CHAPTER 3
THEORY AND METHODS OF VOCATIONAL EDUCATION

A COMPETENT APPROACH TO THE TRAINING OF LAWYERS IN "CYBERTERRORISM"

Ali Jabbar Salih[1], Farouq Ahmad Al Azzam[2]

[1]Ph.D. (Law), Professor, Dean of law college, Faculty of Law, Jadara University, Jordan, e-mail: dr_alijabbar@yahoo.com, ORCID: https://orcid.org/0000-0003-1975-1173

[2]Ph.D. (Law), Assistant professor, Head of the Law Department, Faculty of Law, Jadara University, Jordan, e-mail: alazzamfarouq@yahoo.com, ORCID: https://orcid.org/0000-0001-7407-4828

Abstract. *As a result of the extremely wide use of modern information and communication technologies in all spheres of existence, society has become vulnerable to cybernetic influences. The flows of information transmitted, stored and processed in cyberspace are constantly increasing, which requires their proper protection against unauthorized access for criminal purposes. Given the widespread concern about cyberterrorism and the frequent use of the term "cyberterrorism" today, many international organizations have made efforts to combat this threat. A special place among institutions that can directly or indirectly counter cyberterrorism is occupied by universities that offer bachelor's and master's degrees in law and cyber security, in particular cyber terrorism. The presence of qualified personnel specializing in both legal knowledge and knowledge in the field of information technology will contribute to the creation of prerequisites for effective countermeasures against cyber terrorism in Jordan and in other countries of the world. The purpose of the article is to investigate the role of the law college in training lawyers capable of countering cyberterrorism. In order to assess the influence of external and internal factors on the activities of the Jadara University College of Law, the study conducted a survey of four categories of respondents: students, their parents, employees and employers. All respondents were offered questionnaires with a list of questions, the purpose of which was to reveal the level of awareness regarding the definition of criteria that could potentially be included in the new master's degree program in the specialty "Cyberterrorism". Based on the results of the research, the main competencies that future students of the master's degree "Cyberterrorism" should possess are established, namely: in the field of international law; in the field of international relations; in the field of international and national security; in the field of information technologies; in the field of cyber security; in the field of communication technologies, etc. Hence, Jadar University College of Law makes a direct contribution to the social, cultural and economic development of society, and graduates of the College of Law are important ambassadors of the College and play a key role in maintaining safety in the community and providing space and improving opportunities for members of the local community to access the College of Law and use the various services it provides.*

Keywords: *law; information; information technology; cyber security; cyberterrorism; competent approach; training; lawyer.*

JEL Classification: A23, A29, I28

Formulas: 0; fig.: 2; tabl.: 11; bibl.: 10

Introduction. As a result of the extremely wide use of modern information and communication technologies in all areas of its existence, society has become vulnerable to cybernetic influences, which are increasingly becoming an effective tool for achieving the goal of non-forceful control and management of both state infrastructure objects, enterprises, and individual citizens, their associations The flows of information transmitted, stored and processed in cyberspace are constantly increasing, which requires their proper protection against unauthorized access for criminal purposes. Strengthening cybersecurity is therefore critical to ensure people trust and benefit from innovation, connectivity and automation, and to protect fundamental rights and freedoms, including the right to privacy and protection of personal data, as well as freedom of expression and information.

Given the widespread concern about cyberterrorism and the frequent use of the term "cyberterrorism" today, many international institutions have made efforts to combat this threat. Because cyberterrorism is an international crime, local laws alone cannot protect against such attacks and they require an international response. A country that is a victim of cyber terrorism will rely on international law to redress any damage caused through the application of universal jurisdiction. A special place among institutions that can directly or indirectly counter cyberterrorism are universities that provide bachelor's and master's degrees in law and cyber security, including cyberterrorism. The availability of qualified personnel who specialize in both legal knowledge and knowledge in the field of information technology will contribute to the creation of prerequisites for effective countermeasures against cyberterrorism in Jordan and in other countries of the world.

Literature review. For the first time, concern about the possible consequences of using the World Wide Web was expressed in 1993 by Alvin Toffler, when the general public still knew little about the Internet. Toffler already predicted that terrorists would try to attack the information and telecommunications infrastructure of the United States. Since then, a significant amount of research has been carried out, and the opinions of experts regarding the concept of "cyberterrorism" are polarly divided [1].

The definition of information or cyber terrorism can be found both in international legal documents and draft conventions, as well as in the research of experts on this issue. One of the characteristic features of the definitions of information terrorism is that in the vast majority of them only one aspect of information security is mentioned, namely related to the means of information processing, which narrows the concept of information terrorism, thereby limiting the scope of legal regulation, which does not contribute to effective cooperation of states in the fight against information terrorism [1].However, let us emphasize that there is currently no generally accepted definition. But in the theoretical aspect it is about the integration of such concepts as "terrorism" and "computer crime".

The first examples of "computer terrorism" appeared in the late 1990s, which is connected both with the development of computer networks and with the growing role of computers in all spheres of life. As a result, the attention of various "cyber bullies" and "cyber terrorists" who carry out attacks using unauthorized access to interfere with the normal work of relevant institutions has increased.

Cyber terrorism is defined as a deliberate and motivated attack on information processed by a computer, a computer system or a network, which is associated with a danger to the life and health of people or the occurrence of other serious consequences, if such actions are committed with the aim of violating public safety , intimidation of the population, provoking a military conflict [2].

The first comprehensive treatment of the cyberterrorism threat was performed by the Center on Terrorism and Irregular Warfare (CTIW) at the Naval Postgraduate School (NPS) in Monterey, California. In august 1999, they issued a report on the prospects of terrorist organizations pursuing cyberterrorism. They concluded that the barrier to entry for anything beyond annoying hacks is quite high, and that terrorists generally lack the wherewithal and human capital needed to mount a meaningful operation [10].

Cyberterrorism, they argued, was a thing of the future, although it might be pursued as an ancillary tool.

