_of_NATOs_cyberdefense_posture>.

16. Collin, Barry. The Future of CyberTerrorism: Where the Physical and Virtual Worlds Converge. *11th ANNUAL INTERNATIONAL SYMPOSIUM ON CRIMINAL JUSTICE ISSUES.* [Online] Available at: <http://afgen.com/terrorism1.html>.

17. Green, Joshua. The Myth of Cyberterrorism. *Washington Monthly.* November 2002.

17. Attachment – overview of cyber-crime units within NATO members

Country	Cyber-crime unit	Participates in CCD CoE
Albania	Sector against cybercrime under Ministry of Interior of Albania	No
Belgium	Federal Computer Crime Unit (FCCU) under Federal Judicial Police	No
Bulgaria	Bulgarian Cybercrime Unit	No
Canada	Integrated Technological Crime Unit under Royal Canadian Mounted Police	No
Croatia	Responsibilities distributed among several officers under Organized Crime Department	No
Czech Republic	Information Technology Crime Section	No
Denmark	Cyber warfare unit under the Danish military intelligence service	No
Estonia	Cyber Crime Unit under The Estonian Police; Cyber Crime Unit under Border Guard	Yes
France	Cybercrime Division under Gendarmerie Nationale; OCLCTIC under Police Nationale	No
Germany	Computer Network Operations under Ministry of Defence	Yes
Greece	Cyber Crime Unit under the Police	No
Hungary	High Tech Crime Unit under the Police	Yes
Iceland	Not confirmed	No
Italy	Centro nazionale anticrimine informatico per la protezione delle infrastrutture critiche under Polizia di Stato	Yes
Latvia	Combating Cybercrime and IPR Protection Unit	Yes
Lithuania	Cyber Crime Unit under the Lithuanian Police	Yes
Luxembourg	Section Nouvelles Technologies under Police Judiciare	No
Netherlands	National Hi-Tech Crime Unit under the Dutch National Police Agency	Yes
Norway	High Tech Crime Division under the National Investigation Service	No
Poland	Independence Information Force within the army	Yes
Portugal	National Cybersecurity Center under National Security Office	No

Romania	Cybercrime Unit under General Inspectorate of Romanian Police; Specialised Prosecution Unit under DIICOT	No
Slovakia	Cyber Crime Unit under Slovak Police Force	Yes
Slovenia	Cyber Investigation Unit under the Criminal Police Directorate	No
Spain	Brigada de Investigación Tecnológica	Yes
Turkey	Cyber Army Command	No
United Kingdom	The UK Defence Cyber Operations Group under Ministry of Defence	No
United States	United States Cyber Command under the U. S. Strategic Command	Yes

Author: Jiří Havlíček
Imprimatur: Šimon Presser, Zuzana Netolická
Language correction: Veronika Smělá, Šimon Presser
Graphics: Zuzana Netolická, Thu Thuy Truong
Consultancy: AMO Research center
Released by Association for International Affairs for the XVIII. year of Prague Student Summmit

Model NATO

Association for International Affairs,
Žitná 27, 110 00 Praha 1
Tel./fax: +420 224 813 460,
e-mail: summit@amo.cz,
IČ: 65 99 95 33

»www.amo.cz«
»www.studentsummit.cz«

Top partneři

Generální partner Modelu OSN

The Kellner Family Foundation

Hlavní partner Modelu OSN

G2 OD KOMERČNÍ BANKY

Hlavní partner Modelu NATO

Ministerstvo zahraničních věcí České republiky

Model NATO is co-sponsored by the North Atlantic Treaty Organization

NATO OTAN

Hlavní partner Modelu EU

Evropská komise

Partner konference

Microsoft

Univerzitní partner

Vysoká škola ekonomická v Praze VŠE

Partner zahájení

interhotel AMBASSADOR ZLATÁ HUSA

Partner jednání

KONGRESOVÉ CENTRUM PRAHA

Partneři Modelů

čeps, a.s.

Embassy of Canada
Ambassade du Canada

US embassy

SKUPINA ČEZ

Botschaft der Bundesrepublik Deutschland Prag

Mediální partneři

Hlavní mediální partner

lidovky.cz

RESPEKT

Hlavní mediální partner

LIDOVÉ NOVINY

ISIC INTERNATIONAL STUDENT IDENTITY CARD

Partner Chronicle

METROPOLITNÍ UNIVERZITA PRAHA

ČESKÝ ROZHLAS

Za podpory

Česká televize

Asociace pro mezinárodní otázky
Association for International Affairs

Pražský studentský summit
projekt Asociace pro mezinárodní otázky