BACKGROUND REPORT

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

NATO in 21st century

1. NATO and nuclear weapons

Proliferation of weapons in its basic sense means the increase of arms around the world. While talking about the global security, the proliferation of the weapons of mass destruction is the most dangerous potential threat. This category groups biological and chemical weapons as well as the nuclear ones. The following text will focus only on nuclear threats.

The development of nuclear weapons started in the early 1940s with the "Manhattan" project which ended by the first usage in Japan in August 1945. Soon thereafter, the Soviet Union started to build its own equipment (completed by 1949) and that started the arm race during the Cold War. In 1952 the United Kingdom joined the club of nuclear weapons holders, followed by France (1960) and China (1964). These are the official holders according to the most important treaty in nuclear history – Treaty on the Non-Proliferation of Nuclear Weapons (NPT), which came into force in 1970.

Signers of this treaty made an agreement that states which are already possessing nuclear weapons (NWS) will not proliferate them and the non-NWS states will not accept nor build them. Nevertheless, next to the official possessors we have the unofficial ones, which also have the weapons. These include India and Pakistan (which have developed their arsenals primarily due to mutual enmity) and also Israel. These states have never signed the NPT; on the other hand, North Korea withdrew its signature in 2003. Another question is very suspicious programme of Iran, which signed the NPT as well.

NPT is one of the series of multilateral deals signed through the second half of the 20th century on the topic of disarmament (we can name The Comprehensive Nuclear-Test-Ban Treaty, which bans every signed state from nuclear tests). Another try how to control proliferation were the bilateral deals between the USA and the USSR. Last agreement between the US and the successor of the USSR (the Russian Federation) has been concluded in Prague in April 2010 by a treaty named „New Start". Countries agreed on lowering the amount of holders of nuclear weapons.

For NATO, the subject of proliferation is important due to the fact that the member states which are official holders and possibly threaten by the non-official ones. NATO – NPG (Nuclear Planning Group) is one of the key decision making bodies. It takes decisions on the Alliance's nuclear policy, which is kept under constant review and modified or adapted in the light of new developments. Members participating in NATO's integrated military structure (all member countries except France) are part of the NPG. It meets once a week and at other times as necessary.

But although almost all the countries agreed not to spread the nuclear weapons and signed the NPT, there is still fear that some groups (or even states) may somehow get the nuclear weapon and use it against the rest of the world. These are being reffered as "rogue states" (Iran, North Korea, Syria...) or "rogue groups" (Al-Quaeda, Taliban etc.).

Rogue groups are probably not capable of creating their own weapon, so they would have to get it from someone else. On the other hand rogue states may be capable of creating such a weapon – the reason why Iranian nuclear programme is so feared in the western world.

Sources:
http://www.studentsummit.cz/data/1289435161209BGR_GA_proliferace.pdf

2. NATO and cyber terrorism

The internet has gone a long way since its first variant in 1962 and so has the influence of this technology on people's life. With proceeding implementation of networked devices, we are getting more and more vulnerable to their abuses. The term being used for such acting is "cyber terrorism", usually denoting abusing the internet and technology for criminal or terrorist purposes and activities.

USA has formed several groups for tackling this issue, led by the United States Strategic Command. One of them is "MAJCOM" belonging to US Air Force. Also the Chinese Defense Ministry confirmed the existence of an online defense unit in May 2011, consisting of about 30 security experts called "Blue Team". In May 2011, Israel announced the establishment of the National Internet Defense Taskforce.

NATO has established its own cyber unit called "Cooperative Cyber Defence Centre of Excellence" in 2007 after the cyber-attacks on Estonia in 2007. This agency is located in Tallin, Estonia, is one of 15 accredited "Centres of Excellence". The main focus of the CCD CEO is to improve the cyber defense interoperability of the NATO, to analyze legal side of the issue and to provide proper training to the members. Currently only 9 countries are actively involved, including Estonia, Germany, Italy, Latvia, Lithuania, Slovakia, Spain, Hungary and United States. Turkey has announced the intentions to join the Centre in the near future. Iceland is also discussed as a potential member.

Just as governments, big international corporations are involved in mastering this issue, both for defending themselves and using it as a weapon. Microsoft, Sony, Panasonic, Apple and dozens of other companies from the field of information technology participate in this fight equal in their power with the sovereign states.

It is very important to know what the options of today's hackers[1] are, mainly to separate the reality from books and movies, and therefore avoid discussing nonsense. There are four basic things a hacker can do: steal data, cause damage, deny someone from doing something or fake information.