The NPS study defined three levels of cyberterror capability (Figure 1):

- *Simple-Unstructured:* The capability to conduct basic hacks against individual systems using tools created by someone else. The organization possesses little target analysis, command and control, or learning capability.
- *Advanced-Structured:* The capability to conduct more sophisticated attacks against multiple systems or networks and possibly, to modify or create basic hacking tools. The organization possesses an elementary target analysis, command and control, and learning capability.
- *Complex-Coordinated:* The capability for a coordinated attacks capable of causing mass-disruption against integrated, heterogeneous defenses (including cryptography). Ability to create sophisticated hacking tools. Highly capable target analysis, command and control, and organization learning capability.

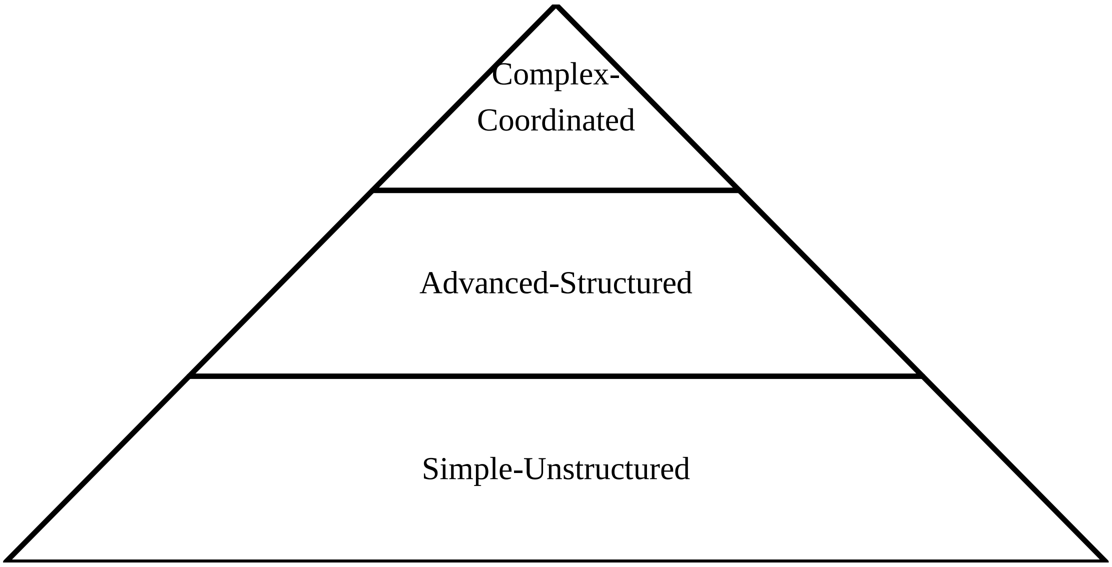

Figure 1. The three levels of cyberterror capability

Source: created by the author based on [10]

They estimated that it would take a group starting from scratch 2-4 years to reach the advanced-structured level and 6-10 years to reach the complex-coordinated level, although some groups might get there in just a few years or turn to outsourcing or sponsorship to extend their capability.

The study examined five terrorist group types: religious, New Age, ethno-nationalist separatist, revolutionary, and far-right extremists. They determined that only the religious groups are likely to seek the most damaging capability level, as it is consistent with their indiscriminate application of violence. New Age or single issue terrorists, such as the Animal Liberation Front, pose the most immediate threat, however, such groups are likely to accept disruption as a substitute for destruction. Both the revolutionary and ethno-nationalist separatists are likely to seek an advanced-structured capability. The farright extremists are likely to settle for a simple-unstructured capability, as cyberterror offers neither the intimacy nor cathartic effects that are central to the psychology of farright terror. The study also determined that hacker groups are psychologically and organizationally ill-suited to cyberterrorism, and that it would be against their interests to cause mass disruption of the information infrastructure.

The NPS researchers applied their general knowledge of terrorists and cyber weapons to evaluate the threat of cyberterrorism. By contrast, my recent work is based on identifying indicators of cyberterrorism. These are pieces of evidence that demonstrate a capability or intent to conduct acts of cyberterror. The ones I have identified so far fall into five categories:

- Execution of cyber attacks. This covers all types of computer network attack, not just acts of cyberterror.
- Cyber weapons acquisition, development, and training. This includes acquisition and distribution of cyber weapons, research and development in cyberweapons, and training in the use of cyberweapons. Activities can take place on-line or in special facilities.
- Statements about cyber attacks. This covers all types of statements relating to cyber attacks, including discussions, declarations of intent, and calls for performing cyber attacks.
- Formal education in information technology. This includes all areas of IT education, but especially studies in network and information security.
- General experience with cyberspace. This covers cyber activities that do not fall within the first four categories, including general use of the Internet for communications and distribution of news and propaganda.

The categories are listed in order of generally decreasing significance; that is, the actual execution of cyber attacks carries more weight than acquisition and development of cyber attack tools, which in turn carries more weight than simply making statements about cyber attacks, and so on. However, the ordering is not strict, as the nature of the evidence also matters. Evidence of a cyber training camp that has been instructing scores of cyber jihadists in attacks against the Supervisory Control and Data Acquisition (SCADA) would be a stronger indicator of cyberterrorism than evidence of a successful web defacement. SCADA and other types of digital control systems are used to monitor and control critical infrastructures such as for electricity, oil and gas, water, dams, and sewage, and are considered likely candidates for cyberterrorist attacks.

The last two categories, formal education in information technology (IT) and general experience in cyberspace are not indicators of cyberterrorism so much as enablers. A terrorist could study computer science, for example, in order to manage information resources such as websites for the organization. Even a focus on network security could be for the purpose of defending terrorist systems and information rather than launching cyber attacks. Still, terrorists with formal education in IT and experience using the technology are in a better position to develop a cyberterror capability than those without this background, so evidence in these categories is relevant to assessing the cyberterror threat.

In seeking evidence relating to these indicators, I considered activities attributable not only to terrorist groups, but also to hackers expressing an alliance or sympathies with such groups. Although the latter may not be willing to engage in physical acts of violence, they may be amenable to causing extensive damage to information resources.

Also, it can be difficult to know the exact relationship between a terrorist group and hackers claiming some sort of affiliation. The Al-Qaeda Alliance Online, for example, appeared to have no formal ties to the terrorist organization, but it might be considered part of the broader jihadi movement associated with it.

