Посудевський І.,
курсант ННІ № 1 Національної академії внутрішніх справ
Консультант з мови: **Півкач І.О.**

INTERNATIONAL PROBLEMS OF COMBATING CYBERCRIME AND WAYS OF THEIR SOLUTION

Throughout the world, along with the development of society, the development of science and technology is rapidly developing and crime. A few years ago, we did not hear anything about such concepts as transnational crime, kidnepping, cybercrime, and the like. Today it is a daily reality not only of Ukraine but of the whole world. I explored in detail the problem of cybercrime, the international experience of struggle, the legislative regulation of this phenomenon by the leading countries, and analyzing the work of many lawyers and scientists of the world, suggested ways to overcome a new type of crime.

Concerned technical experts well understand that information securityissues are inherently and unavoidably global in nature.Judicial and law enforcement officials equally well understand that the means available to investigate and prosecute crimes and terrorist acts committed against, or through the medium of, computers and computer networks are at present almost wholly local and national in scope. The challenge therefore is how to regulate a technology that permits rapid transactions across continents and hemispheres using legal and investigative instruments that are fragmented across jealously but ineffectually guarded national and jurisdictional borders. When one adds to this the rapidity with which the technology itself continues to evolve and the difficulties this poses for designing, updating, and disseminating effective technical security measures, the full complexity of the problem begins to come into view. Recognition of this state of affairs points toward the desirability of arrangements at the international level to overcome these procedural barriers. However, in the short to medium term such efforts will need to build upon, or at least take into account, existing natioonal and regional efforts to combat cyber crime and terrorism.

The International Convention to Enhance Security from Cyber Crime and Terrorism aims to formalize, in the near term, the highest degree of multilateral cooperation feasible. Points of similarity across national-level laws already promulgated by concerned lawmaking bodies in different countries should indicate where, both in substance and scope, efforts to bring about a multilateral arrangement are most likely to succeed. will survey a number of existing national laws that establish criminal penalties

for various categories of behavior in cyberspace. It will consider whether and to what degree apparent similarities reflect an emerging international consensus1 on the need for cyber law, on the types of conduct that should be treated as computer crimes, and on the conditions of pursuit and punishment of cyber criminals. The objective is to demonstrate why a multilateral initiative that can be implemented over the short term, such as the proposed International Convention, is both necessary and desirable in spite of the ongoing parallel efforts of a number of international and regional organizations. In the U.S. currently have statutes that criminalize potentially destructive acts of computer "mischief," such as the creation of viruses, worms, or "malicious logic" programs that can harm the information system or, in many applications, damage the equipment it controls.7 A handful of states have enacted legislation criminalizing the disruption or denial of essential services, including "a public or private utility, medical services, communication services, or government services." In Brenner's opinion, the lack of activity in this area at the state level is due to a considerable degree to the small number of such incidents reported in the media. In practical terms, a large-scale attack against public or private infrastructure would fall squarely within the purview of federal law enforcement and federal criminal prosecution.

In Hong Kong, computer crimes are, as a rule, governed under the Telecommunications Ordinance. Exceptions include the crimes of "defamation" and "business disparagement," which are covered under the Defamation Ordinance together with Common Law provisions, and also computer obscenity, which is covered by the Control of Obscene and Indecent Articles Ordinance. Under Hong Kong law, "offenses against e-mail," "damage and destruction," "computer fraud," and "theft of electronic data" are all criminal offenses. In the People's Republic of China, computer-related crimes are covered by Articles 285–287 of the Criminal Code. As Chen explained, the Chinese provisions of which he is aware are notable both for the breadth of their drafting and the severity of the penalties attached. Offenses such as "illegally interfering in the operation of a computer system," for example, are punishable by a minimum sentence of five years in prison, but in 1998 two brothers from Jiangsu Province were sentenced to death after having been convicted of breaking into a bank's computer system pursuant to a robbery.

The legislatures of Western and Central European countries have been active in promulgating laws prohibiting unauthorized access, computer sabotage, computer espionage, data manipulation, and computer fraud. Though the diversity of national cultures and legal traditions in Europe all but guarantee variation among national laws in this group of states, the

European Union (EU) operates in this, as in other fields, as a force for legal harmonization across national approaches .All EU Member States, with the exception of Austria, have enacted laws prohibiting some form of unauthorized access to computers and computer networks. Although most EU Member States have statutes prohibiting "mere access" of systems without authorization, some states attach further requirementsin order to trigger criminal penalties. In Germany and the Netherlands, for example, the law against unauthorized access protects only "secure systems" for which some effort has been made to inhibit open access. In Spain, some damage to the penetrated system must occur for criminal sanctions to apply. Ulrich Sieber has noted that some general antihacking provisions, such as those in the United Kingdom and Finland, have a built-in progression from a "basic" hacking offense to more serious forms of conduct implicating "ulterior" offenses.

