THEORETICAL AND HISTORICAL PROBLEMS OF LAW AND POLITICS

Olha Novytska
First Secretary Ministry of Foreign Affairs of Ukraine

USE OF THE NEW TECHNOLOGIES BY TERRORIST GROUPS AS A NEW CHALLENGE FOR NATIONAL SECURITY CONCEPTS

The Internet has become an integral part of our life. As in any sphere, it has a good and a bad side to it. The bad side includes its use by cyberterrorists and other criminals, which is recent years has gained more importance due to the improvement of technical profess of such terrorist groups as ISIS. Besides, there has been a considerable raise in the popularity of extremist online rhetoric among young Europeans infatuated with its simplicity and fake truthfulness. Most frequent ways of use of the Internet for terrorist purposes are fundraising, recruiting, communications and content sharing, each having its peculiarities and target audiences. With the enlargement of the pool of web-surfers, mobile Internet users *inter alia*, grow the opportunities for the terrorists to use the technology for their unlawful purposes. The variety of those ways leaves no doubt that this problem concerns each and every one of us. There have already been cases of entire states or their certain governmental and business institutions suffering painful cyber-attacks. At the same time, the agencies working in the sphere of fighting terrorism in the cyberspace also have to deal with such dilemmas as the freedom of speech or faith, which are crucial for the democratic societies, vs national security and the general good, which adds complexity to the already sophisticated issue. The only way to try to curtail the upswing of cyberterrorism may lie in cooperation between all parties involved: the regular people, the governments, the law enforcement bodies and the IT businesses.
Keywords: terrorism, cybercrime, online security, ISIS, Islamic State, mobile security, propaganda, online privacy, freedom of speech.

The plot depicting a possible intrusion in the operations of the fundamental systems of a state, or other forms of cyber-terrorism and hacking has been a staple in Hollywood action movies for a long time, since the era when PCs were not yet so common in households. Furthermore, a personality theft is today one of the main movie plot twists. The number of financial and human resources involved in fighting cybercrimes totals dozens, if not hundreds, of billions of USD. Books, voluminous scientific research dedicated to the "dark side of the brave new digital world", as one may call the cybercriminal sphere, also appear regularly.

Today most research is aimed at building a system from the available information as well as analysis of the strategies the criminals use, more profound scientific works are targeting different sides of the phenomenon of terrorism per se. The aim of this article is to outlay the main points formulated mainly by foreign researchers in the field of cybersecurity.

The last decade made it clear to the entire world that the list of potential threats to the national and personal security since now includes Internet. On the one hand, thanks to the Web and IT crowds of people received new opportunities for communicating, working, improving their lives and lives of people around. At the same time, such benefits of the Net as interconnection of all components and anonymity (if one takes certain precautions) are being more and more actively used by both hackers and terrorist groups. This space has no boundaries, practically every state entity is connected into it, hence to make a tangible damage to a powerful country or a company one does not need a large army of highly trained professionals – sometimes computers of the military are themselves targeted by the terrorists.

Terrorist attacks in the Internet may gain international scale even faster, then, for instance, a cataclysm and to involve all the citizens. To destroy an economy no nuclear bomb is needed today –

a certain software, technical means and a couple of smart people. This has made the organizations dealing with security issues in most Western states draft plans for the emergencies in the information sphere and to perform regular checkups of the governmental bodies. At the same time, both national and international laws in the security sphere lags behind the technical proficiency of hackers and cyberterrorists. Taking into consideration the low level of informational sphere development in many countries, use of cyberwarfare against them looks a highly possible perspective.

Several events that took place during the last couple of years have attracted the attention of the scientific community to the topic of terrorism and online activity of the terrorist groups. The Western experts have written dozens of articles in the scientific and popular journals, blogs – a publication dedicated to the enrollment of women through social networks was even placed in the Russian edition of the Cosmopolitan magazine[1] – the above issue is gaining urgency even in the post-Soviet states. At the same time the question of preventing damage from cyber-terrorism cannot be an object of strictly scientific, theoretical interest as it's connected with a constantly changing and evolving environment.