Although it is not hard to carry out relatively simple cyber attacks using readily available hacking tools, considerably greater skill would be required to develop software to perform original and highly damaging attacks against critical infrastructures. For such attacks, formal education in a field such as computer science or computer engineering would be helpful, especially if the program of study included digital controls sytems and network security. Although courses in information and network security emphasize how to defend against cyber attacks, they inevitably teach something about attacks, as it is not possible to build adequate defenses without a solid understanding of the threat.

A few people with formal education in these areas have been associated with terrorist groups. Sami Al-Arian, the professor at the University of South Florida charged with raising money for Palestinian Islamic Jihad, was in the department of Computer Science and Engineering. Although Al-Arian’s area of specialty did not appear to be network security, Sami Omar Al-Hussayen, the Saudi graduate student at the University of Idaho charged with operating websites used to recruit terrorists, raise money to support terrorism, and disseminate inflammatory rhetoric, was studying computer security in the Computer Science Department. However, neither Al-Arian or Al-Hussayen were convicted of any crimes.

The results of the study showed the lack of systematic generalizations regarding the necessary competencies that should be possessed by persons studying in the specialty "Cyberterrorism" at universities.

Aims. The purpose of the article is to study the role of the College of Law in training lawyers capable of countering cyber terrorism.

Methodology. The basis of the research methodology was the study of the experience of the College of Law, Jadara University by conducting a survey among potential employers of future graduates from the "Cyberterrorism" specialty.

The College of Law was established at the beginning of the establishment of the university in 2006. The College of Law is one of the oldest and largest colleges of the university, and the incubator of its most important departments: Bachelor's and Master's Law, which was established in 2008, and Political Science, which was established in 2018.

The main findings of the study found that the College of Law, Jadara University aims to be a scientific college that provides the community with qualified personnel who possess science and knowledge and are also trained in research to continuously develop performance, meet the needs of the labor market and contribute to the development and service society

An analysis of the student body of the College of Law, Jadara University has shown that the total number of students is increasing every year, which shows the prestige of the College of Law among students, their parents and employers. However, unfortunately, the contingent of master's students is decreasing (table 1).

Table 1. Student contingent of the College of Law, Jadara University for 2020-2022

Degree	Year	The total number of students	The number of graduate students
Bachelor's degree in law and political science	2020	413	117
	2021	507	108
	2022	630	0
Master of Law	2020	165	25
	2021	159	25
	2022	71	0
Master of Laws in Cybercrime	2020	0	0
	2021	12	0
	2022	3	0

In order to assess the influence of external and internal factors on the activities of the College of Law, Jadara University, a survey of four categories of respondents was conducted: students, their parents, employees and employers. All respondents were offered questionnaires with a list of questions, the purpose of which was to identify the level of awareness regarding the definition of criteria that could potentially be included in the new educational program of the master's degree in "Cyberterrorism".

1) *Results of a survey of College of Law students.* 216 participants took part in the student survey, representing all levels of education (Figure 2).

From the point of view of students of the College of Law, indicators related to international cooperation programs and opportunities to obtain international certificates became priorities. Such a position of today's youth is not surprising at the time of the development of intercontinental economic integration, but it can become a threat to the College of Law, if we do not respond in a timely manner to the expansion of the offer of such programs (Figure 3).

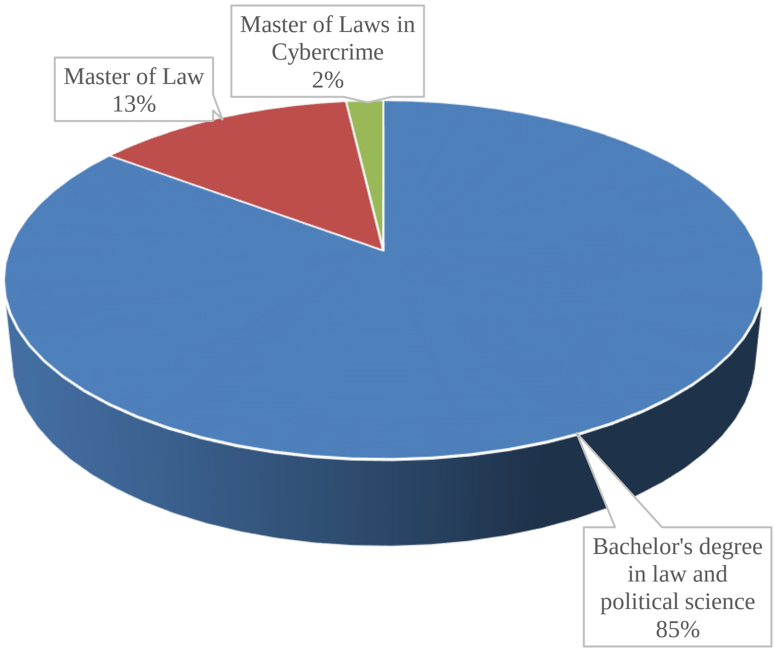

Figure 2. Distribution of College of Law students who took part in the survey by levels and areas of study

