A terrorizmus Rubik-kockája, avagy a fenyegetések komplex megközelítése

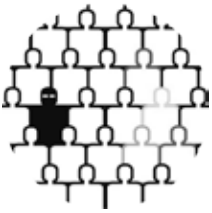
Rubik's cube of terrorism or complex approach to the threats

Nemzetközi tudományos-szakmai konferencia

International scientific and professional conference

DUNA PALOTA

2013. szeptember 30. – október 1.



A terrorizmus Rubik-kockája, avagy a fenyegetések komplex megközelítése

Rubik's cube of terrorism or complex approach to the threats

Nemzetközi tudományos-szakmai konferencia

International scientific and professional conference

DUNA PALOTA

2013. szeptember 30. – október 1.

Szerzőink

Dr. Bencsáth Boldizsár, dr. Buttyán Levente, Kamarás Roland, Ács-Kurucz Gábor, Molnár Gábor – Budapesti Műszaki és Gazdaságtudományi Egyetem Híradástechnikai Tanszék CrySys Adat- és Rendszerbiztonság Laboratórium

Dr. Bognár Balázs tű. alezredes, BM OKF Országos Iparbiztonsági Főfelügyelőség, kritikus infrastruktúra koordinációs főosztályvezető

Dr. Erdődi László, Óbudai Egyetem Neumann János Informatikai Kar Szoftvertechnológiai Intézet, adjunktus, etikus hacker oktató

Gencsy Péter, Magyar Telekom Csoport, biztonsági igazgató

Dr. Hankiss Ágnes, Európai Parlament, képviselő, EP Biztonsági és Védelempolitikai Albizottság, Néppárti Kiberbiztonsági Tanácsadó Testület, tag

Elizabeth Howe, Nemzetközi Ügyészi Egyesület, alelnök, szakmai főtanácsadó (Egyesült Királyság)

Dr. Károlyi László ny. ezredes, Magyar Posta Zrt., biztonsági főigazgató

Prof. Dr. Kovács László mk. ezredes, Nemzeti Közszolgálati Egyetem Hadtudományi és Honvéd-tisztképző Kar, egyetemi tanár

Dr. Révész Balázs, Nemzeti Adatvédelmi és Információszabadság Hatóság, Vizsgálati Főosztály, főosztályvezető

Zala Mihály vezérőrnagy, Nemzeti Biztonsági Felügyelet, elnök

Tartalomjegyzék

Előszó

Az állam abszolút kötelessége, hogy oltalmazza állampolgárait és ennek érdekében elkövessen mindent, ami a jogállamiság határát nem lépi át. Az értékek közösek és állandóak, azonban az egyes kérdések különböző megvilágításban, igen eltérő válaszokat kínálhatnak számunkra.

A felmerülő kérdéseket a szakma és a tudomány egyaránt másként értelmezi. Sajátos szemléletük ütköztetése éppen ezért válhat a szó valódi értelmében értékteremtővé. Szun-Ce A hadviselés törvényeiben úgy szól: *„…soha ne bízzuk magunkat arra, hogy (az ellenség) nem támad meg bennünket, hanem kövessünk el mindent, hogy ne is legyen módja megtámadni bennünket."* Olyan korban élünk, ahol a független csoportosulások a korábban felállított kategóriák egyikébe sem illeszthetők be. A hackerek tevékenysége nehezen minősíthető, de még nehezebb kivédeni támadásaikat. Oktatási, egészségügyi, illetve banki adataink, vagyis a mindennapjainkban meghatározó információink tárolását, de ugyancsak az államszervezet és a legmodernebb haditechnikai eszközök irányítását egytől-egyig informatikai rendszereken keresztül végzik.

A jövő biztonsági kihívásai nem az „utcákon" dőlnek majd el, hanem monitorok előtt és a technológiai fejlettség mellett sokkal lényegesebb lesz egy szakember állomány kiképzése és fenntartása (megtartása) a siker érdekében. A kiberhadseregek jelentik a jövőt és amennyiben meg szeretnénk felelni Szun-Ce intelmének, nem szabad a baj elmaradásában könnyelműen bíznunk.

A konferencia célja tehát nem is lehet más, mint a jövő megalapozásának előkészítése.

Elizabeth Howe

The changing role of the prosecutor in Counter Terrorism since September 11

The International Association of Prosecutors (IAP) is a world wide syndicate of prosecution services and associations as well as individual members which has been in existence since 1995. It has a number of purposes, including the improvement of cooperation and support for the development of skills, learning and good practice for prosecutors so that they can more efficiently and effectively curb criminal activity in every sphere. One of the imperatives for prosecutors which is enshrined in the IAP Standards for Prosecutors[1] is that they should discharge their duties fairly and in accordance with the rule of Law and should „respect, protect and uphold the universal concept of human dignity and human rights" (Standard 1 h).

The tragic and horrific terrorist attacks in USA on September 11th 2001 shook the world and prompted an immediate and strong world wide response.

1 ' The Standards of Professional Responsibility and Statement of the Essential Duties and Rights of Prosecutors' were adopted by the IAP in 1999 and endorsed by the 17th United Nations Commission on Crime Prevention and Criminal Justice in 2008: „Commission on Crime Prevention and Criminal Justice resolution 17/2, entitled 'Strengthening the rule of law through improved integrity and capacity of prosecution services', which contains the Standards of Professional Responsibility and Statement of the Essential Duties and Rights of Prosecutors, developed by the International Association of Prosecutors, as an annex." http://www.unodc.org/documents/commissions/CCPCJ/CCPCJ-ECOSOC/CCPCJ-ECOSOC-00/CCPCJ-ECOSOC-08/Resolution_17-2.pdf

However in 2003 the UN Secretary General, Kofi Annan found it necessary to say as follows:

"Our response to terrorism as well as our efforts to thwart it and prevent it, should uphold the human rights that terrorists aim to destroy. Respect for human rights, fundamental freedoms and the rule of law are essential tools in the effort to combat terrorism-not privileges to be sacrificed at a time of tension"

Also in 2003, UN Resolution 1456 was passed; „states must ensure that any measure taken to combat terrorism comply with all their obligations under international law and should adopt such measures in accordance with international law, in particular international human rights, refugee and humanitarian law"

Why the UN Secretary General was moved to make this statement and why was it necessary to pass resolution 1456?

The security imperative – some may say hysteria – which followed 9/11 led to the commission of significant rule of law abuses. Prosecutors are at the forefront in ensuring that terrorist crimes – notwithstanding the sense of horror and outrage that they evince – are dealt with in accordance with the rule of law and with due regard to human rights – to do otherwise is unconscionable and on a practical level – counterproductive. Lord MacDonald, former Director of Public Prosecutions of England and Wales was quoted as saying in regard to the 9/11 and 7/7/05 (London bombings) attacks, that the country of Britain had sacrificed „*traditional ideals of freedom in the push against terrorism*"

What is Terrorism?

There is no universal definition. The Oxford English Dictionary defines it as „the unofficial or unauthorised use of violence and intimidation in the pursuit of political aims".

With increasing globalisation, the nature of terrorism has over time changed from a domestic to a transnational threat.

Terrorism did not start in 2001, it was prevalent prior that date-eg

Northern Ireland where the fight by the Irish Republican Army(IRA) for cessation from the United Kingdom in order to become part of the Republic of Ireland owes its origins to previous centuries. The jurisdiction of the relatively new International Criminal Court (ICC) in the Hague does not include terrorism, but following the First World War, an attempt to establish an international tribunal to deal with terrorism and which offered a definition of terrorism was abandoned due to the onset of the Second World War. Significantly, here we are in Budapest where an early act of terrorism sparked the First World War-the murder of Prince Franz Ferdinand, the heir to the Austro-Hungarian Empire by Serb/Croat nationals.

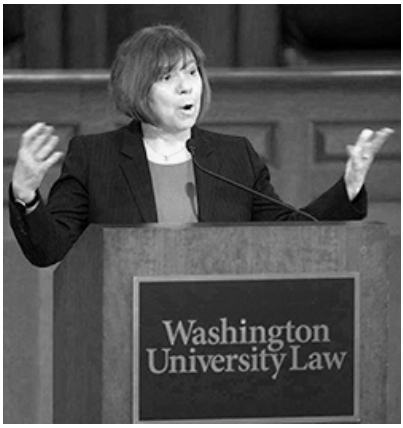
The Global Response to 9/11

The atrocities of 9/11 took terrorism to another level. Only 17 days later there was an immediate, unified and unprecedented response with the passing of UN Security Council Resolution 1373(28/9/2001) – all states to afford one another „the greatest measure of assistance" in connection with criminal investigations or criminal proceedings relating to the financing or support of terrorist acts, including assistance in obtaining evidence in their possession necessary for the proceedings. As a result many regions introduced new or enhanced international cooperation provisions into their legal regimes. Resolution 1373 focused on prosecutions targeting individuals and entities supporting and financing terrorism and also included requirements to bring terrorists to justice. Such requirements and expectations fall to the criminal justice systems of states to administer and enforce and to prosecutors to prosecute-taking account of the interconnection between terrorism and all forms of acquisitive crime.

Other UN responses included the establishment by 1373 of the Counter-Terrorism Committee (CTC) which is at the centre of global efforts to fight terrorism and facilitates technical assistance to states to implement counter terrorism provisions and acts as an interstate coordinator.

In 2005 the Counter-Terrorism Committee Executive Directorate (CTED) was set up, which identifies priority areas and sources funding and requires country reports setting out the extent of their counter-terrorism provision. In 2006, the UN General Assembly adopted the UN Global Counter Terrorism Strategy (UNGCTS).

In October 1998, Resolution 1267 established the sanctions regime. Initially this regime was directed to the Taliban and to Al-Quaida and involved travel restrictions, weapon prohibition and asset freezing. It did not become a particular area of focused interest until 9/11 when 200 were added to the list in the first few months thereafter. There was little redress or the possibility of recourse to challenge listing decisions and there was no independent review of the list and those placed upon it.



In December 2009, the Office of Ombudsman for delisting was established and in 2010 Kim Prost was appointed as Ombudsman (see picture right) to assist the Sanctions Committee of the UN Security Council with delisting petitions (by now only in regard to Al-Quaida). Kim was an 'ad litem' judge of the 'International Criminal Tribunal for the former Yugoslavia' from July 2006 to June 2010 but previously, besides holding a number of other significant positions, she had worked for the Canadian Department of Justice for almost twenty years as a federal prosecutor. Kim has brought much needed 'due process' to the consideration of these petitions and has sought to ensure-so far as she is able-transparency, fairness, disclosure and adherence to the rule of law. To date, of the approximately 33 cases she has dealt with, approximately 19 have been granted.

The universal legal regime against Terrorism

From 1963, 18 international legal instruments for specific acts of terrorism were passed, the principal message being „extradite or prosecute". These legal instruments covered the following acts of criminality-all of which fall under the responsibility of those involved in traditional criminal justice systems; law enforcement, prosecutors and judges.

- Hijacking
- Aviation sabotage
- Violence at airports
- Acts against safety maritime navigation
- Acts against safety fixed platforms at sea
- Acts against internationally protected persons
- Unlawful taking and possession of nuclear material
- Hostage taking
- Terrorist bombings
- Funding of terrorists
- Nuclear terrorism

There have been extensive regional developments following 9/11. The following are some examples.

Europe. Europe has the most developed regional counter- terrorism framework emanating from the Council of Europe (CoE), Organisation for Security and Cooperation in Europe (OSCE) the European Union's institutions and agencies (EU). Eurojust (the European Unions's Judicial Cooperation Unit) was set up in 2002 to support investigations and prosecutions in member states of serious forms of crime, including terrorism. Most referrals to date have related to membership of terrorist organisations, but Eurojust was instrumental in providing assistance following the Madrid bombings in 2004. Eurojust facilitates the exchange of information, supports the issue and execution of European Arrest Warrants (EAWs), facilitates investigation and evidence gathering eg through the interception

of telecommunications and enables the seizure of assets which may be used to finance terrorism. It is also responsible for the Terrorism Convictions Monitor (TCM), an overview of terrorism related judicial developments and analysis.

Africa. The 1998 attacks in Kenya and Tanzania provided an impetus for enhanced counter-terrorism provision in Africa which culminated in the creation by the African Union in 2010 of a Comprehensive African anti-terrorist model law.

Central Asia. Asean Convention on Counter Terrorism -2007

MENA (Middle East and North Africa)

South East Asia

Western Hemisphere

Challenges, these include the following;

- The Criminal Justice response-v-military/security response. The rising interest of security in decision making is arguably taking a higher priority than the observance of human rights, but getting the public to care in the face of terrorist atrocities, is an uphill task. In a recent poll in the USA, 26% of Americans favoured torture where terrorism was involved, 45% were neutral.
- Cooperation within the 'Intelligence' community is vital but there need to be safeguards and an element of oversight
- In the name of counter-terrorism there is a proliferation of practices undermining human rights and the rule of law. These include:
  - Prolonged detention without charge
  - Ill treatment of detainees
  - Extraordinary rendition
  - Abuse of principle of non-refoulement (the practice of not returning individuals who may be offenders to their country of origin if there would be a serious risk of Human Rights violations).

More generally – there is a need to avoid the 'Guantanamo Bay' effect where terrorist suspects treated outside traditional criminal justice procedures are seen as 'special' and may even be hailed as martyrs or heroes.

The United Kingdom experience

Detention without charge and the period involved has been highly controversial. The Anti Terrorism Crime and Security Act 2001 imposed 7 days detention without charge following 9/11. In 2003 the period was increased to 14 days but in 2006 the period was increased to 28 days following the London bombings. In 2012 the period was reduced to 14 days following a review by the Independent Reviewer of Terrorism. Other controversial measures have been Control Orders introduced in 2005, which restricted the movement and activities of terrorist suspects. These were replaced by Terrorism Prevention and Investigation Measures (TPIMS) in 2012 which are to a limited extent, less restrictive eg. no relocation imposed but added surveillance.

Operation Vivace

Prosecution of the attempted bombings in London on 21st July 2005.

Events on 21st July:

Three explosions on London underground trains:

- Shepherds Bush – 1225hrs
- The Oval - 1230hrs
- Warren Street – 1240hrs
- One explosion on a double decker bus in Hackney – 1330hrs
- 5th unexploded device discovered on 23rd July 2005 abandoned on waste ground in Wormwood Scrubs
- Devices concealed in rucksacks
- Main charge of all devices failed to detonate.
- No deaths or serious injuries

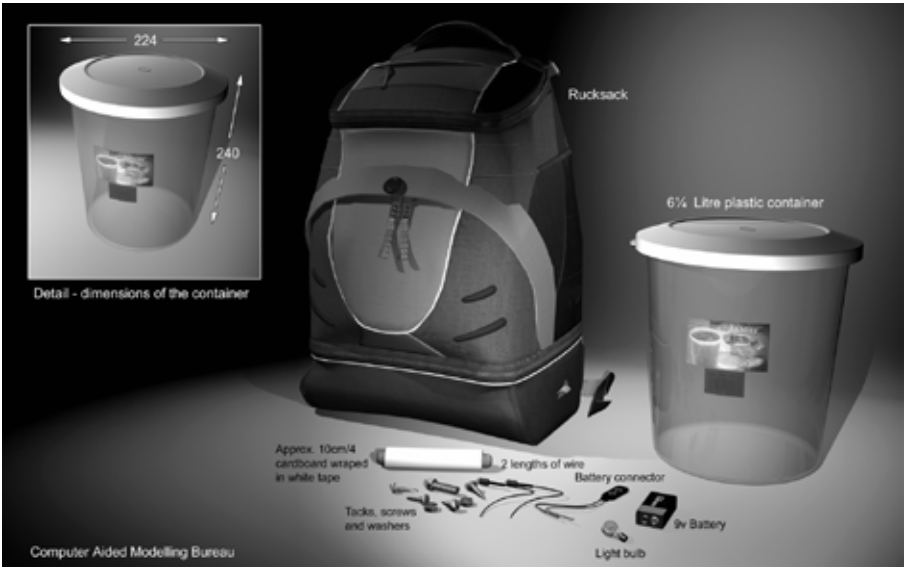
There was an extensive manhunt for the suspects of the 4 explosions.

Stills from CCTV were published internationally.

Remains of one of the devices recovered from Shepherds Bush tube

Bomb factory (58 Curtis House), home of Yassin Omar

Left: Arrest of Muktah Said Ibrahim



Model of the device

Findings and sentences

Ibrahim, Mohammed, Omar and Osman were found guilty of conspiracy to murder and were sentenced to life imprisonment – each to serve a minimum of 40 years.

Mohammed and Osman appealed against sentence. The Appellate Judges dismissed the appeal and said: ***„These were merciless and extreme crimes. As they were rightly meant to be, the sentences were severe and extreme. Beyond doubt, however, they were utterly justified."***

These Terrorists were brought to justice with due regard for human rights and the rule of law.

Elizabeth Howe OBE
General Counsel of the International Association of Prosecutors
Chief Crown Prosecutor, England and Wales

The author would like to acknowledge with thanks the contributions of Anton du Plessis Managing Director, Institute for Security Studies, South Africa: David Scharia, Senior Legal Officer and Coordinator, Legal and Criminal Justice group, UN Security Council, Counter-Terrorism Committee Executive Directorate: Sue Hemming Head of Special Crime and Counter Terrorism Division, Crown Prosecution Service, England and Wales: Kim Prost the Ombudsman of the United Nations Security Council's 1267 Committee for the Al-Quaida Sanctions List, Michèle Coninsx, President of Eurojust

Dr. Károlyi László

Hungarian Post Ltd's Emergency Situation Portfolio, its Exposure to Cyberthreats and Countermeasures

Hungarian Post Ltd. (hereinafter referred to as Post), as a universal service provider wishes to compete in new market segments and satisfy the 21st century customers' demands, apart from retaining its traditional service palette. At present day the Post has become the largest and most dynamically progressing cash services provider of Hungary.

The Post has a social capital developing role as well. *„Social capital is defined as the norms and social relations embedded in the social structures of society that enable people to co-ordinate action and to achieve desired goals."* [1]

The role and importance of social capital is very complex: it is paramount to the improvement and progress of an efficient civil society, competitive economy, progressing democracy, good government, general welfare and health standards. Social capital has become a factor of competitiveness in itself. The Post is a public institution that has a responsibility and duty to keep in mind customer and civil requirements to a higher degree even when making changes based on economic considerations. This requires a background knowledge that can portrait the social impact and context of those changes as well.

At the same time, the Post has a significant social organizer and community creator role. *„First, the teacher left, then the library was closed, and although the community house was still there, it was veiled by decay. The volunteer firefighter team was gone just the same as the general store. The small post office has become the single institution where the world's affairs could be discussed."* [2]

Given the Post's role in social history, it plays a key role in Hungary from

1 NARAYAN, Deepa: Bonds and Bridges, Social Capital And Poverty, World Bank, 1999. 8. p.
2 Gábor Kozma: Kivonuló kisposták (Disappearing small post offices), Vas Népe, 2003.

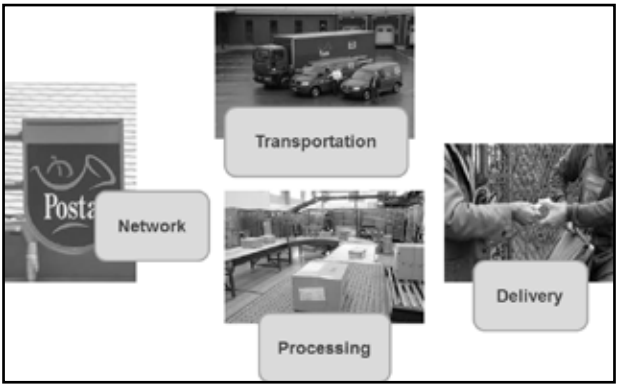
the social-state organization perspective. Even considering its dependency on the operability of other critical infrastructure elements, the Post can provide an alternative solution in a general emergency when the governmental and administrational control systems are damaged.

The Post is the only nationwide service provider that can substitute damaged telecommunications and information-transfer services, using its historically refined technologies. Based on its structure, number of employees, technical and technological capabilities, the Post can augment and support government administration in case of crises.

The Post's activities are highly organized and are made competitive and efficient by the synchronized co-operation between mutually depending systems (logistics, retail unit network etc.).

On a high level of social progress, people have a natural demand easy and regular access to frequently used and important products and services. Such demands by citizens and consumers are satisfied by various institutions, service providers and companies. These organizations need to run in a smooth and balanced way. Any disturbances affecting the daily routine impacts the operation of institutions, companies and people's comfort.

A smooth and balanced operation is thus in everybody's interest. This, however, is not a given asset, but the result of careful and comprehensive prevention and planning.



The four main pillars of the universal postal services at risk (Fig. 1.)

Recent natural and civilizational crises suggest that reasonable and

comprehensive defensive preparations could have prevented or lowered and limited the impact of these. Whining after the incident doesn't help. Preventive care and investment is preferred over damage control.

Network

The Post provides its services by operating 2700 sites on 3200 localities. Rendering these services depend on the availability of some fundamental conditions. In order to accept mail items for delivery, skilled staff, partially or fully operating infrastructure, cash supply, cash transportation, logistics services (mail item processing), IT background, Integrated Postal Network, company intranet and a telephone network are required.

Postal service locations (properties), postal assets and equipment, forms, office supplies, IT assets, IT network and human resources are critical for the network.

The primary threats in order of frequency (and not in order of impact) are natural and civilizational catastrophes. Secondary threats are (external) workers' strikes or a lack of internal capacity. Third rate threats are acts of terrorism, sabotage, and the possibility of attacks on IT systems should also not be played down.

The partial or full fallout of the network would have serious operational impact on the service sector e.g. delivery companies, payment of utility bills etc. A fallout in the accepting for delivery of, or delivery of official documents would impact state and government institutions as wall as the police and national security sector. The disruption of postal services would affect all areas of the society.

Transportation

Several thousand cars and nearly one thousand motorcycles and scooters are currently used for the delivery of mail items. Cars used in delivery start from more than 300 localities. This car pool serves all postal service providing

facilities nationwide, and in the case of mobile post offices, serve as service providers themselves. This means that service quality is heavily dependent on road conditions and traffic. Critical to service is the availability of fuel and a broad road-blocking demonstration may cause considerable threats to postal services.

In case of a disruption of postal services, the financial and banking sector, all national economy actors, state governance and institutions, telecommunications and personal official administration would be affected.

Processing

Nationwide processing services are based on a national processing center (National Logistics Center, NLC) and twelve regional processing sites, making it a 13 node-network. Furthermore, the International Office of Exchange (IOE) provides the connection to and from international mail item delivery. Newspapers and direct marketing items are processed by the Journal Logistics site. NLC has automated sorting processes, whereas other sites use solely manual processes to sort mail items.

The main task of NLC is to process the nearly 800 million letter items and approx. 10 million packages annually. NLC is located near Budapest in Budaörs. In case of a fallout of NLC, no temporary site takes over its activities, rather, the workload gets allocated to various sites and post offices in Budapest.

The main mission of the International Office of Exchange (IOE) is to receive and send international delivery items from and to abroad and to forward incoming items to the national postal network. IOE handles approx. 30 million letter mail items and 100 thousand packages annually.

In case of a fallout of IOE, processing can be resumed on the minimal acceptable level in a relatively short period of time, by reallocation. The required capacity and technology are available.

The Journal Logistics site's mission is the handling of newspapers (sorting

and forwarding, mostly from print shops to post offices) nationwide. The volume runs up to 6.5 million dailies and approx. 40 million miscellaneous papers annually. As a secondary activity, the site also processes CRM delivery items.

In case of the total fallout of IOE and Journal Logistics site, NLC could be used as a backup.

Based on the above, the critical entities of the processing network are the NLC, IOE and Journal Logistics site. Further critical IT systems are the Integrated Postal Network, Integrated Entry System and International Delivery Item Database.

In case of a total fallout of the NLC, post offices in Budapest and transportation sites can serve as backups. In case of the fallout of the Journal Logistics site or IOE, the workload and resources would be reallocated to the NLC and the postal site on Baross square.

Regional postal processing sites (RPPS) are not considered to be critical entities, because the complete fallout of single sites are handled by planned substitutes.

Any disturbances in critical entities jeopardize external systems as well:

- Pension, payment and money orders may arrive late to the delivering post offices, delaying their payment.
- Cash transfer orders (postal cheques) may arrive late to the delivering post offices, delaying their payment processing to utilities, insurance companies etc.
- Daily newspapers may arrive late to the delivering post offices, thereby losing their news value.
- Mail items and packages may arrive late to the delivering post offices, considerably impacting small and medium sized companies.
- Newspaper subscription payment processes may be delayed, in turn delaying the delivery of newspapers.

Delivery

In case of a partial or total fallout of the home delivery service, 1st priority delivery items' daily delivery must be ensured. The delivery of 2nd priority delivery items can be delayed to D+3 and D+5 days. Capacity problems from the lack of resources are categorized below:

- 1st degree: maximum 20% of the delivery routes are jeopardized from service providing aspects
- 2nd degree: 20-50% of the delivery routes are jeopardized from service providing aspects
- 3rd degree: more than 50% of the delivery routes are jeopardized from service providing aspects OR a 2nd degree capacity issue has remained unsolved for more than 2 days.

In case of the first two categories, services can be provided by work organization methods. In case of the most severe (3rd degree) capacity issue, delivery can be performed by a contracted third party and in the case of some specific products and following communication with the addressee, delivery can be provided on postal sites.

Possible threats to delivery are strikes and natural catastrophes, typically floods and ground waters. These can impact on a national level or locally, strikes can be external or internal, partial or complete, impacting all personnel in delivery. Service can be provided based on Government decree[3], GT&C (General Terms and Conditions) and the Post's internal regulations.

The Post's dependency on external infrastructures

The Post cooperates with strategic partners in the financial, IT/ telecommunications, energy providing and supply, waterworks-utilities and (public) transportation. These customers have significant delivery turnovers

3 79/2004 Government Decree

in mail items, logistics and financial products/services.

With its large nationwide network, presence, turnover and service types the Post has a considerable dependency on its operational environment. Dependency is significant on other critical infrastructure elements and their operability and quality, such as:

- energy supply
- internet service
- public utilities
- transportation
- communications

The conveying of impacts of socially significant services can increase the criticality if these are directly or indirectly through another infrastructure – in the same magnitude or socially increased – impacting their environment[4]. This danger is inherent in the Post's operations.

Probable sources of threats

There are two types of entities in our economic and social environment: one that can create emergencies and another that is impacted by such emergencies. Both of these can be affected by natural catastrophes. With its large nationwide network, presence, turnover and service types the Post has a considerable dependency on its operational environment. All attributes of

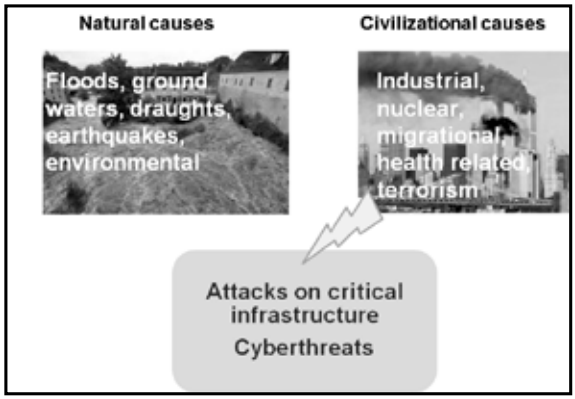


Fig. 2. Classification of crises.

