HADMÉRNÖK

VIII. Évfolyam 4. szám - 2013. december

Papp Zoltán
pappz.szeged@gmail.com

INFORMATION TERRORISM

Abstract

People talk more and more about different terrorist acts and their perpetrators. Information-terrorism can be examined from several sides. It can be approached form personal composition, motivation, or goals of the criminal act, or either the applied technical means, Furthermore, we must keep in mind that with society developing and changing, terrorism – within this information-terrorism – changes as well, especially regarding personal composition, development of technical means and changes of methods and goals. As a result, compared to the past, terrorism has become more complex. To reveal the real dangers of information-terrorism the changes terrorist acts have gone through with regards to personal and technical levels and the way the mentioned subjects join to each other has to be highlighted.

A világban egyre több szó esik különböző terrorcselekményekről és azok elkövetőiről. Az információs terrorizmus több oldalról vehető vizsgálat alá, ez alapján megközelíthető a bűnelkövetés személyi összetétele, motivációi, céljai vagy akár az alkalmazott technikai eszközök irányából. A megnevezett területeken túl nem szabad figyelmen kívül hagyni, hogy a társadalom fejlődésével, változásával a terrorizmus, ezen belül az információs terrorizmus együtt változik, ide értve ennek személyi összetételét, a technikai eszközök fejlődését, valamint a módszerek, célok változását. Ennek eredményeképpen napjainkban a terrorizmus egy másik arcát mutatja, egy, a korábbiakhoz képest lényegesen összetettebb oldalát. Az információs terrorizmus valós veszélyeinek feltárásához rá kell világítani, hogy a korábbi időszakokhoz képest a terrorcselekmények személyi és technikai szinten milyen változásokon mentek keresztül, valamint hogy a megnevezett témakörök miként kapcsolódnak össze.

Keywords: *terrorism, information-terrorism, information society ~ terrorizmus, információs terrorizmus, információs társadalom*

INTRODUCTION

More and more reports on differently committed terrorist acts and the perpetrators appear in the media. Today a major portion of these operations are attacks carried out in the "traditional" physical scene and committed in the "usual" manner but more and more news surface which – if analyzed – reflect scaring perspectives regarding the expectable development of terrorism. One of the most expressive, most often recited depiction is: "While Bin Ladin's finger is on the trigger of an AK 47, his cousin's is on a computer mouse." This depiction well expresses the generation change and the new direction expectable in terrorism. [1]

While politics and its adjustments mostly affect the ideology of terrorism, the technical/technological development can be caught in the method of a terrorist act being executed and partly in the way of choosing targets. Every technical accomplishment, spreading and acquirable technology appears right away in the argosy of terrorist methods, so when examining the phenomenon it is necessary to also analyze how technical/technological development influences the methods of terrorism and what effect it has on the composition of perpetrators. Nowadays we are witnessing the inevitable incursion of info-communication means and technologies and the new possibilities provided by them have already appeared in the stock-in-trade of terrorists.

According to a generally accepted, non-legal definition, terrorism is the strategy of using or threatening to use violence with the primary goal to cause fear and disorder and by it attain specific political results or profound ruling power. Fear is concomitant of every form of violence, but in the case of terrorism this footing is opposite, maximum victims of violence are in symbolic relation with the real goal of the terrorist act, their selection is of secondary importance, mostly coincidental. [2]

Society and its members can be threatened and kept in fear in several ways. It is almost evident that the greatest effect on today's information society can be accomplished via information systems providing undisturbed operation With respect to the fact that currently the operation of all infrastructures is supported by information sub-systems, the above statement is prominently true. Information-terrorism – due to the fact that we are facing a relatively new phenomenon – yet has no complete definition uniformly accepted by specialists of information technology but in literature two definitions seem to be delineating which have been phrased by the FBI and Kevin Coleman security expert. According to the FBI "cyber-terrorism is a criminal act perpetrated by the use of computers and telecommunications capabilities, resulting in violence, destruction and/or disruption of services to create fear by causing confusion and uncertainty within a given population, with the goal of influencing a government or population to conform to a particular political, social, or ideological agenda." On the other hand, Coleman says that "the premeditated use of disruptive activities, or the threat thereof, against computers and/or networks, with the intention to cause harm or further social, ideological, religious, political or similar objectives or to intimidate any person in furtherance of such objectives" represent information terrorism.

The two definitions have an essentially different viewpoint regarding the background of the problem. The first considers information infrastructures as means, while the second definition sees information infrastructures as targets of terrorists. However these days, information infrastructures are understood as a confined part, sub-system of different critical infrastructures, thus at the present state of information technology all infrastructures are operated, directed and controlled by different, complex, articulated and functional info-communication systems (…) so the whole of and part of them are considered as critical infrastructures [3], thus the implicates in the two above definitions are accomplished at the same time, therefore it would be expedient to unite the two definitions.