However, in our mind, one should make a firm distinction between cyberterrorism proper and a terrorism using the digital sphere for its purposes, and cybercrime – usual hackers or network penetrators. Not all terrorists are also active in the digital space and not all cyberterrorists are ready to come out into the real world. On the other hand, such organizations as the Islamic State of Iran and Levant/Syria (ISIS or Daesh by its Arabic acronym) use all the spheres so one can put them in both groups. It is such organizations that are of the highest interest both from the practical and the theoretical-exploratory points of view and are therefore the focal point of the article below.

All the members of the sphere of cyberterrorism or cyberattacks can be roughly divided into the following groups[2]:

1. States developing their defense or attack potential as a part of national military force;
2. Delinquents acting, first of all, with the aim of earning unlawful profit;
3. Business companies – foremost willing to secure their confidential information, and sometimes attacking their competitors' networks;
4. Terrorist organizations, using web resources to satisfy their own practical goals as well as to carry out cyberattacks;
5. Anarchists striving to harm the system of all-over computer use in general in order to dismantle the existing order.

The first country that suffered from a deliberate cyberattack was Estonia. Its governmental networks became targets for a massive aimed assault, the result of which was a stimulus for the state to begin literally an informational breakthrough. Today all the banking operations there are done electronically and the data encrypting system is considered the best in the world.

Another state that was forced to speed up the development of cybersecurity sphere due to numerous tries to break the normal functioning of its business and governmental structures, is Israel. Today this small country controls about 10% of the international market of the means of informational security, the turnover of which in 2015 was estimated at 86 USD[3]. In 2010 with the help of hacker software Stuxnet, that most experts believe was developed jointly by Israelis and Americans, a considerable damage has been made to the functionality of the Iranian nuclear reactor in Natanz[4]. Although all parties refrained from publicizing their official positions regarding the grounds for such insinuations, the act is considered the first example of a specific development and utilization of cyber warfare by one sovereign state against another.

Despite any country, including Ukraine, already having a history of suffering from hacker attacks on the servers of organizations of high importance for their very existence, such attacks are usually performed by separated activist groups or governmental structures of another state. So far no evidence exists

[1] Как террористы ИГИЛ вербуют женщин в Сети? *Космополитан-Россия, 25 ноября 2015.* <https://www.cosmo.ru/lifestyle/society/kak-terroristy-igil-verbuyut-zhenshchin-v-seti/>.

[2] Yoram, Schweitzer, Gabi, Siboni, Einav Yogev (2013). Cyberspace and Terrorist Organizations. *Cyberspace and National Security, Selected Articles.* <http://din-online.info/pdf/in1e.pdf>.

[3] Gartner: в 2017 году мировой рынок средств информационной безопасности вырастет на 7%. <https://www.computerworld.ru/news/Gartner-v-2017-godu-mirovoy-rynok-sredstv-informatsionnoy-bezopasnosti-vyrastet-na-7>.

[4] Шрайер, Ф., Викс, Б., Винклер, Т. (2013). *Кибербезопасность: дорога, которую предстоит пройти*. Женева.

of impressive cyber actions by terrorist groups, who use the World Wide Web with slightly different purposes[1]:

1) Propaganda: to promote their ideas, program documents, leaders' speeches and vision of the existing problems;

2) Recruiting volunteers and educating: defining and attracting potential participants, disseminating instructions and materials;

3) Fundraising, collecting donations from persons and financing: to attract financial resources by requests from bogus charities as well as steal personal information of credit card holders;

4) Communication: managing operations, including use of available encoding means such as free or cheap software;

5) Defining targets and collecting information regarding potential objects available in open online resources.

The information disseminated by the terrorists is usually aimed at three different types of recipients: the existing and potential adherents, international community and mass media, and citizens of the other party. There's a concrete aim for any of the above audiences: for instance, materials drafted for the representatives of foreign mass media and foreign citizens comprise efforts to invent a historic base and pseudo-religious fundament for the activities of the groups on the basis of separate citations from cult books like the Quran or the Bible in order to explain violence towards otherwise-minded and a certain activity in general. Another goal is to seed in that audience fear of either a real terrorist act or of its possibility. There is even such notion as Cyber fear – stimulating tensions in the society in order to make the feeling of a real danger as tangible as possible. Videos are also used by the terrorists to confirm their acts in order to satisfy the "request" from the financial donors. In some respect it makes such materials similar to porn distributed on a pay-per-view basis.