4 Council Directive 2008/114/EC Article 2. point a)

critical infrastructures apply here – with one exception. The Post does not create environmental catastrophes but is impacted by them. Further, and as seen before, the Post has a significant dependency on the state and quality of critical external infrastructures.

Postal organizations, institutions and companies run risks of a wide variety of dangers and catastrophes. The source and trigger of catastrophes is a key factor in their classification. Based on these, catastrophes are classified in two main groups (see Fig. 2.).

Natural crises

- water damages (damage of utilities, floods, ground water)
- geological catastrophes (earthquakes, drops in the ground)
- weather damages (unusually strong gales, lightning)

The frequency of these sources of threats have considerably increased in recent years and will become significant emergency factors in the future. Their impact will mainly be felt in the affected postal sites, disturbing postal network operation and making transport and delivery more difficult.

Civilizational crises

- Industrial (blasts, hazardous material fallout, dangerous waste production, radioactive fallout),
- transportational (roads, railroads, air- and waterways),
- political(crises-revolution, national-, racial- or religious conflicts, terrorism),
- agricultural (forest clearing, chemicalization, destruction of florae),
- economic (poverty, delinquency, collapse of national economy),
- environmental (water-, air-, ground pollution),
- wars,
- other (strikes, social conflicts, civil wars).

Given Hungary's security situation, wars and large migrations are not to be expected in the near future, however, they are considered in emergency planning.

Strikes are real threats in general, sectorial or postal frameworks. They may impact the operation of postal network and processing and may make the transfer and delivery of items more difficult.

The Post is only lightly prone to terrorism and as a result, the probability of occurrence of the listed threats is low. Nevertheless, they have to be taken into consideration in contingency planning.

- Bombings, attacks (on state institutions, power lines, telecommunications centers, broadcasters, airports, internet service providers etc.)
- Attacks on key personnel operating the above listed systems
- Crimes (forceful acquisition or destruction of data)
- Manipulation or stoppage of control systems

High risk postal units and services

Postal Clearing Center (PCC)

The Postal Clearing Center (PCC) is an independently operating single clearing center. Its activities are fundamental to the company. Continuous operation of the PCC is paramount to providing cash transfer and banking services.

The partial or complete fallout of the PCC may result in the delay or forfeit of cash transfers. The fallout of automated processing does not only affect consumer cash transfers, but has a significant impact on interbank money transfers as well. The latter has international repercussions, because the Post guarantees the timely settlement of transfers for foreign financial institutions.

In case of an extreme disaster situation and given the several millions of daily transactions, the fallback to a manual workaround process from both the human resource and the operational background point of view cannot or can only be implemented in a very long period of time. Such a discontinuation of settlement services for two or three days may result in the

partial halt of domestic commerce and international financial transactional activity. This would damage Hungarian economy by billions. We have created a comprehensive defensive and preparative plan that includes alternative solutions (backup site, processing machines) along the defensive measures.

International Office of Exchange (IOE)

The delayed delivery of items in an international relation may result in cost increases, revenue drops or fallout, loss of trust and international goodwill.

National Logistics Center

The reorganization of processing does not adversely impact companies, institutions or people and do not affect continuous business operation. The comprehensive defensive-preparative plan contains such simulated exercises that can be used to test the smoothness of transition.

The processing step is in the middle of the delivery process chain. In case it is adversely impacted, it will result in delayed delivery, decreased sorting depth or even fallout of delivery flows. Operational issues in the PCC, NLC and IOE impact on the national level, while regional processing units' issues have regional impacts.

Dangers and threats to the Post

The number of dangers and threats that universally effect the postal organization is limited. Most, if not all of the natural crises can be excluded since they do not negatively affect or block the operation of the entire postal network.

The number of postal sites with chemical-, nuclear- or flood threats is significant and the number of affected employees is several thousands.

Postal operations for the most part are not continuous sequences of technological steps. This means that any disturbances, batch stops or other negative effects do not cause major disruptions on multiple servicing end-points.

Status of emergency readiness

The Post has created the „Security and Crises Management Strategy" document to coordinate emergency handling and preparational tasks, lay out fundamentals and assets and to fit into the national frameworks for handling national security and non-national security emergencies.

The preparation for and the carrying out of tasks during a qualified period are performed by designated[5] postal service providers and those service providers that are part of the IT and electronic telecommunications system and the postal support system.

The 2012/CLIX law on postal services requires the Post to prepare for qualified and emergency periods. Tasks and the working conditions are laid out in a Government decree[6] to ensure that postal services are available for national security purposes and that their requirements are satisfied with the highest priority. The decree[7] on the designation of postal service providers participating in defense tasks and their preparational tasks require the Post to carry on operations during qualified and emergency periods. It requires the preparation and execution of tasks with respect to its service provision during qualified periods.

An internal postal regulation[8] with the highest authority describes the tasks and their planning during a qualified period. This internal regulation requires that the Post participates in economic preparations, makes available resources for defense purposes and creates and operates a civil defense organization when called upon. Furthermore, the Post must ensure the carrying out of tasks during a qualified period by planning and preparations.

The detailed instructions concerning defensive tasks during a qualified period are also described in a high level internal regulation[9]. This contains

5 26/2010. (III. 31.) Decree of the Ministry of Transport, Telecommunications and Energy

6 241/2004. (VIII. 16.) Government Decree

7 26/2010. (III. 31.) Decree of the Ministry of Transport, Telecommunications Communications and Energy

8 54/2005. internal regulation issued by the Chief Executive Officer

9 3/2008. internal regulation issued by the Chief Security Officer

the management and preparational tasks of defense organizations. It also lays out ways to safeguard human life and material assets and the defense against forces impacting operability during an emergency or qualified period. Further, the regulation defines the process of creating, managing and using civil defense organizations as well.

There are defensive plans to preempt or decrease the effect of impacts on the Post. These plans (Corporate disaster recovery plan, Pandemic plan, Post Partner disaster recovery plan, IT Disaster Recovery Plan, Business Continuity Plan) are required by the above mentioned laws. Stockpiling was not done due to economic reasons. Substituting organizations were not defined due to the large number of post offices. On a strategic and operational level, there are designated organizations that start to handle issues based on existing plans, without direct assignments.

IT system vulnerabilities

Only the partial or total damage or fallout of services by the IT support would have a general impact on postal services. Approximately 2-5 days are required to switch over to manual workarounds for mail item processing and delivery in case of partial or total IT fallout.

The Post's IT and emergency handling experts continue to analyze the impacts of a physical or IT attack by malicious organizations or persons against the informational infrastructure operating the Post's organization. Vulnerability is there due to the dependency on complex technical, IT and communications systems and the interconnected network elements. [1] We have plans to test emergency regulations in simulated exercises. During the course of these exercises we launched attacks on the integrated IT and communications systems and analyzed the damages they may suffer.

IT disaster events that can potentially impact systems may occur in the data center systems and infrastructure of a company that provides services to the Post. These service providers naturally have operation- and business

continuity plans, emergency, fire and disaster handling plans. These are provided in the frame of concluded Service Level Agreement and the Post is not responsible for their review and update.

Cyberspace and cyber war

The Post's systems run the same risks of attacks from cyberspace like any other government, utility, banking etc. systems. [2] This vulnerability is a market competition factor and should be minimized as much as possible. Cyberspace is the space created by computer systems and networks, storing electronic data and processing online transactions and communication.

Some forms of this „war" are:

- Cyber espionage: a foreign state acquiring data from government systems in a clandestine way. Its scope is usually significant as well as the damage is, but it does not threaten the country's operation directly because it does not cause system fallout.
- Cyber terrorism/hacktivity: aims to stop certain systems or change end user front ends (deface) or steal data with the eventual aim of disclosure. Generally effects just one or a small number of systems. The damage is usually not significant and does not affect the operation of a country but causes significant loss of prestige.
- Cybercrime: has similar attributes to cyber espionage with the difference that it usually effects one organization and aims to acquire and sell specific information.
- Cyber warfare: one state launching an attack on another state with the aim of disrupting or blocking the other state's social or economic operation. It may come as a sideline to armed conflict. Its scope and the damages are huge and jeopardizes the operation of the entire country.

Contrary to conventional war, this war has no rules and the perpetrators are usually unknown (Fig. 3.) Its targets are information infrastructure, assets and services. There are no bombers or missiles that can be picked up by ra-

dar; and the route to target is unseen. Another major difference is that while the allegiance of an attacking army is easily distinguishable, this is virtually impossible to tell in cyberspace.

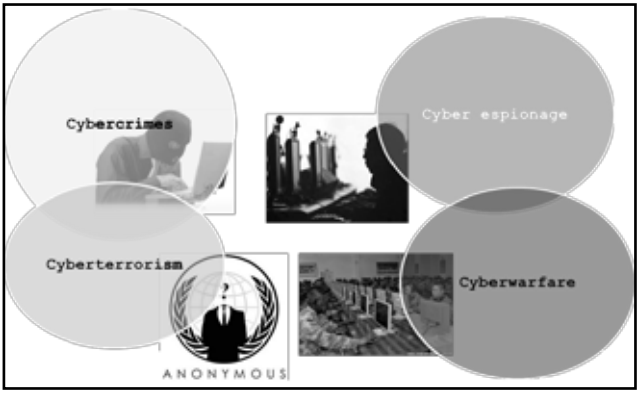


Fig. 3. Cyber operations.

The world stands before a change of international magnitude regarding the defense of cyberspace. Making the internet more secure is of great importance for Hungary as well, because the IT sector presents one of the biggest growth possibilities of the economy.

It is safe to say that something similar to the Geneva Conventions would be required in cyberspace as well. Without this, some countries may become defenseless and more powerful countries may hijack their infrastructure. It has never been easier to become a cybercriminal than today. It is well known that anyone can acquire a cyber-weapon for a few hundred dollars that gathers banking codes from the targeted computers. The software even comes with 24/7 product support.

According to international experiences, increasingly powerful threats have to be reckoned with in the field of postal service as well, especially in the case of banking and financial transactional systems, and especially on the following fields:

- Virus attacks, malware, trojans
- Data theft attacks
- Phishing
- Data manipulations, hacking of websites
- Denial of service attacks (DDoS)

- Spamming

Apart from the preparation for external sources of risks, internal risks have to be minimized as well, such as:

- Inhomogeneous IT architecture due to changes in technology
- Distributed, non-centralized local systems
- Key user activity, lack of oversight
- Deliberate or accidental loss of data
- Illicit use of network assets (data leakage, internet, external webmails)
- Varying level of computer literacy
- Lack of IT incident warning system
- Lack of 7/24 IT security oversight

We have implemented various data- and information security mechanisms in the controlling environment and the technical systems after considering possible risks:

Control environment

- Controlled, documented environment
- Regular risk assessment
- Logging and log analysis
- DMZs
- Controls (ad-hoc, regular, built in processes): external, internal, penetration
- Human control: employee hiring, checking during employment, training

Technical systems

- Data leakage prevention system
- Central log analysis system
- Central virus protection, content- and spam filtering systems
- Public key infrastructure
- Document protection
- Vulnerability management
- Limiting internet access and the use of external peripheries, blocking guest WiFis

Summary

Primarily, the Post responds to risk factors affecting business continuity and the scope of activities by risk prevention. The use of substitute third parties, high availability assets, availability of redundant and spare assets and keeping them in independent fire sections, regular daily system backups, storing weekly/monthly backups in different locations, backup communication or IT network routes, reliable vendors and administrators provide adequate protection.

A possible disaster scenario can be the loss of a region, when data connection is lost with that particular region. The service provider uses redundancy to maintain the service. In case of a total fallout of basic infrastructure, the vis maior clauses in contracts will come into force. Low probability, low business impact risks (eg. PCs falling out) can be handled with business continuity plans. The necessary actions to resume regular operations are defined by the Post when the risks occur.

IT disaster recovery exercises, training courses including exams for the personnel, consultations and cooperation with Government's Computer Incident Response Team (Gov CERT Hungary) and with the Ministry of the Interior, National Directorate General for Disaster Management, National Industrial Safety Operation and Critical Infrastructure Protection Network Safety Centre are regularly on the agenda. All these measures form the framework of IT security.

Dr. Károlyi László PhD. ny. ezredes, Magyar Posta Zrt. biztonsági főigazgató

REFERENCES

[1] A hálózati társadalom sérülékenysége http://www.nato.int/docu/review/2002/issue2/hungarian/features2.html (download 2014. március 24.)

[2] Zsolt Haig – László Kovács: Fenyegetések a cybertérből, Nemzet és biztonság. I. évfolyam, 5. szám. Budapest, 2008. május, pp.: 61-69 ISSN 1789-5286

[3] László Károlyi: A Magyar Posta Zrt. veszélyhelyzet kezelési rendszere, Gazdasági Élet és Társadalom, 2011. I-II. szám, pp.: 231-240 ISSN 2060-7466

Prof. Dr. Kovács László

A közszolgálati hivatásrendek oktatásában meghatározó biztonságfelfogás, valamint az ezzel összefüggő kutatás-fejlesztés a Nemzeti Közszolgálati Egyetemen

A Nemzeti Közszolgálati Egyetem (NKE) 2012. január 1-én alakult meg a Zrínyi Miklós Nemzetvédelmi Egyetem, a Budapesti Corvinus Egyetemből kiváló Közigazgatás-tudományi Kar és a Rendőrtiszti Főiskola, mint jogelőd intézmények bázisán.

Az új egyetem megalakulásával a felsőfokú közszolgálati szakemberképzés egyik legfontosabb intézményévé vált hazánkban. A jogelőd intézmények átalakulásának, így az új integrált egyetemnek célja, hogy a közszolgálaton belül a honvédelem, a polgári közigazgatás, a rendészet és a nemzetbiztonsági szolgálatok személyi állományának képzését végezze. Tegye mindezt úgy, hogy az említett ágazatokban dolgozók hivatástudatát és szakértelmét erősítse, azok oktatása során hangolja össze a képzés tartalmi részeit, tervezze meg az utánpótlásképzést, a közszolgálati felsőfokú szakemberképzéshez pedig egységes intézményi bázist nyújtson.

Az egyetem létesítésekor az egyik kiemelt cél az volt, hogy az egyetem az érintett hivatásrendek specilitásainak szem előtt tartásával, az azokban megjelenő erősségek kiemelésével, olyan intézmény jöjjön létre, amely az erőforrásokkal hatékonyan gazdálkodik, és mindezek mellett az életpálya és előmeneteli rendszerben is meghatározó szerepet vállalva járuljon hozzá a közszolgálati szakemberek képzéséhez.

A Nemzeti Közszolgálati Egyetem

A Nemzeti Közszolgálati Egyetem megalakulása

2010 év közepén a Honvédelmi Minisztérium, a Közigazgatási és

Igazságügyi Minisztérium a Belügyminisztérium, valamint a tervezett új egyetemhez csatlakozó felsőoktatási intézményhez képviselőiből egy munkabizottság alakult meg. A munkabizottság előzetesen egy olyan koncepciót fogadott el, amely felvázolta az egységes egyetem létrehozásának különböző kérdéseit.

Ezt követően három albizottság megalakítására került sor (oktatási-kutatási, szervezeti-vezetési és infrastruktúra-finanszírozási, jogi-felügyeleti albizottság). A három albizottság fő feladata egy kormányhatározati javaslat előkészítése volt az új egytemen vonatkozásában, ugyanakkor az albizottságok több feltáró jelentést is készítettek különböző témakörökben. [1]

Az albizottságok előkészítő munkájának eredményeként 2010. december 15-én került elfogadásra a 1278/2010. (XII.15.) Korm. határozat, amely – egyebek mellett – előírta a létesítésről szóló törvény, illetve a szervezetre, működésre, a hallgatói és oktatói jogállásra vonatkozó törvény megalkotását. [2]

A Nemzeti Közszolgálati Egyetem létesítéséről szóló 2011. évi XXXVI. törvényt (a továbbiakban: Létesítési tv.) 2011. március közepén fogadta el az Országgyűlés.

„Az Országgyűlés felismerve, hogy a közszolgálaton belül a polgári közigazgatás, a rendvédelem, a honvédelem és a nemzetbiztonsági szolgálatok személyi állományában a hivatástudat és a szakértelem erősítése összehangolt és tervezett utánpótlásképzést tesz szükségessé, továbbá a pályaelhagyás helyett a társadalom számára hatékony munkavégzés biztosítására a közszolgálati életpályamodellt támogató továbbképzési rendszert kell működtetni, a közszolgálati felsőfokú szakemberképzést egységes intézményi alapokra kívánja helyezni." [3]

Ez a törvény rendezte a létesítés alapvető szabályait, a megvalósítás ütemtervét és a résztvevő intézmények, testületek feladatait, valamint azok működését. A törvény rendelkezéseinek megfelelően, megalakult az új egyetem Előkészítő Testülete, valamint a Gazdálkodási Előkészítő Bizottság. A Létesítési tv. értelmében az egyetem fenntartói jogait az úgynevezett Fenntartói Testület útján a honvédelemért, a közigazgatásfejlesztésért és a rendé-

szetért felelős miniszterek közösen gyakorolják. [3]

A fenntartói jogok gyakorlására feljogosított Fenntartói Testület az alakuló ülését a törbényben meghatározott módon és időben megtartotta, a fenntartó miniszterek által delegált tagok kijelölése megtörtént. [1]

Mindezeket követően a Fenntartói Testület elfogadta az Ideiglenes Szenátus választási szabályzatát, amely alapján az új egyetem Ideiglenes Szenátus (ISZ) tagjainak megválasztása megtörtént, és a testület 2011. július 12-én megtartotta alakuló ülését. Az ISZ mandátuma és feladatai az egyetem új Szenátusának megválasztásáig – 2012 decemberéig – tartott.

2011-ben született meg a Nemzeti Közszolgálati Egyetemről, valamint a közigazgatási, rendészeti és katonai felsőoktatásról szóló 2011. évi CXXXII. törvény. E törvény 10. §.-a rendelkezik egy igen fontos tényezőről, amely az egyetem Intézményfejlesztési Tervének elkészítését, valamint annak folyamatos felülvizsgálatát határozta meg. [4]

A Nemzeti Közszolgálati Egyetem emblémája
(forrás: NKE Arculati kézikönyv)

Az Intézményfejlesztési Terv a működési hatékonyság fokozását célozza. A megfogalmazott célok lehetőséget biztosítanak a korábban létrejött szervezet hatékonyságának növelésére és az alapvető infrastrukturális lemaradások megszüntetésére. Az egyetem létrehozása természetszerűleg kapcsolódik a megalkotáskor érvényben lévő Kormányprogram célkitűzéseihez. Ezek közül néhány fontos célkitűzés a következő:

- a magyar állam tekintélyének helyreállítása;
- a közbiztonság és a törvényes rend erősítése a közigazgatás és a közszolgálat személyi állományának elkötelezettségén és szakmai felkészültségén alapulva;

- a polgári közigazgatási, a honvédelmi, a nemzetbiztonsági és a rendészeti szerveknek olyan életpályamodell kialakítása, amely már a felsőfokú szakemberképzés időszakában megteremti a hivatás iránti elkötelezettséget, biztosítja a professzionális képzést és a gyakorlatorientált oktatást, valamint a hivatásrendek közötti átjárhatóságot.

Az egyetem megalakításakor kitűzött célok megjelennek az Intézményfejlesztési Tervben. Mindezek alapján a fenntartók és az intézmény is egyaránt érdekelt ezen célkitűzések elérésében és az azokban megfogalmazottak teljesítésében, mert az hosszabb távon az oktatói és adminisztrációs létszám racionálisabb kihasználását, a megtakarítások növelését, ezáltal a fenntartási-üzemeltetési költségek csökkenését eredményezi. [1]

„Egyetemünk alapításával természetesen nem a múltat kívánta megismételni az Országgyűlés. Intézményünk elsődleges célja a polgári közigazgatás, a rendvédelem, a honvédelem és a nemzetbiztonsági szolgálatok személyi állományának magas színvonalú képzése. Ezzel együtt az egységesülő közszolgálati életpályák közötti átjárhatóság megteremtésének támogatása a képzések oldaláról. Mindezek megvalósításához a 2012. január 1-jén megalakult Egyetemünk becsülendő szakmai örökséget kapott. Közvetlen jogelődeink (...) a magyar közszolgálati szakemberképzés történeti hagyományainak letéteményesei voltak. Emellett az Egyetem nemcsak az 1808-ban alapított Ludovika Hadi Akadémia szellemi utódja, hanem a közigazgatás-tudományok és a rendészeti ismeretek XVIII. században megkezdett oktatásának is folytatója." [5]

A Nemzeti Közszolgálati Egyetem felépítése

Az egyetem szervezeti struktúrája oktatási szempontból három egyetemi karra, és négy (karközi) intézetre tagozódik.

A három egyetemi kar:

- Hadtudományi és Honvédtisztképző Kar;
- Közigazgatás-tudományi Kar;
- Rendészettudományi Kar.

Az egyetem (karközi) intézetei:

- Katasztrófavédelmi Intézet;
- Nemzetbiztonsági Intézet;
- Nemzetközi Intézet;
- Vezető- és Továbbképzési Intézet.

Az egyetem oktatása meghatározó módon a Bolognai-folyamatra épül. Ennek megfelelően az intézmény alapképzési szakokat (BA, BSc), mesterképzés szakokat (MA, MSc) és doktori (PhD) képzést folytat.

Az egyetem jelenleg három doktori iskolával – Hadtudományi Doktori Iskola, Katonai Műszaki Doktori Iskola, Közigazgatás-tudományi Doktori Iskola – rendelkezik. A rendészettudományok területén pedig egy új doktori iskola felállítását tervezi az NKE.

Terjedelmi korlátok miatt jelen írás a három egyetemi kar rövid bemutatására, illetve a biztonságpercepció kialakításának, kutatásának és folyamatos figyelemmel kísérésének egyik legfontosabb bázisát jelentő Stratégiai Védelmi Kutató Központ tevékenységének rövid vázolására tud csak vállalkozni.

A Hadtudományi és Honvédtisztképző Kar a több mint kétszáz éves magyar nyelvű felsőfokú tisztképzés hagyományait megőrizve végzi a honvéd tisztjelöltek szakmai felkészítését alapképzésben és mesterképzésben. A karon három intézet – a Katonai Vezetőképző Intézet, a Katonai Üzemeltető Intézet és a Katonai Logisztikai Intézet – keretein belül folyik a képzés, valamint a képzéseket is megalapozó hadtudományi és katonai műszaki kutatás. A kar doktori iskoláiban (Hadtudományi Doktori Iskola és Katonai Műszaki Doktori Iskola) megszerzett (PhD) doktori fokozat birtokosa jó esélyekkel indulhat mind az állami, mind a versenyszférában a legkülönbözőbb szakterületeken magasabb vezetői, oktatói és kutatói munkakörökért folytatott versenyben. A kar Katonai Felsővezetői Tanfolyamot is gondoz, amelyen a közeljövő katonai felsővezetői tanulnak. Ezen a tanfolyam rendszeresen részt veszenek külföldi hallgatók is. A karon tanuló honvéd tisztjelőlt hallgatók nyelvi készségeinek elsajátítását az Idegennyelvi és Szaknyelvi Központ biz-

tosítja, a Nyelvvizsga Központ pedig angol nyelvből általános, valamint szaknyelvi jelleggel, akár STANAG 3 szintig, illetve a francia nyelv tekintetében a megfelelő szintű ARMA nyelvvizsga kibocsátására jogosult. Mindezeken túl a kar a tudományos utánpótlás biztosítása érdekében kiemelkedő tevékenységet folytató szakkollégiumi rendszert is támogatja, amelynek keretében szoros szakmai és tudományos kapcsolatokat ápol az immár 10. évfordulóját ünneplő Biztonságpolitikai Szakkollégiummal, illetve a Puskás Tivadar Műszaki Szakkollégiummal. [6]

A Közigazgatás-tudományi kar korszerűsített szervezeti struktúrával, részben megújult oktatói állománnyal és modernizált képzési programokkal áll a megújuló hazai közigazgatás szolgálatában. A kar oktatási tevékenysége magában foglalja az általános ismeretek átadását a közjog, a közpolitika, a közpénzügyek, a közszolgálat, valamint a közigazgatási menedzsment területén ugyanúgy, mint a speciális szakigazgatási „tudás" biztosítását. Az átadott ismeretanyag folyamatosan az állam, a közigazgatási szervek, valamint a társadalom irányából érkező elvárásokhoz igazodik. Így biztosítható, hogy a kar szakjait elvégző diplomás pályakezdők a közszolgálat területén jól hasznosítható, naprakész tudással rendelkezzenek. A közigazgatás önálló szakmaiságában kiemelkedő mérföldkő a közigazgatás-tudomány önállóvá válása. E tudománynak akadémiai elismerése tette lehetővé, hogy 2013. szeptemberében elinduljon a Közigazgatás-tudományi Doktori Iskola. A kar célja, hogy a felsőfokú közigazgatási oktatás a „jó állam" eszméjének megvalósítását szolgálja, a kar jelmondatának megfelelően: Pro Publico Bono. [7]

A Rendészettudományi Kar a hazai felsőoktatásban továbbra is egyedüliként folytat rendészeti képzést. A Kar a rendészeti ágazat szervei, így különösen a Rendőrség, a Büntetés-végrehajtás, a Nemzeti Adó- és Vámhivatal, az Országos Katasztrófavédelmi Főigazgatóság, valamint a Bevándorlási- és Állampolgársági Hivatal és a magánbiztonsági szféra számára képez tiszti, közalkalmazotti, köztisztviselői és kormánytisztviselői munkakörök betöltésére hivatott, felsőfokú szakképzettségbel rendelkező szakembereket. A kar

speciális képzés jellegéből adódóan arra törekszik, hogy erősítse a hivatástudatot és a szakértelmet a jövő ágazati szakembereiben. Ennek megfelelően magas színvonalú tudást ad át a hallgatóknak, valamint mindezek mellett a kar felkészíti hallgatóit az elvárt magatartásformákra és személyiségjegyekre, amelyek a rendészeti szerveknél elengedhetetlenül szükségesek. A kar hallgatói nappali és levelező munkarendben három éves alapképzési, valamint levelező munkarendben két éves mesterképzési szakon folytatják tanulmányaikat. Mindemellett a kar rendelkezik három féléves szakirányú továbbképzésekkel is. A kar tudományos területen megvalósítandó célja a Rendészettudományi Doktori Iskola megalapítása és elindítása. [8]

A Stratégiai Védelmi Kutató Központ (SVKK) az 1992-ben alapított Stratégiai és Védelmi Kutatóintézet jogutódjaként működik az NKE Nemzetközi Intézet keretein belül. A központ jelenleg az egyetlen állami finanszírozású, biztonságpolitikával foglalkozó kutatóintézet hazánkban. Az SVKK fő tevékenysége a magyar biztonság- és védelempolitikai döntések előkészítésének érdekében stratégiai, biztonság-, védelem- és katonapolitikai kutatások, elemzések és értékelések készítése. A központ nemzetközi biztonsági kutatócsoportja az európai biztonsági architektúra fejlődését, a kelet-közép-európai biztonság fejleményeit, a posztszovjet régiót, a magyar biztonságpolitikát és a terrorizmust, míg stratégiai és védelmi kutatócsoportja a fegyveres erők demokratikus ellenőrzésének alakulását, a társadalom és a haderő kapcsolatát, valamint a honvédség szervezeti és strukturális kérdéseit vizsgálja. Az intézet kutatási eredményeit számos formában publikálja, amelyek között megtalálható a Nemzet és Biztonság című folyóirat, de a központ e mellett rendszeresen közread dokumentumköteteket és szöveggyűjteményeket is a magyar biztonságpolitika, a NATO, az Európai Unió alapdokumentumaival. Igen fontos, és a biztonságtudat kialakításában előkelő szerepet betöltő kiadvány a Védelmi Tanulmányok sorozat, melyben eddig 61 tanulmány látott napvilágot. [9]

Biztonságfelfogás és az ezt támogató kutatás-fejlesztési projektek a Nemzeti Közszolgálati Egyetemen

A biztonságfelfogás kialakításának és fejlesztésének egyik legfontosabb eleme azoknak a kutatásoknak a folytatása, amelyek az adott felsőoktatási intézmény szakmai profiljába illenek. A kutatások, illetve a kutatás-fejlesztések, azok eredményeként létrejövő új tudás elengedhetetlen az oktatás fejlesztéséhez.

