Cybercrime Prevention And National Strategies

Cavad Velizade
Master degree student of Criminal Law,
Law Faculty, Baku State University

Key words: computer systems, investigation processes, registration requirements, identification of users, central administration and technical standards

ABSTRACT

This article is dealed with the cybercrime, prevention against and national legislations, and activities. Cybercrime is considered one the most dangerous threats for the development of any state; it has a serious impact on every aspect of the growth of a country. Government entities, non-profit organizations, private companies and citizens are all potential targets of the cyber criminal syndicate. The prevention of cyber criminal activities is the most critical aspect in the fight against cybercrime.

Açar sözlər: kompüter sistemləri, istintaq prosesləri, qeydiyyat tələbləri, istifadəçilərin müəyyənləşdirilməsi, mərkəzi idarəetmə və texniki standartları

XÜLASƏ

Məqalə kibercinayətkarlıq, onun qarşısının alınması və dövlətlərin milli qanunvericiliyi, fəaliyyətindən bəhs edir. Kibercinayətkarlıq hər bir dövlətin inkişafı üçün ən təhlükəli təhdid hesab olunur və ölkə inkişafının hər aspektinə ciddi təsir göstərir. Qeyri-kommersiya təşkilatları, özəl şirkətlər və vətəndaşlar kiber cinayətlərin potensial hədəfləridir. Kibercinayətlərin qarşısının alınması kibercinayətkarlığa qarşı mübarizədə ən mühüm aspektdir.

Ключевые слова: компьютерные системы, процессы расследования, требования к регистрации, идентификации пользователей, центральное управление и технические стандарты

РЕЗЮМЕ

Эта статья съезжались с киберпреступностью, предотвращение и против национальных законодательств, а также деятельности. Киберпреступность считается одним из наиболее опасных угроз для развития любого государства; это оказывает серьезное влияние на каждый аспект роста страны. Государственные учреждения, некоммерческие организации, частные компании и граждане являются потенциальными объектами кибер-преступный синдикат. Предотвращение кибер-преступной деятельности является наиболее важным аспектом в борьбе с киберпреступностью.

The “cybercrime industry” operates exactly as legitimate businesses working on a global scale, with security researchers estimating the overall amount of losses to be quantified in the order of billions of dollars each year. In respect to other sectors, it has the capability to quickly react to new business opportunities, benefiting from the global crisis that – in many contexts – caused a significant reduction in spending on information security.

Prevention means to secure every single resource involved in the business processes, including personnel and IT infrastructure. Every digital asset and network component must be examined through a continuous and an evolving assessment. Government entities and private companies must cooperate to identify the cyber threats and their actions—a challenging task that could be achieved through the information sharing between law enforcement, in-

telligence agencies and private industry [2].

Security must be addressed with a layered approach, ranging from the "security by design" in the design of any digital asset, to the use of a sophisticated predictive system for the elaboration of forecasts on criminal events. Additionally, sharing threat information is another fundamental pillar for prevention, allowing organizations and private users to access data related to the cyber menaces and to the threat actors behind them.

At the last INTERPOL-Europol conference, security experts and law enforcement officers highlighted the four fundamentals in combating cybercrime as:

1. Prevention
2. Information Exchange
3. Investigation
4. Capacity Building

In September 2014, Troels Oerting announced the born of the Joint Cybercrime Action Taskforce (J-CAT) with the following statements that remark the necessity of an efficient collaboration between the entities involved, not excluding the Internet users.

Prevention activities must be integrated by an effective incident response activity and by a recovery strategy to mitigate the effects of cyber incidents. Once an event is occurring, it is crucial to restore the operation of the affected organization and IT systems. Recovery from cybercrime is composed of the overall activities associated with repairing and remediation of the impacted systems and processes. Typically, recovery includes the restoration of damaged/compromised data and any other IT assets [5].

Law-enforcement agencies can now use the increasing power of computer systems and complex forensic software to speed up investigations and automate search procedures. It can prove difficult to automate investigation processes. While a keyword-based search for illegal content can be carried out easily, the identification of illegal pictures is more problematic. Law-enforcement agencies are taking action to restrict uncontrolled access to Internet services to avoid criminal abuse of these services. In Italy and China, for example, the use of public Internet terminals requires the identification of users [3].