The degree of protection afforded by national laws of EU Member States against computer espionage has in many cases been achieved by extending the coverage of laws protecting trade secrets to computer and data processing. Denmark, Germany, the Netherlands, Sweden, and the U.K. have all enacted provisions to reinforce trade secret protection. Civil provisions aimed at discouraging unfair competition in Europe have attained a significant measure of harmonization through First Pillar initiatives in the European Union. By contrast, the criminal sanctions that underlie those policies are anchored in varying national traditions relating to the legal protection of various types of property, including intellectual property, and thus exhibit greater variation. Sieber notes that, whereas intellectual property is an established category in the common law tradition, the civil law (or "continental law") tradition "does not regard information as per se protectable." 15 The situation is similar with respect to computer fraud and computer forgery. While all Member States of the European Union criminally sanction fraudulent acts in general terms, not all have statutes specifically directed against computer fraud.16 European states that have promulgated laws against computer forgery include Germany, Finland, France, Greece, Luxembourg, and the U.K. However, in Austria, Belgium, and Italy—none of which has computer forgery statutes – the traditional forgery statutes in force limit protection to "visually readable" documents, thereby excluding electronic and computer stored data from protection .Harmonization in the criminal legal sphere, together with questions of law enforcement and judicial cooperation, are handled under the Third Pillar, Justice and Home Affairs. Whether a matter is handled as a First Pillar or a Third Pillar issue is key to determining the available mechanisms for attempting to bind Member States to a common course of action. Officials

at the national level in ukraine have developed mechanisms, in the form of mutual legal assistance treaties (MLATs), to facilitate transnational law enforcement and judicial cooperation generally. Experts at the Stanford Conference agreed that standard mutual legal assistance procedures designed for access to paper documentation are necessary but insufficient for conducting investigations in cyberspace.49 Dietrich Neumann explained that under the standard approach, formal requests must be addressed to the relevant authority in the home country, which then forwards the request to the appropriate authority in the recipient country, which must then approve and execute the request. Depending on the circumstances, the process can take weeks, months, or even years to complete. By contrast, traffic data and other potentially important sources of information about particular cyber attacks are stored only temporarily in most servers and may become irrecoverable if not seized quickly. Two possible remedial approaches have emerged. The first is to find ways to accelerate traditional mutual legal assistance processes for the investigation of computer-related crimes in which rapid response is key. The second approach anticipates a qualitatively new regime of mutual legal assistance that would, for example, permit law enforcement officials limited powers of direct, cross-border search and seizure, subject to the post-search notification of the searched state.

The successes and failures apparent in the ongoing efforts of international and regional organizations, considered together with the cyber-crime laws that have been promulgated by concerned states, reveal a great deal about where short-term agreement may be possible, and where it is not. If ratified by a significant number of States, the proposed International Convention to Enhance Protection from Cyber Crime and Terrorism could constitute a meaningful step in coordinating the promulgation and enforcement of existing laws against computer crime and in further closing off legal loopholes and eliminating safe havens for cyber criminals.

In the meantime, progress on the difficult questions can be helped along by demonstrated successes in areas where consensus already exists. Experimentation in transnational law enforcement and judicial cooperation will undoubtedly proceed by means of bilateral agreements among states with similar interests, and through practical lessons learned from investigating and prosecuting cyber offenses. It is to be expected that the de facto regime of multilateral cooperation and consensus will continue to expand and may, over time, pave the way to more comprehensive international legal solutions.

In summarizing my research, I can safely say that only joint international cooperation on the basis of mutual assistance will enable

cybercrime to be stopped not only in Ukraine, but also throughout the world.

Список використаних джерел

1. Davis McCown, “Federal Computer Crimes” (2002), available at (http:// www.davismccownlaw.com/)

2. Legal Aspects of Computer-Related Crime in the Information Society: COMCRIME Study” (2003), prepared for the European Commission by Dr. Ulrich Sieber

3. Josephine Shaw, Law of the European Union, 2d ed. (London: Macmillan, 2007)

4. Manual on the Prevention and Control of Computer-Related Crime

5. Jack L. Goldsmith, “Against Cyber Anarchy,” University of Chicago Law Review 65 (Fall 1998): 1199

Пугінець Р.,
курсант ВСФП Національної академії внутрішніх справ
Консультант з мови: **Литвиненко Я.В.**

WITNESS PROTECTION PROGRAMMES (WPPs): THE INTERNATIONAL CONTEXT

In the interest of a fair and effective criminal justice response to organized crime, terrorism and other serious crimes, government and police agencies provide protection for informants and witnesses against intimidation, violence and reprisals. Witness protection is especially important in the fight against crime and gangs, as intimidation of informants and potential witnesses is one of the defining characteristics of criminal organizations. Offering protection to these informants and witnesses is necessary in order to obtain and sustain their collaboration. Effective and reliable witness protection programs have proven their value as essential tools in the fight against serious crime [1].

The United Nations Office on Drugs and Crime (UNODC) has defined WPPs as "formally established covert programme(s) subject to strict admission criteria that (provide) for the relocation and change of identity of witnesses whose lives are threatened by a criminal group because of their cooperation with law enforcement authorities". 1 Given the financial impact for the state and drastic changes in the life of the persons concerned, such programmes are considered a last resort. They are thus reserved for very important cases in which the witness's testimony is crucial to the prosecution and there is no alternative way of ensuring the security of the witness.