INFORMATION-TERRORISM

As a result of technical development, media and the faster than ever spreading news reaching greater number of people and transporting messages of terrorists to the members of information society greatly affects the present form and methods of terrorism. For accomplishing their goals, terrorists of the 21st Century consciously make use of and exploit information infrastructures of information society. For their illegal activities via these systems they:

1. *Spread their ideology in an active and passive way:* By using new technologies (communication and community solutions) and operating homepages they are able to actively communicate their motivation and goals, address society and – in a passive way – reach that people in different forums communicate about them which is a way of gaining publicity.
2. *Attempt to gather sympathizers and recruit members and supporters:* The above methods provide a perfect possibility for the groups conducting the above mentioned illegal activity to contact people agreeing with their ideology, to get feedback from them and to draw those committed to their gals into their acts or even let them into a group itself.
3. *Collect sources:* Those executing terrorist acts need to apply different sources (infrastructure elements, computing capacities, etc.) for carrying out certain operations which they physically lack. They can obtain these sources from their supporting sympathizers or even illegally via intruding different systems (i.e. botnets).
4. *Finance operations:* For a majority of illegal operations to be executed within the cyber-space great expertise is required besides obtaining the valuable means. To purchase or learn these means or expertise financial sources have to be drawn in. With using information systems the information-terrorists can effectively raise the necessary assets, either from the sympathizers or by illegal means like fraud (hoax), intruding financial systems, obtaining and selling private and business data, etc.
5. *Search for targets:* Information systems are perfectly suitable for terrorists to identify potential targets. They use different information technologies [i.e. broadcasting (political, scientific-informative), Internet] for talent-spotting helping them in screening geographical areas, industrial branches, periods, events, etc.
6. *Collect information:* Many sensitive data can be obtained in the different information systems of the majority of chosen targets although the access to some databases are restricted, not ever enquirer can access them (although they can be attacked with different methods also), but information suitable to cause disturbance to the normal operation of the target can be collected from open sources as well. The different community portals where the users may post data providing valuable assistance for attacking the targeted system – indifferent for outsiders – may gradually become a larger platform for collecting information.
7. *Destroy:* With using information system, different techniques, technologies and their combinations other information infrastructures may be attacked effectively.

In case of illegal operations carried out in cyber-space the fact that numerous solutions (i.e. proxy servers, TOR, etc.) exist which assure a relatively extent anonymity for the perpetrators is of great benefit. Also the physical positioning of the attackers and targets is of great importance since the meaning of physical distance in this form of terrorism can hardly be elucidated. Frontiers mean no obstacles for perpetrators when carrying out the operation, but at the same time, frontiers often mean significant, impassable legal or technical obstacles for the attacked infrastructure or for the authority "representing" it when taking counter-measures to prevent or perhaps reconnoiter perpetrators.

INFORMATION-TERRORISM

Often in cases of cyber-criminal or information-terrorist acts the reports or commentates present the perpetrators as "ordinary" criminals or terrorists but these individuals are quite far from the stereotypes evolved in society. While cyber-criminals – fearing the consequences –try to keep their activities in secret the information-terrorists – stemming from the core of terrorism – try to communicate the "results" of their acts to as many as possible. Although the used means are the same in both cases – or at least show a great overlapping -, their motivation and goals are much different. While criminals mostly attack economic (banking) and large industrial systems for financial benefits, terrorists destroy communication, traffic and public utilities, at times of conflicts they disturb the communication of police forces, thus can abate police forces' efficacy.

A common momentum coming from the overlapping of applied methods is that the masterminds of cyber-criminal and terrorist acts are in possession of extremely high level of expertise and have university degrees. Furthermore, they plan their covert or transparent operations with extreme circumspection and manipulate it with extent patience and discipline for months even. Based on the obtained outgrowths, positive and negative experiences they refine their methods. They are the ones who can be considered as the upper caste of information terrorism, the most dangerous stratum because – in spite that behind their motivations emotions excited for different reasons – in place of precipitated fit of passion they are able to react with well planned rejoinder throughout which they can optimize the resources at their disposal, the reasonably attainable goal, the target's inadequate security and naturally the security measures. If not as a separate caste, perpetrators (mostly employees) indirectly representing danger by illegally using, disclosing, leaking information in their possession relevant to sensitive infrastructure (with regards to all of it, part of it, or its vulnerability, etc.) can be considered as a part of the upper caste, since with their act they endanger security or corrupt effective operation. Those can be considered as part of the secondary caste that do not possess outstanding knowledge of information technology but conform to the goals of terrorists, with the software created by the upper caste and with their direction take part in the attack or in the preparations. Although the typical form of attack regarding this caste is a DDoS attack, many other methods exist and are available when attacks can be perpetrated with instruments available in commerce or by modifying them, or just with equipment compilable at home, so many unsuccessful attempts, smaller of larger trials and errors can be expected from them.