The most well known type of abuse of the internet is called spam and most people are acquainted with it. It is not considered to be a hacking attack, but it is a very significant internet threat. Its purpose is to send to users not demanded emails

[1] Sometimes the term *"cracker"* is more appropriate

containing advertisements, links with viruses or simply get the user confused and cheat him. Spam is mostly being spread using giant virtual computer and server networks that are infected and altogether called the botnet. Botnets are not only used for this purpose and the biggest ones have more than 200,000 active members per 24 hour period[i]. Defeating such botnet is very difficult as it can use as many possible IP addresses[2] as it has members and is decentralized. The only protection is available on the end user side – not to get infected by malicious software. The estimated volume of spam is between 80 and 90% of all sent emails.[ii]

One of the most popular attacks these days is called SQL injection. Since business intelligence and corporate or government data are mostly stored in databases, which for compatibility reasons all use single scripting language (SQL), it is very universal to choose this type of attack. Also it is not difficult to learn how to perform it[iii] , but neither it is hard to protect yourself against it.[iv] The main point about SQL injection is in using clever manipulation of punctuation in forms. The purpose can be to get into private zones of websites and gain elevated rights (e. g. to change a websites content) to do some minor damage, gain private data or completely destroy them. Today most programmers are aware with this type of attack and most websites are appropriately protected.

Another type of attack is called "sniffing". The main thought is to catch packets on their way through the computer network and read included data. When a packet[3] is sent, it makes its way through many servers and computers before it reaches its destination. All these places are possibly able to read it, although there are reasons or methods of avoiding this. Because usually these servers are not under hacker's control, he is supposed to redirect the traffic through his own server, so he is able to perform the attack. The network traffic is based on so-called routing information, which is used for directing IP packets to their right directions, and can be quite easily faked. The protection against this type of attack is encryption of both transmitted data and routing information. The most famous encryption method is called SSL and is usually implemented in most known web services.

Last but not least, today's most famous attack is called [Distributed] Denial-of-service ([D]DoS). It does what the name says. It tries to make users unable to get to a specific service. This type of attack is lately widely used and has appeared many times in the media. The main reason is that it is not very difficult to perform it when you have a strong supporter, which can be a government or a big network of world wide spread users. Also there is just a little chance to set protection against. There are five basic types of this attack. Most known is making so many requests to a server that this cannot process all of them and crashes, or in the better variant, all its capacity is aimed at fulfilling these requests and nobody else can make one. Another one is disruption of routing information. Last one we will name is creating an obstruction between a user and the server in some other way that they can no longer communicate.

---

2 IP address is used for addressing computers in networks

3 Communications on a network between computers is partitioned into smaller packages of data, called *packets*

i http://www.darkreading.com/security/security-management/208808174/index.html

There are also other mostly undocumented types of attacks which rely on using security holes in a system, thus creating backdoors to computers or computer networks, providing the attacker partial or complete access to there.

Now let's review several practical examples and affairs on this topic:

In 2003 the U.S. government computers were attacked and data were stolen from computer networks, including those of NASA or Lockheed Martin[4]. This action is called "Titan Rain" and is considered to be the biggest cyber-attack in history. The attacks are thought to have been perpetrated by the Chinese military.[v]

The Estonian cyber-attacks in 2007 were performed using DoS, causing many state organizations' websites unavailable. It is considered to be the second biggest attack after the Titan Rain. Estonian foreign minister Urmas Paet accused the Russian Federation of taking part in this action, but on September 6, 2007 Estonia's defense minister admitted he had no evidence of linking this attack to Kremlin. As of January 2008, an ethnic-Russian Estonian national has been charged and convicted. Later, a member of the Russian State Duma announced that the attack has happened on his impulse. On March 10, 2009 a representative of Kremlin-backed youth group Nashi[5] has claimed responsibility for the attack.[vi]

On June 29, 2007 Microsoft U.K. website was defaced [6] and replaced by Saudi Arabian flag[vii], and on May 2008 many Chinese websites were attacked using SQL injection.[viii]

In April 2010, 15% of the world internet traffic has been directed through Chinese state-owned telecommunications company [7] for a 20-minute period. The traffic was supposed to include packets from US government and military networks. Although the data were encrypted, possibility of their sniffing exists.[ix]

The latest cyber-actions occurred during years 2008-2011 with the popularization of the hacker group called "Anonymous", which was established during 2003 and 2004. "Anonymous" is a civil initiative with an intention to protect civil rights that are