Apart from namely violence scenes, the availability of a fast and quite easy outreach to a large audience via mobile Internet connection gives the terrorists an opportunity to distribute, for example through social networks, fake news, rumors, gossips and the like unconfirmed information in order to carry out acts of sabotage, to frighten people etc.

As for the dissemination of "ideological materials", some experts distinguish three types of the rhetoric used by the terrorist groups (TG) to justify their activities[2]:

– "We have no choice". A TG depicts itself as a victim persecuted by the other party;

– "We are fighting for freedom", tries of delegitimizing and demonizing of a provisional state, which forces its peaceful citizens to grab at their guns;

– "We want only peace and welfare" – of course, on the TG conditions.

Lately electronic video content has been distributed by terrorist most often – first of all, video is easier to perceive than a written message, secondly, it can be watched by even those who are not good at reading, thirdly, videos have a potential of becoming viral and attracting large audiences. And the last – a video of say decapitation has a much higher influence on psychics than a description of it.

During the last years a lot of attention has been attracted to the Internet activity of such TG as ISIS. Unlike, say, Al Qaeda or Taliban, ISIS has been regularly broadcasting videos filmed in HD high quality practically on a professional level: with their own scenarios, well-thought "props" and basically clear idea (to plant fear and break the resistance of civilians who were unlucky to find themselves under the rule of either the TG or its enemy).

Some experts believe that in the modern unstable world such utmost aggression and over-violence can attract masses of people, giving them impression that the group is so powerful and undefeatable that by joining it they will change their life for a brighter, even if shorter, one. The idea of a world-over caliphate also attracts the new adherents by its seemingly being authentic, "true" and ancient.

Here we should touch upon another aspect. People living for years under the circumstances of violence and lack of basic human liberties, sometimes even of the opportunities to satisfy their basic everyday needs, are not so inclined to support extremism and terrorism of ISIS as the young people in Europe, perverted by the Western democracy and freedom. A 2015 survey showed a larger percent

[1] Eben Kaplan "Terrorist and the internet". *Council on foreign Relations*. <https://www.cfr.org/backgrounder/terrorists-and-internet>.

[2] Как террористы используют Интернет – Национальный центр информационного противодействия терроризму и экстремизму в образовательной среде и сети Интернет. <http://xn--h1ajgms.xn--p1ai/articles/?ELEMENT_ID=122>.

of support for ISIS ideas among the Europeans than representatives of Middle Eastern countries. While only 3% of Egyptians, 5% of Saudis and 1% of Lebanese spoke of the TG positively, the same reaction was typical for 7% of British and 16% French respondents[1].

Some groups show a tendency to "adjust" their propaganda efforts in tune with the requirements and preferences of their "target audience". Apart from videos, through their own or "partner" web-sites they distribute, for instance, video games, where kids aged 7 and up can try themselves at being "Allah's fighters" killing American soldiers[4]. For instance, Palestinian TG HAMAS's site for kids Al-Fateh lists cartoons with characters looking like those of Disney Pictures and fairy tales with repeated messages of hatred towards Israel, jihad against infidels and martyrdom. Adolescents are typically addressed through chat rooms and forums. Special attention is paid by the terrorists to female audiences, including not only Muslim migrants, who are often employed as interpreters into the immigration country's language, but local Europeans being attracted by the abovementioned glory of "machoism" and "truthfulness" surrounding the image of the hitmen.

Propaganda of violence and the philosophy of a TG is closely connected with another issue – enlistment of the new members and training of the active one. Of course simple transfer of information with electronic means cannot substitute a neophyte's training in special camps, but, for instance, a scheme of assembling a bomb at home is a real example of interaction of an organized group and separate people. The list of most "popular" works includes "The Terrorist Manual" and "An Anarchist's Cookbook", "Encyclopaedia of Jihad" and others. There were cases when after exchanging information seemingly obedient civilians decided to go and arrange a terrorist act[2]. During such exchange of information with the help of new technologies TGs read the visitors' data in order to try to establish a connection and enrol new members. Sometimes the willing neophytes get in touch with the TG on their own over the Internet: they become regulars in certain chat rooms and forums, disseminate jihadist propaganda and so on.