Biztonság összetevői és területei az NKE-n (szerk.: Kovács L.)

A Nemzeti Közszolgálati Egyetem három nagy hivatásrend – honvédelem, rendvédelem, közigazgatás – oktatását integrálja. Így az egyes hivatásrendek különböző területein születő kutatási, kutatás-fejlesztési eredmények megjelenhetnek a másik két terület oktatásában is. Erre az egyik legjobb példa az NKE úgynevezett közös, közszolgálati modulja. Ez a modul 14 tárgy oktatását, ismereteinek átadását, és egy közös zárógyakorlat megtartását jelenti. A három hivatásrend alapvető ismereteit magába foglaló tantárgyak kötelezőek minden NKE-s alapképzésben résztvevő hallgató számára. Ezek a tárgyak következőek:

- általános politológia;
- általános szociológia;
- alkotmányjog;
- vezetés- és szervezés elmélet;
- közigazgatási funkciók és működés;
- hadelmélet és katonai műveletek;

- biztonsági tanulmányok;
- közszolgálati logisztika;
- rendészet elmélete és a rendészeti eszközrendszer;
- az állam szervezete;
- közszolgálati életpályák;
- nemzetbiztonsági tanulmányok;
- katasztrófavédelmi igazgatás;
- közpénzügyek és államháztartástan.

Az oktatásba átültetett kutatási eredmények közvetlen és közvetett hatással is bírnak, hiszen hozzájárulnak a jövő közszolgálati szakemberei felkészítéséhez.

Az NKE számos kutatási projektet vezet, amelyek között megtalálható például az Államreform Operatív Program (ÁROP) keretében végzett Jó Állam Kutatások és Kutatóműhely.

Terjedelmi korlátok miatt azonban jelen írás csak két kutatás-fejlesztési, illetve az alaprendeltetéshez kapcsolódó feladatot támogató tudományos utánpótlás és tehetséggondozó projektet kíván röviden bemutatni.

2012. január 1-én indult a két éves futamidejű, az NKE és az Óbudai Egyetem konzorciumi formájában végzett TÁMOP-4.2.1.B-11/2/KMR/2011-0001 projektje, amelynek célja a kritikus infrastruktúra védelem területén nemzetközi színvonalon, és nemzetközi együttműködésben végzett kutató-fejlesztő tevékenységhez szükséges kritikus tömegű humánkapacitás konszolidációja, szükség szerinti fejlesztése, valamint az e területeken végzett innováció támogatása volt. A projekt négy kiemelt kutatási területre fókuszált: (1) a nagy megbízhatóságú, hibatűrő, ún. „öngyógyító" infrastrukturális alrendszerek; (2) az egyes alrendszerekből származó adatok integrált kezelése; (3) az alrendszerekben történő elosztott számítások és az alrendszerek közötti biztonságos kommunikáció; illetve (4) a biztonsági szint állami intézményrendszer, üzemeltetők és tulajdonosok, állampolgárok együttműködése révén történő fenntartható növelése. Leegyszerűsítve: (1) Adatintegráció; (2) Kommunikáció; (3) Öngyógyító rendszerek; (4) Civil partnerség. [10]

Az NKE a projekt közel 1 milliárd forintos összköltségvetésében 442 786 440 Ft összeget fordíthatott a jóváhagyott kutatási célok elérésére. A projekt eredeti futamideje 2012. január 1-2013. december 1. között volt, de a pályázat támogatója a hosszabbításra vonatkozó konzorciumi kérelmet – mely a pénzügyi adminisztráció maradéktalan elvégzését szolgálja – elfogadta, így 2014. március 31-e a projekt fizikai befejezésének határideje. Az indikátorok területén már 2013 októberében meghaladta a 100%-ot a teljesítés, a pénzügyi felhasználás 2013. december 31-én 323 025 950 Ft (73%) volt az NKE részéről, a meghosszabított határidő végére a felhasználás tervezetten megközelíti, illetve eléri a 100%-ot.

E projekt megvalósításában a partnerekkel együtt 112 oktató-kutató, 30 szakértő, 28 leendő oktató-kutató, 33 külföldi szakértő vett részt, akik a projekt időtartalma alatt 132 hazai és nemzetközi cikket írtak, 11 könyvet készítettek, 4 szabadalmat nyújtottak be, 140 konferencia előadás tartottak, további 43 tanulmány és stratégia kidolgozásában vettek részt, valamint 70 egyéb tudományos témájú dolgozatot készítettek.

A TÁMOP-4.2.2/B-10/1-2010-0001 azonosítószámú „Kockázatok és válaszok a tehetséggondozásban" (KOVÁSZ) nevet viselő projekt célja az volt, hogy segítse az egyetemi tehetséggondozást, ezen belül a Tudományos Diákköri tevékenységet, a szakkollégiumok működését, valamint járuljon hozzá a tudományos utánpótlás biztosításához. A projekt kezdete 2011. november 1., befejezése pedig 2013. október 31. volt, költségvetése pedig közel 65 millió Ft. Az NKE a projektben tervezett indikátorokat jelentősen túlteljesítette. A konstrukció támogatásával megvalósult publikációkból levonható az a következtetés, hogy a projekt megfelelő indukáló szerepet játszott a kutatók publikációs aktivitásának növelésében.

A projekt segítségével 3 könyv, 12 könyvfejezet, 30 cikk jelent meg, mindebből négy idegen nyelven. A konferencia előadások száma jelentősen meghaladja a vállalt értéket. A konstrukció segítségével 6 hazai, illetve nemzetközi konferencia valósult meg, így megfelelő számú tudományos rendezvény állt

rendelkezésre az oktatók és kutatók, valamint nem utolsó sorban a hallgatók számára bemutatni és a tudományos közélet előtt megmérettetni a kutatási eredményeiket. Bár a projekt céljai között elsősorban nem az eszközbeszerzés szerepelt, de a projekt segítségével beszerzett eszközpark (kutatási infratsruktúra fejlesztése) hosszú távon szolgálja az egyetemi oktatás-kutatás ügyét. A vállalt képzéseket, valamint a támogatott K+F projekteket 100%-ban sikerült teljesíteni a munkába bevont 215 fő oktató és kutató, és a 410 fő hallgató segítségével. [11]

Összefoglalás

A Nemzeti Közszolgálati Egyetem, mint hazánk legfiatalabb felsőoktatási intézménye 2012. január 1-én alakult meg. Az egyetem bár még csak két esztendőre tekinthet vissza, de a jogelődök története több, mint 200 éves hagyománnyal büszkélkedhet.

Egy egyetem életében 2 év rendkívűl rövid idő. Ugyanakkor a közszolgálati hivatásrendek oktatásában, a jövő közszolgáinak felkészítésében, illetve a ma munkatársainak tovább és átképzésében már ezen idő alatt is elkezdődött az az új, egységes szemléletű munka, amelynek egyik alapja egy olyan biztonságfelfogás kialakítása, amely alapján a jövő kihívásaira egzakt választ lesznek képesek adni a jelenleg még az egyetem padsoraiban ülő hallgatók.

Az NKE-n folyó kutatások, valamint kutatás-fejlesztések nagymértékben hozzájárulnak e biztonságfelfogás folyamatos alakításához, hiszen csak a tudományos kutatások eredményei, majd azok beépítése a különböző tananyagokba adhat valóban hiteles és reális alapot ahhoz, hogy az egyetem ellássa az alaprendeltetéséből adódó feladatát: a haza szolgálatában.

Kovács László egyetemi tanár, Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Kar

Felhasznált irodalom

[1] A Nemzeti Közszolgálati Egyetem Intézményfejlesztési Terve, NKE, Budapest, 2012.

[2] 1278/2010. (XII. 15.) Korm. határozat a Nemzeti Közszolgálati Egyetem létrehozásáról.

[3] 2011. évi XXXVI. törvény a Nemzeti Közszolgálati Egyetem létesítéséről.

[4] 2011. évi CXXXII. törvény a Nemzeti Közszolgálati Egyetemről, valamint a közigazgatási, rendészeti és katonai felsőoktatásról.

[5] http://uni-nke.hu/egyetem/rektori-koszonto

[6] http://hhk.uni-nke.hu/karunkrol/bemutatkozas

[7] http://ktk.uni-nke.hu/karunkrol

[8] http://rtk.uni-nke.hu/karunkrol

[9] http://nit.uni-nke.hu/oktatasi_egysegek/strategiai-vedelmi-kutato-kozpont/bemutatkozas

[10] TÁMOP-4.2.1.B-11/2/KMR/2011-0001 projekt megvalósíthatósági tanulmánya.

[11] Padányi József: a TÁMOP-4.2.2/B-10/1-2010-0001 projekt összefoglaló jelentése, NKE, 2014.

Dr. Bognár Balázs

A létfontosságú rendszerek és létesítmények védelmének nemzeti szabályozása

A katasztrófavédelem megújult szervezeti felépítésben a BM OKF Országos Iparbiztonsági Főfelügyelőségen belül kiemelt területként jelentkezik a létfontosságú rendszerek és létesítmények védelmével kapcsolatos feladatok ellátása, a potenciális kritikusi infrastruktúra elemek beazonosítása, valamint a kijelölt elemek hatósági felügyelet alatt tartása.

2008-ban jelent meg a kritikus infrastruktúrák azonosításáról és kijelöléséről, valamint ezek védelmi fejlesztéseinek szükségességéről szóló 2008/114/EK tanácsi Irányelv, melyet tagállami kötelezettségünk átültetni a hazai jogrendbe. A hazai Zöld Könyv megjelenése után 2010-ben kapott új lendületet a hazai létfontosságú rendszerek és létesítmények védelmével kapcsolatos szabályozások kidolgozása. A 1049/2010-es kormányhatározat a belügyminiszter hatáskörébe utalta a nemzeti kapcsolattartó pont feladatait és az európai kritikus infrastruktúrák védelmével kapcsolatos kérdések koordinálását. 2012-ben létrejött egy tárcaközi bizottság, mely az energetikai és közlekedési szektor vonatkozásban kidolgozta az azonosítási kritériumokat és felmérte a hazánkban található európai uniós kritikus infrastruktúrákat.

A BM OKF Országos Iparbiztonsági Főfelügyelőség tevékenységi körén belül kiemelt helyet foglal el a kritikus infrastruktúra védelmi szakterület, melynek egyik fő tevékenységét a jogalkotási és szabályozási feladatok végrehajtása képezi. Ennek eredményeképpen 2013. március 1. napján hatályba lépett a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény, valamint a hozzá kapcsolódó 65/2013. (III. 8.) általános végrehajtási kormányrendelet. A jogszabály célja egyrészt a létfontosságú rendszerelemek azonosítása, másrészt a kijelölés megtörténte után a megfelelő szintű - humán, fizikai és informatikai - védelem biztosítása.

A törvény az alapvető fogalmak meghatározásán túl – többek között – rendelkezik a nemzeti és az európai létfontosságú rendszerelemek kijelöléséről, az üzemeltetői biztonsági terv-készítési kötelezettségről, a biztonsági összekötő személy kijelöléséről, a nyilvántartás és ellenőrzés szabályairól, a szankcionálásról.

A létfontosságú rendszer elemek azonosítási és kijelölési szabályait tartalmazó ágazati jogszabályok hatálybalépésétől kezdve 180 nap áll rendelkezésre az üzemeltetőknek az azonosítási jelentéseik elkészítésére, melyeket az ágazati kijelölő hatóságok az ágazati kritériumok alapján, míg a katasztrófavédelem a horizontális kritériumok alapján vizsgálnak.

A létfontosságú rendszerek és létesítmények beazonosítása eredményeképpen kialakul a rendszereknek (és rendszer elemeknek) az a köre, melyek hálózatbiztonságát a jövőben a katasztrófavédelem hivatott felügyelni, ugyanis a törvény a hivatásos katasztrófavédelmi szerv központi szerve feladatkörébe helyezte a létfontosságú rendszerelemek védelmével kapcsolatos hálózatbiztonsági intézkedések koordinációját, a hálózatbiztonság fenntartásának elősegítését, és a hálózatbiztonsággal kapcsolatos események elemzését, értékelését. Ezen feladatokat erősítette az elektronikus információs rendszerek kormányzati eseménykezelő központjának, ágazati eseménykezelő központjának, valamint a létfontosságú rendszerek és létesítmények eseménykezelő központja feladat- és hatásköréről szóló 233/2013. (VI. 30.) kormányrendelet hatálybalépése is.

Fenti feladatok ellátására a BM OKF megtette az első lépéseket. 2013. március 19-én átadásra került és megkezdte működését az Országos Iparbiztonsági Főfelügyelőség keretein belül a Létfontosságú Rendszerek és Létesítmények Informatikai Biztonsági Eseménykezelő Központja (LRLIBEK), egyelőre elsősorban iparbiztonsági események kezelésével, gyakorlatok, ellenőrzési akciók koordinálásával. Emellett folyamatosan bővíti a hálózatbiztonsági szakmai tevékenységet és a bevont rendszerek körét, és kialakítja a működési protokollokat, szabályrendszereket. Az LRLIBEK a magyar és

nemzetközi hálózatbiztonsági szervezetektől a Kormányzati Eseménykezelő Központon keresztül kapott riasztások kezelésére – a nemzeti létfontosságú rendszerek és létesítmények érintettsége esetén – számítástechnikai sürgősségi reagáló egységként működik folyamatos rendelkezésre állással.

Az elmúlt időszakban számos olyan – iparbiztonsági szakterületet érintő – esemény következett be, melynek kezelése, felszámolása során a BM OKF-en kialakított eseménykezelő központ hathatós szakmai háttértámogatást nyújtott.

A villamosenergia-rendszer jelentős zavara és a villamosenergia-ellátási válsághelyzet esetén szükséges intézkedésekről szóló 285/2007. (X. 29.) Korm. rendeletnek megfelelően – a Rotációs Kikapcsolási Rendben szereplő – alapvető és létfontosságú felhasználók körét a megyei (fővárosi) katasztrófavédelmi igazgatóság állapítja meg. A Rotációs Kikapcsolási Rend kötelező felülvizsgálata és aktualizálása, valamint az elmúlt időszak gyakorlati tapasztalatai alapján az alapvető és létfontosságú felhasználók besorolása érdekében 2007. évben kidolgozott első szempontrendszer felülvizsgálata és módosítása – az energetikai szakemberekkel egyeztetetten – 2011-ben kezdődött meg és 2012-ben készült el. Az alapvető és létfontosságú felhasználók kijelölési eljárásáról szóló új, 98/2012. sz. főigazgatói intézkedés alapján a fővárosi és megyei katasztrófavédelmi igazgatóságok pontosították és kijelölték a védett fogyasztók körét, így megújításra kerülhetett a Rotációs Kikapcsolási Rend, melyet a Magyar Energetikai és Közmű-szabályozási Hivatal 2013-ban hagyott jóvá.

Az elmúlt években nagy hangsúlyt fektettünk a nemzetközi szakmai tevékenység előmozdítására. Számos kritikus infrastruktúra védelmi szakmai találkozókon képviseltettük magunk, ahol lehetőség nyílt a tapasztalatok, a legjobb gyakorlatok megosztására. A társszervekkel és tudományos testületekkel kiváló az együttműködést alakítottunk ki, melynek köszönhetően hatékonyabban előmozdítható a szabályozás megvalósítása.

A létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvényben és a hozzá kapcsolódó 65/2013. (III. 8.) Korm. rendeletben, valamint az energetikai létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 360/2013. (X. 11.) Korm. rendeletben foglalt feladatok végrehajtásához kapcsolódóan 2014. január 1-el várhatóan további 9 ágazati kormányrendelet (Közlekedés, Agrárgazdaság, Egészségügy, Pénzügy, Ipar, Infokommunikációs technológiák, Víz, Jogrend – Kormányzat, Közbiztonság - Védelem) lép hatályba.

A katasztrófavédelem szervei az uniós és a nemzeti azonosítási, kijelölési eljárás során szakhatóságként , nyilvántartó hatóságként , javaslattevő hatóságként , meghatározott monitoring, ellenőrzési , koordinatív , nemzeti kapcsolattartó és hálózatbiztonsági elemző-értékelő feladatokat látnak el 2014-ben.

Összességében elmondható, hogy a létfontosságú rendszerekkel és létesítményekkel jogszabályok elfogadása megfelelő alapot biztosít ahhoz, hogy Magyarország komoly lépéseket tegyen a létfontosságú rendszerek és létesítmények védelme érdekében.

Dr. Bognár Balázs PhD tű. alezredes
kritikus infrastruktúra koordinációs főosztályvezető

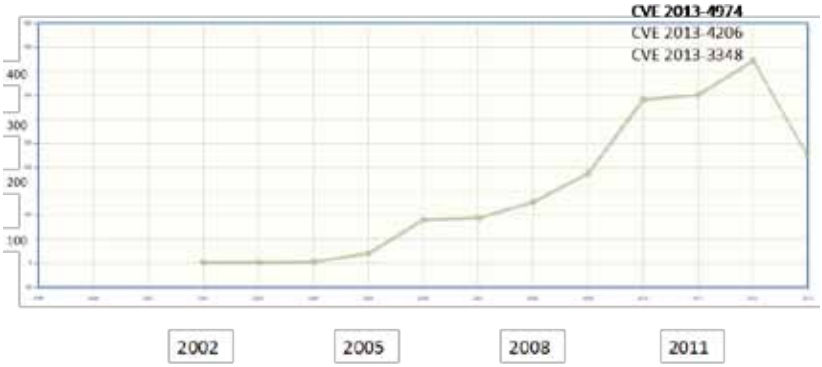
Erdődi László

Memória korrupciós sérülékenységek kiaknázási lehetőségei

Az előadás témája a memória korrupciós sérülékenységek kiaknázási lehetőségei. A memória korrupció a szoftver sérülékenységek egyik legveszélyesebb formája. Jobb esetben a támadó a hiba kiaknázásával „csak" szolgáltatás-megtagadásra tudja kényszeríteni a szoftvert, rosszabb esetben a támadó képes lehet akár tetszőleges támadó kódsorozat lefuttatására az operációs rendszeren akár távolról is. Az előadás áttekinti a memóriakorrupciós sérülékenységek kiaknázásának változását a kilencvenes évektől napjainkig, emellett bemutatásra kerülnek a legújabb kutatási eredményeink a témában.

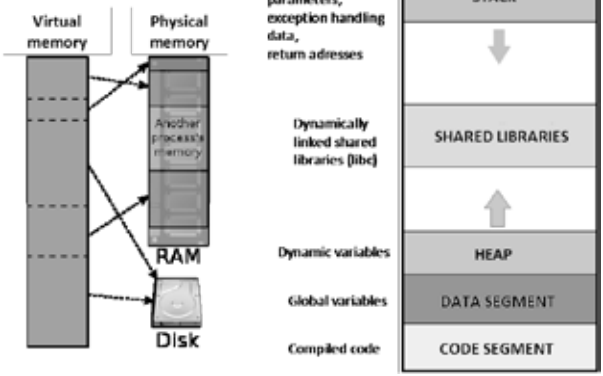
A memória korrupció története egészen a nyolcvanas évek közepéig nyúlik vissza. Az első puffer-túlcsordulásos hibát a unix sendmail programjában használták ki. Az ilyen típusú sérülékenységek száma azóta is folyamatosan növekszik. A kilencvenes évektől kezdve számos szoftverhibát sikerült kihasználni az Interneten keresztül is. A CVE adatbázis a 2000-res évek elejétől kezdve tartalmazza a memória korrupcióra visszavezethető 0day sérülékenységek regisztrált számát. Ez a szám láthatóan folyamatosan növekszik.

A 2013-as évre vonatkozó adat még nem végleges. Három 0day sérü-



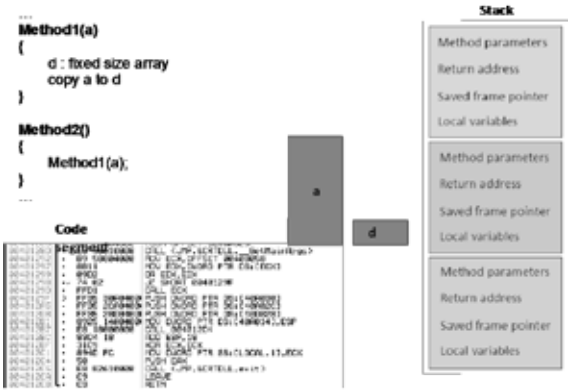
lékenység külön feltűntetésre került a legújabbak közül. Ebből az egyik a PUTTY program egy hibája, a második a real player lejátszó egy sérülékenysége és szintén idei az acrobat egy 0day sérülékenysége. Ezek a hibák nem kis szoftverekben vannak jelen. Egy rosszindulatú támadó olyan szoftverekhez készíthet támadó kódokat amelyet milliók használnak. Nagyon fontos, hogy folyamatosan vizsgáljuk ezeket a hibákat, hogy megértsük miért születnek, hogyan változnak és hogy lehetőség szerint megjósoljuk milyen formában fordulnak majd elő a jövőben.

Tekintsük a memória korrupciós sérülékenységek okait. Amikor az operációs rendszer elindít egy folyamatot, nincs információja arról, hogy a folyamat mennyi memóriát igényel. Szoftverjeink interaktívak, a memóriaműveletek jelentős része futásidőben történik. Mindezek miatt az operációs rendszer egy jelentősen nagy memóriát foglal minden egyes folyamatnak virtuálisan. Valójában minden folyamatnak csak annyi memória van foglalva a memóriában amennyit éppen használ. A virtuális és a fizikai memória közötti konverziót az operációs rendszer végzi futásidőben. Egy folyamat futása során metódusok hajtódnak végre. A szálak a saját stack szegmenesüket használják a metódus-végrehajtási adatok (metódusok paraméterei, visszatérési cím, lokális változók) tárolására. A dinamikus memóriaműveletek a heap szegmensen történnek, melyeket láncolt listában tárol a folyamat. A virtuális memóriában így az adat és a kód együtt található, amely számos komoly kihívást és veszélyforrást jelent. A virtuális memória számos olyan érzékeny részt tartalmaz, amely során akár egy adat megváltoztatása módosíthatja a program



rendeltetésszerű futását. Ha a forráskód nem tökéletes a rosszindulatú támadó beavatkozhat a folyamat futásába és egy számára kedvező nem betervezett használat-esetet kényszeríthet ki.

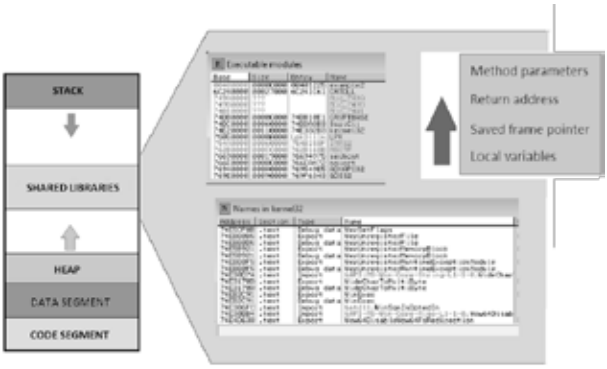
A memóriakorrupció számos formája ismert. A stack korrupciója a metódus visszatérési címének átírása miatt vagy a kivételkezelés hibája miatt következik be, heap korrupció (pl. double free vagy use-after-free sérülékenységek pl. heap spray.vel kombinálva) esetén a heap adatait tároló láncolt lista egy mutatója kerül felülírásra.



A jobbra lévő ábrán tekintsük át a klasszikus puffer-túlcsordulásos sérülékenységet a 90-es évekből. A metódusok a folyamatban egymás után hajtódnak végre és a metódus adatai a stacken tárolódnak. Az ábrán az látható, hogy az egyes metódus a kettes metódusból lett meghívva összesen egy paraméterrel, amelynél viszont nem történ semmilyen méretellenőrzés. A paraméter megfelelő megválasztásával a metódus visszatérési címét felül lehet írni és ez vezet a program rendeltetésszerű használatának megváltozásához. Később a hasonló jellegű hibák kikerülése miatt a fordítók bevezették a stack cookie használatát. A stack cookie-t a fordító a metódus visszatérési címe és a metódus lokális változói közé helyezi, így ha a támadó túlírja a lokális változók értékeit nem csak a visszatérési cím, de a stack cookie értéke is megváltozik. Az operációs rendszer minden metódusból való visszatérés során ellenőrizni tudja hogy megváltozott-e a stack cookie értéke a metódus futása során és amennyiben igen, úgy leállítja a folyamatot. A Microsoft Visual Studio fordítója pl. a GS jelzőflaget használja az előbbi feladatra. Figyelembe véve azonban a szükséges időtöbbletet amelyet a stack cookie kétszeri kiolvasása és

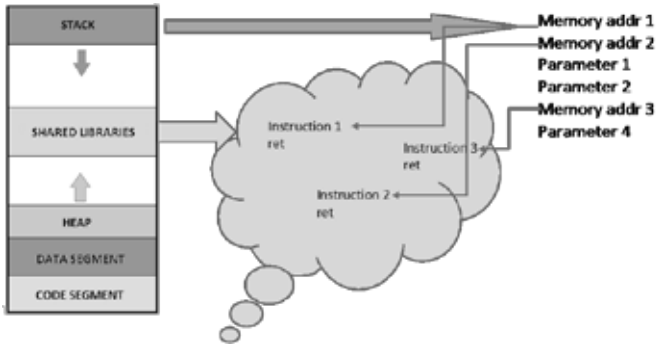
összehasonlítása jelent minden egyes metódus-végrehajtás során, egyértelmű, hogy a stack cookie használata erősen a sebesség rovására megy. Emiatt a fordítók optimalizálják a stack cookie-k használatát, tehát nem minden esetben kerülnek bele a metódus stack keretébe. 2005-ben az Internet Explorer esetén már megtörtént, hogy egy ilyen stack cookie optimalizáció vezetett egy sérülékenységhez.