Source: Created by author based on survey data

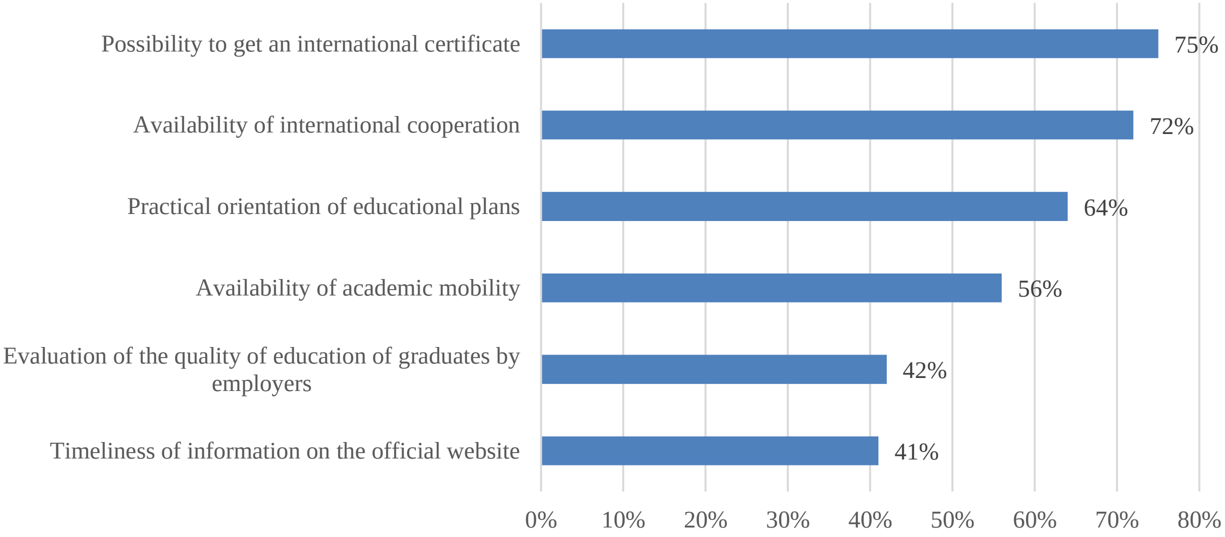

Figure 3. Priority criteria determined by students

Source: Created by author based on survey data

In their answers, the surveyed students indicated the main competencies they would like to have after completing their studies (Figure 4).

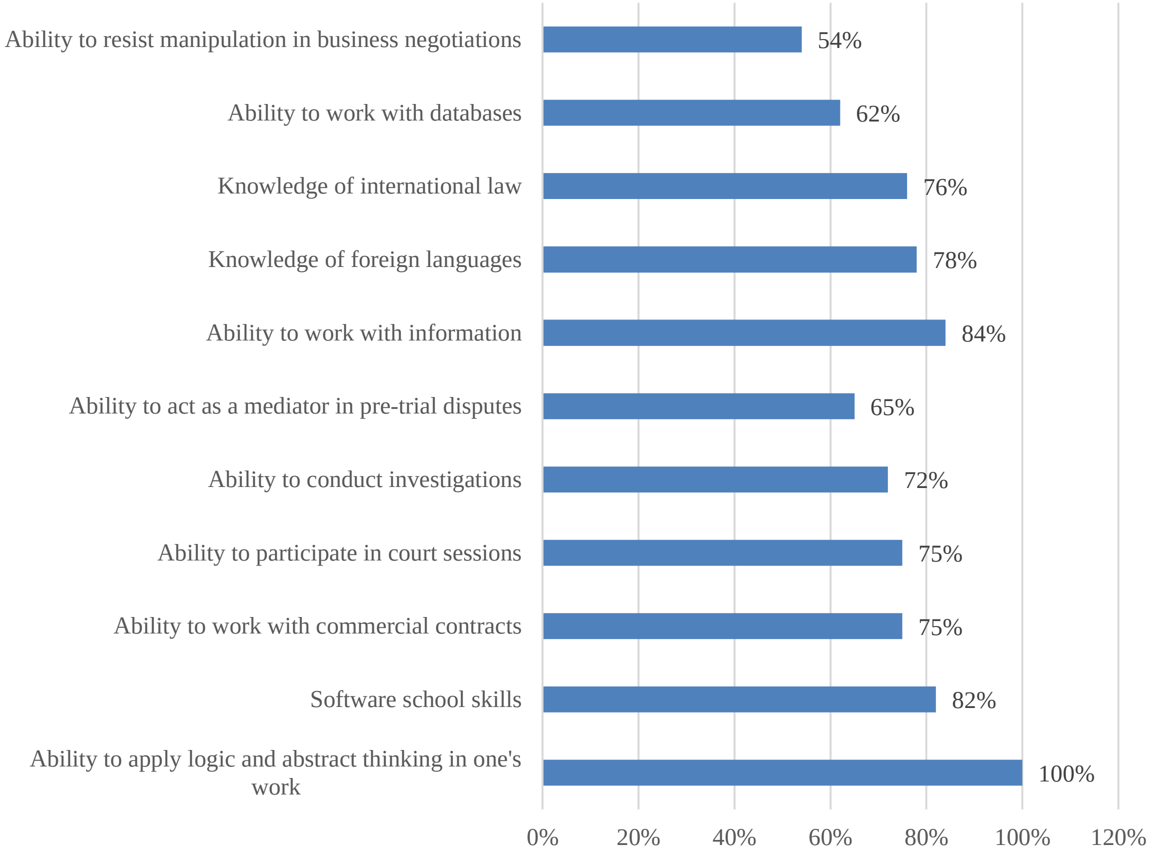

Figure 4. Priority competencies identified by students

Source: Created by author based on survey data

Analytical thinking (100%), ability to work with information (84%), soft skills (82%) and knowledge of foreign languages (78%) are among the main competencies that College of Law students seek to acquire during their studies. According to the students who took part in the survey, it is precisely such competencies that will contribute to their active employment after graduation.

2) *Results of a survey of parents of College of Law students.* The survey of this category of respondents was conducted among parents of students of the College of Law, Jadara University. 312 participants took part in the survey, whose answers allow us to identify the five main indicators that guided them when choosing an educational institution for their children's admission (Figure 5).

If we talk about the priorities in choosing an educational institution, then we can observe the common position of two categories of respondents - practical orientation of curricula (84%), the possibility of obtaining an international certificate (82%) and the presence of international cooperation (78%).