But the closest connection between the use of IT and social networks by TGs is observed in the sphere of fundraising. The most frequent way to gather funds is to send spam with numbers of electronic accounts, e.g. PayPal, where the supporters can send money. Apart from that there were cases when the terrorists stole personal data of credit card holders and then laundered their money through dozens of accounts in several countries until they became totally impossible to trace. During one such scheme the data of about 1400 British citizens were stolen, later approximately 1.6 mln. pounds were collected and used on 180 sites to disseminate propaganda and finance terrorist activities in a number of countries[3]. Apart from that, some TGs create fake charities that finance terrorist activities under the auspices of humanitarian actions.

Mobile Internet is yet another factor of additional terrorist threat. According to Ericsson company, the number of active mobile Internet users worldwide reached 7,8 bln. persons[4]. With view of such wide spread of mobile devices with online access, the opportunities to break into a network of an organization grow manifold as such gadgets are frequently also connected to the office and home networks via Wi-Fi routers. According to the information of McAfee Labs[5], the first quarter of 2017 alone showed the appearance of more than 1.5 mln. new appearances of malware. At the same time some experts in the sphere of cyber-security and anti-hacking state, that although the feasibility of someone's mobile device being hacked is clear in this or that scope to most users, many developers of mobile apps are neglecting the requirements of security and use a weak encryption.

The TGs use all the benefits that the new technologies, Internet and social networks can offer. Although some networks (for instance, Facebook) try to effectively control and ban appearance and existence of separate accounts, groups and pages connected with terrorist activity, xenophobia, racism and extremism, it's hardly feasible to extinguish them completely and to prohibit them from appearing again.

In their turn, the means helping to monitor the web sites' activities and analyze the dynamics of the activity there, to examine the potential audience are also developing, plus the general level of knowledge

[1] Smith, Lee (2014). Why the Teenage Girls of Europe Are Joining ISIS. *Tablet Magazine.* <http://www.tabletmag.com/jewish-news-and-politics/186397/teenage-girls-europe-isis>.
[2] Weimann, G. (2004). How Modern Terrorism Uses the Internet. *United States Institute of Peace Special Report 116.* <https://www.usip.org/publications/2004/03/wwwterrornet-how-modern-terrorism-uses-internet>.
[3] *The Use or the Internet for Terrorist Purposes* (2012). Vienna.
[4] Ericsson Mobility Report November 2017. <https://www.ericsson.com/en/mobility-report/reports/november-2017>.
[5] Collett, Stacy. Five new threats to your mobile security. <https://www.csoonline.com/article/2157785/data-protection/five-new-threats-to-your-mobile-security.html>.

about the problem also evolves. Some cybersecurity experts consider communication and PR the main mechanism of preventing the terrorists' influence from strengthening. For instance, while attracting new recruits and dissemination of information is done mainly in open communication, it gives the opportunity to dismantle the myths and ideas of the terrorists. At the same time it's impossible to fight those myths effectively without understanding the reasons for citizens' radicalization, mainly young people in their 20s, showing this understanding and discussing the possible alternative ways of solving them.

Human rights dilemma in anti-terrorist activities in the Internet is a special issue, especially concerning the rights for privacy and freedom of speech as well as the primate of security demands of the other citizens and the country as a whole. While the newest technologies of searching, following and analyzing the actions of the potential terrorists can give and opportunity to prevent the terrorist attacks and illegal activity, in the hands of authoritarian governments and rulers they can and will become mechanisms of further strengthening one's control over the people and infringing the main human rights and freedoms. In a faraway perspective even the most democratic countries can witness this leading to erosion of the values those countries were built upon, the destruction of the notion of democracy per se which, in the long run, is the global goal of the terrorists. There's a problem in a number of countries, for instance, with taking the offenders to court for instigating terrorist acts, including promotion of corresponding video materials through social networks: the material should contain a direct indication of the presence of a well-thought design as well as the confirmation that the material and a real or planned act are connected. For instance, a textbook on producing explosives, unless it contains something like "This type of bomb we advise to use in blowing bridges and railway stations" will not be accepted in court as a material with an appeal for carrying out terrorist acts. Such nuances are, on the one hand, guarding a person's interests and does not allow the law enforcement bodies to put citizens behind the bars without solid reasons, and on the other hand – make the work of making the real culprits respond for their actions more difficult.