Sok esetben a támadónak nincs szüksége arra, hogy saját támadó kódot írjon. A kernel önmagában is számos veszélyes metódust tartalmaz, amennyiben egy metódus visszatérési címét át lehet írni valamely veszélyes kernel függvény (pl. winexec) címére, akkor a támadónak már csak a metódus megfelelő paraméterekkel történő meghívásáról kell gondoskodnia. Az ilyen típusú támadást „return to libc" támadásnak nevezik. A jobbra látható ábrán a kernel32.dll exportált metódusainak egy része látható a címeikkel együtt. Szerepel köztük a winexec címe is.



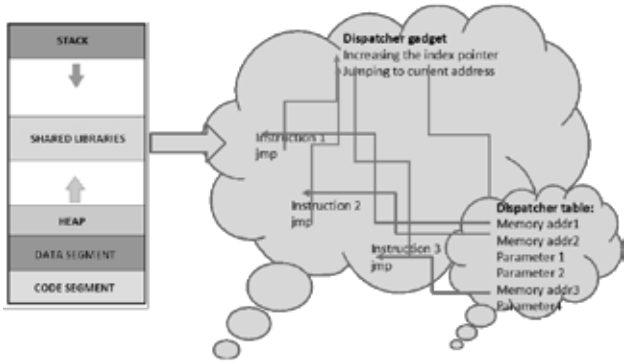
A return to libc támadásnak számos korlátja van a támadó szempontjából. Habár a kernel számos hasznos metódust tartalmaz támadási szempontból, ugyanakkor mégsem képes a támadó tetszőleges kód végrehajtására, mivel összesen egy kernel metódust van lehetősége meghívni. 2007-ben áttörés történt ezzel kapcsolatban a Return Oriented Programming (ROP) megjelenésével. Kiderült, hogy nincs is szükség egyáltalán támadó kód írására, mivel a támadó kód összerakható apró részletekből (gadgetek) amelyek egyébként is benne vannak a folyamat virtuális memóriájában. Egy gadget általában az osztott könyvtárak egy apró kódrészlete amely egy vagy több apró a támadó számára hasznos assembly utasításból és egy ezt követő assembly ret utasí-

tásból áll. Amennyiben a támadó kódot apró assembly utasítások sorozatára bontjuk fel és mindegyikhez találunk megfelelő gadget-et a memóriában, úgy a támadó kód lefuttatható egyszerűen a gadgetek címeinek és paramétereinek stackre történő egymás utáni írásával. Ez esetben minden lépés során a program futása a stack tetején lévő címre ugrik. Amennyiben az adott címen lévő gadgetnek paraméterre van szüksége, azt fel tudja venni a stackről. A gadget végén lévő ret utasítás pedig gondoskodik a következő gadget végrehajtásáról, így tehát a gedgetek egymás után lefutnak. A Return Oriented Programming bizonyítottan Turing teljes, így tetszőleges támadó kód (amely összerakható a memóriában lévő utasításokból) lefuttatható vele.

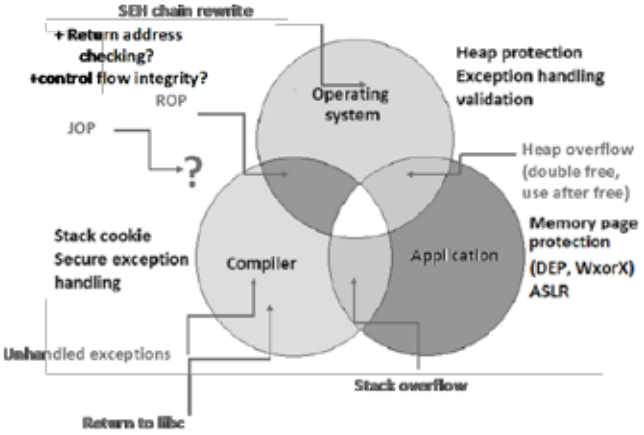


2011-ben a Return Oriented Programming egy általánosítását publikálták, ez a Jump Oriented Programming. A stack szegmens és a ret utasítások egyáltalán nem szükségesek a Jump Oriented Programokhoz. A támadó kód ebben az esetben is apró assembly kódrészre van felbontva, de egy-egy gadget nem ret utasítással hanem egy úgynevezett „indirect jump" utasítással végződik. A stack helyett a Jump Oriented Programming a dispatcher gadgetot használja, amely egy a memóriában található virtuális táblázatból folyamatosan kiolvassa a következő gadget címét és a program futását erre a címre irányítja. A gadgetek végén található indirect jump utasításoknak köszönhetően minden gadget végrehajtása után a vezérlés visszakerül a dispatcher gadgethoz. A Jump Oriented Programming is Turing teljes és a legtöbb védekező mechanizmus hatástalan ellene beleértve azokat is amely a Return Oriented Programming esetén működtek (pl visszatérési cím ellenőrzők).

Foglaljuk össze mi tud védelmet nyújtani a memória korrupció ellen. Az ideális eset az lenne, ha a szoftverek egyáltalán nem tartalmaznának hibákat.



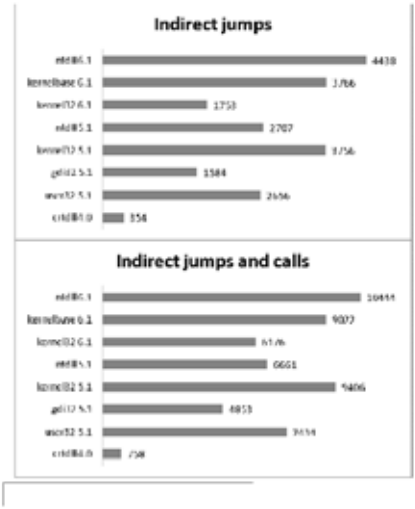
Ettől eltekintve viszont az alábbi ábrán látható módon három dolgot lehet említeni amelynek szerepe lehet a memóriakorrupció elleni védekezésben. Az alkalmazás számos dolgot tud megtenni a biztonságért, pl. az egyes memória lapokat vagy csak olvashatónak vagy csak végrehajthatónak beállítva. De a return to libc támadásoktól kezdve ez hatástalan, mivel nem kerül ténylegesen végrehajtandó kód adatokat tartalmazó szegmensrészre. A címtér randomizálás is valamely védelmet nyújthat, de gyakran ez is megkerülhető. A fordító is számos védelmet biztosíthat, pl a stack cookie elhelyezésével, de ez sem tökéletes védelem az stack cookie optimalizáció miatt. Végül az operációs rendszer is védekezhet, mint pl. a heap esetében. Mit nyújt valójában védelmet a legújabb támadás típusok pl. a Jump Oriented Programming ellen? További két védekezési módszert meg lehetne említeni, amely a gyakorlatban kevéssé elterjedt: ebből az egyik a visszatérési cím ellenőrzés (return address checking) és a



teljes vezérlés ellenőrzés (control flow integrity). A visszatérési cím ellenőrzés megfelelő Return Oriented Programming esetén, de a Jump Oriented Programokkal szemben hatástalan. A teljes vezérlés ellenőrzés elméletben minden ellen hatásos, de az erőforrásigénye óriási.

A továbbiakban a saját eredményeinket mutatjuk be. A Jump Oriented Programming jó megoldásnak tűnik a memória korrupció kiaknázása során ezért a Jump Oriented Programing programok legkritikusabb részét vizsgáltuk a dispatcher gadgetokat. A kutatás célja az volt, hogy megkeressük a dispatcher gadgetként is funkcionáló memóriarészeket a különböző kerenelekben. A Windows xp, 7 és 8 valamint különböző ubuntu verziókat vizsgáltunk. A kérdésre a válasz, hogy egyértelműen léteznek ilyen kódrészek a gyakorlatban is. A feltűntetett táblázatban látható néhány ezek közül.

File	Address	Opcode
crtdll.dll 5.1.2600	73d3a066	add ebx,0x10 jmp dword ptr ds:[ebx]
crtdll.dll 5.1.2600	73d3a0f2	add ebx,0x10 jmp dword ptr ds:[ebx]
user32.dll 5.1.2600	77d63ae9	add esi,edi jmp dword near [esi-0x75]
ntdll.dll 5.1.2600	7c939bbd	add ebx,0x10 jmp dword near [ebx]
ntdll.dll 5.1.2600	7c93c4db	sub edi,ebp call dword near [edi-0x18]
kernelbase. dll 6.2	75e6e815	sub esi,edi call dword near [esi+0x53]
ntdll.dll 6.2	77c94142	add ebx,0x10 jmp dword near [ebx]
ntdll.dll 6.2	77ca8c9	add ecx,edi jmp dword near [ecx+0x30]
ntdll.dll 6.2	77ca9dc0	add eax,edi call dword near [eax-0x18]
ntdll.dll 6.2	77cbcaca	add ebx,edi call dword near [ebx+0x5f]

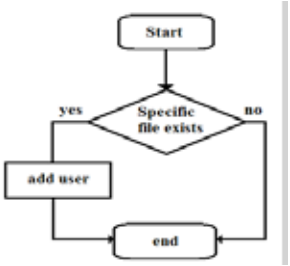


Példaképpen elkészítettem egy Jump Oriented Programot windows xp-re amely a winexec metódus hívja meg adott paraméterekkel. A feladathoz mindössze néhány gadget-ra volt szükség. Mivel mind a Return Oriented és mind a Jump Oriented programming Turing teljes, így a következő szerkezetek végrehajtására kell alkalmasnak lenniük: adat olvasása és írása a memóriából, feltételek kiértékelése, ciklusok végrehajtása, metódus hívások. Kutatá-

Address from the beginning of the dispatcher table	Value	Opcode	Function
0x00	77d65dda	pop eax std jmp ecx	sets eax to WinExec
0x10	77d5fa07	add esi,edi jmp ecx	sets esi to command string
0x20	77d482f6	xor edi,edi jmp ecx	zero edi
0x30	7c81ebb8	push edi jmp ecx	push zero on the stack
0x40	77d62d94	push esi std jmp ecx	push command string on the stack
0x50	7c9409ce	xchg esi,eax std jmp ecx	sets esi to WinExec

0x60	7c8306f0	mov edi,ebp jmp ecx	sets edi to dispatcher gadget
0x70	77f45ce1	call esi jmp edi	execute WinExec
0x80	77d482f6	xor edi,edi jmp ecx	zero edi
0x90	7c81ebb8	push edi jmp ecx	push zero on the stack
0xa0	77d65dda	pop eax std jmp ecx	sets eax to ExitProcess
0xb0	7c9409ce	xchg esi,eax std jmp ecx	sets esi to ExitProcess
0xc0	7c8306f0	mov edi,ebp jmp ecx	sets edi to dispatcher gadget
0xd0	77f45ce1	call esi jmp edi	execute ExitProcess

sunk során megvizsgáltuk, hogy lehetséges feltételes utasításokat végrehajtani Return Oriented Programokkal a gyakorlatban. Három különböző módszert vizsgáltunk, ebből az elsőt az eredeti Return Oriented Programmingról szóló cikkben publikálták. A második és harmadik saját megoldás volt. Az alábbi ábrán látható blokkdiagramban látható utasítássorozatot próbáltuk végrehajtani. Ha egy adott nevű fájl létezik, a program hozzáad egy felhasználót a rendszerhez, végezetül pedig bezárja a folyamatot. A gyakorlati megvalósításhoz sikerült mindhárom feltételes utasítás végrehajtáshoz megfelelő gadget-okat találni, az utolsó megoldás mindösszesen 5 gadget-ot igényelt.



Végezetül megvizsgáltuk milyen egyszerűsített módon lehetne leírni a return oriented és a jump oriented programokat. Természetesen már léteznek olyan eszközök amelyek hasonló célt szolgálnak, de ezek előre meghatározott feladatokra tudják csak a Return Oriented programokat összeállítani. A bemutatott megoldásunk tulajdonképpen egy leíró nyelv, amellyel tetszőleges támadó kód egyszerűen leírható és könnyen állítható elő belőle Return Oriented és Jump Oriented program. Gadget-ekre van szükség pl. arra hogy adatot írjunk az

adat szegmensre. Egy 32 bites rendszeren egyszerre 4 byte-nyi adat írható a memóriában néhány gadget-tal. Ha a memóriacím vagy az adat nullát is tartalmaz ehhez akár 7 gadget végrehajtására is szükség lehet. Erre bevezettük a write4 leírást, amely pont ezeket a gadget-ek keresi meg és állítja megfelelő sorrendbe. A write utasítás hosszabb adat kiírására is alkalmas, ez az utasítás a write4 alapján dolgozik, és sok gadget-ot foglal magába. A „net user add" string memóriába történő írása egyetlen sorral megadható a leíró nyelvünkkel. Ugyanilyen megfontolásokkal bevezettük a feltételes utasítás és a metódushívás egyszerűbb leírását is a Return és Jump Oriented programokhoz. Ezzel a módszerrel a Return Oriented és a Jump Oriented programok leírása is lényegesen egyszerűbb lett. Az alábbi ábrán látható mintaleírás kiírja a try.txt stringet az adatszegmensre, meghívja az fopen metódust. Amennyiben ennek visszatérési értéke nulla (nem létezik a fájl) kilép a folyamatból, egyébként pedig hozzáad egy felhasználót a rendszerhez.


```
1: write:dataseg_addr1:filename_string          write:00400000:try.txt
2: call:fopen_address:dataseg_addr1:filemod     call:7c560122:00400000:0
3: if:address_of_gadget_cmp eax,0:6:4           if:77c7d230:6:4
4: write:dataseg_addr2:name of executable       write:00400010:net user user1 pwd1 /add
5:call:winexec_addr:dataseg_addr2               call:7d77501c:0400010
6:call:exitprocess_addr                         call:7c210254
```

Az előadás során a memória korrupciós hibák kiaknázásának számos módját tekintettük át bemutatva saját kutatási eredményeinket is a témában. Az elhangzottak ellenére látható, hogy számos kérdés még nincs megoldva a témában.

Felhasznált Irodalom

[1] S. Hacham, „The geometry of innocent flesh on the bone: Return-into-libc without function callc (on the x86)", Proceedings of CCS 2007, ACM Press, 552-561

[2] T. Bletsch, X. Jiang, and V. W. Freeh, "Jump-oriented programming: a new class of code-reuse attack," ASIACCS ,11, Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security, ACM New York, NY, USA pp. 30-40, March 2011.

[3] R. Roemer, E. Buchanan, H. Shacham and S Savage, "Return- oriented programming: systems, languages and applications" ACM Transactions on Information and System Security, Vol. 15, No. 1, Article 2 pp:1-34, March 2012

[4] P. Chen, X. Xing, B. Mao, L Xie, X. Shen and X. Yin, "Automatic construction of jump-oriented programming shellcode (on the x86) ASIACCS ,11, Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security, ACM New York, NY, USA pp. 20-29, March 2011.

[5] L. Davi, A. Sadeghi and M. Winandy, "ROPdefender: A detection tool to defend against return-oriented programming attacks" ASIACCS ,11, Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security, ACM New York, NY, USA pp. 40-51, March 2011.

[6] M. Kayaalp, M. Ozsoy, N. Abu-Ghazaleh and D. Ponomarev, "Branch regulation: low-overhead protection from code reuse attacks", ISCA ,12 Proceedings of the 39th Annual International Symposium on Computer Architecture, IEEE Computer Society Washington, DC, USA, pp 94-105, 2012.

[7] J. Li, Z. Wang, X. Jiang, M. Grace and S. Bahram, "Defeating return-oriented rootkits with „return-less" kernels", Proc. of the 5th ACM European Conference on Computer Systems , Paris, France, pp. 195-208, April 2010.

[8] J. Min, S. Jung, D. Lee, T. Chung, "Jump oriented programming on Windows platform (on the x86)", ICCSA 2012, Part III, LNCS 7335, pp. 376-390, Springler Verlag, 2012

[9] L. Erdődi, "Finding dispatcher gadgets for jump oriented programming code reuse attacks", INES 2013 • IEEE 17th International Conference on Intelligent Engineering Systems • June 19-21, 2013, Costa Rica, pp. 333-338

[10] L. Erdődi, "Attacking X86 windows binaries by jump oriented programming", 8th IEEE International Symposium on Applied Computational Intelligence and Informatics • May 23–25, 2013 • Timisoara, Romania, pp. 321-325

[11] http://cvedetails.com

Dr. Bencsáth Boldizsár, dr. Buttyán Levente, Kamarás Roland, Ács-Kurucz Gábor, Molnár Gábor

Az információgyűjtés feladata és lehetőségei informatikai támadások megelőzése és kezelése céljából

A Budapesti Műszaki és Gazdaságtudományi Egyetem Hálózati Rendszerek és Szolgáltatások Tanszékén működő CrySyS Adat- és Rendszerbiztonsági Laboratórium több, mint tíz éve tevékenykedik az adatbiztonság területén. Nagy sajtóvisszhangot célzott malware támadások kezelése kapcsán kapott: 2011-ben a laboratórium publikált először részletes vizsgálati eredményeket az általuk Duqu névre keresztelt malware-ről, amelyet ismeretlenek célzott támadásokra használtak Európában és későbbi adatok alapján közelkeleti célpontok vonatkozásában is. Később több más, vélhetően államok által támogatott malware alapú célzott támadással is foglalkozott a laboratórium, ilyenek a Flame, melynek áldozatai főként a Közel-Keleten voltak, később 2013-ban a MiniDuke és TeamSpy támadássorozatok.

Az ilyen támadásokkal kapcsolatos információszerzést ma az ún. „malware threat intelligence" néven összegezhetjük, ami azt jelenti, hogy olyan információgyűjtést kell végezni, amelyik hasznosítható, döntésre előkészítő információt képes összegyűjteni malware alapú támadások esetében.

Vizsgálataink során sokszor működtünk együtt különféle partnerekkel, osztottunk meg információt, és kaptunk is hasznos adatokat. Ennek kapcsán megismertünk, kitanultunk és kialakítottunk egyfajta metodológiát, amely a hasznos információk hatékony összegyűjtésére vezet. Ennek kapcsán mutatunk be cikkünkben néhány kulcspontot, eszközt, trükköt, amelyek segíteni tudják az információgyűjtés folyamatát.

Ezen a területen sem lehet megmondani, hogy mi a legjobb következő lépés, így mi sem egy receptkönyvet kívánunk adni,hanem ötleteket és eset-

tanulmányokra épülő tapasztalatokat, amelyek segíthetnek a hatékony ügykezelésben.

Threat Intelligence

A threat intelligence, vagyis a fenyegetésekkel kapcsolatos hírszerzés célja, hogy a támadók kártékony aktivitásáról információkat tudjon összegyűjteni a következő célok szerint:

- az információk belső és külső információforrásokból származhatnak,
- az információforrások lehetnek nyilvánosak és bizalmasak is,
- a cél annak megértése, hogy mi történik egy rendszerben, ennek egy része technikai jellegű információgyűjtés, pl. malware elemzés, de nagyrésze egyéb információgyűjtési feladat,
- minél több forrást érdemes használni, hogy a begyűjtött információ (kiértékelve a forrásokat) a lehető legpontosabb legyen.

A folyamatnak olyan különleges célokat is figyelembe kell vennie, mint például az, hogy az információgyűjtés nem szivárogtathat információkat a támadók irányában. Informatikai területen ez egy különösen bonyolult probléma: egy DNS bejegyzés lekérdezése, egy weblap elérése, vagy bármilyen email rögtön riaszthatja a támadót, hogy valaki vizsgálja a támadási folyamatot, és így a vizsgálat könnyen befolyásolhatja a vizsgált tevékenységet is.

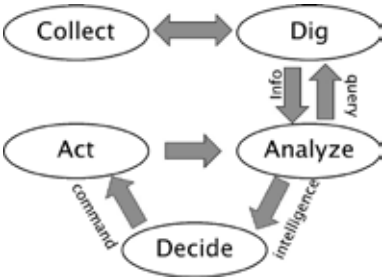
Milyen kérdésekre várunk választ az információgyűjtés folyamatában?

Teljes listát nehéz készíteni, de az alábbiak mindenképpen a célterületbe tartoznak:

- Milyen fenyegetéssel nézünk szembe?
  - Milyen eszközöket használ a támadó?
  - Mekkora a támadók erőforrásainak mértéke?
  - Mi lehet a támadó célja?
  - Attribúció – ki is lehet a támadó?
- Mik a veszélyek a mi oldalunkon?
  - Milyen tulajdonaink vannak, amiket támadhatnak?

- Mi történhet, ha a támadás folytatódik?
- Mi legyen a válasz?
  - Mi a leghatékonyabb út, hogy kezeljük az ügyet?
  - Kivel kell információt megosztani, kit kell figyelmeztetni, hogy hasonló támadások történhetnek?
  - Mi legyen a válasz a támadásra, és mi történjen ezután?

A hatékony információgyűjtés folyamatát ezen a területen egy több kört tartalmazó folyamatábrával szemléletetjük.



Információgyűjtés tevékenységei és összefüggései

A jobbra látható folyamat elemei a következők. A malware alapú célzott támadásoknál többnyire van adat előzményekről, ésa támadó sokszor újra felhasználja korábbi eszközeit, ezért a vizsgálatok során fel kell használnunk minden eddigi összegyűjtött tudásunkat. Ezt fejezi ki a „collect" tevékenység. Folyamatosan adatokat gyűjtünk, amelyeket nagy adatbázisokban tárolunk. Ilyen adatok lehetnek IP címek, de még inkább korábban használt malware minták milliói. Ez a „bigdata", az a nagy adat, amelyben kutatva olyan információk kerülhetnek elő, amelyek máig felhasználhatóak lehetnek.

Természetesen a legnagyobb baj a nagy adattárakkal az, hogy önmagukban értéktelenek. Ki kell nyerni belőlük az információt, ezt hivatott jelölni az ábrán a „dig" adatkinyerési tevékenység. Ez az a folyamat, amiben a kutató valamilyen elvek alapján kapcsolódó adatokat keres, megpróbál további információkat kinyerni az általa vizsgált folyamatról.

Az adatkinyerés célja, hogy valamilyen vizsgálati módszerek, keresési kifejezések, vagy más jelölők segítségével a nagy adatbázisból ki tudjon gyűjteni minden olyan információt, amelyek érdekesek, hasznosak lehetnek a vizsgálat kapcsán. Tipikusan mindenféle olyan minta, amely vélhetően kapcsolatban lehet a vizsgált támadással. Természetesen sok téves pozitív találat is lehetsé-

ges, ahol a kinyert mintának valójában nincs semmi köze a támadáshoz, de az már a vizsgálatot végzők feladata, hogy ezen hibákkal foglalkozzanak.

Amint az adatbányászati folyamatban kigyűjtésre kerültek az aktuális analízishez („analyze") kapcsolódó információk, a kiértékelési rendszerbe kerül az információ, mint minden más adat a támadásról. Az információk gyűlnek: új kérdések merülnek fel, újra és újra adatokat gyűjtünk a nagy adatbázisból a kigyűjtött információk alapján finomítva lekérdezéseinket. Ez a körkörös folyamat egész addig folyik, mígnem elég adatot gyűjtünk arra, hogy előkészüljünk egy döntéshez. A döntéseket egy „actionable intelligence" azaz döntésre is használható információgyűjtés előzi meg, pontosan ezen a folyamaton estünk túl. Ha elég információ gyűlt össze, akkor előkészíthetünk döntéseket a támadásokkal kapcsolatban.

A döntések lehetnek nagyon aprók is: Tiltsunk ki egy IP címet a hálózatunkból. Hiába apró a döntés, óriási súlya van. Amint egy támadót kitiltunk, felismerheti, hogy vizsgálják támadását. Egy egyszerű tiltás kapcsán is előfordulhat, hogy a támadó nemcsak nyomait, hanem a célrendszerek fontos adatait is letörli, vagy bármilyen más olyan reakcióval lép fel, ami súlyos gondokat okozhat.

Nem lehet tehát átgondolatlan lépéseket tenni, még a legegyszerűbb esetben sem. Sajnos az incidenskezelők feladata a lehetetlenséget közelíti, hiszen meg kellene jósulniuk a kimenetelt minden döntés kapcsán, legyen az egy egyszerű tiltás, újraindítás vagy törlés.

A folyamatábrában a döntést egy művelet elvégzése („act") kísérheti, amely visszahat a kiértékelés („analyze") folyamatra, és így minden döntés és művelet változtat az egész elvégzésén is, majd természetesen visszahat az analízis-bányászat-tárolás folyamat körére is.

Milyen információkat használatunk fel a folyamat során?

Cégen belüli ellenőrző eszközök információi

- AV (anti-virus) termékek
- IDSs (IntrusionDetection Systems) and SIEMs (SecurityIncident and

Event Management Systems) adatai
- log analízis eszközök eredményei
- DNS monitorozás
- honeypots (csapdák, csapdaszámítógépek, csapdarendszerek)
- külső forrásokból származó információk: biztonsági szervezetek, projektek, vendorok, egyetemek, CERT-ek, non-profit szervezetek, vagy akár elhivatott egyénektől származó információk (lehetnek nyíltak, zártak, vagy kereskedelmileg elérhetőek), minta gyűjtemények: malware minták, domainek, IP feketelisták stb.

Összességében elmondhatjuk, hogy információforrások tekintetében nincs hiány. Többnyire nem az a gond, hogy nincs lehetőség begyűjteni egy információt, hanem az, hogy az adott szervezet nem ismeri az információforrást, vagy képtelen vele együttműködni. Szinte minden esetben az információ ott van az orrunk előtt, de fel kell ismerni, hogy az információ fontos és begyűjthető, enélkül kiaknázatlan, haszontalan marad.

Esettanulmány

2012 decemberében ismeretlen támadók támadást intéztek magyar banki ügyfelek ellen. Az ügyfelekhez phishing e-mailt küldtek, csatolt fájljuk egy futtatható fájl egy malware volt. Aki elindította, az megfertőződött, és később, ha az 5 célzott bank közül az egyiknél online banki műveletet végzett, úgy a támadók meghamisíthatták akaratát, és pénzét akár más mennyiségben és más célpont felé utalhatták el, mint azt a célzott akarta.