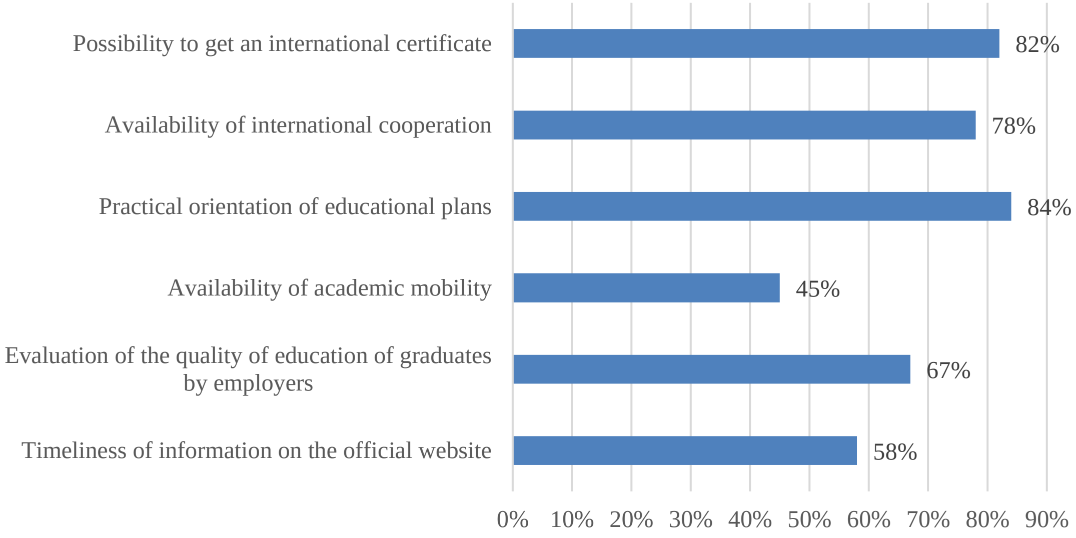

Figure 5. Priority criteria defined by parents of College of Law students
Source: Created by author based on survey data

Among the main competencies that, in the opinion of students' parents, their children should possess after completing their studies, there are both general competencies regarding logical thinking and knowledge of foreign languages, as well as special competencies depending on the specialty chosen by the students (Figure 6).

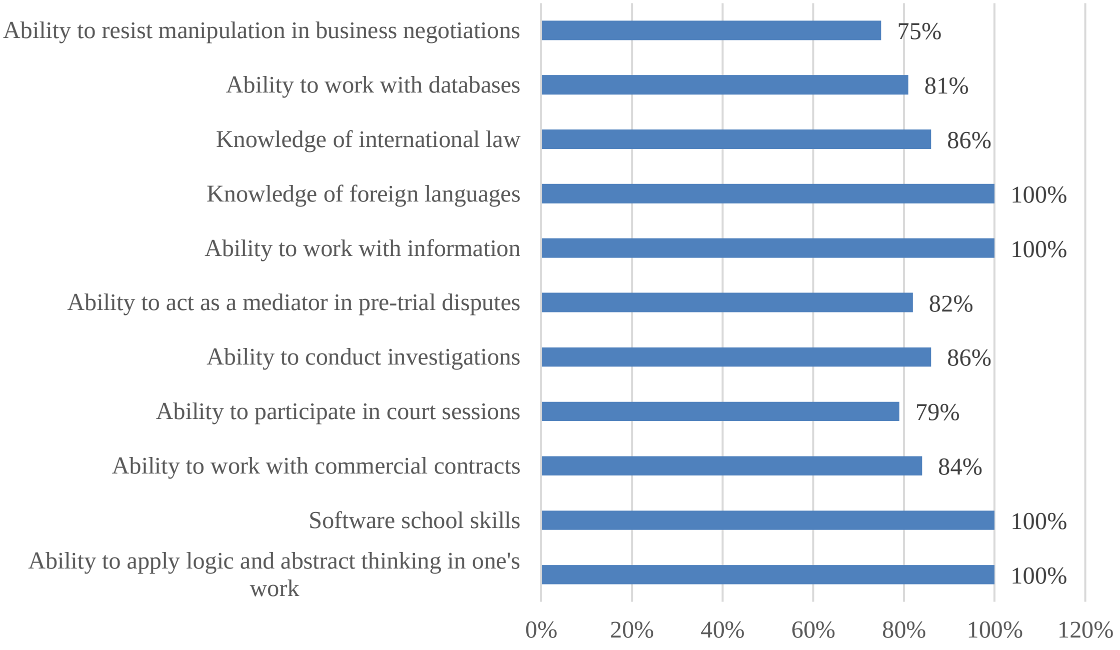

Figure 6. Priority competencies identified by parents of College of Law students
Source: Created by author based on survey data

Respondents also proposed several options for additional criteria:

- The psychological climate in the educational institution, the student's desire to study or not to study in this educational institution;

- The number of graduates employed by their specialty;

- Correspondence of the level of teaching and knowledge of teachers to modern trends in the IT field (that is, does the knowledge acquired by students meet the requirements of employers);

- Feedback from parents;

- The atmosphere of the establishment, comfort and friendliness; creative projects, student events.

3) *Results of a survey of employees of the College of Law.* All college employees took part in the survey. From the point of view of employees, the five indicators that should become a priority in the work of the college regarding the formation of a positive image should include "Practice-oriented curricula", "Availability of academic mobility", "Evaluation of the quality of education of graduates by employers", "Evaluation of the quality of education by graduates" and "Involvement of employers in the discussion of educational programs" etc. (Figure 7).

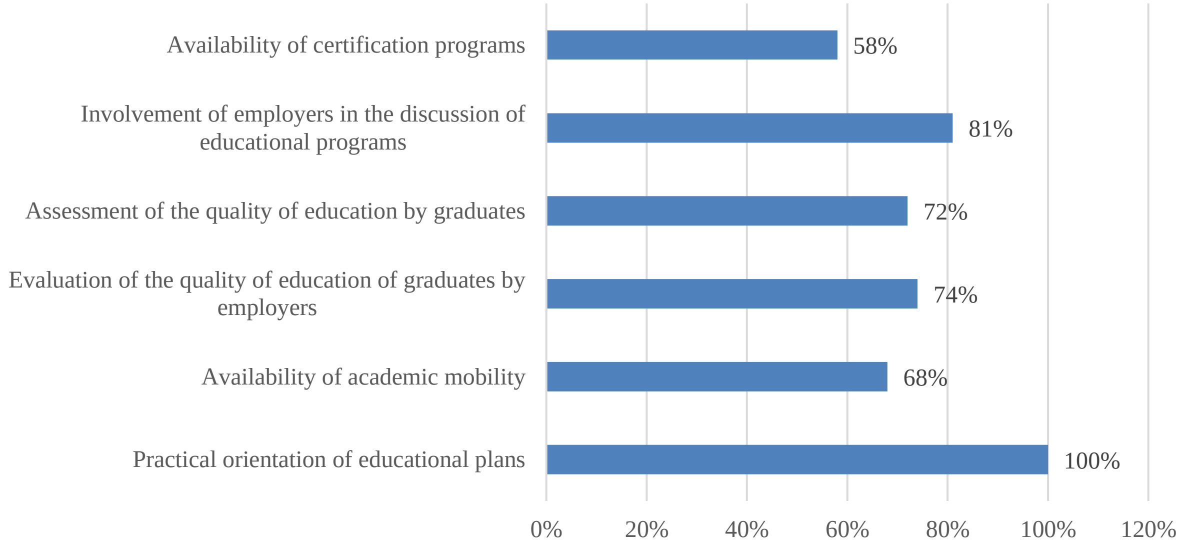

Figure 7. Priority criteria determined by College of Law staff

Source: Created by author based on survey data

Some of the indicated respondents also named among the important indicators in the formation of a positive image of the College of Law:

- efficiency of the internal system of ensuring the quality of education and educational activities;

- development of personal autonomy of education seekers, freedom of choice of educational opportunities;

- involvement of the maximum number of willing education seekers in scientific, innovative and creative projects, with rewards for achievements;

- creation of an alumni association to acquaint students with stories of personal success of graduates, holding meetings with famous scientists, successful lawyers, politicians, public intellectuals, philosophers, writers;

- healthy environment of the institution.

- the issue of spiritual, cultural and patriotic education.

Among the core competencies, which, according to the employees of the College of Law, should be logical thinking (100%), knowledge of commercial contracts (95%), the ability to conduct investigations (89%), work with information (88%) and arrays of data (88 %) (Figure 8).

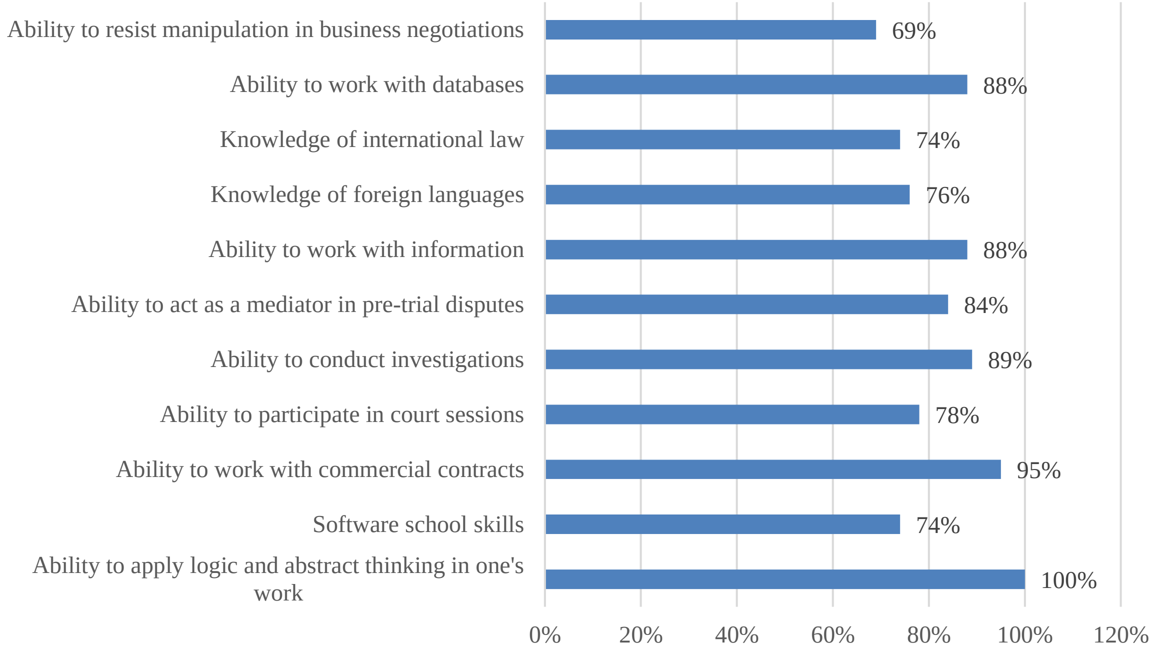

Figure 8. Priority competencies identified by College of Law staff

Source: Created by author based on survey data

At the same time, we would like to draw attention to the fact that knowledge of international law and the availability of soft skills were noted by only 74% of the surveyed employees.

4) *Employer survey results.* In our opinion, an important issue in determining the attractiveness of the College of Law was to involve in the survey employers who are the most interested party in obtaining highly qualified specialists, creating jobs, thereby ensuring successful employment of graduates.

86 participants took part in the survey of the specified category of respondents, representing sixteen areas of activity. Representatives of the spheres of activity "Commercial companies", "Public sector", "Small business", "Law enforcement agencies", "Law offices", "Courts", "Mediators" and "Others" made up the specific weight (Figure 9).

Analysis of the survey results helps to understand which, from the point of view of employers, indicators in the work of the College of Law are important in the formation of popularity in the market of educational services. The definition of the priority criteria related to the practical skills of graduates - "Practice-oriented curriculum" and "Evaluation of the quality of education of graduates by employers" is quite clear.