---

4 Supplier of US Army

5 Russian political youth movement declaring to be anti-fascist movement

6 Changing the websites look and content in order to draw attention or send a message

7 *"China Telecom"*; est. 2002; over 300,000 employees; providing approx. 46 Gbps of connection

ii http://securitylabs.websense.com/content/spamPercentage.aspx

iii http://www.soom.cz/index.php?name=articles/show&aid=167

iv http://php.vrana.cz/obrana-proti-sql-injection.php

v http://www.breitbart.com/article.php?id=051212224756.jwmkvntb&show_article=1

vi http://arstechnica.com/security/news/2007/05/massive-ddos-attacks-target-estonia-russia-accused.ars

vii http://rcpmag.com/articles/2007/06/29/hacker-defaces-microsoft-uk-web-page.aspx

viii http://www.pcworld.com/businesscenter/article/146048/mass_sql_unjection_attack_targets_chinese_web_sites.html

ix http://betanews.com/2010/11/17/redirection-of-internet-traffic-by-chinese-state-isp-worries-experts/

related to freedom, and consists of volunteers all around the world grouped into different branches. There is no leading party or a person.

Starting with 2008, the Anonymous have gotten to the media attention after attacking websites of the Church of Scientology using DDoS during action called "Project Chanology."[x] Prank calls and fake black faxes were also involved. This was a reaction to the Church's complaints about copyright breaking after leaking of their videos to YouTube. [8] Three waves of protests against the Church followed, each having around 8000 participants. In late June 2008, the "Epilepsy Foundation" forums were defaced and replaced by a flashing screen possibly causing an epilepsy seizure to specific visitors.[xi] Anonymous was accused for this attack, but possibility of setting the attack on them by the Church has appeared. The same year Anonymous successfully defaced the "Support Online Hip Hop" websites and flooded their forums.[xii]

In 2009, the Anonymous defaced the websites of "No Cussing Club" and leaked owner's personal information. Together with "The Pirate Bay" it launched the "Iranian Green Party Support" with title "Anonymous Iran" and started the "Operation Titstorm" by bringing down websites of Australian Government after enactment of censorship of pornography containing small breasted women, which were generally considered to be under age.[xiii]

In 2010, several Bollywood companies hired the "Aiplex software"[9] company to perform DDoS attack on sites not responding to copyright breaking notices. As a revenge, the Anonymous also performed the DDoS attack, first on the Aiplex software sites, afterwards on initiating Bollywood companies.[xiv]

The same year, the "WikiLeaks affair" came to light and popularized the Anonymous group. WikiLeaks published on its websites many top secret documents leaked from US state organizations. After requests of proper US state offices, Amazon, Visa, PayPal and Mastercard have refused to provide services to WikiLeaks.[xv] As a revenge, DDoS attack has been performed on all of these[xvi], making their services unavailable for several hours. The Anonymous confessed to be the performer. Websites of the Swedish prosecutor were also brought down after imprisonment of Julian Assange, the WikiLeaks founder.

---

8 Video sharing web portal owned by *Google*

9 Company specializing on bringing down websites disturbing copyrights using illegal methods, usually hired by Hollywood or Bollywood

x http://ohinternet.com/Project_Chanology

xi http://www.wired.com/politics/security/news/2008/03/epilepsy

xii http://www.mtv.com/news/articles/1590117/hiphop-sites-hacked-by-apparent-hate-group.jhtml

xiii http://www.wired.com/threatlevel/2010/02/anonymous-unfurls-operation-titstorm/

xiv http://www.geek.com/articles/news/4chan-forces-aiplex-and-mpaa-websites-offline-with-ddos-attack-20100918/

xv http://blogs.villagevoice.com/runninscared/2010/12/wikileaks_betrayed_by_media.php

xvi http://boingboing.net/2010/12/08/in-pro-wikileaks-act.html

On April 2, 2011, the Anonymous launched massive attack on the Sony Corporation. Firstly, personal data of users of the "Playstation Network" were stolen, followed by bringing down the entire gaming network and other related Playstation websites. This operation was a reaction to legal actions against George Hotz and Alexander Egorenkov for breaking the Sony console security system and providing 3rd party applications for Playstation 3.[xvii]

In June 2011, the Anonymous announced on Twitter that they have successfully leaked about 1 gigabyte of secreted NATO documents.[xviii] As a proof, 10 pages long document has been published, entitled "Outsourcing of Balkan CIS Support". According to the Anonymous the data are very sensitive and their publishing would be very irresponsible.