A few cases in 2016, connected with the refuse of Apple to provide the FBI access to the telephones of suspects in terrorist acts in the USA provoked heated discussions on this topic both in the society in general and among the security and law enforcement professionals. The reason of the refuse was that the company did not want to disclose the secrets of its software and therefore endanger millions of other users. According to FBI, the issue was settled with the help of hacking instruments provided by a third party[1], but the details were never published, which leaves more questions than answers but at the same time gives both Apple and FBI a chance to keep their faces.

The officials of almost any postindustrial country – those countries being today the main aim of all terrorists, ISIS foremost – from time to time say that Internet companies like Google and Facebook are not active enough in fighting online content containing propaganda of violence and are not using all the means available to fight the use of social networks by the TGs in order to communicate and coordinate their actions. Apart from that, social networks are often accused of disseminating fake news as well as of tolerance towards users, whose pages contain frightening, aggressive materials, child porn and violate the copyright.

The officials of all ranks the companies must bear more responsibility for the use of their products. On the one hand, the huge human and technological capacities of these giants really provide opportunities for effective content control and prevention of illegal activity (we speak about open Internet, of course – the opportunities of the deep web deserve a separate discussion). On the other hand, the technological progress and breach of law come and in hand since times immemorial: for instance, in 1834 in France a group of criminals managed to create a system of illegal bond trading with the help of mechanical telegraph machine, which the police managed to uncover only 2 years later[2]. At the beginning of the Internet era the absence of limitations bestowed by other means of information transfer was what facilitated its bustling development and helped enrich the worldwide web with the information of the most different type, on any topic as well as stimulated the fastest ever capitalization of the technical companies that have since then evolved from small "workshops" into omnipresent and omniscient monsters. Naturally, those monsters would be utmost interested in preserving the status-quo, hence the not always warm attitude towards the official statements: for instance, that the officials are trying to use the companies to solve difficult social

[1] Raymundo, O. It's official: FBI won't share its secret iPhone hack with Apple. <https://www.macworld.com/article/3061934/security/fbi-wont-share-its-iphone-hack-with-apple-because-its-unfamiliar-with-the-code.html>.

[2] Tech firms could do more to help stop the jihadists. <https://www.economist.com/news/leaders/21723110-legal-restrictions-must-be-proportionate-and-thought-through-tech-firms-could-do-more-help>.

problems like public aggression and bullying. The online businesses are partly right in that using social media for example for recruiting is only a part of the terrorist danger and that it's physically impossible to scan every post of every user.

Here we should pay attention to the dilemma of the freedom of speech, religion, conscience and the necessity to limit those freedoms. Again, as with the propaganda issue, it's very difficult to draw a line between a simply statement in social networks (some posts, even on neutral topics, are very close to hate speech and look like calls to uproot the existing order, but are in reality a users' way of "letting the steam out" – and "the real bad thing". At the same time, while the topic-starter him/herself does not have any far-fetching plans, the post may come into resonance with a mood of another user who maybe lacked these arguments to finally make up his/her mind to get a rifle and go shoot people. All the above brings us down to the thesis that socializing, especially teenagers and youth, becomes more and more important as a counterweight to "internetizing". It's understandable that we are not going back to the times when people lived in small communities and knew each other, but at least it's worthwhile to know the life of your children or parents. It's an axiom for psychologists that people with more diverse and stable social connections cope easier with different crises – and it's the person in crisis that all terrorists most actively hunt for.