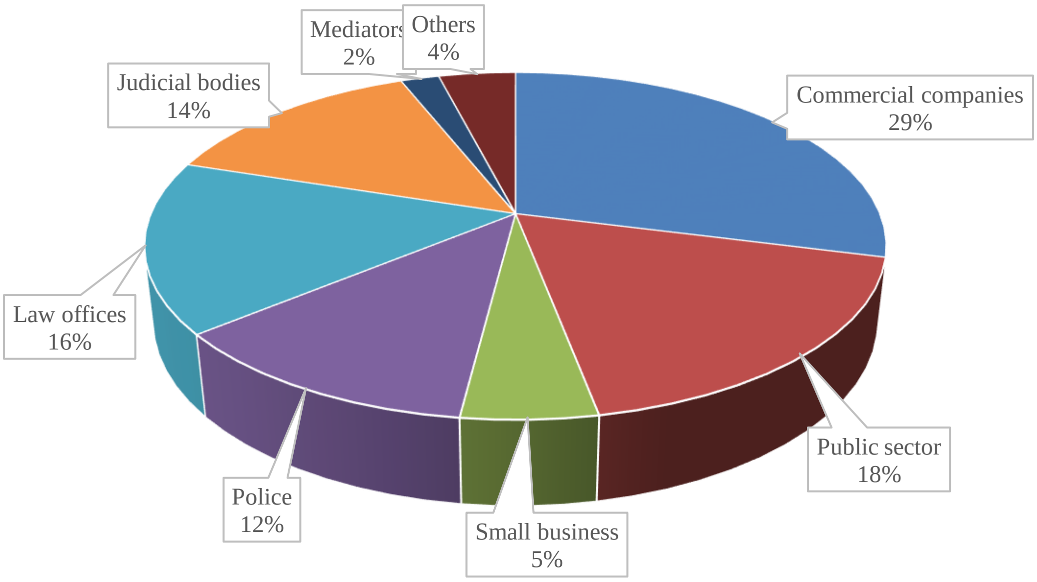

Figure 9. Distribution of employers according to spheres of activity

Source: Created by author based on survey data

The indicator related to the cooperation of educational institutions with representatives of the labor market regarding the formation of educational and professional programs received a high level (Figure 10).

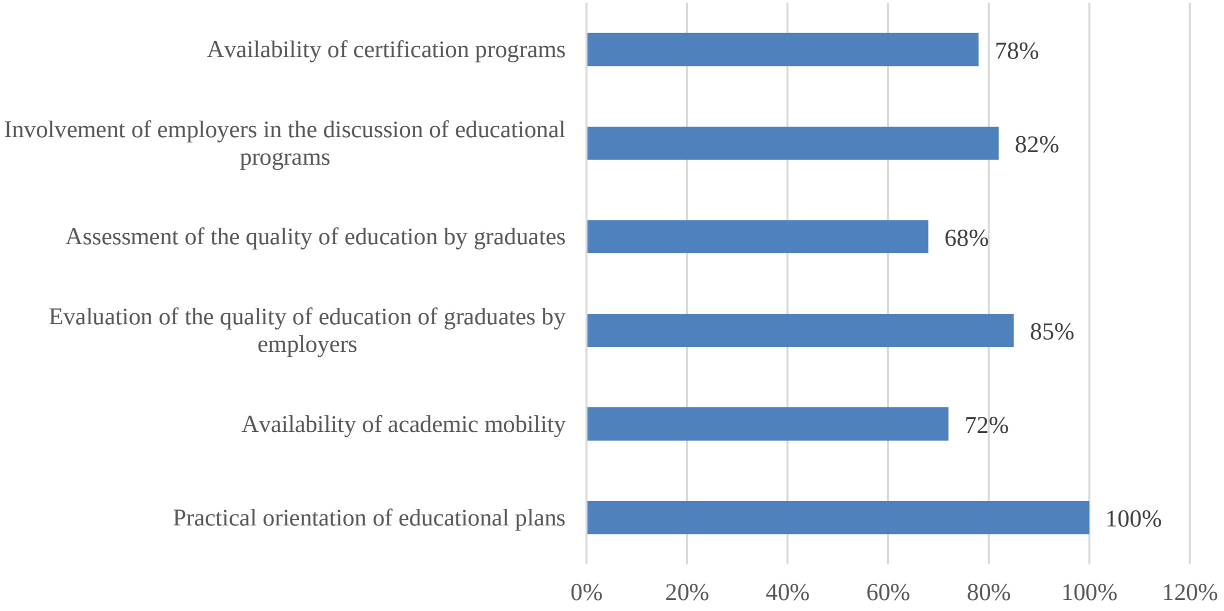

Figure 10. Priority criteria defined by employers

Source: Created by author based on survey data

Regarding the main competencies that graduates of the College of Law should possess, the majority of employers named: logical thinking (100%), ability to work with information (94%) and databases (92%) (Figure 11).

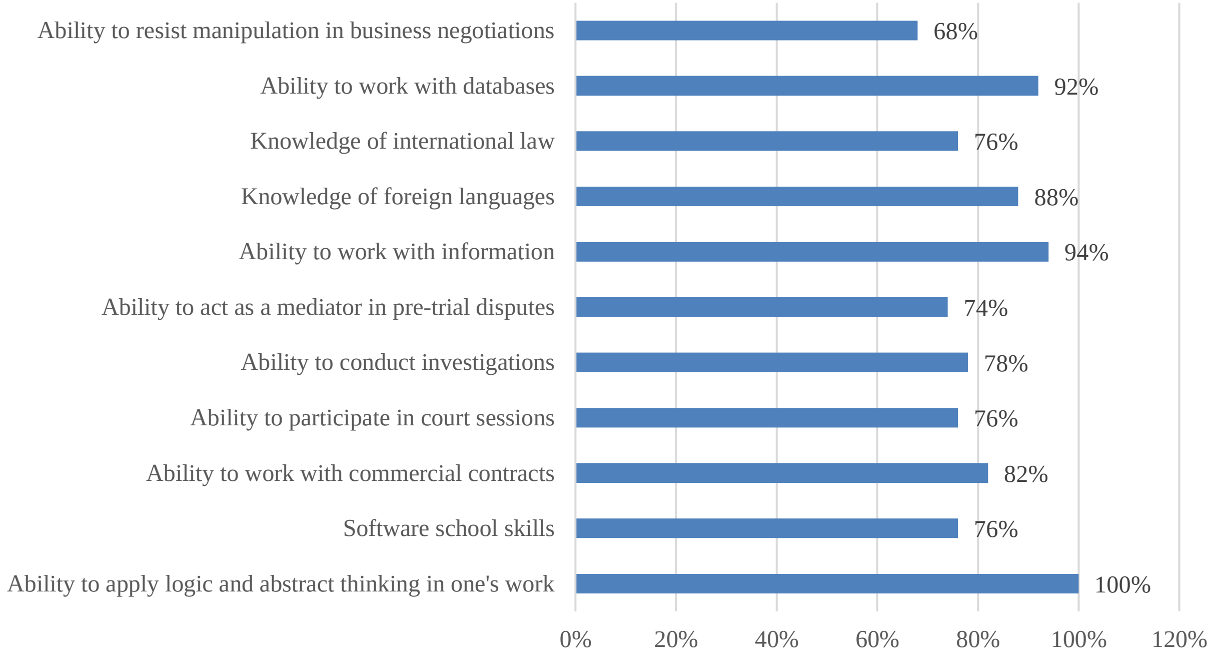

Figure 11. Distribution of criteria by employers

Source: Created by author based on survey data

The majority of employers who took part in the survey indicated that logical thinking and the ability to work with information were prioritized over special legal skills, although they also played a significant role in the training of future lawyers.