A támadás különlegessége, hogy az injektált banki üzenetek jó magyar tudással készültek, ellentétben a tipikus, majdnem érthetetlen GoogleTranslate fordítással. A támadást hosszabb távú megfigyelés alá vettük. Berendezéseinken védett körülmények között vizsgáltunk néhány céltudatosan fertőzött virtuális számítógép viselkedését. Később, 2013 tavaszának végén arra lettünk figyelmesek, hogy a támadók valamiért az addig használt Zeus alapú támadó malware minták mellé új malware kódokat telepítettek. Ezen új kódok segít-

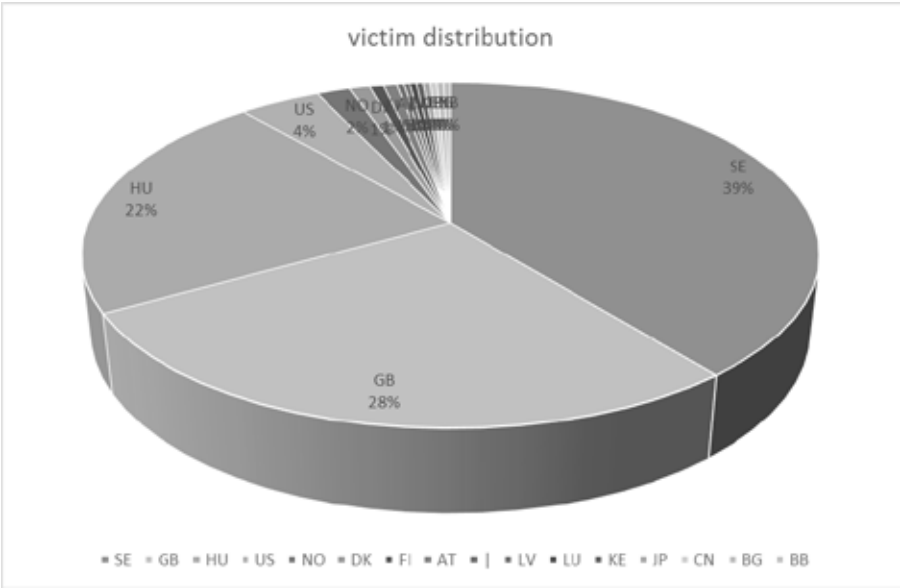
ségével számos funkció volt elérhető, legfőképpen adatlopás jellegű lehetőségek a fertőzött gépről.

Az új támadó modulok saját magukat „RCAPP" (vélhetően remotecontrolapplication) néven nevezték. Érdekes módon a fő modul Delphi nyelven írodott és egy ismert kereskedelmi SDK-t, a „RealThinClient" modult használta kommunikációra, a fejlesztők nem fordítottak sok gondot a saját fejlesztésre.

Érdekes trükkje a támadásnak, hogy a Windows registryben tárol egyes kódrészleteket kódolt formában, pl. a következő címek alatt:

- Software\Google\Update\network\secure
- Software\Adobe\Adobe Acrobat
- Software\Google\Common\Rlz\Events

A malware-nekvan VNC és Socks proxy modulja a megfelelő hálózati működés céljára.



A támadás különlegessége mégis leginkább az, hogy valamilyen oknál fogva a megfertőzött kliens, amikor bejelentkezik a vezérlőszerverre, adatokat

tölt le a többi áldozatról. Ez nem egy szokványos megoldás, hiszen így valójában a rendszer adatokat szivárogtatott hozzánk, védekezőkhöz a fertőzött gépekről.

Az adatok között szerepel a megfertőzött gépek neve, Windows verziója, adatok a gép bekapcsolásának idejéről, hálózati sebességéről.

Milyen módon és irányokból sikerült adatokat begyűjteni a támadásról?

- Technikai információkat nyertünk a támadók trükkjeiről, módszereiről, amelyek segítik a detekciót.
- Kereséseink során sikerült a nagyméretű malware adatbázisainkban hasonló mintákat keresni, köztük egy olyan mintát is, amelyben orosz nyelvű üzenetben olvasható, hogy az eszközt hogy kell bekonfigurálni. Vélhetően orosz nyelven beszélő fejlesztők kereskedelmileg értékesített szoftveréről van szó.
- A malware által begyűjtött áldozati adatok szerint .hu, .se, .uk, és .dk áldozatok voltak a legnagyobb számban.
- Az OpenDNSUmbrellaSecurityGraph rendszerében megvizsgáltuk a felhasznált C&C szerverekkelkapcsolatos lekérdezések popularitását, ami megerősítette a célterületre vonatkozó információkat.

SECURITY FEATURES

SecureRank 2 (rescaled)	3.53
ASN score	-0.25
Prefix score	-0.61
RIP score	-0.72
Popularity	11.32
Requester geo distribution	GB (25.00 %) HU (25.00 %) DK (25.00 %) US (12.50 %) SE (12.50 %)
Requester geo distribution (normalized)	HU (79.04 %) SE (9.97 %) DK (9.04 %) GB (1.83 %) US (0.12 %)

OpenDNSUmbrellaSecurityGraph adatok az RCAPP által használt egyik domain vonatkozásában

- Értesítéseink alapján és más ismeretlen folyamatok kapcsán a támadók ismert szerverei leállításra kerültek.

Összességében az ügy kapcsán elmondhatjuk, hogy az adatgyűjtés, a folyamatos megfigyelés segít az egyébként akár láthatatlan események megfigyelésében és dokumentálásában. Ha nem vizsgáljuk az ügyet, senki nem fedezi fel a fenti érdekes információkat. Azt is látni kell azonban, hogy az adatgyűjtés eredménye korlátozott, nem értettük meg, miért az adott országok voltak a célpontok, sem azt, hogy mi a támadó célja, de talán sikerült segíteni, hogy a támadás megszűnjön és az áldozatok értesüljenek a problémáról.

Fontos azt is megérteni, hogy többnyire egy kérdés megválaszolása, egy begyűjtött adat újabb és újabb kérdéseket és felvetéseket hoz, és ezek egy része soha nem kerül megválaszolásra. Normális folyamat tehát, hogyha egy vizsgálat végeredménye a hasznosítható információk mellett seregnyi megválaszolatlan kérdést is tartalmaz.

Dr. Bencsáth Boldizsár
Dr. Buttyán Levente
Kamarás Roland
Ács-Kurucz Gábor
Molnár Gábor
Budapesti Műszaki és Gazdaságtudományi Egyetem
Hálózati Rendszerek és Szolgáltatások Tanszék
CrySyS Adat- és Rendszerbiztonság Laboratórium

Gencsy Péter

Biztonságos ország – biztonságos szolgáltató

A Magyar Telekom (MT), mint vezető nemzeti telekommunikációs szolgáltató, számos szempontból az ország biztonságának is fontos tényezője. A MT a hagyományos vezetékes és mobil hang- és adatátviteli szolgáltatásokon kívül igen széles palettát nyújt ügyfeleinek, előfizetők millióihoz fűz minket kapcsolat számos szolgáltatás (internet, TV csatornák, tartalmak, TV szolgáltatások, stb.) révén.

Alapvető fontosságú, hogy egy olyan szervezet, amely tényező az ország biztonsága tekintetében, az maga is ennek erős láncszeme legyen, biztonságosan működjék és biztonsággal nyújtsa szolgáltatásait. Ezáltal tud egy biztonságos szolgáltató az ország, a lakosság biztonságáért felelős szervekkel egy erős láncot alkotni, azokkal gördülékenyen együttműködni.

A feladat nehéz, hiszen manapság számos kihívással kell az MT-nak szembenéznie, veszélyekkel kell megküzdenünk. Miért vagyunk – és a hasonló szolgáltatók is - veszélyeztetettek?

Mert

- Közép-Európa és Magyarország egyik meghatározó vállalata vagyunk,
- integrált szolgáltatásokat nyújtunk,
- jelentős értékű üzleti működés, milliárdos tenderek, akvizíciók, stb.,
- ügyfélkörünk „igazi kihívást", értékes célpontot jelenthet,
- sok millió személyes adatot és cégadatot (telekommunikációhoz kapcsolódó) kezelünk,
- nagyon sok outsourcing partnerünk, külső alvállalkozónk van (cca. 3500!), a kontrolljuk nehéz,
- sajnos nem tudunk eleget költeni a biztonságra, (Mennyi is az „elég"?)
- kritikus infrastruktúraszolgáltatók (létfontosságú infrastruktúra) vagyunk és kiszolgálunk más létfontosságú infrastruktúra szolgáltatókat és

kormányzati szerveket is.

Elsőrendű érdekünk adataink és hálózataink védelme

- Integrált szolgáltatóként elsőrendű érdekünk ügyfeleink adatainak és a hálózataink védelme.
- Védenünk kell rendszereinket saját üzleti érdekünkből is és közérdekből is, valamint egyes törvényi kötelezettségek kapcsán is.
- Szolgáltatásaink folytonosságot követelnek – kiesés üzleti veszteséget jelentene, illetve biztonsági kockázat is lehet
- Szolgáltatás leállás ügyfeleinknek, üzletfeleinknek is üzleti veszteséget jelenthet.
- A MT lehet célpont is, de a hálózatainkon keresztül is indíthatnak támadásokat

Kritikus (létfontosságú) infrastruktúrák – Törvényi háttér

- 2012. évi CLXVI. tv. a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről
- 1249/2010. (XI. 19.) Korm. határozat az európai kritikus infrastruktúrák azonosításáról és kijelöléséről
- 2080/2008. (VI.30.) Korm. határozat a Kritikus Infrastruktúra Védelem Nemzeti Programjáról
- Európai Bizottság Zöld könyv (létfontosságú infrastruktúrák védelmére)
- 2011. évi CXXVIII. tv. a katasztrófavédelemről
- 1035/2012. Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról
- 2011. évi CXII. tv. az információs önrendelkezési jogról és az információszabadságról
- 2003. évi C. tv. - az elektronikus hírközlésről

Kritikus infrastruktúra horizontális kritériumai

- Személyi veszteség (áldozatok száma)

- Gazdasági hatás (pénzügyi kár, szolgáltatásromlás)
- Társadalmi hatás (lakosság érintettsége)
- Politikai hatás (közbizalom)
- Környezeti hatás (épített vagy természeti környezet)

Ágazati kritériumok

- 2014. január 1.-től az „Infokommunikációs technológiák" a BM Országos Katasztrófavédelmi Főigazgatóság hatáskörébe kerülnek
- Jelenleg az infokommunikáció nem létfontosságú rendszerelem!
- Az OKF dönthet, melyek a kritikus infrastruktúrák - csak a kijelölési eljárás után válhatunk azzá, ágazati kijelölések, szabályozások várhatók

A Magyar Telekomnak, mint biztonságos szolgáltatónak, magának is biztonságosan kell működnie. Egy nyereségorientált, tőzsdei cég esetén a biztonságra, annak „üzemeltetésére", fejlesztésére vonatkozó döntéseket kockázatelemzés után hozzák és az üzleti kockázatokkal arányos biztonsági szintet tartanak fent. Egy törvényi kötelezettségekkel is bíró távközlési szolgáltató esetében ennek a biztonságnak ki kell egészülnie egyéb tényezőkkel, amelyek létesítésére és fenntartására vonatkozóan nem mindig lehetséges az üzleti logika törvényei szerint dönteni. Ezért is igen fontos az aktuális és részletes szabályozási környezet.

Célpont lehet egy telekommunikációs szolgáltató? Sajnos igen!

A MT maga és – hálózatainkon, szolgáltatásainkon keresztül – ügyfeleink is támadások célpontjai lehetnek. Az elmúlt időszakban jellemzően a különböző indíttatású támadások egyre szervezettebbek, egyre jobban kimunkáltak, egyre szélesebb körűek, globalizálódnak, egyre „profibbak". Nem csak informatikai jellegű támadásokról kell beszélni, lehetségesek lehetnek a szolgáltatási szint rontására irányuló kísérletek, előtérbe kerültek az információbiztonsági incidensek lehetőségei is.

A veszélyek, kockázatok, támadások, problémák sora szinte végtelen lehet, néhány példa következik.

A külső támadások példái:

- illetéktelen hozzáférés,
- kártékony kódok,
- klasszikus hackertámadás,
- adathalászat,
- szabotázs,
- törvénytelen lehallgatás, stb.

Belső eredetű problémák:

- kiszivárogtatás,
- social engineering,
- szabályok megszegése,
- üzleti döntések hibái,
- outsourcing, külső partnerek felőli kockázatok,
- társszolgáltatói problémák,
- belső szabotázs, stb.

Külső egyéb okok:

- a rendszerek működéséből adódó műszaki és egyéb hibák,
- kapacitás-elégtelenség,
- infrastruktúra hiba (pl. energia),
- természeti katasztrófa.

Egy cég működésében a fentiek, ill. az ilyen helyzetek megfelelő, hatékony kezelése létfontosságú, ezért az üzletmenet-folytonosság menedzsmentnek (Business Continuity Management, BCM) és a krízis menedzsmentnek (CM) is nagy figyelmet kell kapnia.

Hatósági elvárások a kritikusinfrastruktúra-szolgáltatók felé

- Informatikai üzletmenet folytonossági terv (BCP) és katasztrófa-helyreállítási terv (DRP) kidolgozása, dokumentációja, karbantartása, tesztelése.
- A belső informatikai folyamatok előírás és szabvány szerinti fenntartása, dokumentációja és kontrollja.

- Incidenskezelési kötelmek
  - Bejelentések kezelése, megszabott határidejű beavatkozás, visszajelzés
  - Részvétel hatósági munkacsoportokban
  - Incidenskezelő rendszer használata
  - Adatszolgáltatás
  - Együttműködés a CERT-(ekk)el

A Magyar Telekom meglévő biztonsági rendszerének néhány eleme

A Magyar Telekom nagyon magas biztonsági szinten szolgáltat, nemzetközi standardokat alkalmaz:

- ISO 27001, Információ Biztonsági Irányítási Rendszer (ISMS) (2008-tól)
- ISO22301, Üzletmenet-folytonosság (BCMS) (2011 projektindítás, tanúsítvány: 2014)
- Katasztrófa elhárítási tervek (DRP)
- Hálózati katasztrófa elhárítási tervek
- Informatikai katasztrófa elhárítási tervek
- Incidenskezelés
- Teljes, integrált hálózatfelügyelet (réz, optika, radio, koaxiális és IP hálózatok) (NOC, SNOC)
- teljes szolgáltatásmenedzsment (vezetékes és mobil hang-, adat- és szélessávú szolgáltatások, TV, valamint IP alapú szolgáltatások
- fejlett vállalatbiztonság (integrált biztonsági rendszert működtetünk: fizikai biztonság, információ és adatvédelem, visszaélés (fraud) megelőzés, forensic vizsgálati funkciók, szabályozások, IT biztonság, tudatosítás, oktatás, kommunikáció, stb.).

Néhány példa a vállalatbiztonság rendszerelemeire:

- Épületek biztonsági osztályba sorolása (bázisállomás, torony, kihelyezett fokozat, technológiai épület)
- IT rendszerek biztonsági osztályba sorolása

- Információs vagyonleltár
- Hierarchikus kulcsrendszer
- Kiemelt kábelvédelem, gerinchálózat védelme
- Megszakító létesítmények védelme
- Rádiós hálózatvédelem
- Támadás detektálás
- Központi LOG gyűjtés és elemzés
- NAC (Network Admisson Control) rendszer
- Kockázatkezelés
- Sebezhetőségi vizsgálatok
- Mobil eszközök biztonsága
- Irodai környezet védelme
- Rendszeres, nagy létszámú biztonságtudatosítási felmérés és oktatás
- Erőteljes, széleskörű biztonsági kommunikáció

Dilemmák

Standardok, biztonsági szintek, arányosság

- Egységes nemzetközi (EU) és hazai biztonsági standardok és definíciók hiánya
- Biztonsági szintek és az arányosság kérdése (piac - állam - EU) -> Kire vonatkozik? (Technológia? Felhasználó?)
- Kinek mi az érdeke?

Felelősség és szerepek - Hol a határ?

- Meddig tart a piac felelőssége, és hol kezdődik az államé?
- A piac felelősségének határa: ami üzleti racionalitással, működés mellett vállalható
- Az állam szerepe: egy ország szempontjából létfontosságú rendszerek védelme
- Az állam szerepe: felügyelet, koordináció, követelménytámasztás, kontroll, audit, stb.

- Kritikus adatok, folyamatok rendszere felsorolásszerűen, vagy módszertannal?

Költségek – A biztonság értéke

- A legfontosabb kérdés: Ki fizesse a biztonság költségeit? Hol a határ?
- Alapvetés: Annyit érdemes rákölteni, amennyit az információ ér, és…
- Biztonság értéke: Amekkora kár érhet bennünket egy káresemény során (kockázatelemzés)
- Piaci logika szerint: a kockázatokkal arányosnak kell lennie a ráfordításoknak
- Állami logika szerint: a lehető legmagasabb biztonsági szint közérdek (vs. forráshiány)
- Egy másik álláspont szerint az igénybevevő (felhasználó) fizesse a biztonság költségeit

A biztonság pénzbe kerül, nagyon sok pénzbe. A biztonság alapérdekünk.

- Határ a csillagos ég.
- Nincs 100%-os védelem, azt csak megközelíteni lehet.
- Mi is erre törekszünk.
- Felelősségek? (Állam, Szolgáltatók, Gyártók)
- Ugyanakkor vannak olyan biztonsági lépések, elemek, amely nem kerülnek pénzbe, csak meg kell lépni!

Összefoglalás

- Rendkívüli komplexitású hálózatot érő, globális támadások ellen kell védekeznünk
- Globális rendszerben kell gondolkodni
- A Magyar Telekom kritikus infrastruktúra és számtalan kritikus infrastruktúrát szolgál ki.
- Az érdekeltek mindegyikének folyamatosan együtt kell működni
- Világos elvárások, szabályok, kontrollok, auditok, tanúsítás kell
- Mi van a fejekben? – tudás, tudatosítás, tudatosság

- Tisztában vagyunk a felelősségünkkel.
- Magas technológiai szint
- Szervezett, globális üzemeltetési rendszer
- Magasan képzett, tudatos, folyamatosan fejlesztett munkatársak
- Legjobb iparági gyakorlatok (DT) alkalmazása
- Nagyon jelentős mértékű tartalék erőforrások
- Nyitottak vagyunk az együttműködésre

De egyedül nem megy – csak Együtt, Veled.

Gencsy Péter
biztonsági igazgató
Magyar Telekom csoport

Dr. Révész Balázs

Magánszféra kontra biztonság – egyensúlyra törekedve

„Eljöhet az idő, amikor senki sem lehet biztos benne, hogy a szavait nem rögzítik-e későbbi felhasználás céljából, amikor mindenki attól fog félni, hogy legtitkosabb gondolatai már nem a saját, hanem a kormány tulajdona, amikor a legbizalmasabb, legintimebb beszélgetéseket buzgó és kíváncsi fülek figyelik. Amikor ez az idő eljön, a magánszféra és vele együtt a szabadság is eltűnik majd." (Osborn v. United States)

„Ami megkülönbözteti az állam által vívott háborút attól, amit az ellenségei vívnak az az, hogy az egyik a törvényekkel összhangban harcol, míg a másik azokkal ellentétesen. […] Az erkölcsi fegyver nem kevésbé fontos, mint bármely más fegyver, és talán fontosabb is – és nincs hatékonyabb morális fegyver, mint a jogállamiság." (Kawasma v. Minister of Defense)

A 2013-ban napvilágot látott információk szerint az amerikai Nemzetbiztonsági Ügynökség korlátlanul megfigyelte, rögzítette, tárolta és elemezte az interneten folytatott kommunikációt. A soha nem látott méretű adatkezelést a számítástechnikai fejlődés, illetőleg a történelmi háttér, a terrorellenes háború tette lehetővé. E fejlemények pedig óhatatlanul felszínre hozták a biztonság és a magánszféra, illetőleg a személyes adatok védelméhez fűződő jog közötti évtizedes vitát. Akár a magánszféra védelmezői, akár a biztonság pártiak szemszögéből értékeljük a helyzetet, arra jutunk, hogy a szembenálló nézetek között nincs, vagy csak nagyon kevéssé van átjárás. A biztonság és a magánszféra között megbomlott az egyensúly.

A Nemzeti Adatvédelmi és Információszabadság Hatóság munkatársaként természetesen az érintettek személyes adatok védelméhez fűződő jogát

kell szem előtt tartanunk. Miként azonban látni fogjuk, a biztonság garantálása mellett is nyomós érdekek szólnak, amelyek figyelmen kívül hagyása csakúgy káros következményekkel járna, mint a magánszférába való korlátozás nélküli beavatkozás az állam részéről. Szükségessé vált tehát az utóbbi szempontok mérlegelése is a vita során.

A következőkben ezért arra teszünk kísérletet, hogy bemutassuk a biztonság kontra magánszféra konfliktust, elsősorban az azzal kapcsolatos adatvédelmi dilemmák szemszögéből. Ennek keretében először felvázoljuk azt, hogy milyen változásokat hozott 2001. szeptember 11-e a magánszféra védelme terén. Majd értékeljük és elemezzük a versengő érdekeket, illetőleg az említett konfliktusban felmerülő érveket és indokokat. Végezetül javaslatot teszünk a magánszféra és biztonság közötti új egyensúly megteremtésére.

A világ 9/11 után

Amikor 2001. szeptember 11-én a Világkereskedelmi Központ ikertornyai összeomlottak, egy új korszak kezdődött el. Megkezdődött a világméretű terrorellenes küzdelem (War on Terror). Míg a korábbi háborúk során az ellenség látható volt, addig a terroristák és a terrorszervezetek ellen vívott harcban a kormányok alapvetően a sötétben tapogatóznak. Az ellenfél ugyanis rejtőzködik, szemben a klasszikus katonákkal nem visel egyenruhát, megkülönböztető jelzést, illetőleg a fegyverét sem hordja nyíltan. Elegendő csupán a 2005-ös londoni vagy madridi, illetőleg a 2013-as bostoni robbantások elkövetőire gondolni. A terroristák azonban nem maradnak örökké fedezékben, az arra alkalmas pillanatban, váratlanul támadnak, és cselekményük hatalmas – emberi és anyagi – áldozatokat követelhet. Ami még ennél is károsabb az az, hogy a terrorcselekmények alkalmasak a lakosság nyugalmának és biztonságérzetének megzavarására. Az így kialakult általános közhangulat pedig kihatással lehet az állam, a társadalom és a gazdaság működésére is. A terrorfenyegetettség jelentette bizonytalansági faktor ugyanakkor egy konstans készültségi állapotot eredményez, azaz a kormányoknak folyamatosan lépéseket

kell tenniük annak érdekében, hogy megelőzzék a támadásokat, amelyekhez hatalmas mennyiségű információra van szükség.

A 21. században az internet az emberek mindennapjainak részévé vált: segítségével ma már tulajdonképpen a bolygónk bármely pontjával kapcsolatot teremthetünk és információkat oszthatunk meg bárkivel, emellett kétségtelen előnye a rendszernek, hogy lehetővé teszi a tikosított, illetőleg az anonim kommunikációt is. Az internet e két előnyét a terrorszervezetek is felismerték, amelyet jól jelez erőteljes jelenlétük a világhálón.[1] Számos dzsihádista honlap működik ma, amelyek céljai meglehetősen eltérőek lehetnek. Ezek egy része a szélsőséges, fundamentalista eszmék terjesztésére szakosodott, mások az ideológiailag elkötelezett személyek toborzását tűzték ki célul. Sajnos olyan tartalmak is fellelhetők szerte az interneten, amik különböző öngyilkos merényletekhez használt eszközök előállításáról szólnak. Vannak, akik azt mondják, hogy ezek nem pontos receptek, mások viszont egyes ügyek kapcsán azt állítják, hogy sokszor katonai hírszerzési forrásokból származó útmutatások, instrukciók is megtalálhatóak bennük. A terrorista szervezeteken belüli szigorú alá-fölérendeltségi viszonyok átalakulása, a szervezeti struktúrák mellérendeltségi kapcsolatok irányába történő átrendeződése továbbá szükségessé tette az internet, mint kommunikációs csatorna alkalmazását annak érdekében, hogy a központ és az egyes terrorista sejtek közötti kapcsolattartás biztosított legyen, valamint hogy a csoportok is könnyedén együtt tudjanak működni.[2]

A terrorellenes háborúban alkalmazott legmodernebb hírszerző eszközök elsődleges célja az előzőekben bemutatott internetes kommunikáció és adatforgalom monitorozása. Minden állam rendelkezik nemzetbiztonsági törvénnyel, amely lehetővé teszi a veszélyes elemek megfigyelését, amennyiben bizonyos garanciák – leggyakrabban bírói engedély és felügyelet – teljesülnek. Ezen intézkedések jellemzően ideiglenesek, azaz a veszély elhárulásával vagy

1 Ian Brown – Douwe Korff (2009) 120.
2 Uo.

elhárításával egy időben megszűnnek. A terrortámadások jelentette folyamatos fenyegetettség miatt azonban fennáll a veszélye annak, hogy az eredetileg csak átmeneti megfigyelés állandósul, ami hosszú távon rendkívül káros hatásokat eredményezhet.

A megfigyelés folyamatossá és világméretűvé válása a 2001-es terrortámadások óta sajnos megtörtént.[3] Amíg a Wikileaks-ügy arra hívta fel a világ figyelmét, hogy a terrorellenes háború zászlaja alatt az Egyesült Államok és szövetségesei, mint magukat demokratikusnak valló államok olyan jogellenes tetteket követtek el, amelyek szükségessé teszik egy megfelelő ellenőrző és – adott esetben – jogorvoslati mechanizmus kiépítését.[4] Addig a Snowden-ügy végérvényesen beleégette a nemzetközi közvélemény emlékezetébe: az Egyesült Államok Nemzetbiztonsági Ügynöksége az interneten folyó bármely kommunikációt megfigyel, rögzít, eltárol és elemez annak érdekében, hogy kiszűrjön bárminemű fenyegetést. Ez azonban nem csak a külföldi államok, hanem az USA saját állampolgárainak magánszféráját is érintette, amely azzal járt, hogy megroppant a kormány és a polgárok közötti bizalmi viszony. Egy állam akkor tud hatékonyan és jól működni, hogyha az említett bizalom fennáll nem csak a kormányzat és az átlagemberek, de a központi hatalom és a köztisztviselők, a hivatásos jogviszonyban állók között is. Amikor az amerikai polgárok arról értesültek, hogy titkos bíróságok működnek[5], amikor arra utaló információk látnak napvilágot, hogy a különböző számítógépes eszközök, hardware-ek védelmét – kormányzati kérésre – maguk a gyártók gyengítik, holott költséges kampányok keretében hívják fel a polgárok figyelmét a saját számítógépes rendszereik védelmére[6], merőben új helyzettel szembesülünk.

3 Vö. Mary Wai San Wong (2002) 250-256.

4 Adam D. Moore (2011) 21.

5 Fisa court documents reveal extent of NSA disregard for privacy restrictions (http://www.theguardian.com/world/2013/nov/19/fisa-court-documents-nsa-violations-privacy, 2013-09-03).

6 Gyengített titkosítás és backdoor NSA-nyomásra? (http://www.hwsw.hu/hirek/50902/nsa-snowden-lehallgatas-backdoor-titkositas.html, 2013-09-09).

A nyilvánosságra került információk azonban nemcsak az amerikai végrehajtó hatalom és polgárai közötti bizalmat rendítették meg, de kihatással voltak az Egyesült Államokkal együttműködő más – elsősorban európai – országoknak a saját polgáraival fennálló viszonyára, valamint a szövetséges hatalmak egymás közötti kapcsolataira[7].

A Snowden-ügy hatásait az államok és polgáraik, valamint az államok egymás közötti kapcsolataira még nehéz lenne felmérni, erről még a nemzetkőzi agytrösztök is csak találgatni tudnak.[8] Annyi bizonyos ugyanakkor, hogy amíg 2001. fordulópontot jelentett a terrorizmus elleni harc szempontjából, addig 2013. a magánszféra védelme tekintetében indított el jelentős változásokat. A terrorellenes háború keretében végzett hírszerző tevékenység napvilágra kerülése ugyanis ráirányította a közvélemény és a – nemzeti és nemzetközi – jogalkotók figyelmét arra, hogy megfelelő egyensúlyt kellene kialakítani a megfigyeléssel érintett érdekek között.