However, there are arguments against such identification requirements. Although the restriction of access could prevent crimes and facilitate the investigations of law-enforcement agencies, such legislation could hinder the growth of the information society and the development of e-commerce. It has been suggested that this limitation on access to the Internet could violate human rights. For example, the European Court has ruled in a number of cases on broadcasting that the right to freedom of expression applies not only to the content of information, but also to the means of transmission or reception. In the case Autronic v. Switzerland, the court held that extensive interpretation is necessary since any restriction imposed on the means necessarily interferes with the right to receive and impart information [6]. If these principles are applied to potential limitations on Internet access, it is possible that such legislative approaches could entail violation of human rights. The Internet has millions of webpages of up-to-date information. Anyone who publishes or maintains a webpage can participate. One example of the success of user-generated platforms is Wikipedia, an online encyclopaedia where anybody can publish[3]. The success of the Internet also depends on powerful search engines that enable users to search millions of webpages in seconds. This technology can be used for both legitimate and criminal purposes. The ongoing discussions about Internet governance suggest that the Internet is no different compared with national and even transnational communication infrastructure. The Internet also needs to be governed by laws, and lawmakers and law-enforcement agencies have started to develop legal standards necessitating a certain degree of central control. The Internet was originally designed as a military network based on a decentralized network architecture that sought to preserve the main functionality intact and in power, even when components of the network were attacked. As a result, the Internet's network infrastructure is resistant to external attempts at control. It was not originally designed to facilitate criminal investigations or to prevent attacks from inside the network. Today, the Internet is increasingly used for civil services. With the shift from military to civil services, the nature of demand for control instruments has changed. Since the network is based on protocols designed for mili-

tary purposes, these central control instruments do not exist and it is difficult to implement them retrospectively, without significant redesign of the network. The absence of control instruments makes cybercrime investigations very difficult. One example of the problems posed by the absence of control instruments is the ability of users to circumvent filter technology using encrypted anonymous communication services. If access providers block certain websites with illegal content (such as child pornography), customers are generally unable to access those websites. But the blocking of illegal content can be avoided, if customers use an anonymous communication server encrypting communications between them and the central server. In this case, providers may be unable to block requests because requests sent as encrypted messages cannot be opened by access providers [1].

Many data transfer processes affect more than one country. The protocols used for Internet data transfers are based on optimal routing if direct links are temporarily blocked. Even where domestic transfer processes within the source country are limited, data can leave the country, be transmitted over routers outside the territory and be redirected back into the country to the final destination. Further, many Internet services are based on services from abroad, e.g. host providers may offer webspace for rent in one country based on hardware in another. If offenders and targets are located in different countries, cybercrime investigations need the cooperation of law-enforcement agencies in all countries affected. National sovereignty does not permit investigations within the territory of different countries without the permission of local authorities. Cybercrime investigations need the support and involvement of authorities in all countries involved. It is difficult to base cooperation in cybercrime on principles of traditional mutual legal assistance. The formal requirements and time needed to collaborate with foreign law-enforcement agencies often hinder investigations. Investigations often occur in very short time-frames [2]. Data vital for tracing offences are often deleted after only a short time. This short investigation period is problematic, because traditional mutual legal assistance regime often takes time to organize. The principle of dual criminality also poses difficulties, if the offence is not criminalized in one of the countries involved in the investigation. Offenders may be deliberately including third countries in their attacks in order to make investigation more difficult. Criminals may deliberately choose targets outside their own country and act from countries with inadequate cybercrime legislation. The harmonization of cybercrime-related laws and international cooperation would help. Two approaches to improve the speed of international cooperation in cybercrime investigations are the G8 24/7 Network and the provisions related to international cooperation in the Council of Europe Convention on Cybercrime.

Based on experience, it may be difficult for national authorities to execute the drafting process for cybercrime without international cooperation, due to the rapid development of network technologies and their complex structures. Drafting cybercrime legislation separately may result in significant duplication and waste of resources, and it is also necessary to monitor the development of international standards and strategies. Without the international harmonization of national criminal legal provisions, the fight against transnational cybercrime will run into serious difficulties, due to inconsistent or incompatible national legislations. Consequently, international attempts to harmonize different national penal laws are increasingly important. National law can greatly benefit from the experience of other countries and international expert legal advice.

Offenders use ICTs in various ways in the preparation and execution of their offences. Lawenforcement agencies need adequate instruments to investigate potential criminal acts. Some instruments (such as data retention) could interfere with the rights of innocent Internet users. If the severity of the criminal offence is out of proportion with the intensity of interference, the use of investigative instruments could be unjustified or unlawful. As a result, some instruments that could improve investigation have not yet been introduced in a number of countries. The introduction of investigative instruments is always the result of a trade-off between the advantages for law-enforcement agencies and interference with the rights of innocent Internet users [4]. It is essential to monitor ongoing criminal activities to evaluate

whether threat levels change. Often, the introduction of new instruments has been justified on the basis of the "fight against terrorism", but this is more of an farreaching motivation, rather than a specific justification per se.

References

1. Hayden, Cybercrime's impact on Information security, Cybercrime and Security, IA-3.

2. Hale, Cybercrime: Facts & Figures Concerning this Global Dilemma, CJI 2002, Vol. 18, available at: www.cjcenter.org/cjcenter/publications/cji/archives/cji.php?id=37

3. Gercke, The Slow Awake of a Global Approach Against Cybercrime, Computer Law Review International, 2006.

4. Gercke, National, Regional and International Approaches in the Fight Against Cybercrime, Computer Law Review International 2008.

5. Broadhurst, Development in the global law enforcement of cyber-crime, in Policing: An International Journal of Police Strategies and Management, 29(2), 2006.

6. UN Manual on the Prevention and Control of Computer-Related Crime. United Nations publication, Sales No. E.94.IV.5, available at: ww.uncjin.org/Documents/EighthCongress.html