In its turn, the development of IT sphere goes with such a speed that the traditional ways to ensure security are simply not working. For instance, according to "The Kaspersky Laboratory", 320 thousand new viruses are written every day, and the number of attacks only on Android-operated gadgets since 2016 has multiplied fivefold[1]. It's not always possible to track the attack, which made some experts say that it's impossible to improve the level of national informational security without improving the overall personal informational literacy and security: as a parallel to personal hygiene ("wash your hands with soap"), it's highly important to inject the citizens with fundamental rules of informational hygiene ("don't open strange attachments"). For instance, both persons and companies tend to publish online in the Internet and social networks certain confidential information which can then be collected, analyzed and used with terrorist purposes. For such purposes one can use, say, GPS data and geo-tagging: by markers of the pictures with objects or persons of interest, by directly tracking the handheld and so on. The saying "Measure seven times cut once" is becoming as fresh as ever before. Every user should think twice whether it's really necessary to participate, say, in a rally to try to win a panda pen, if it requires to grant access to the contacts and photos, and the main issue should be – why do the organizers need such data?

Until recently the issues of informational security were not so acute for Ukraine – and then the military action on the Eastern part of the country came. Although the separatists lack the same technical and financial capacities as, say, ISIS, they do have a lot of activity and desire to "study the international experience" in this sphere. Mainly the activity of the so-called DNR and LNR is concentrated on propaganda. The romantic flair of their activity is mainly based on the thesis of "reluctance" ("we have no other choice") and illegitimate nature of Kyiv government ("we are fighting for freedom"). Besides, the Internet was used for recruiting and fundraising. At the beginning of the Anti-terrorist operation there was a massive exchange of sensitive and classified military information from Ukrainian army and defense bodies. There had been news reports that the enemy used cell provider data to track the movement and location of Ukrainian army (for instance, they searched social networks for the phone numbers of the serving military persons and volunteers and then by triangulation located those people. They also located towers with more cellular activity in the given coordinates).

With the view of all above, one can say that with time the TGs' activity online will not decline because it gives them opportunity to achieve rather good efficiency with comparatively small expenses, at least in the sphere of fundraising and communications. The technologies of tracking potential terrorists and criminals, fighting cyber crime will also be developing. Perhaps, who will be the winner in this competition belongs on every single person as well as possibilities for the law enforcement bodies to act fast for every challenge and do the necessary forecasts.

If we draw a parallel with the car traffic (are the car manufacturers responsible for say drunk driving? How do we minimize the number of car accident victims?), then the possibility to secure full security in the digital world is closing to zero; however, the use of a combination of approaches will give the opportunity

[1] 93% кибератак можно предотвратить: на Belarus IGF обсудят безопасность в интернете. <https://bel.biz/afisha/articles/93-kiberatak-mozhno-predotvratit-na-belarus-igf-obsudyat-bezopasnost-v-internete>.

to achieve rather feasible results. Technological means and ways, considerate policy of the companies and states, improvement of the citizens' knowledge and personal responsibility together with more accessible higher education and efforts on solving at least part of the most acute social problems can bring impressive fruit. An important role is played also by cooperation – if, say, people will not be too lazy to report materials containing violence slogans or other illegal information and the companies will check at least 50% of those reports (like the providers in Germany are required to do today), and the advertisement companies will not work with resources where their ads can border with the like content hence diminishing the income of the providers – the overall improvement of online safety is more than likely.

In the legal sphere it would be advisable to be more detailed about the requirements towards content and strict about punishment for incompliance. Ukrainian laws dealing with Internet, copyright and other connected issues, is rather contradictory, vague and not clear enough which leaves enough space for both criminal activity and power misuse by the law enforcement bodies (or, more exactly, for tries to harass companies – the so-called "masked shows" with filmed extortion of servers etc. which in the era of cloud technologies is basically a show-off for the bosses and intimidation of the entrepreneurs than real struggle with money laundering or piracy).

Apart from that it's not a secret for a long time that many businesses with access to private information – like mobile service providers – sometimes share their client databases, in the best scenario with their partners and not on the level of say an angry ex-worker. Message spam with warnings about allegedly closure of bank accounts or cards, or trophies that can be collected after one "simply" sends an SMS on a said account/ provides a security code to the card or sends a certain amount by money transfer – you name it – have long become some kind of another side of our reality. During the military events of 2014 people's habit of constantly "hanging" online with the GPS location available resulted in a number of tragic incidents with unnecessary victims.