Biztonság, magánszféra védelem és a személyes adatok védelméhez fűződő jog

A témával foglalkozó szakirodalom egységes abban, hogy az állampolgárok korlátlan megfigyelését három védendő alapvető érdek, a biztonság, a magánszféra tiszteletben tartása és az adatvédelem mentén tárgyalja.

A biztonság az egyik legősibb és legalapvetőbb elvárásunk és jogunk. Központi eleme természetesen az állampolgárok érdekeinek, életének védelme mindenfajta bel- és külföldi veszélyektől.[9] Emellett ugyanakkor a biztonság

7 Merkel says US spying on allies has shattered trust in Obama as European leaders unite in anger at summit (http://www.dailymail.co.uk/news/article-2475792/Angela-Merkel-leads-anger-Obama-US-spying-EU-summit.html, 2013-10-24).

8Austen D. Givens: The NSA Surveillance Controversy: How the Ratchet Effect Can Impact Anti-Terrorism Laws (http://harvardnsj.org/2013/07/the-nsa-surveillance-controversy-how-the-ratchet-effect-can-impact-anti-terrorism-laws/, 2013-10-01).

9 Emanuel Gross (2004) 108.

alkalmazási köre kiterjed minden olyan helyzetre, amelyek hatással lehetnek az állam azon képességére, hogy a nemzet jólétét biztosítsa.[10] Az állampolgárok életének védelme és a rendfenntartás mellett így egyike azon alapvető, kollektív nemzeti céloknak, amelyek megvalósítása az államok elsődleges feladata. Ahogy az az Osman v. United Kingdom ügyben is megfogalmazást nyert: *„Az államokat pozitív kötelezettség terheli a polgáraik életének megóvásáért"*. [11] Biztonság nélkül továbbá kivitelezhetetlenné válna az emberi jogok, valamint az egyéni és kollektív érdekek garantálása is. Egy kaotikus, bizonytalan helyzetben lévő országban a demokratikus értékek biztosítása hamar háttérbe szorul. Könnyen belátható tehát, hogy a biztonság érvényesüléséhez kiemelkedő érdekek fűződnek, és ezért jogi védelmet élvez. Az abszolút biztonság elérése azonban csupán utópisztikus vágyálom lehet, arra csupán csak törekedni tudnak az államok. Mindazonáltal e törekvéseknek is megvannak a maguk korlátai.[12] Ezek közé tartozik különösen a magánszférához és a személyes adatok védelméhez fűződő jog.

A magánszférához való jog fogalma nehezen meghatározható. Alapvetően az emberi személyiség védelmét, a magánélet sérthetetlenségét és a cselekvési autonómiát takarja. Ez tulajdonképpen egy szabadságjog és mint ilyen, védelmet nyújt a polgárok számára magánéletüknek az állami hatóságok általi önkényes zaklatása ellen. Ebben a tekintetben a magánszférához és a biztonsághoz való jog összefonódik: az egyén akkor érezheti magát biztonságban, hogyha egyben szabad is, illetőleg akkor lehet szabad, hogyha biztonságban érzi magát.

A magánszférához való jog megítélése nagyon eltérő az Egyesült Államokban és az európai gondolkodásban. E jog megjelenését a 19. század végére, pontosabban Samuel Warrennek és Louis Brandeisnek a Harward Law

10 Emanuel Gross (2004) 108.

11 Osman v. the United Kingdom, 28 October 1998, § 115, Reports of Judgments and Decisions 1998-VIII.

12 Emanuel Gross (2004) 108.

Review hasábjain 1890-ben megjelent „The Right to Privacy" című tanulmányához kötik.[13] A szerzők e művükben fogalmazták meg először, hogy a személy és a tulajdon teljes védelmet élvez, előbbinek ezért joga van az egyedülléthez (right to be let alone), amit a kormányzattal szemben is érvényesíteni kell.[14] E tanulmány indította el aztán a magánszférához való jog kialakulását az amerikai joggyakorlatban. Jelentőségét jól mutatja az Egyesült Államok Szövetségi Legfelsőbb Bíróságának Olmstead kontra Egyesült Államok ügyben hozott ítélete, amelyben az akkor már alkotmánybíró Brandeis kifejtette, hogy *„[az Alkotmányozók] biztosították a jogot az egyedülléthez a kormányzattal szemben – a legátfogóbb és a civilizált emberek által a legnagyobbra becsült jogot"*.[15] Az amerikai szabályozás jellemzője ugyanakkor az is, hogy csupán „eshetőleges" védelmet nyújt: már kezdettől fogva a szabadságot, mint alapvető jogot, és az otthon szentségét tekintették a legfontosabbnak. Ezzel szemben Európában – és így van ez Magyarországon is – a magánszféra védelme fő eszközének az emberi méltóságot, az egyénnek a közösség által kialakított nyilvános képét tartjuk: a polgárok ugyanis attól félnek a leginkább, hogy az ő megítélésük kerülhet veszélybe bizonyos információk napvilágra kerülése által.

A védett magánszféra, a magánélet tág fogalom, amelynek körébe számos jogosultság beletartozik. Ilyen például a személyes és társadalmi kapcsolatok kiépítésének joga, a személyes fejlődéshez való jog, a magánlakás-, a levelezés- és egyéb kommunikáció védelme, az egyén intimszférájának kialakításához való jog és a sort még hosszan lehetne folytatni.[16] Témánk szempontjából az lényeges, hogy ide tartozik a polgárok személyes adatok védelméhez fűződő joga is.[17]

13 Samuel D. Warren – Louis D. Brandeis (1890) 193.

14 A tanulmány előzménye az volt, hogy Warren egy tehetséges ügyvéd volt, aki elvette egy gazdag és befolyásos politikus feleségét. Ennek következtében az élete egyik napról a másikra megváltozott, ugyanakkor az újdonsült férj a média érdeklődésének középpontjába is került. Egyre több újságíró zaklatta, amit a szerző nem viselt el. Felkereste ezért jogász barátját, Brandeist-t és megírták az említett nagy hatású művet.

15 Olmstead v. United States, 277 U.S. 438,

16 Majtényi László (2008) 579-580.

17 L. például Avilkina and Others v. Russia, no. 1585/09, § 30, 6 June 2013.

Az adatvédelem az érintettek magánszféráját hivatott védeni azáltal, hogy előírja a személyes adatok kezelésével kapcsolatos szabályokat, valamint hogy biztosítja azokat a jogi eszközöket, amelyek a polgárok információs önrendelkezési jogának hatékony gyakorlásához szükségesek. Tehát *„nemcsak azt garantálja, hogy az egyének háborítatlanul élhessék a magánéletüket, hanem azt is, hogy ne váljanak kiszolgáltatottá, esetlegesen jogosulatlan információgyűjtések és visszaélések eszközévé"*.[18] Ez különösen fontos az információs társadalom korában, amikor az adatok, mint piaci értékkel bíró egységek megszerzése és kezelése már nem egyedül a kormányok célja lett, hanem az egyes gazdasági szereplőké is. A digitális forradalom következtében ugyanakkor átalakult a magánszférához való jog tartalma is, az *„már nem az egyedülléthez, hanem az adataink feletti ellenőrzés fenntartásához fűződő jogot jelenti"*.[19]

Az adatvédelem ma már egy sui generis jog, amely Európában rendelkezik a legerősebb jogi védelemmel a világon. Ezek közül az egyik legfontosabb az Európai Parlament és a Tanács által 1995. október 24-én elfogadott, a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról szóló 95/46/EK irányelv. Kiemelendő, hogy az adatvédelmi szabályozás célja eredetileg nem volt más, mint hogy az Unión belüli gazdasági együttműködést, a szabad piac működését az egyes eltérő tagállami szabályozások ne befolyásolják. A kereskedelem és a gazdaság szabadsága olyannyira fontos volt mindig is az adatvédelem kialakulásában és a jog fejlődésében, hogy sokáig a közös piac szabályozásával foglalkozó főigazgatósághoz tartozott az adatvédelmi feladatok koordinálása. Az ún. adatvédelmi irányelv szabályait azonban elsősorban nem a digitális környezetre alakították ki. Az uniós jogalkotók ezért egy új, specifikus jogszabály megalkotása mellett is döntöttek, amelynek eredménye az Európai Parlament és a Tanács által 2002. július 12-én elfogadott, az elektronikus hírközlési ágazat-

18 Péterfalvi Attila et al. (2013) 265.

19 Giovanni Pascuzzi: Il diritto dell'era digitale (2nd ed.). Bologna, 2006. (idézi: Paolo Guarda (2008) 1.)

ban a személyes adatok kezeléséről, feldolgozásáról és a magánélet védelméről szóló 2002/58/EK irányelv lett.[20]

Fontos továbbá az Európa Unió Bíróságának, valamint az Emberi Jogok Európai Bíróságának joggyakorlata is. Előbbit azért érdemes kiemelni, mivel az ítéletei, így az adatvédelemmel kapcsolatos döntései is minden egyes európai uniós tagállam vonatkozásában kötelező érvényű. A strasbourgi székhelyű testület pedig következetesen érvényre juttatta a személyes adatok védelmének követelményeit a terrorizmus elleni intézkedéseket érintő ügyekben.[21]

Végezetül kiemelnénk az Európai Bizottság tanácsadó szerveként működő ún. 29-es Munkacsoportot, amely lényegében az uniós adatvédelmi biztosok és hatósági elnökök munkacsoportja. Feladatuk az említett irányelvek rendelkezéseinek értelmezése a vonatkozó egységes tagállami gyakorlat kialakítása érdekében, és iránymutatások kibocsátása a tagállami jogalkalmazás vonatkozásában. A 29-es Munkacsoport már 2001. szeptember 11-e után azonnal reagált a terrorizmus elleni harc és az adatvédelem kapcsolatára. Az e tárgyban kiadott állásfoglalásában hangsúlyozta, hogy a terrorellenes háborúval kapcsolatban kiegyensúlyozott megközelítés szükséges, és hogy egyes technikai módszerek alkalmazásánál tovább az államok nem terjeszkedhetnek túl.[22] Kiemelte továbbá, hogy a magánszféra tiszteletben tartásához és a személyes adatok védelméhez fűződő jogokat még a nagy hirtelenséggel, sürgős eljárásban elfogadott intézkedések tekintetében is érvényesíteni kell. A 29-es Munkacsoport ugyan elismerte: a terrorizmus elleni harc alapvető vonása, hogy a demokráciánk fundamentumát képző alapvető értékeket megőrizzük, mivel ezek azok, melyek ellehetetlenítik az elsődlegesen az erőszak alkalmazását célul kitűző erőket. A testület ugyanakkor azon a véleményen volt, hogy

20 Ezt nevezik elektronikus hírközlési adatvédelmi vagy e-privacy irányelvnek.

21 L. például Klass and Others v. Germany, 6 September 1978, Series A no. 28.

22 Opinion 10/2001 on the need for a balanced approach in the fight against terrorism (WP 53) (http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2001/wp53_en.pdf, 2013-12-15).

az annak keretében meghozott intézkedések hosszú távon az alapjogokra és azok érvényesítésre is káros hatással lehetnek. Ezért kizárólag „hasznos" vagy „célszerű" intézkedések nem korlátozhatják az alapvető szabadságokat.

Magánszféra kontra biztonság

A személyes adatok védelméhez fűződő jogból további elvek és jogosultságok vezethetők le. Alapvető elvárás, hogy a személyes adatok kezelése tisztességes és törvényes legyen, vagyis a személyes adatokon végzett műveletek során mindenkor be kell tartani a vonatkozó jogszabályok előírásait.[23] Érvényesülnie kell továbbá a célhoz kötöttség elvének, amelynek értelmében csak előzőleg és pontosan meghatározott, jogszerű célból szabad személyes adatokat kezelni.[24] Ebből következően a cél nélküli, ún. „készletező" adatgyűjtés és tárolás jogellenes.[25] Lényeges, hogy az adatminimalizálás elvének megfelelően csak az adatkezelés céljának megvalósulásához elengedhetetlen, a cél elérésére alkalmas személyes adat kezelhető, kizárólag a cél megvalósulásához szükséges mértékben és ideig. [26] Fontos alapelv továbbá az adatminőség elve, amely azt a kötelezettséget foglalja magában, hogy a kezelt személyes adatok pontosak, teljesek és naprakészek legyenek.[27] Az adatok kezelője köteles úgy megtervezni és végrehajtani az egyes adatkezelési műveleteket, hogy biztosítsa az érintettek magánszférájának védelmét. Gondoskodnia kell ezért az adatok biztonságáról, így meg kell tennie azokat a technikai és szervezési intézkedéseket és kialakítani azokat az eljárási szabályokat, amelyek az adat- és titokvédelmi szabályok érvényre juttatásához szükségesek.[28]

23 Révész Balázs – Somogyvári Katalin (2012) 81-83.

24 Az Alkotmánybíróság a 35/2002. (VII. 19.) AB határozatában kifejtette, hogy „[a]z információs önrendelkezési jog gyakorlásának feltétele és egyben legfontosabb garanciája a célhoz kötöttség". Idézi Czine Ágnes (2006) 120.

25 L. 15/1991. (IV. 13.) AB határozat, ABH 1991, 40-57.

26 Paolo Guarda (2008) 73.

27 Révész Balázs – Somogyvári Katalin (2012) 80.

28 Révész Balázs (2012) 109-118.

Az információs önrendelkezési jog lényegi tartalma, hogy az érintett érdemi döntést hozhat személyes adataival kapcsolatban, felügyelheti azok kezelését. Ebből következően az adatalanyokat többletjogosultságok is megilletik az adatkezelés vonatkozásában. Ezek közül az egyik legfontosabb az, amelynek értelmében az érintett tájékoztatást kaphat személyes adatainak kezelésével kapcsolatos fontosabb tényekről. A hibás adatok kezeléséhez, illetőleg a jogellenes kezelt adatokhoz köthető a helyesbítéséhez, valamint az adatok törléséhez vagy zárolásához fűződő jog.[29] Továbbá, amennyiben az egyént sérelem érte az adatkezelés vonatkozásában, úgy megilleti a jogorvoslathoz való jog, vagyis az, hogy bíróság előtt érvényesíthesse követelését.

Bár az adatvédelmi szabályozás rendkívül szigorú, a személyes adatok védelméhez fűződő jog nem abszolút jellegű, azaz bizonyos érdekek vagy célok megvalósítása érdekében korlátozni lehet.[30] Ezek közé tartoznak a bűnügyi és a nemzetbiztonsági célok is. A személyes adatok védelméhez való jog korlátozása azonban még ebben az esetben sem lehet parttalan: minden egyes esetben mérlegelni kell az egymással versengő érdekeket (balance of interest) a szükségesség és arányosság elvének tiszteletben tartása mellett. Elegendő ehelyütt az Emberi Jogok Európai Bíróságának állandó ítélkezési gyakorlatában kialakított szigorú kritériumrendszerre utalni.[31] A testület szerint rendőri és biztonsági szervezetek általi adatgyűjtésnek mindenekelőtt megfelelő törvényi felhatalmazáson kell alapulnia. Az adatkezelés lehetővé tevő jogszabálynak kellően pontosnak, világos megfogalmazásúnak és bárki számára hozzáférhetőnek kell lennie. A megtett intézkedéseknek továbbá meg kell felelnie a szükségesség követelményének, amely egy nyomós társadalmi érdek meglétét feltételezi. A bűncselekmények megelőzését, illetve üldözését, valamint nemzetbiztonság garantálását a bíróság természetesen elfogadja, mint

29 L. bővebben Somogyvári Katalin (2012) 151-170.
30 L. Emberi Jogok Európai Egyezménye 8. cikk 2. bekezdés.
31 Ian Brown – Douwe Korff (2009) 126-127.

olyan jogszerű célnak, amelynek érdekében az államok bizonyos jogokat korlátozó intézkedéseket tehetnek, utóbbiaknak azonban arányban kell állniuk az elérendő célokkal. Az automatikus egyedi döntés meghozatalánál, illetve a profilalkotásnál pedig fokozottan kell érvényesülnie az érintetti jogoknak. A Bíróság joggyakorlata megerősítette továbbá, hogy a jogorvoslat lehetőségét mindenki számára, minden esetben – utólag a titkos megfigyelésnél is – biztosítani kell. A célhoz kötöttség elvének alkalmazása a gyakorlatban azt jelenti, hogy az eljáró szerveknek el kell különíteni a „hard" és a „soft" adatokat, valamint az adatalanyokat megfelelően tipizálni kell a kapcsolódó személyekre, a véletlenszerű kapcsolatokra, és a gyanúsítottakra. Ehhez kell társítani megfelelően elválasztva, a célhoz kötöttség elvével biztosítva az adatokat. Végső soron pedig biztosítani kell a népképviseleti ellenőrzést is.

Az internetes kommunikáció korlátlan megfigyelése súlyos veszélyeket rejt magában az érintett személyek személyes adatai és magánszférája tekintetében. A folyamatos, „egy esetleges későbbi terrorveszély elhárítása" érdekében folytatott adatgyűjtés sérti az célhoz kötöttség elvét. Az összegyűjtött adatok automatikus rendszerezése, kategorizálása, valamint az adatokból levont következtetések alkalmazása, vagyis a profilozás téves következtetései káros hatással lehetnek az egyén társadalmi és magánéletére is. A megfigyelés titkossága továbbá ellehetetleníti az érintetti jogok gyakorlását, különös tekintettel a tájékoztatáshoz és a jogorvoslathoz való jogra. Az ezzel kapcsolatos első bírósági ítéletekre azonban még várni kell.[32]

A Snowden-ügynek, amellett, hogy ráirányította a figyelmet a terrorellenes háború keretében végzett adatgyűjtések problémájára, ismét felszínre hozta azokat a véleményeket, amelyek vagy a biztonság vagy a magánszféra védelmének szélsőséges érvényesülését hangoztatják. A biztonság mellett szól az ún. „Bízz bennünk!" (Just trust us) érvelés, amely azt hirdeti, hogy

32 GCHQ faces legal challenge in European court over online privacy (http://www.theguardian.com/uk-news/2013/oct/03/gchq-legal-challenge-europe-privacy-surveillance

az állam elsőrendű kötelezettsége a nemzetbiztonság és az állampolgárok jólétének garantálása, a biztonság és a magánszféra közötti egyensúlyt ezért azoknak kell megteremtenie, akik e tekintetben döntéshozók.[33] A „Nincs mit titkolni" (Nothing to hide) elmélet szerint a megfigyelés által a magánszférában okozott kárt kell összemérni az ilyen típusú intézkedések által elérni kívánt céllal. A biztonság, tekintettel egy demokratikus államban betöltött szerepére, mindig megelőzi a magánszféra védelméhez fűződő érdekeket.[34] Amennyiben tehát egy állampolgárnak nincs mit titkolnia, semmilyen információt nem lehet felhasználni ellene, a magánszférájába történő hatósági beavatkozás ezért nem is okozhat kárt. Végezetül, a „Biztonság mindenekfelett" (Security trumps) argumentum értelmében, *„amennyiben a magánszféra és a biztonság konfliktusba kerül, utóbbi győzedelmeskedik – […] a biztonság sokkal fontosabb, mint a magánszféra"*.[35] Egyes biztonságpárti elméletek elmennek egészen addig az „ideálisnak" titulált utópisztikus helyzetig, ahol kis robotok masíroznának közöttünk, akik mindent rögzítenének, beleértve az otthonunk történéseit is. Így lényegében, ha minden mindig dokumentálva lenne, akkor egy semleges értékű, hatalmas adatbázis jöhetne létre. Kiválóan lehetne rekonstruálni és igazolni azt, ami a múltban történt. Így aztán a bizonyítás is könnyen megtörténhetne a bíróságok előtt. Nagyon szélsőséges szemléletek ezek az elméletek, azonban általában azt látjuk, hogy mindig a biztonság felé billen el a mérleg nyelve, mert kis apró lépésekben az emberek hajlandóak a magánszférájukból feláldozni azért, hogy nagyobb biztonságra tegyenek szert. Hosszú távon ugyanakkor ezekből az önkorlátozásokból jöhet létre a teljes megfigyelés állapota.

Természetesen léteznek a magánszféra elsőbbségét hirdető nézetek is, amelyek mindenfajta titkos megfigyelést elvetnek. A totális állami önkorlá-

33 Adam D. Moore (2011) 3-9.
34 Uo. 9-12. (e nézőpont kritikáját lásd Daniel J. Solove (2011)).
35 Uo. 13. (lásd még Kenneth Einar Himma (2007) 859-922.).

tozás azonban azzal a veszéllyel jár, hogy veszélybe kerülhet a nemzet léte és biztonsága. Ez viszont – ahogy arra már korábban kitértünk – negatívan befolyásolja az emberi jogok érvényesülését is.

Olybá tűnhet, hogy a fentebb ismertetett nézetek gyökeresen ellentmondanak egymásnak. Van azonban egy közös vonásuk, az, hogy mind „nulla végösszegű" érvelések. Az egyik vagy másik versengő érdek érvényesülését csak a szembenálló érdek „kárára" képesek elképzelni: azaz, ha a növeljük a biztonság szintjét, a magánszféra védelme szenved csorbát és fordítva. Ezen elméletek közötti arany középutat elérni nagyon nehéz feladat. Az egyensúly megtalálása azonban mind fontosabb, és egyben sürgetőbb feladattá is válik. A technikai fejlődés ugyanis abba az irányba halad, hogy egyre több adatot, nagyon rövid idő alatt és nagyon gyorsan képesek leszünk feldolgozni. Ez ugyan még elsősorban a magánszektorra igaz, azonban a kormányok is igyekeznek a legújabb módszereket a saját szolgálatukba állítani.

Új kihívások

Az utóbbi néhány évben új kihívások jelentek meg az életünkben. A legjelentősebbek közé tartozik a Big Data-jelenség, a kormányzati adatbányászat, valamint az Európai Unió azon törekvése, hogy a 95/46/EK irányelvet egy egységes adatvédelmi rendelet váltsa fel, amelyben már helyet kapna a felejtéshez való jog is.

A Big Data-jelenség, mely Amerikából eredeztethető, ahol merőben mások az adatvédelmi elvárások, sokkal nehezebben értelmezhetőek és dolgozhatóak fel jogilag. A probléma elsősorban abból adódik, hogy az adatminimalizálás elve, ami az adatvédelem meghatározó elvárása, merőben ellentétes a Big Data-jelenség elvárásaival. Az anonimizáltan gyűjtött adatok gyűjtése és feldolgozása, ha az azonosíthatóság feltételei később sem lesznek adottak, nem sérti az említett elvet. Amennyiben viszont az azonosíthatóság lehetősége fennáll, akkor már nehezen lesz elképzelhető, hogy a hatalmas adatbázisokban található információk az adatkezelés célja szempontjából elengedhe-

tetlenül szükségesek, illetőleg a cél elérésére alkalmasak lesznek.[36]

A kormányzati adatbányászat, vagyis bizonyos elemek azonosítása nagy mennyiségű adat között, szintén érdekes jelenség. Az már most világosan látszik, hogy a terrorizmus elleni harcban sikerrel lehet azonosítani, például bizonyos gyanús szavak azonosítása és kiszűrése céljából.[37] Ezeket először a telefonbeszélgetések megfigyelése során alkalmazták a nemzetbiztonsági szolgálatok, majd kiterjesztették azt – a technika fejlődésével – a hatalmas adatmennyiséget generáló internetes kommunikációra is. Egy e-mail tartalmának elemzése így ma már viszonylag egyszerűen megoldható lett. További jelentős újítás várható a felhőalapú adattárolás terén, különösen annak fényében, hogy egyre több kormány alakít ki saját kormányzati felhőt. Az ott tárolt adatok adott esetben szintén az adatbányászati technológiák célpontjává válhatnak.

A felejtéshez való jog kodifikálása nagy előrelépés lenne az információs önrendelkezési jog szempontjából, másrészt a gyakorlatban számos problémát felvetne. E jog garantálásával ugyanis lehetőség kínálkozik arra, hogy utólag bizonyos tartalmakat végleg eltávolítsunk az internetről.[38] Ez rendkívül hasznos lesz azoknak, akik meggondolatlanul töltöttek fel adattartalmakat magukról az internetre. Amennyiben viszont a végleges eltávolítás megtörténik, és bizonyos történéseket meg nem történtté nyilvánítunk, akkor nehezen lehet majd később ezekhez az adatokhoz hozzáférni.

Konklúzió

Az előzőekben bemutatott kockázatok, illetve technikai újítások mind arra engednek következtetni, hogy új egyensúly megtalálása szükséges a magánszféra védelme és a biztonság garantálása között. Ennek megteremtése és fenntartása azonban rendkívül nehéz feladat.

Milyen eszközök állnak rendelkezésünkre e célból? Mindenekelőtt az

36 L. Omer Tene – Jules Polonetsky (2013) 240-273.
37 Vö. Daniel J. Solove (2008) 343-362.
38 L. Robert Kirk Walker (2012) 257-286

oktatás, különösképpen az adatbiztonsági ismeretek oktatása. Azáltal, hogy a felhasználókat megtanítják a biztonságra és követik is a biztonsági intézkedéseket, lényegében a nemzetbiztonságot és a kormányzati biztonságot erősítik. Ugyanakkor a saját kormányaik részéről érkező – esetlegesen magánszférát sértő – beavatkozásokat is ki tudják ezzel zárni. Ide sorolhatjuk az internetes tartalmak fokozott kontrollját is, amelyek kétségtelen, hogy a véleménynyilvánítás szabadságával ellentétesek, de a megelőzésben fontos szerepük lehet. A fiatalok ugyanis nagyon sok olyan tartalomhoz juthatnak hozzá az interneten, amelyek károsak, vagy veszélyesek lehetnek. Az államoknak – köztük Magyarországnak is – arra kell törekednie, hogy bizonyos információkat könnyedén el tudjon távolítani, elérhetetlenné tudjon tenni, hogyha az a nemzeti érdekekkel, vagy akár például a Nemzeti Gyermekvédelmi Programmal nem lenne összeegyeztethető.

Nagyon fontos a már meglévő transzparencia növelése is. A Wikileaks- és a Snowden-ügyek alapjaiban rengették meg a polgárok bizalmát. Ez arra enged következtetni, hogy nem tartható tovább az az állapot, hogy a biztonsági szervezetek eltitkolják a tevékenységüket, és csak minimális vagy félrevezető információt szolgáltatnak a közvélemény számára. Nemrég a BBC-n megkérdeztek egy brit alsóházi képviselőt, valamint egy biztonsági szakembert arról, hogy szerintük mennyire kellene a terrorizmus elleni harcban átláthatóvá tenni ezeknek a szerveknek a működését.[39] A képviselő ezzel kapcsolatban elmondta, hogy lényegében hetente jár a szolgálatokhoz, mint nemzetbiztonsági bizottsági képviselő, és minden alkalommal elé tárják azokat a bizonyítékokat, amelyek a polgárok jogainak korlátozását indokolják. Azzal szembesül, hogy konkrét esetek vannak, komoly a fenyegetettség, és hogy a biztonsági szervezeteknek mindig egy lépéssel a terrorista csoportok előtt kell járniuk. Úgynevezett „egy nyugodt nap már jó" harcot folytatnak azért, hogy meg tudják akadályozni a terrorcselekményeket. Most már azonban nem elég az, ha azt mondják, hogy az

39 UK security services scrutinised by MPs and public (http://www.bbc.co.uk/news/uk-politics-24048186, 2013-12-15).

adatainkra szükségük van, hogy megóvjanak minket, tényszerűen – természetesen anonimizáltan – kommunikálni kell a polgárok felé a terrorizmus elleni harc sikerét azért, hogy ez az együttműködés közös lehessen, és azt érezze a polgár, hogy átláthatóan működnek ezek a szervezetek.