3. NATO enlargement

How it began

North Atlantic Treaty Organization (NATO) was founded on 4 April 1949 by the signing of the North Atlantic Treaty in Washington D.C. The founding countries were Belgium, Canada, Denmark, France, Iceland, Italy, Luxembourg, the Netherlands, Norway, Portugal, the United Kingdom and the United States of America. In the beginning, NATO was mostly a political coalition, but during the Korean War (June 1950 – July 1953) politicians realized that further military cooperation is necessary to be able to defend against the threats from the USSR.

The main reason for founding such a coalition was to counter the rising influence of the Soviet Union and prevent it from further expansion to western Europe. That is why it was very important that Turkey and Greece joined NATO in 1952 to secure the southern border thereby not allowing the USSR to expand. Moreover, these countries were and continue to be the easternmost and the southernmost member states of NATO.

Western Germany became a member of NATO in 1955 after long discussions. This was a hard decision as many experts were opposing the idea of arming the German forces few years after the Second World War. But finally, politicians decided that the threat of Soviet expansion is much worse than that of having Western Germany join the Alliance.

Exception, S'il vous plaît

In the 1960's a problem emerged. France demanded a priviliged position within NATO alongside the United States and the United Kingdom. However this ambition war rejected by the alliance and therefore, in 1966, the president Charles de Gaulle

[xvii] http://www.theinquirer.net/inquirer/news/2041179/anonymous-takes-playstation-website-playstation-network

[xviii] http://news.cnet.com/8301-13506_3-20081890-17/anonymous-still-accessing-downloading-nato-data/

decided to leave the military structures of NATO and to focus instead on France's own military strength, leadership and development. But despite of this, France did participate in military operations of NATO e.g. in the Balkan peninsula, Afghanistan etc. Formally, France rejoined NATO in 2009.

In 1974 Greece followed the French and withdrew its military forces from NATO, but their motivation was completely different. It was a consequence of the Turkish invasion to Cyprus, but this withdrawal was much shorter than that of France, it lasted only 6 years until 1980.

Cold War period

During the Cold War, and since the Western Germany has entered NATO, only one country joined the Alliance – Spain in 1982, several years after it gained freedom and democracy following the death of general Franco. The fact that Spain was the only country that joined was that in these days NATO was directly bordering with the USSR and to the east, there were not countries able to join (or willing to join, such as Finland or Sweden).

After the fall of communism

After the breakdown of the USSR many countries began to strive to join the Alliance to ensure that Russia will not try to gain back its former power and territories, that is why the Czech republic, Hungary and Poland entered NATO in 1999 and Bulgaria, Estonia, Latvia, Lithuania, Romania, Slovenia and Slovakia in 2004. In the last round of 2009, it has been Albania and Croatia who joined the Alliance.

Bosnia and Herzegovina and Montenegro have also expressed their interest to become members of NATO and have started the Intensified Dialogue Programme, the first step to join the Alliance.

Troubles with name

For the admittance of a new member a unanimous consensus of all current states is required. That is why another state willing to join the alliance – Macedonia – was not allowed to join the Alliance because of Greece. There is a long dispute about the name "Macedonia", because the Greeks claim that it is a historical name of a territory in northern Greece. Therefore, Macedonia is still not a member of NATO, although they have tried to join the Alliance as early as Slovakia in 2004. The Greeks seem to be adamant even after all attempts to persuade them from the rest of NATO. Therefore, probably the only way of solving this problem is to rename Macedonia.

Who will not be next

The future of NATO's enlargement is not clear. Because the eastern borders of NATO have reached the area of influence of Russia and the Russian Federation is of course not willing to allow NATO to enlarge and thereby weaken its influence. Countries bordering with current eastern countries are mostly in Russian sphere of influence

and that is most likely the reason, why for example Ukraine stopped the Intensified Dialogue Programme and quitted the attempts to become a member of NATO. Also Kazachstan, Belarus, Armenia and several other countries have stated they are not willing to join the Alliance (and aggravate the Russians).