Moreover, repeated server failures of the state bodies and law enforcement organizations of Ukraine highlighted the less than adequate attention both to the technical side (old hardware, unreliable software) and to the human resources issue (lack of incentives for real professionals, nepotism). It would be no exaggeration to say that so far we managed through without serious problems only because the hackers lack real interest in our systems and the informational space of Ukraine is still underdeveloped (for instance, most medical institutions still keep patient documents in paper). Full ignorance by many users of all thinkable security requirements (visits to unfamiliar sites – often from the workplace, provision of personal information on dubious resources, lack of antivirus software on the PCs) creates additional loopholes for the criminals and terrorists. Ah the same time such situation cannot go on forever, and the earlier our society realizes that on every level – the easier will it be to divert really serious problems.

References:

1. Kaplan, Eben (2009). Terrorist and the internet". *Council on foreign Relations*. <https://www.cfr.org/backgrounder/terrorists-and-internet>.
2. Ericsson Mobility Report November 2017. <https://www.ericsson.com/en/mobility-report/reports/november-2017>.
3. Weimann, G. (2004). How Modern Terrorism Uses the Internet. *United States Institute of Peace Special Report 116*. <https://www.usip.org/publications/2004/03/wwwterrornet-how-modern-terrorism-uses-internet>.
4. Smith, L. (2014). Why the Teenage Girls of Europe Are Joining ISIS. *Tablet Magazine*. <http://www.tabletmag.com/jewish-news-and-politics/186397/teenage-girls-europe-isis>.
5. Raymundo, O. It's official: FBI won't share its secret iPhone hack with Apple. <https://www.macworld.com/article/3061934/security/fbi-wont-share-its-iphone-hack-with-apple-because-its-unfamiliar-with-the-code.html>.
6. Collett, Stacy. Five new threats to your mobile security. <https://www.csoonline.com/article/2157785/data-protection/five-new-threats-to-your-mobile-security.html>.
7. Tech firms could do more to help stop the jihadists. <https://www.economist.com/news/leaders/21723110-legal-restrictions-must-be-proportionate-and-thought-through-tech-firms-could-do-more-help>.
8. *The Use or the Internet for Terrorist Purposes* (2012). Vienna.
9. Schweitzer, Yoram, Siboni, Gabi, Yogev, Einav (2013). Cyberspace and Terrorist Organizations. *Cyberspace and National Security, Selected Articles*. <http://din-online.info/pdf/in1e.pdf>.
10. Gartner: v 2017 godu mirovoj rynok sredstv informacionnoj bezopasnosti vyrastet na 7% [Gartner: in 2017, the global market for information security will grow by 7%]. <https://www.computerworld.ru/news/Gartner-v-2017-godu-mirovoy-rynok-sredstv-informatsionnoy-bezopasnosti-vyrastet-na-7>. [in Russian].
11. Kak terroristy IGIL verbujut zhenshhin v Seti? [How do the ISIS terrorists recruit women online?]. *Kosmopolitan-Rossija, 25 nojabrja 2015*. <https://www.cosmo.ru/lifestyle/society/kak-terroristy-igil-verbuyut-zhenshchin-v-seti/> [in Russian].

12. Kak terroristy ispol'zujut Internet [How do terrorists use Internet]. *Nacional'nyj centr informacionnogo protivodejstvija terrorizmu i jekstremizmu v obrazovatel'noj srede i seti Internet* [The National Center for Information counteraction to terrorism and extremism in the educational field and the Internet]. <http://xn--h1ajgms.xn--p1ai/articles/?ELEMENT_ID=122> [in Russian].
13. Shrajer, F., Viks, B., Vinkler, T. (2013). *Kiberbezopasnost': doroga, kotoruju predstoit projti* [Cybersecurity: the way to be passed]. Geneva. [in Russian].
14. 93% kiberatak mozhno predotvratit': na Belarus IGF obsudjat bezopasnost' v internete [93% of cyber attacks can be prevented: on Belarus IHF to discuss security on the Internet]. <https://bel.biz/afisha/articles/93-kiberatak-mozhno-predotvratit-na-belarus-igf-obsudyat-bezopasnost-v-internete> [in Russian].