Kiemelnénk még, hogy szükség lenne a világos, átlátható, jogilag szabályozott ellenőrzési mechanizmusokra is.

Az adatvédelmi felügyelő szervek nagyon kritikusak a jelenlegi helyzettel szemben. Egyensúlyra azért kell törekedni és közösen gondolkodni a megfelelő jogi szabályozásról és garanciákról, hogy elkerüljük azt, amit még 2004-ben a brit adatvédelmi biztos mondott, hogy lényegében alvajárás történik a megfigyelési társadalom irányába.

dr. Révész Balázs főosztályvezető
Vizsgálati Főosztály, Nemzeti Adatvédelmi és Információszabadság Hatóság

Felhasznált irodalom

Ian Brown – Douwe Korff (2009): Terrorism and Proportionality of Internet Surveillance. In: European Journal of Criminology, 2009. No. 2. 119-134.

Czine Ágnes (2006): A titkos információgyűjtés néhány jogértelmezési kérdése. In: Fundamentum, 2006. No. 1. 119-125.

Emanuel Gross (2004): The Struggle of a Democracy against Terrorism – Protection of Human Rights: The Right to Privacy versus the National Interest – the Proper Balance. In: Cornell International Law Journal, 2004. No. 1. 101-165.

Paolo Guarda (2008): Data Protection, Information Privacy, and Security Measures: An Essay on the European and the Italian Legal Frameworks. In: Ciberspazio e diritto, 2008. No. 1. 65-91.

Kenneth E. Himma (2007): Privacy Versus Security: Why Privacy is Not an Absolute Value or Right. In: San Diego Law Review, 2007. No. 4. 859-922.

Majtényi László (2008): Az információs jogok. In: Halmai Gábor – Tóth

Gábor Attila (szerk.): Emberi jogok. Osiris Kiadó, Budapest, 2008. 577-635.

Adam D. Moore (2011): Privacy, Security, and Government Surveillance: Wikileaks and the New Accountability. In: Public Affairs Quarterly, 2011. No. 2. 1-24. (http://paq.press.illinois.edu/25/2/moore.html, letöltés: 2013-09-03)

Péterfalvi Attila et al. (2013): A Közigazgatás adatkezelő tevékenysége. In: Gellén et al.: A közigazgatás funkciói és működése. Nemzeti Közszolgálati és Tankönyv Kiadó, Budapest, 2013. 265-295.

Révész Balázs – Somogyvári Katalin (2012): Az adatkezelés elvei. In: Péterfalvi Attila (szerk.): Adatvédelem és információszabadság a mindennapokban. HVG-Orac, Budapest, 2012. 73-89.

Révész Balázs (2012): Az adatbiztonság követelménye. In: Péterfalvi Attila (szerk.): Adatvédelem és információszabadság a mindennapokban. HVG-Orac, Budapest, 2012. 109-118.

Daniel J. Solove (2008): Data Mining and the Security-Liberty Debate. In: University of Chicago Law Review, 2008. No. 1. 343-362.

Daniel J. Solove (2011): Nothing to Hide - The False Tradeoff between Privacy and Security. Yale University Press, New Haven, 2011.

Somogyvári Katalin (2012): Az érintettek jogai és érvényesítésük, előzetes tájékoztatás és tiltakozás. In: Péterfalvi Attila (szerk.): Adatvédelem és információszabadság a mindennapokban. HVG-Orac, Budapest, 2012. 151-170.

Omer Tene – Jules Polonetsky (2013): Big Data for All: Privacy and User Control in the Age of Analytics. In: Northwestern Journal of Technology and Intellectual Property, 2013. No. 5. 240-273.

Robert K. Walker (2012): The Right to be Forgotten. In. Hastings Law Journal, 2012-2013. No. 1. 257-286.

Samuel D. Warren – Louis D. Brandeis (1890): The Right to Privacy. In: Harvard Law Review, 1890. No. 2. 193.

Mary Wai San Wong (2002): Electronic Surveillance and Privacy in the United States after September 11, 2001: The USA-PATRIOT Act. In: Singapore Journal of Legal Studies, 2002. No. 1. 214-270.sdgfdfsf

Dr. Hankiss Ágnes

Kihívások és ellentmondások a terrorizmus elleni harcban

A terrorizmus természete – a geopolitikai erőterek folyamatos és heves változásainak a függvényében – állandó és sokszor nehezen nyomonkövethető átalakulásokon megy keresztül. Előadásomban a terrorizmus két olyan vonatkozásával foglalkozom, amely kihívásokkal és ellentmondásokkal szembesítheti a rendvédelem és a terrorelhárítás szakembereit.

Magányos elkövetők

Kérdés, hogy a magányos elkövetőket újkeletű és önálló jelenségként kezeljük-e vagy pedig úgy fogjuk fel, mint a terrorizmus diverzifikációs folyamatának legújabb állomását. A kérdéskört elemző tanulmányok többségéből azt látom – megelőlegezve ezzel egyben a végkövetkeztetést –, hogy a „magányos farkasok" problémáját a diverzifikációs folyamat összefüggéseiben kell vizsgálnunk. Mindenekelőtt talán nem felesleges dióhéjban összefoglalni a diverzifikációs folyamat lényegét. A diverzifikáció eredetileg azt jelenti – amint ez köztudomású –, hogy a terrorista mozgalmak központi ereje és vezetése szétesik, és a legkülönbözőbb helyi csoportok, sejtek nevezik ki magukat egy adott térségben az Al-Kaida letéteményeseinek. Bin Laden halála óta ez a diverzifikációs folyamat felgyorsult. Vagyis, az ellenfélnek nincs könnyen felismerhető és azonosítható arca, székhelye és vezére; az arca és a maszkja folyton változik, mozgásban van, elsősorban a lokális válságövezetek dinamikája szerint. A „franchise-rendszerben" működő terrorista mozgalmak klasszikus példája a Sahel-régió. A Sahel-régió talán legveszélyesebb és legveszélyeztetettebb országa ma Mali. Az iraki diktatúra bukása és az Arab Tavasz történései jelentős szerepet játszottak abban, hogy militáns iszlamista sejtek vették át az uralmat és teremtettek polgárháborús

viszonyokat a térségben. A tuaregek négy különböző csoportja, egymással is rivalizálva, meghonosította a permanens erőszakot a térségben. Belső viszonyaik nehezen átláthatóak: míg a tuaregek között például négy törzs tekinti magát az Al-Kaida helyi megbízottjának, valójában csupán az egyikük az, amelyik valóban az Al-Kaida önálló szárnyaként működik... (A tuaregeket korábban a Khadafi-rezsim támogatta és egyszersmind kordában is tartotta...). Az Arab Tavasz által elindított diverzifikációs folyamat, Egyiptomtól Sziriáig, mára szinte nyomonkövethetetlenné vált: az érintett országok bomlásfolyamatai, erőszakhullámai és fegyveres harcai a terrorista toborzás számára már-már kimeríthetetlen „piacot" teremtettek. Megjósolhatatlan, hogy a sokféle politikai csoportosulásból melyek válhatnak terrorista mozgalmak melegágyává és utánpótlásává.

A diverzifikációs folyamat másik – mostanában elég vészjósló – oldala az a fajta radikalizáció, amely nem a válságövezetekben, hanem az Egyesült Államokból vagy Európa országaiból sodor terrorista csoportok vonzáskörébe jómódú polgári családokból származó fiatalokat. Amerikában vagy Európában születtek, legfeljebb a szüleik vagy a nagyszüleik jöttek valamelyik harmadik országból. Ők azok, akik elsősorban az interneten keresztül ismerkedhetnek meg terrorista ideológiákkal, kapcsolódhatnak be a terjesztésükbe, és vehetik fel a kapcsolatot olyan csoportokkal, akiknek a hatására útrakelnek, és akár maguk is terrorista merényletek részesévé vagy elkövetőjévé válhatnak. Idézhetjük Dosztojevszkij „Ördögök" című regényének a mottóját, amely Puskin egyik versének részletével, már-már látnoki erővel jeleníti meg a modernkori radikalizáció foglalatát: „Ha megölsz, se látok nyomot / ismeretlen már e táj /Alighanem ördög vezet / összevissza körbejár."

Az elmúlt években azonban olyan elkövetők állították reflektorfénybe a „magányos farkas" dilemmáját, akik nem feltétlenül kötődnek akár eszmeileg, akár gyakorlatilag az Al-Kaida tipusu terrorista mozgalmakhoz. Például Breivik. Vagy a londoni merénylő, aki lefejezett egy brit katonát Londonban,

a nyílt utcán. Ha az ember az elmúlt évekre visszagondol, megállapítható, hogy mind a rendvédelmi szakemberek, mind az állampolgárok számára az egyik legriasztóbb jelenség ezeknek a magányos elkövetőknek a feltűnése. Az ilyen típusú cselekmények azért is rendkívül ijesztőek, mert amíg egy központi irányítású, Al-Kaida típusú terrorizmusról beszélünk, addig az állampolgár a maga biztonságérzetét arra a hitre építheti, hogy országának rendvédelmi szervei, együttműködve más országok szerveivel, képesek lehetnek felderíteni és megelőzni a merényleteket. A Breivik-tipusú magányos elkövetők viszont olyan emberek, akik a lelkükben munkáló téveszméknek és agresszív fantáziáknak engedve, elszigetelten követik el a tettüket, amelyik ily módon megjósolhatatlan és kivédhetetlen.

A „magányos farkas" kifejezés különben az 1990-es évek végéről származik. Konkrétan a fehér faj felsőbbrendűségét hirdető két szélsőségestől, Tom Metzgertől és Alex Curtistől, akik a „szabadúszó terrorizmus" („freelance terrorism") híveiként arra bíztatták követőiket, hogy taktikai megfontolásból mindig egyedül, elszigetelten kövessenek el erőszakos cselekményeket. Az ilyen magányos elkövetők nem feltétlenül a dzsihadista terrorizmus ideológiájához kapcsolódnak. Lehetnek szélsőjobb vagy szélsőbal indíttatásuak. (A szeparatista terrorcselekményekre itt most nem térnék ki).

A szélsőbaloldali terrorizmussal, legalábbis globális méretekben, ma már kevéssé kell számolnunk. Ennek nyilvánvaló oka, hogy a Szovjetunió összeomlásával megszűnt az a központ, nevezetesen Moszkva, amely a szélsőbalos extremizmus fő támogatója és fenntartója volt (ha ezt nyíltan nem is vállalta). A Hamvas Béla Intézetben két, saját kutatásainkat összegző könyvet publikáltunk arról, hogyan álltak a kommunista rendszerek és titkosszolgálataik a nemzetközi terrorizmus, például a Carlos-csoport vagy általában a Vörös Brigádok mögött. Ma már állami szinten legfeljebb Dél-Amerika bizonyos országaiban kaphatnak támogatást, ahol azonban maga az állam tekinthető sok tekintetben extremistának. Nem tudjuk mit hoz a jövő; nehéz volna megjósolni, hogy a gazdasági válság vagy az európai intéz-

ményrendszer válsága mikor hívhat életre ismét szélsőbalos mozgalmakat. De – bocsássák meg az aktuálpolitikai felhangját annak, amit mondok –, amikor egy politikai csoportosulás az általa nem szeretett miniszterelnök szobrát ledönti, és a levágott és szétvert szobor darabjaival és fejével rugdalózik, és közben a magyar himnusz trágár verzióját énekli, akkor elgondolkozom azon, hogy ez a szó szimbolikus értelmében vuduista performance, a maga brutalitásában nem tekinthető-e valamiféle szélsőbalos extremizmus előszelének vagy előjátékának.

A szélsőjobboldali mozgalmak, bár erősödni látszanak, ellenségképük különbözősége miatt nem igen tudnak közös eszmerendszer és közös cél jegyében egyesülni. Az európai szélsőjobboldali mozgalmak azért nem képesek közös nevezőt találni, mert amig egyikük a bevándorlás ellen visel hadat, de nem rasszista alapon, a másiknak a cigánygyűlölet és az antiszemitizmus a vezérmotívuma. Ez pedig megnehezíti a közös fellépést. Gondoljanak például arra, hogy a régebbi időszakokban, a csecsen terrorizmus „hőskorában", azért nem tudtak érdemben összefogni az Al-Kaidával, mert hiába volt közöttük habitusbeli hasonlóság, a csecseneknek Oroszország volt a fő ellenfele, az Al-Kaidának viszont Amerika. Hazai viszonyoknál maradva, a magyar szélsőjobb vagy radikális jobb – nem akarnék itt a fogalmi különbségtételben elmerülni –, amikor európai szövetségeseket keres a hasonszőrüek között, rendre beleütközik abba, hogy az európai szélsőjobb szemében az antiszemizmus nem különösebben vonzó portéka. Szélsőjobboldali terrorcselekménynek tekinthetők a romagyilkosságok, amelyek szerencsére elszigeteltnek bizonyultak. Mindazonáltal azok, akik a mérsékelt jobboldalon megengedőleg, sőt olykor összekacsintólag tekintenek a szélsőjobboldali megnyilvánulásokra, ha tetszik, ha nem, osztoznak a felelősségben, ha a „szalonnácizmus" egy adott helyen és időben átcsap erőszakos cselekménybe.

De valójában kik is a magányos elkövetők, és mi vezeti el őket a tettig? Kérdés, hogy elsősorban klinikai pszichológiai keretben kell-e őket értelmeznünk, vagy inkább a terrorizmus ujabb diverzifikációs jelenségeként tudunk róluk

hiteles képet alkotni. Számos tanulmány próbálja meg lélektani fogalmakkal meghatározni a „magányos farkasok" tipusait. Az igazság az, hogy ezek kissé mesterkélt kategorizálásoknak tűnnek. A legáltalánosabb tipologizálás talán az, amelyik megkülönböztet „káosz-terroristát" és „karrier-terroristát". Tipikus „káosz-terrorista" Breivik, aki ha egyszer nekilendül, hatalmas pusztítással járó merényletet követ el, majd gyakorlatilag föladja magát. Ezzel szemben a „karrier-terrorista", például egykor Ted Kazsinszky, a Unabomber, húsz éven keresztül küldözgette a levélbombáit mindenfelé... Nekem úgy tűnik, hogy ez a tipologizálás a jelenség mélyebb megértéséhez és megelőzéséhez sokat nem ad hozzá. A kérdés inkább az, hogy ezek a „magányos farkasok" valóban magányosak-e, vagy ha csak virtuálisan is, de tagjai valamilyen „falkának". (A farkas egyébként falkában vadászik, ennyiben a metafóra nem is igazán pontos...). Melyik volna az előnyösebb a terrorelhárítás szempontjából? A válasz nem egyértelmű. Egyfelől a falka mindig veszélyesebb, hisz összesíti az erőket; ugyanakkor a felderíthetősége több eséllyel kecsegtet, hiszen a hírszerzés és az elhárítás a maga megszokott módszereivel feltérképezheti a falka hálózatát, és követheti a tevékenységét. De ha egy magányos elkövető valóban magányos, akkor voltaképpen a klinikai pszichológia területén mozgunk, ahol a terrorelhárítás tehetetlen, illetve beleütközik mindazokba a nehézségekbe, amelyekbe egy klasszikus sorozatgyilkos azonosítása ütközik. Úgy látom, hogy a terrorizmus kutatói, a terrorelhárítás szakértői az esetelemzések alapján egyre inkább hajlanak arra, hogy a magányos elkövetők többsége, ha másként nem is, az Interneten keresztül már az első időszakban bekapcsolódott valamilyen virtuális terrorista közösség kommunikációs világába. Minden jel arra mutat, hogy azokat, akiket mi magányos elkövetőnek gondolunk, az interneten keresztül toborozzák és radikalizálják (és esetenként kiképzik). Azok a konkrét eseteket, amelyeket itt megemlítenék, az iszlamista terrorizmus világából merítem, mivel a legbőségesebb példatár itt áll rendelkezésünkre. Engedjék meg, hogy röviden ismertessem egy olyan vizsgálat eredményeit, amelyet a West Point Counter Terrorism Center folytatott le. Nyolcvan olyan támadást elemeztek,

amelyet „magányos farkasok" követtek el, 1993 és 2010 között. Több mint 45 elkövetőnél sikerült felderíteni és bizonyítani, hogy az Interneten keresztül is kaptak kiképzést és eszmei muníciót. Egy 2012 januárjából származó felmérés szerint közel 8000 olyan honlap működik az interneten, amelyik részben kódoltan, részben teljesen nyílt formában, kifejezetten terrorista tartalmakat közvetít, és ötletekkel szolgál olyan emberek számára, akik valamilyen személyes lelki okból fogékonnyá váltak az erőszakra. Számos szerző vélekedik úgy, hogy a „magányos farkasokban" az Al-Kaida új stratégiája testesül meg. Az Al-Kaida elveszítette fő központjait és vezéreit; másod-, sőt, harmadvonalbeli vezetői közül is sokat letartóztattak. Ezért elkezdtek új stratégián gondolkozni. 2003-ban például már különböző extremista fórumok arra bíztatják olvasóikat, hogy ne várjanak központi instrukciókra. 2006-tól kezdve létezik az Inspire nevű honlap, a dzsihád egyik fő kommunikációs felülete, ahol kifejezetten ilyen címmel jelennek meg dolgozatok: „Hogyan harcolj egyedül?", vagy „Hogyan hozzál létre kis sejteket a központtól függetlenül?". Vagy: 2011-ben egy videót köröznek, amelynek a fő üzenete az, hogy „Ne másra építs, hanem te magad hajtsd végre a feladatot!". 2012 májusában az Inspirenek két olyan száma is megjelenik, amely arról szól, hogyan kell megkeresni és támogatni a magányos elkövetőket. A new york-i rendőrség nemrégiben az internetes beépülés céljából létrehozott egy Kiberhírszerző Egység-et, amelynek a tagjai belépnek ezekre a honlapokra. A sikeres beépülésre pedig bomlasztási stratégiákat építenek: ez a terrorelhárítás egyik igéretes eszköze lehet. De hadd említsem meg még a „The Organisation and Structure of National Terrorism" néven futó spanyol programot. A terrorizmussal foglalkozó írások és tanácskozások visszatérő eleme az a jogos kesergés, hogy az Internet valóságos paradicsomot teremtett a terrorizmus és a szervezett bűnözés számára. Manuel R. Torres, spanyol elemző viszont abból indul ki, hogy az Internet a terrorizmus számára nem csupán kiaknázható előnyt jelent, hanem kivételes sebezhetőséget is. Permanens paranoia forrását. A terrorizmus elleni harcban pedig ezt a sebezhetőséget kell minél jobban kihasználni. A hálózatok tag-

jai nem igen mernek saját otthoni gépükön kommunikálni, mert az könnyen azonosítható. Az iszlám országokban pedig még az internetes kávézó sem áll rendelkezésre, ahol anonim módon lehetne levelezgetni... 2010 nyarán az Inspire oldalai megsérültek. Csupán az első néhány oldala volt olvasható – a hírszerző szervek sikeres bomlasztási tevékenységének köszönhetően –, ami pánik-spirált indított be. A dzsihadista hálózat minden tagja elkezdte lázasan küldözgetni az üzeneteket, hogy mindenki mindent töröljön, még a jelszavait is. Így voltaképpen saját magukat számolták fel, és az egész network tulajdonképpen elhalt, annélkül, hogy a terrorelhárításnak pusztán a kibervédelem hagyományos eszköztárára kellett volna hagyatkoznia.

Külön is említhetők az úgynevezett dzsihádista fantomcsoportok. Olyan csoportok, amelyek azzal a céllal tartanak fenn, hogy az adott országban, a társadalomban stresszhelyzetet hozzanak létre. Beharangoznak olyan merényleteket, amelyeket egyébként nem szándékoznának, vagy nem tudnának elkövetni. Céljuk csupán az állandó pszichológiai hadviselés ébrentartása. Ezekkel a fantomcsoportokkal kapcsolatban egyébként – a terrorelhárítás szempontjából – megint csak együtt jelentkeznek a kihívások és az ellentmondások. Kihívást jelent a beépülés, azaz a sebezhetőség kiaknázása. Más oldalról viszont, az ellentmondások síkján, furcsa históriákról is lehet olvasni. A CIA és a szaúdi hírszerzés együtt létrehoztak egy nagyon sikeresen működő ál-fantom honlapot, és „csaliként" közzétették egy amerikai katonai alakulatok ellen készülő támadás tervet. Ámde a Pentagont nem avatták be a titkos műveletbe. Úgyhogy a katonai hírszerzés egy perc alatt szétverte és megsemmisítette azt, amit a CIA és a szaúdi hírszerzés sok hónapos munkával felépített. De említhetnénk eseteket a holland titkosszolgálat gyakorlatából is. Mindazonáltal, a kibervédelem mellett, a kiberbeépülés a jövő egyik fontos eszközének tűnik, amelyre hatékony bomlasztási stratégiákat lehet építeni.

De ha az ellentmondásoknál tartunk, még valamiről érdemes szót ejteni. Az FBI 2012-ben nagyon komolyan ráállt arra – Önök persze ezekről a dolgokról sokkal többet tudhatnak, mint jómagam, aki csupán a nyilvános for-

rásokra hagyatkozhat –, hogy beépüljön nem csak az internetes honlapok világába, hanem magukba a terrorista csoportokba is. Így sikerült meghiusítani merényleteket, többek között Tampa-ban vagy Chicago-ban. De ennek előzményeként az FBI fedett ügynökei látták el kocsikra szerelhető bombákkal ezeket a terroristákat, és az FBI fizette ki hitelkártyával például egy olyan terrorista repülőjegyét, aki Afganisztánba ment egy merényletet végrehajtani. Hát erre mondják, köznapi kifejezéssel, hogy egy kicsit „necces". Mert ha ellátnak egy terroristát bombával beépülési céllal, az nyilván siker a terrorelhárítás számára, a legkisebb gikszer esetén azonban mindez tragédiába torkollhat.

Mindehhez azonban érdemes hozzátenni és az összkép megítélésében figyelembe venni a legfrissebb adatokban megmutatkozó trendeket. A terrorizmussal gyanusított és a terrorista cselekményt elkövető muszlimok száma mind az Egyesült Államokban, mind Európában csökkenő tendenciát mutat. 2012-ben 8 ember lett vallási indíttatású terrorizmus áldozata. Európában – az Europol értékelése szerint – a terrorizmussal összefüggésbe hozható letartóztatások száma 2006-hoz képest 2011-re több, mint 400 esetről 300 alá csökkent. Míg 2007-ben 137, 2011-ben már csupán 45 terrorizmussal összefüggő vádemelés történt. 2011-ben Európában nem történt terrorista cselekmény. 2012-ben azonban vallási indíttatású terroristák 6 támadást vittek véghez az EU területen. A vallási indíttatású terrorizmushoz kötődő letartóztatások száma 122-ről 159-re nőtt 2011 és 2012 között. Az Europol megállapítása szerint egyre több úniós állampolgárt szemelnek ki terrorista csoportok emberrablás céljából. Aggasztó és veszélyes jelenség, hogy az EU állampolgárai közül továbbra is egyre többen utaznak terrorista ideológiák és szándékok vonzásában a Közel-Keletre, Afganisztánba, Pakisztánba és Szomáliába. Ami az úgynevezett etno-nacionalista és szeparatista terrorizmust illeti, 2012-ben két ember vált szeparatista terrorizmus áldozatává, beleértve egy észak-írországi börtönőrt. 167 támadást hajtottak végre és 257 egyént tartóztattak le az Európai Únió területen ilyesfajta bűncselekmények kapcsán. Szélsőbaloldali és anarchista terrorista támadásra 2012-ben az EU-ban 18

esetben került sor, és 24 személyt tartóztattak le négy úniós tagállamban. Az olasz anarchistákhoz egyre több erőszakos cselekmény köthető, amelyekhez lőfegyverek használata is társul. Mindazonáltal 2010 óta a szélsőbaloldali terrorizmus vonatkozásában is csökkenő tendencia tapasztalható. Szélsőjobboldali támadást két esetben regisztráltak 2012-ben, és tíz embert tartóztattak le. A szélsőjobboldal megerősödéséhez tevőlegesen és erőteljesen hozzájárul az Internet, a közösségi média. Veszélyforrást jelentenek a birtokukban lévő fegyverek.

A terrorizmus finanszírozása

Amikor terrorfinanszírozásáról beszélünk, alapvetően három dologra gondohatunk:

- műveleti költségekre: ez alapvetően a merénylet kivitelezésének a költsége,
- adminisztratív vagy működési költségekre: ez magának a terrorszervezetnek, a network-nek a fenntartása,
- a merénylők családtagjainak a dotációja.

A terrorista csoportok számára a legfontosabb az adminisztratív, azaz a működési költségek biztosításasa, mert ha arra nincs meg a pénz, akkor a szervezet széthullik. Egy-egy merénylet műveleti költsége viszont döbbenetesen alacsony ahhoz képest, amilyen következményekkel jár. Sok száz halottal és sebesülttel járó merényletet is lehetséges 10-20 ezer dollárból kivitelezni. Közismert, hogy szeptember 11. 4-500 ezer dollárba került, a balii robbantás 20-35 ezer, a madridi amerikai becslés szerint 10 ezer dollárba (a spanyol hírszerzés szerint 60 ezer dollárba, de ez mindegy is, mert ha tíz, ha hatvan, az összeg mindenképpen triviális a sok száz halotthoz képest, akiket maga után hagyott). A finanszírozáshoz szükséges összeg nagyságát a szervezeti struktúra határozza meg. A hierarchikusan felépülő szervezet fenntartása jóval drágább, mint az önmagukat is finanszírozni képes, diverzifikálódott hálózatok ellátása forrásokkal. Az önfenntartó, a központi irányításról leszaka-

dó sejtek nem igen képesek globális horderejű cselekményeket végrehajtani. Ami az öngyilkos merénylők családtagjainak a dotációját illeti, akár egyszeri összegként, akár életjáradékként, nem növeli meg jelentősen a költségeket, mivel az öngyilkos merénylők jelentős része gazdag vagy legalábbis jómódú családból származik. Másrészt sok esetben számíthatnak adományokra: Szaddam Husszein például 25 ezer dolláros sikerdíjat fizetett öngyilkos merénylők hozzátartozóinak. A szeptember 11-i támadás volt az utolsó olyan merénylet, amelyet teljes egészében az al-Kaida finanszírozott; 2002-re a globális finanszírozás kifulladt. A mai robbantások döntő többsége önfinanszírozó csoportok akciójának tekinthető. Más szóval, magának a terrorizmusnak a diverzifikációjával együtt a finanszírozás diverzifikációja is megkezdődött.