SOCIOLOGICAL BACKGROUND

When analyzing terrorist acts committed in cyber-space it is necessary to examine who were the ones to conceive of and carry out the attack and in what way did they get to their act. A wide range of forensic science is investigating the sociological background of becoming a criminal, with the process that results in the individual breaking those social behavior patterns, norms, values, attitudes which allow him/her to become a socially integrated person.

The first socializing scene for an individual is the family and the close milieu. An individual takes part in micro and macro-social groups through his/her whole life affecting him/her in a positive of negative way. During identification a child gets attached to those who are the closest to him/her, in other words mostly to his/her parents and family. Later this circle expands having an effect on the development of personality, behavior and social virtue to a different extent and in a different way.

When analyzing generations it can be established that a few decades ago the influencing power of the family on the development of personality was stronger than today. Nowadays the positive pattern of parents is more and more de-emphasized. The reasons of this may be the large number of divorced parents, the parents' continuous struggle with the lack of time they

can spend with raising their children. The development of personality in childhood or adolescence are greatly influenced by the pervasive strength of companionships and groups which in time take over the place of the family in the primary social scene. In the early life stages criminal acts are characteristically committed in groups and are mostly crimes against property. There are several reasons to these phenomena like the influencing power of the group, the position of the person within the group, undeveloped personality, boredom or just a thirst for adventure. Furthermore, in later stages of life, changes happening in a person' living conditions, like for example unemployment or hunger, can turn somebody onto the route of delinquency since the person may think that this is the only possibility to keep up a standard of living (i.e. keep his/her house) of provide the necessary material needs for his/her family. [4]

Nowadays science is developing to a greater extent demanding education to keep up with it, so a greater emphasis is put in information technology which the majority of students are greatly interested in. One of the reasons is that for a child or adolescent emotionally and physically neglected – living in either good or bad social circumstances – family, space expands by the Internet. He/she can become a part of virtual worlds lacking from his/her real life, via the different community sites he/she can belong somewhere. The role of community and becoming members of gangs has increased in the process of socialization but at the same time the features of crimes committed has changed as well.

Another problem is that many parents are not adept in information technology, they do not perceive the concomitant dangers, or if they do have some idea of it they tend to lessen its severity and are rather happy to see their children near them and not "sauntering on the streets" even thought the gangs of the virtual space are at least as dangerous.

In addition another factor has to be mentioned that can urge someone to commit a crime. These are those special situations that add up to distinctive behavior and a person with a high criminal potential may come to a decision in a given circumstance resulting in a crime. In case of information terrorists, a momentum to be highlighted is the person himself/herself, or a vindictive reaction, a kind of justice, vengeance to a putative or concrete offense against a person, group or any symbol important to him/her. An outstanding circumstance is that in case of illegal acts committed in the cyber-space the perpetrators tend to trivialize the gravity of their acts, they do not consider them as common law crimes. The fact that they most likely identity will remain faceless may give them further incitement.

In case of information terrorism – with respect to the special circumstances of illegal activity – the perpetrators do not come from the lower stratum of society since the know-how obtainable in higher education and the expensive high-tech equipment are usually ready for the middle or upper class young people who being interested in or in the possession of special knowledge may even specialize in the different methods and targets (i.e. hackers, crackers, phreaks, hacktivists).

Overall it may be stated that the reason of an individual becoming an information terrorist is multiple. The behavior pattern mediated towards him/her during his/her life by the family and the companionship and the type and number of special effects influencing him/her during his/her life is of great importance. Furthermore, it is significant how the person reacts to all this being proficient in information technology that eventually determines the criminal potential of the person to information terrorist acts.

SUMMARY

Summarizing the above we may establish that the personal content of criminal acts and the stock-in-trade of means used for perpetration have significantly changes with the march of time. A few decades ago generations passed on the "knowledge" necessary criminal offences that have by now been taken over by the thirst for guided studies and the attainment of sophisticated computing skills used by the individual to take the smallest risk possible when committing a given crime.

With the sophisticated knowledge of the operation of computer systems the identity of the perpetrator remains hidden; the risk is less than is the physical presence. It is no longer necessary for an information terrorist to appear on the site according to the "old methods", giving possibilities to make mistakes; it is enough to have a quite high level of computing skills.

Examining the terrorist acts and the circle of perpetrators is delineating that anti-life and destructive acts are characteristic of terrorists of low intelligence and education, while the perpetrators of information criminal acts are individuals of high intelligence quotient who were not socialized on the social periphery.

References

[1] NATO Mirror 16 2001/2002 winter

[2] http://hu.wikipedia.org/wiki/Terrorzmus (downloaded 28 May 2013)

[3] Zoltán Papp: Possible attacks against critical information infrastructures, with special respect to attacks against computer networks, ZMNE, Lead (2009)

[4] Dr. András Csúri: Young adulthood, as a stage of criminal law relevance. PhD thesis (2008).