Results&Discussion. Based on the results of the research, the main competencies that future students of the master's degree in "Cyberterrorism" should possess were summarized, namely: competencies in the field of international law; competences in the field of international relations; competencies in the field of international and national security; competencies in the field of information technologies; competences in the field of cyber security; competences in the field of communication technologies, etc.

Summarizing the results of the review of scientific works and the results of the survey, we consider it necessary to propose the introduction of new disciplines that will complement the existing curricula and allow students to acquire new competencies that meet the requirements of the modern labor market in the specialty "Cyberterrorism" (table 2).

So, the College of Law, Jadara University makes a direct contribution to the social, cultural and economic development of the society and the graduates of the College of Law are important ambassadors of the College and play a key role in maintaining safety in the society and providing space and improving opportunities for members of the local community to obtain access to the College of Law and take advantage of the various services it provides.

Table 2. The need to introduce new disciplines for students

Subjects	Competences
International law	- demonstrate knowledge of international law in the field of information protection
International relations	- - demonstrate understanding of the essence of globalization processes and analyze their impact on international relations; - - to demonstrate in-depth knowledge of international and national security problems, international and internationalized conflicts, approaches, methods and mechanisms of ensuring security in the international space and in the foreign policy of states; - - identify and forecast political, diplomatic, security, social and other risks in the field of international relations and global development; - - evaluate and analyze international and foreign policy problems and situations, propose approaches to solving such problems; - - to organize and conduct independent studies of international relations problems using scientific theories and concepts, scientific methods and interdisciplinary approaches
International security	- - to demonstrate in-depth knowledge of international security problems, international and internationalized conflicts, approaches, methods and mechanisms of ensuring security in the international space and in the foreign policy of states; - - evaluate and analyze international and foreign policy problems and situations, propose approaches to solving such problems; - - to organize and conduct independent studies of international relations problems using scientific theories and concepts, scientific methods and interdisciplinary approaches
National security	- demonstrate in-depth knowledge of national security issues, international and internationalized conflicts, approaches, methods and mechanisms for ensuring security in the international space and in the foreign policy of states
Cyber security	- - demonstrate knowledge of international law in the field of information protection; - - demonstrate practical skills of users with computer equipment and software; - - the ability to assess the quality, appropriateness, completeness, effectiveness, and adequacy of information and directly sources of information for a specific purpose or policy of the organization (including the authority and timeliness of information)
Communication technologies	- - demonstration of the ability to critically evaluate the textual or graphic characteristics of digital media, their social contexts and trends, orientation, as well as economic and cultural significance; - - the ability to assess the quality, appropriateness, completeness, effectiveness, and adequacy of information and directly the source of information for a specific purpose or policy of the organization (including authority and timeliness of information); - - demonstration of the ability to analyze (comparison, contrast, summary), interpret and highlight information from many sources, which is collected using quality management tools from the conditions of further development of the organization

Conclusions. The article examines the etymology of the term "cyberterrorism" in historical retrospect. The main stages of training of cyber security specialists in different countries of the world were studied and the main competencies possessed by persons who commit cyber-terrorist crimes were analyzed. The main competencies that graduates of the College of Law, Jadara University should possess in order to counter cyber-terrorist threats have been clarified. Four groups of respondents were surveyed: students, their parents, college employees, and employers regarding the core competencies that college graduates should possess. The author's view on the need to introduce new disciplines for students studying cyberterrorism and countering it is offered. We believe that the proposed changes will allow the College of Law, Jadara University to acquire the image of a center for combating cyberterrorism.

References:

1. Toffler, Alvin. (1991). Powershift: Knowledge, Wealth, and Violence at the Edge of the 21st Century. New York : Bantam Books.
2. Defending against Cybercrime and Terrorism: A New Role for Universities URL: https://heinonline.org/HOL/LandingPage?handle=hein.journals/fbileb74&div=7&id=&page=
3. Cohen, F. (1987). Computer viruses: Theory and experiments. *Comput. Secur., 6,* 22-35.
4. Collin B. (1997). Future of Cyberterrorism: *The Physical and Virtual Worlds Converge. Crime and Justice International*; 13(2), 15-18.
5. Daniel M. Stewart & Eric J. Fritsch (2011). School and Law Enforcement Efforts to Combat Cyberbullying, Preventing School Failure: Alternative Education for Children and Youth, 55:2, 79-87, DOI: 10.1080/1045988X.2011.539440
6. Finn, J. (2004). A survey of online harassment at a university campus. *Journal of Interpersonal Violence*, 19: 468–483.
7. Ybarra, M. L., Mitchell, K. J., Wolack, J. and Finkelhor, D. (2006). Examining characteristics and associated distress related to Internet harassment: Findings from the Second Youth Internet Safety Survey. *Pediatrics,* 118: 1169–1177. [Crossref], [PubMed], [Web of Science ®], [Google Scholar]
8. Sameer Hinduja & Justin W. Patchin (2011) Cyberbullying: A Review of the Legal Issues Facing Educators, Preventing School Failure: Alternative Education for Children and Youth, 55:2, 71-78, DOI: 10.1080/1045988X.2011.539433
9. Öğün et al. TERRORIST USE OF CYBER TECHNOLOGY. (2021) *Eskişehir Technical Univ. J. of Sci. and Tech*. B – Theo.Sci. Vol: 9 – 2021 Iconat Special Issue 2021
10. Dorothy E. Denning. A View of Cyberterrorism Five Years Later. URL: https://apps.dtic.mil/sti/pdfs/ADA484928.pdf.

Received: February 15, 2023
Approved: March 30, 2023