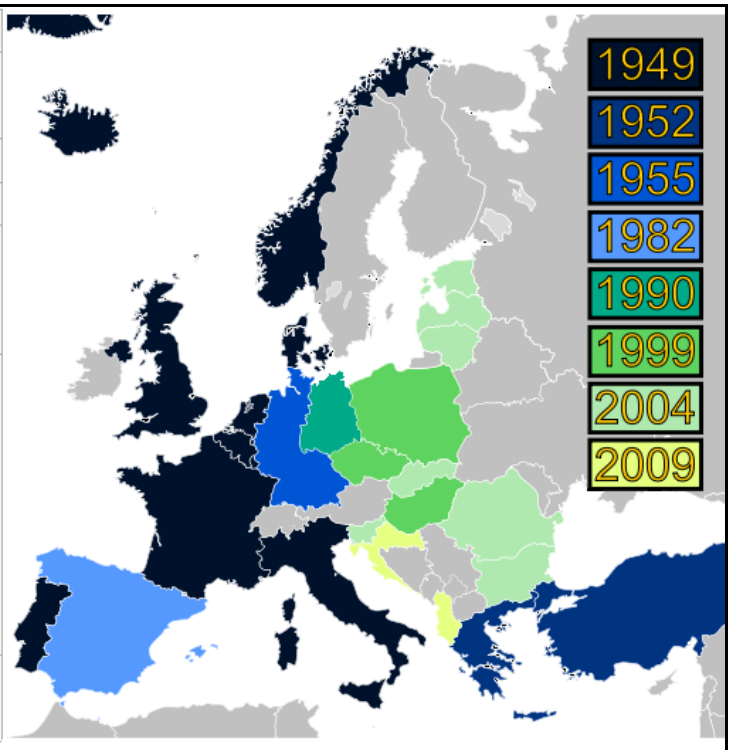
In case of Serbia the reason is slightly different. They are also not willing to join because of the NATO intervention in 1999, the majority of population is not in favor of NATO and even their signing of the Partnership For Peace Programme is considered a big success.

Furthermore, when it comes to the European countries situated inside NATO's borders such as Austria and Switzerland, the main problem is their policy of neutrality and non-alignment. That is why in case of these neutral countries, namely Finland, Sweden, Ireland, Austria and Switzerland, the chances that they will seek to join the Alliance are slim.

The biggest question of future enlargement

The biggest question mark lies in Georgia, a country that wishes to strengthen bonds with the western world and weaken the Russian influence over its territory. In a referendum in 2008, majority of 77% of the population voted in favor of joining NATO. But the problem lies in huge numbers of Russian population in some regions of Georgia as well as numbers of Russian forces on the territory. Of course, the Russians are not in favor of withdrawing the forces and letting Georgia join NATO.

Date	Country	Enlargement
February 18, 1952	Greece	First
	Turkey	
May 9, 1955	Germany	Second
May 30, 1982	Spain	Third
March 12, 1999	Czech Republic	Fourth
	Hungary	
	Poland	
March 29, 2004	Bulgaria	Fifth
	Estonia	
	Latvia	
	Lithuania	
	Romania	
	Slovakia	
	Slovenia	
April 1, 2009	Albania	Sixth
	Croatia	



http://en.wikipedia.org/wiki/Enlargement_of_NATO

http://www.nato.int
http://www.globalresearch.ca
http://en.wikipedia.org
http://www.natoaktual.cz
http://www.acus.org

Zpracování a redakční úprava: Kateřina Pleskotová, Šimon Presser, Jiří Havlíček

Grafická úprava a tech. spolupráce: Zuzana Procházková

Vydala Asociace pro mezinárodní otázky pro potřeby XVII. ročníku Pražského studentského summitu.

Model NATO

Asociace pro mezinárodní otázky,
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

Zastoupení Evropské komise v České republice

PARTNER ZAHÁJENÍ

interhotel AMBASSADOR ZLATÁ HUSA

PARTNER JEDNÁNÍ

KONGRESOVÉ CENTRUM PRAHA

UNIVERZITNÍ PARTNER

VYSOKÁ ŠKOLA EKONOMICKÁ V PRAZE VŠE

DODAVATELÉ SLUŽEB

VYŠEHRAD 2000 group

KONFES KONGRESOVÁ TECHNIKA www.konfes.cz

KONICA MINOLTA

zátiší group

kofola original

inspiro solutions

Hasičská vzájemná pojišťovna, a.s.

newton media

KOPR software

PEKAŘSTVÍ

SUBWAY

CoProSys COMPUTER · PROGRAM · SYSTEM

MEDIÁLNÍ PARTNEŘI

RESPEKT

HOSPODÁŘSKÉ NOVINY

ÚSTAV MEZINÁRODNÍCH VZTAHŮ PRAHA iir

natoaktual.cz

EurActiv.cz Vaše internetová brána do Evropy

PARTNER CHRONICLE

METROPOLITNÍ UNIVERZITA PRAHA

Asociace pro mezinárodní otázky
Association for International Affairs

Pražský studentský summit
projekt Asociace pro mezinárodní otázky