Terrorfinanszírozás forrása lehet a legális kereskedelem. Bin Ladennek például Szudánban 30 cége működött 3000 alkalmazottal. Manapság a legkiképzettebb terrorista csoportok már arra is képesek, hogy alvó ügynököket, vakondokat telepítsenek nagy állami cégekbe, intézményekbe, akik évekig nem csinálnak semmit, adatokat gyűjtenek. Amikor kell, akkor aktiválják őket.

A másik fő forrás a szervezett bűnözés. A szervezett bűnözés fontos piacának tekinti a terrorizmust; és sokszor a szervezett bűnözés jelenti a terrorizmus anyagi és technikai utánpótlását. Közismert, hogy elsősorban kábítószer-kereskedelemre, emberrablásra, embercsempészetre gondolhatunk. Talán egyetlen adat: az Europol legfrissebb becslése szerint mintegy 3600 szervezett bűnözői csoport működik az Európai Unió területén, és ezek potenciálisan, az egymásrautaltság függvényében mind terrorfinanszírozóvá is válhatnak. Szerencsére a CBRN anyagok vonatkozásában ez a kereskedelem még nem bontakozott ki. A nukleáris eszközök terén nem ismerünk konkrét eseteket, csak idejében meghiusított kísérleteket. De működő kapcsolatról, szervezett bűnözés és terrorizmus között, a radiológiai, biológiai vagy a vegyi anyagok kereskedelmét illetően sem beszélhetünk.

Az egyik legfőbb kihívásként említhetők, amivel a terrorelhárítás a finanszírozás felderítésében szembenéz azok a non-profit egyesületek, nem-

kormányzati szervezetek (non-govermental organizations, NGO-k), amelyek gyakran jótékonysági fedőszervként működve terrorista csoportokhoz juttatnak el komoly összegeket. A terrorelhárítás kardinális feladata, hogy képes legyen azonosítani az efféle adományok igazi forrásait. A leleplezés rendszerint a pénzmosás módozatainak a felderítésén keresztül történik. A klasszikus pénzmosás és a terrorfinanszírozást szolgáló pénzmosás között van azonban egy lényegi különbség. A hagyományos pénzmosás célja, hogy egy már elkövetett cselekményből származó fekete pénzt bevonjanak a legitim pénzügyi rendszerekbe. A terrorista csoportok azonban azért futtatják át a pénzt legális vagy legálisnak látszó szervezeteken, hogy az összeget eljutassák olyan csoportokhoz, akik abból finanszírozhatják cselekményeiket. Ezek döntően olyan jótékonysági szervezetek, amelyek a válságövezetekbe utazva működnek látszólag humanitárius tevékenység fedésében. A megelőzés és a felderítés számára problémát jelent egyrészt az, hogy nagyon gyakran ernyőszervezetek alatt működnek úgy, hogy maga az ernyőszervezet legitim. A másik probléma pedig adatvédelmi: az NGO-k sokasága nyilván valóban az, aminek látszik. Ha őket is monitoring alá vennék a rendvédelmi szervek – amit egyébként az Európai Unióban sokan forszíroznak –, ellenőrzésük komoly adatvédelmi aggályokat gerjesztene. Magánszemélyek adományaival kapcsolatban például az USA-ban figyeltek fel arra, hogy mivel adójóváírással jár számos ilyesfajta szponzoráció, az emberek nem vizsgálják meg, hogy valójában milyen szervezet az, akinek adományoznak. Kínálkozó példa az úgynevezett Nemzetközi Szolidaritási Mozgalom, amely rengeteg pénzt szedett be turizmus-támogatás és különféle vallások kölcsönös megismertetésének a fedőtörténetével, miközben kifejezetten terrorfinanszírozási küldetést töltött be.

Lehetne még néhány szót ejteni arról, amikor terrorszervezeteket államok támogatnak. Az államok terrorfinanszírozó szerepével kapcsolatban azonban felmerülnek olyan kérdések, amelyek sokkal inkább erkölcsi és világszemléleti, mintsem rendvédelmi természetüek. A merényleteket elkövető vagy megkisérlő tálibok joggal számítanak terroristáknak; rejtett támogatásuk

is joggal minősül terrorfinanszírozásnak. Ugyanakkor azonban köztudomású, hogy ugyanezeket a tálibokat, amikor anno Afganisztánban ugyanolyen eszközökkel támadták a szovjet katonákat, mint most a NATO katonáit, a CIA képezte ki, azaz az USA támogatta. Akkoriban azonban nem tekintette őket a világ terroristának. Az államokkal szembeni fellépés persze túlmutat a terrorelhárítás mozgásterén; noha reálisan számolni kell azokkal a rejtett dotációkkal, amelyek államoktól érkeznek különböző terrorista csoportokhoz.

A világ hét vezető ipari országa, az Európai Közösség és nyolc másik állam részvételével 1989-ben megalapította a Pénzügyi Akció Munkacsoport-ot (Financial Action Task Force, FATF). A FATF ajánlásai kezdetben kizárólag azt tűzték ki célul, hogy megakadályozzák a bankokon és a pénzintézeteken át történő pénzmosást. Mára azonban az FATF a terrorizmus finanszírozásának megakadályozására komplex nemzetközi normarendszert dolgozott ki, és 2012 februárjában elfogadott egy sor új ajánlást. Ajánlásaik között szerepel:

1. A normarendszer implantálása az úniós tagállamok jogrendszerébe

2. A pénzmosás és általában a terrorizmus finanszírozásának bűncselekménnyé nyilvánítása, egységesen a tagállamokban, a megfelelő jogharmonizációs eljárások végrehajtásával.

3. A terrorfinanszírozásra szolgáló vagyonok zárolása és lefoglalása minden tagállamban.

4. A gyanús pénzügyi tranzakciók jelentésének a kötelezettsége. A tagállamoknak kötelezniük kell a pénzintézeteiket, hogy a pénzügyi tranzakciókhoz minden esetben csatolják a feladó azonosíthatóságára szolgáló adatokat (név, számlaszám, a küldemény célja).

5. Külön figyelmet kell fordítani a nem elektrónikus uton történő pénzátutalásokra.

6. Készpénz futárok ellenőrizhetősége. A tagállamoknak elsősorban a bejelentési kötelezettség előírásával és elmulasztásának a szankcionálásával biztosítania kell azt, hogy minden, a határon átlépő készpénz- és értékpapírszállítmány nyomonkövethető és azonosítható legyen.

7. Nemzetközi kooperáció szorgalmazása, folyamatos információcsere, közös szabályrendszer kidolgozása.

8. Non-profit szervezetek pénzügyi tevékenységének az átláthatóságát garantáló eljárások biztosítása. A megelőzés érdekében célszerű megkövetelni, hogy a non-profit szervezetek maximálisan átláthatóan működjenek, kizárólag hivatalos bankszámlákat használjanak, és az átutalásokat ellenőrizhető csatornákon bonyolítsák.

Az ajánlásokkal összhangban a résztvevő országokban Pénzügyi Hírszerző Egységek (FIU) létrehozására került sor. Minden uniós tagállamnak létre kell hoznia egy pénzügyi hírszerző egységet (FIU), amely felel az olyan információk átvételéért, igényléséért, elemzéséért, és az illetékes hatóságokkal történő megosztásáért, amelyek pénzmosással, illetve terrorizmus finanszírozásával állhatnak kapcsolatban. A tagországoknak biztosítaniuk kell a FIU számára a feladatai ellátásához szükséges forrásokat, valamint azt, hogy a FIU hozzáférhessen minden szükséges pénzügyi, igazgatási és nyomozati információhoz. Az irányelv hatálya alá tartozó intézmények és személyek késlekedés nélkül kötelesek a gyanús ügyletekről bejelentést tenni a FIU-nak.

Az Európai Tanács a pénzügyi átláthatóságot célzó állásfoglalása alapján az Európai Bizottság még 2005-ben javaslatot tett a non-profit szervezetek és ernyő-szervezetek átvilágíthatóságára – de ez mai napig nem intézményesült. A Bizottság tanulmányokat rendelt a tagállamok helyzetéről. Az első tanulmány 2008-ban jelent meg, azzal a következtetéssel, hogy az NGO-kal kapcsolatos vád és feltevés nem elég megalapozott. 2010-ben, majd 2011-ben a Bizottság nyilvános konzultációt kezdeményezett a fő résztvevőkkel. Az Europol is éves értékeléseiben (TE-SAT) közzétesz a non-profit szervezetek és a terrorizmus kapcsolataira vonatkozó megállapításokat. Az Europolnak itt is központi szerepe van a tagállami tapasztalatok és stratégiák összehangolásában és koordinálásában, valamint a közös standardek kimunkálásában. Az EU Hírszerzési Központja is végez folyamatos fenyegetés-értékeléseket a terrorfinanszírozás csatornáiról, szereplőiről és várható trendjeiről. A nem-

zetközi normák 2012 februárjában közzétett módosítása nyomán az Európai Bizottság úgy döntött, hogy a szükséges módosítások beillesztése érdekében haladéktalanul aktualizálja az uniós jogi keretet. A jogi előírások javasolt frissítését az Európai Parlamentnek és a Miniszterek Tanácsának rendes jogalkotási eljárás keretében kell majd elfogadnia.

Dr. Hankiss Ágnes képviselő, Európai Parlament
az EP Biztonsági és Védelempolitikai Albizottság
Néppárti Kiberbiztonsági Tanácsadó Testület tagja

Zala Mihály

Kiberfenyegetettség elemzés az elektronikus terrorizmus elhárítását célzó intézkedések körében

Az internet és a digitális eszközök ugrásszerű és jelenleg is folyamatosan növekvő térhódításával mindennapjaink szerves részévé vált a digitális lét, a kibertér. A gazdaságilag jelentős, de legalább számottevő helyet képviselő országokban napjaink legfontosabb kommunikációs forrásává az internet lépett elő.

Ebből következően napjainkban a gazdaságilag, társadalmilag jelentős támadások szervezése és kivitelezése már döntően a kibertérben zajlik, így kiemelt jelentőségűvé váltak a különböző kibervédelmi képességek.

Az Nemzeti Biztonsági Felügyelet (továbbiakban NBF) is rendelkezik a kibervédelmi képességek terén kapacitással, melyeket a különböző kapcsolódó magyar szerveken kívül NATO és EU szinten is megoszt.

A társadalom digitalizálódása következtében, ami rohamos gyorsasággal terjed ki az élet minden területére, a kibervilágban is egyre nagyobb kockázat. Ennek kivédésére az egyik legfontosabb képesség a kiberfenyegetettség elemző kapacitás. Az NBF ez irányú megközelítésében a legfontosabb a prevenció.

A továbbiakban az erre alkalmazott módszerek kerülnek bemutatásra gyakorlati példákkal szemléltetve, valamint az NBF kibervédelmi képességei, különös tekintettel a kiberterror cselekmények megelőzésével kapcsolatban.

Bevezetésként egy kis összefoglaló az elmúlt hónapban (2013. szeptember) történt és a nyilvános média által is közzétett kiberfenyegetettségekről, illetve kibertámadásokról, amely az elmúlt hónapok fényében nem volt kiemelkedő, teljesen átlagosnak tekinthető.

- Belgiumi vonatkozásban például a Belgacom informatikai rendszerében fedeztek fel egy olyan malware fertőzést, melyet, tekintve, hogy információszerzésre használtak, először az amerikai NSA-nek tulajdonítottak,

nem sokkal később azonban kiderült, hogy valószínűleg a brit GCHQ volt a „kémkedő".

- Jól látható az USA és Szíria közötti események (vegyi támadások) médiában is azonnal megjelent lenyomata, melyek a politikai, gazdasági helyzet miatti fokozott kiberfenyegetettség és az ezzel kapcsolatban megjelenő intézkedésekről szóló hírek formájában jelentkeztek.
- A kibereseményekkel is összefüggő hírek kulcsszavait elemezve az USA és Izrael közötti, a médiában is megjelent kibereesemények által generált kapcsolat is szépen megjelenik, melyet az okozott, hogy az AnonGhost (az Anonymous egyik ága) bejelentette, hogy újabb kibertámadást tervez az izraeli weboldalak ellen.
- Szintén 2013. szeptemberi kiberesemény Brazília, USA és Szíria vonatkozásában a NASA sub domain-jének deface-elése, melyet brazil hacker-ek követtek el, Obama Szíriával kapcsolatos háborús tervei ellen tiltakozva.
- Az eset azonban széleskörű derültséget okozott a hacker világban, ugyanis a hackerek eredetileg az amerikai NSA oldalát vették célpontba, azonban vagy egy betűt elnézve, vagy mert a NASA-nál könnyebben találtak kihasználható sérülékenységet,mint az amerikai NSA-nél, végül nem az eredetileg deface-elésre szánt oldalt sikerült feltörni.
- Nagy számban jelentek meg a ransomware fertőzésekkel kapcsolatos hírek is. A ransomware-ek a malware-ek egy olyan, 2013 óta kiemelkedően nagy számban terjedő fajtájái, melyek valamilyen fenyegetéssel pénzt próbálnak szerezni a fertőzött gép felhasználójától. Ez általában azt jelenti, hogy használhatatlanná teszik a számítógépet vagy elérhetetlenné a rajta lévő, illetve rajta keresztül elérhető és írható adatokat, az eredeti állapot visszaállítását pedig egy olyan azonosítóhoz kötik, amit az áldozat bizonyos összeg kifizetése után kaphat csak meg. Elterjedt módszer, hogy az áldozat megtévesztése céljából a tájékoztató a visszaállításért fizetendő összegről és a kapcsolódó egyéb teendőkről a rendőrség vagy

egyéb hatóság nevében jelenik meg.

- A szíriai helyzet kapcsán a médiában egyre gyakrabban jelenik meg a cyberwarfare fogalma is, továbbá az újabb zero-day sérülékenységek, az azokat kihasználó exploitok, például az Internet Explorer éppen publikált egyik sérülékenysége okán.

A felsorolt, a médiában is megjelenő hírek kulcsfogalmaiból és az azokhoz tartozó információk elemzéséből megállapítható például, hogy egyes sérülékenységek mely hacker csoportoknak kedveznek.

Az elemzések eredményeként a kihatásokat, következményeket viszonylag nagy pontossággal fel lehet mérni, vagyis előre jelezhetők az egyes események kibervilágra gyakorolt hatásai, beleértve a kiberfenyegetettségeket is. Mindez megfelel Barabási-Albert László Villanások című könyvében leírtaknak is, mely szerint bárkinek a viselkedéséből nagy valószínűséggel meg lehet állapítani, mit fog tenni később, esetleg a vele kapcsolatban állók mit fognak tenni az ő viselkedése hatására.

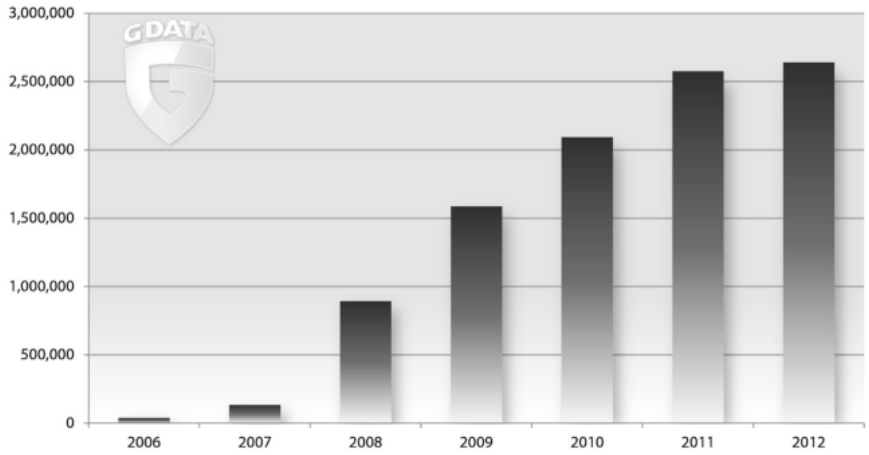
Mindehhez nem kellet senkit külön lehallgatni, kizárólag a bárki számára elérhető hírekből:

- meglepően nagy pontossággal megállapítható, hogy például az egyes sérülékenységeknek, hacker csoportoknak mi mindenre van, illetve lehet kihatásuk,
- valamint az is látszik, hogy kiberfenyegetettségek tekintetében is, nem meglepő módon, rendkívül magas a kapcsolódó politikai, gazdasági, társadalmi események száma.

Hasonlóképpen visszanézve az elmúlt évek eseményeit, kijelenthető, hogy a terrorcselekmények alakulása szintén erős összefüggést mutat kibertér használatának elterjedésével.

Ez alapján jól látszik, hogy a terrorcselekmények száma jelentőset zuhant a ’99-es dotcom válság idején. A következő mérföldkő pedig 2011. szeptember 11-i terrortámadás volt, aminek nagy része, az előzőekkel ellentétben már a kibertérben szerveződött.

2006 környékétől pedig ugrásszerű növekedés történt az „újszerű" terrorcselekmények számát illetően, ami nem mellesleg egybeesik a malware-ek, APT (Advanced Persistent Threat) támadások, vagyis a célzott kibertámadások növekedésével, amit az alábbi, a G-Data nevű vírusírtó cég által készített grafikon mutat, melyen az évente újonnan megjelenő malware-ek számszerű összesítései kerültek bemutatásra.



A terrorcselekmények és a kibertér bővülése tehát egyértelmű összefüggést mutat.

Ha a '99-es dotcom válság során tapasztalt visszaesés okát keressük, akkor azt nagy valószínűséggel az okozta, hogy a terrorista csoportok ez idő alatt folyamatosan azon dolgoztak, hogy a korábban alkalmazott módszereiket hogyan ültessék át a kibertérbe. Ez az időszak átmenet volt egy már „jól bejáratott" és egy akkor még kevésbé ismert, de az előzőeket egyértelműen leváltó rendszerek között.

A '90-es évek végén kezdett el igazán terjedni az internethasználat. A kibertér ugrásszerűen bővült, a politikai, gazdasági élet kulcsfontosságú műveleteket végző rendszereit, vagy azok egy részét csatlakoztatták az internethez.

Tekintve, hogy gyakorlatilag minden rendszer sérülékeny, ha egyetlen

olyan pontja is van, melyen keresztül csatlakozik az internetre, vagy akár csak közvetve, egy másik internetre már korábban csatlakozott eszközhöz, akkor még a „zárt" rendszerként kezelt hálózat is kitett az internet felől érkező támadásoknak. Vagyis a kiberfenyegetettség napjainkban gyakorlatilag mindent és mindenkit érint, beleértve a kritikus infrastruktúrákat, az ellátási láncot is.

Az informatikai rendszerek sérülékenységeit előszeretettel használják fel nemcsak terror, hanem egyéb politikai, gazdasági, társadalmi célú támadásokhoz, amiknek a kéretlen e-mailek ma már egyre kisebb részét képezik. A támadások sokkal összetettebbekké váltak, tekintve, hogy többféle és azonos vagy nagyon hasonló komponenseket használnak fel minden egyes célzott támadás során. Ezeket a komponenseket pedig a szintén a '90-es években kifejlődött és napjainkban gyakorlatilag „virágzó" „kiberalvilág" a megfelelő internetes fórumokon, webáruházakban pénzért árulja.

Mindebből következően a célzott kibertámadások nagyon nehezen detektálhatók, a támadás célja pedig még nehezebben, hiszen sok esetben kiberbűnözőktől vásárolják az egyes komponenseket, így még nehezebb megtalálni az eredeti elkövetőt.

Ahogy a támadás, úgy annak hatékony megelőzése, vagy ha a már bekövetkezett annak kezelése is rendkívül összetett, de egyáltalán nem lehetetlen. A kulcstevékenység az együttműködés. **A kiberfenyegetéseket lehet tehát kezelni, melyhez a következőket szükséges alapul venni és megfelelően alkalmazni.** Az információs rendszerekben a felhasználók, rendszer és szabályok rendszerének harmóniája határozza meg az információ biztonságát. Azaz, ha a felhasználók képesek a rendszereket kezelni, ha a rendszerek valóban a felhasználói igényeket támogatják. Ha a rendszerekben kialakíthatóak olyan szabályok, amiknek a mentén biztosítható a felhasználói adatok biztonsága, valamint a felhasználók motiváltak a szabályok betartására, akkor lehet valódi biztonságról beszélni.

A harmónia rendszeresen változik a rendszer alkotóelemei között, a sérülékenységek, a károkozás lehetőségeinek és a rosszindulatú szándék kialakulásának okán.

- Ha egy rendszer nem megfelelően támogatja a felhasználókat, vagy azok nem tudják rendesen használni azt, akkor sérülékenységek alakulnak ki.
- Ha a szabályzatok, biztonsági kontrolok nem megfelelőek jogosulatlan adatkezelés, hozzáférések lehetősége merül fel
- Ha a felhasználók nem tartják be a szabályokat, megjelenik a rosszindulatú szándék.

Tehát, hogy mindez hatékonyan működjön:

- fel kell tárni és lehetőség szerint ki kell javítani a sérülékenységeket. (Sajnos több okból kifolyólag, pl. alkalmazásspecifikáció, nem minden esetben javítható az adott sérülékenység),
- ismerni kell az információs rendszerek hálózatát, vagyis milyen információ illetve milyen rendszer honnan érhető el, mivel van összekapcsolva. Egy rendszer sérülékenysége kihatással van/lehet a vele bármilyen kapcsolatban (nemcsak fizikai) álló másik rendszerrel (milyen lehetőségek állnak rendelkezésre a kompromittációhoz).
- fel kell mérni, milyen célból érdeklődhetnek egy információs rendszer után (például ipari kémkedés). Ennek ismeretében lehet fókuszálni az fenyegetett rendszerekre, így a védekezés is hatékonyabb.

Ahhoz, hogy ezt a három fő területet a lehető leghatékonyabban kezejük és ezáltal a fenyegetettségeket is hatékonyan csökkentsük, illetve az esetlegesen bekövetkezett támadásokat kezeljük, a „belépő" a CTAC, vagyis a kiberfenyegetettség elemző képesség.

Védekezés és incidenskezelés szempontjából ezt a területet jelenleg szinte teljes mértékben figyelmen kívül hagyják, pedig kulcsszerepe van a támadások megelőzésében. Megfelelően használva kivédhető a jelenleg bekövetkező támadások akár 80%-a is. Ennek persze az egyik legfontosabb feltétele a szervek és intézmények együttműködése, mind hazai, mind pedig nemzetközi szinten.

Mindez a gyakorlatban a hatékony információmegosztás köré szerveződik, vagyis:

- az észlelt támadások jelzése

- visszajelzés az intézkedési tervjavaslat végrehajtásáról, vagy adott esetben annak részben vagy egészben való meghiúsulásáról és annak okairól
- a kapcsolódó szervek informatikai rendszereinek aktuális biztonsági állapotáról (például mit és milyen verziójú alkalmazásokat használnak), tekintve, hogy ezek az információk például egy malware vagy egyéb célzott támadás esetén jelentősen gyorsabb és hatékonyabb intézkedést tesznek lehetővé.

Ugyanakkor a CTAC során feldolgozott információk teremtik a talán leghasználhatóbb alapot kiberbiztonsági szituációs gyakorlatok számára, amik segítségével szintén nagymértékben növelhető a kiberfenyegetettségek elleni védekezési képesség.

Az NBF munkájában mindez az alábbi módon jelenik meg:

- OSINT (Open Source Intelligence) – a kibertérhez kapcsolódó, az interneten és egyéb „nyílt" adatbázisokban elérhető információk
  - napi szintű nyomon követése,
  - rendszerezése,
  - elemzése,
  - „fenyegetettségi" faktorokba való sorolása.
- Indokolt esetben a kapcsolódó hazai és nemzetközi szervek, intézmények
  - figyelmeztetése a lehetséges veszélyekre,
  - intézkedési tervjavaslat készítése.
- Időszaki jelentések készítése az aktuális kiberhelyzetről.

Az NBF gyűjti és rendszerezi a már bekövetkezett és a publikus médiában is közzétett támadásokat.

Csak ezeknek az információknak a megfelelő elemzésével is rengeteg minden kiolvasható a kiberfenyegetettségekre vonatkozóan.

Például megállapítható, hogy az egyes hacker csoportok

- milyen típusú módszerekkel dolgoznak,
- milyen hatásfokkal,
- illetve milyen típusú intézmények, valamint informatikai rendszerek és

alkalmazások a lehetséges áldozatai az adott csoportnak.

Vizsgálva az egyes csoportok például politikai, vallási irányultságát, a politikai, gazdasági eseményekkel összevetve az is előrejelezhető, hogy éppen melyik csoporttól, vagy akár országból várható valamilyen kiberaktivitás.

Visszatérve az együttműködésre, mindez a következő módon segítheti a mostaninál jóval hatékonyabban a kiberfenyegetettségek elleni védekezést: az aktuális politikai, gazdasági, társadalmi helyzet ismeretében nagy eséllyel megállapítható a fenyegetettség, vagy támadás okának háttere, a potenciális elkövetők támadási módszerei.

Előrejelezhető:

- milyen típusú informatikai rendszerek, alkalmazások a várható célpontok.
- mely informatikai rendszerek, alkalmazások rendelkeznek az adott csoport által jellemzően kihasznált sérülékenységgel.

Az NBF munkájában ez például a gyakorlatban úgy valósul meg, hogy, amennyiben a helyzet súlyossága indokolttá teszi, elhárítást célzó intézkedési tervet is készít, illetve „korai riasztás" formájában összefoglalja és kiküldi a kiberfenyegetettségeket kezelő központi szervnek (GovCERT) az aktuális kiberesemény leírását, aki azonnal szétküldi a szükséges helyekre, ahonnan visszajelzést is küldenek a kapcsolódó tevékenységekről.

A visszajelzések kiértékelése pedig nagyban segítheti a későbbi kiberfenyegetettség, vagy kibertámadás esetén szükséges gyorsabb és hatékonyabb reagálást.

Amennyiben ezt a fajta együttműködési rendszert sikerül megvalósítani és működőképessé tenni, Magyarország méltán mondhatja el magáról, hogy a kiberfenyegetettségek kezelésében világviszonylatban is a lehető leghatékonyabb módszert alkalmazza, és ezzel nemcsak hazai, hanem nemzetközi szinten is sokat tehet a kiberfenyegetettség mértékének csökkentésében.

Zala Mihály vezérőrnagy
elnök, Nemzeti Biztonsági Felügyelet

A konferencia pénzügyi támogatói:

Hanns Seidel
Alapítvány

Magyar Posta Zrt.

MVM Magyar
Villamos Művek Zrt.

MOL Nyrt.

Nemzeti Média- és Hírközlési Hatóság

Kiadja a BM Oktatási, Képzési és Tudományszervezési Főigazgatóság
Felelős kiadó: Dr. Dános Valér ny. á. rendőr vezérőrnagy, főigazgató
Nyomdai munkák: King Company Kft., Tamási
Tördelés és nyomdai előkészítés: HBU Kft., Kozármisleny
Készült 400 példányban, 2014-ben

A kiadvány szakmai támogatói

ISBN 978-963-868
9789638686220

Belügyminisztérium Oktatási, Képzési és Tudományszervezési Főigazgatóság
www.rvki.hu