351.74/6.1(4-672 EU)

▪ **dr Dalibor Kekic**
Academy of Criminalistic and Police Studies, Belgrade

EU Intelligence Network: ENFOPOL

Abstract

ENFOPOL (Enforcement Police) is a European electronic intelligence network, which is able to fully track and monitor all types of electronic communications. Police have connected the EU states and it is organized after the ECHELON (Electronic Surveillance Operation) – the U.S. intelligence network, which includes: Australia, New Zealand, Canada and Great Britain. European police cooperation on this basis has been established in the form of working groups – the police-squad experts, gathered from all EU countries, primarily in the field of the fight against cyber-crime. These experts have determined the legal way to promote, attain and improve the fight against contemporary forms of security threats, terrorism, organized crime, and the like.

Key words: ENFOPOL, cyber crime, organized crime, terrorism, intelligence network, the European Union.

Introduction

Modern electronic devices have not only become a matter of prestige, but also a pressing need, for both state and non-state organizations. Some experts and scholars view them as a product of a "complex interdependence", while others deem that they have been created as a result of electronic revolution and therefore have to be an integral part of life.

Notwithstanding the above, many criminal and terrorist organizations see the inventions related to electronics as an opportune tool for their activities and as a way to get rich. All potential terrorists and criminals use modern means of communication to perform tasks for their criminal hubs[1]. The share of electronic crime in the "gross criminal product" generated through activities of, one could say, global organized crime, has reached hundreds of billions of U.S. dollars at the end of the previous century, which is considerably more than the gross domestic product of 90% of the countries in the world.[2]

Joseph Nye sees the reasons for this trend in relation to people, material goods and the advancement of electronic means in: the growing economic interdependence of countries (the need for more effective relations between them), the process of modernization and urbanization, as well as the development of communication in the developing countries (encouraging the transfer of power from the state government to the private sector), the spreading of military technology, which increases the power of the less economically developed countries and changes the order in which current issues get solved in world politics.[3]

In this multitude of new technologies, especially the Internet, there have been numerous attempts at fraud and secret correspondence between the headquarters and the cells of terrorist and criminal organizations

After 11 September, distraught with panic and wishing to cut off all possible access routes to its electronic means, the U.S. began to push the issue of ECHELON, the U.S. electronic network. ECHELON was originally conceived as an intelligence surveillance system for monitoring the Soviet Union and its allies, but in time it developed into a spy network for monitoring terrorist organizations and detection of international drug cartels. The ECHELON system is simple in its structure. All its members belong to the English-speaking countries: Australia, New Zealand, Canada, the USA and the UK.

1 Internet, 02/06/10, http://mail.sarai.net/pipermail/reader-list/2001-June/000163.html.
2 Dragan R. Simic, *Nauka o bezbednosti – savremeni pristupi bezbednosti*, Official Gazette of FRY, Faculty of Political Sciences, Belgrade, 2002, p. 40.
3 R. Keohane & J. Nye Jr, (1989), Power and Interdependence (2nd ed.), Little, Brown, p. 12.

All these countries are part of the intelligence alliance UKUSA (UK–USA Security Agreement), which was established for the purpose of intelligence-sharing.[4]

Inception of ENFOPOL

The idea of the ENFOPOL appeared first towards the end of the last century, put forward behind the scenes the International Law Enforcement Telecommunications Seminar – ILETS. ILETS was a co-operation between the EU countries in the planning of a surveillance system for lawful interception of telecommunication. Certain European parliamentary bodies, as well as law enforcement officials from many EU countries, met in separate meetings, fora and sessions of the European Parliament to discuss the requirements of individual representatives for intercepting communications. The staff met under the auspices of the ILETS. The FBI initiated the establishment of the ILETS. Three years later the EU citizens were advised of these events.[5]

The ENFOPOL is a product of secret cooperation within the ILETS. The extent of this group's influence on the EU policy is well confirmed by the following statement: "Following the second ILETS meeting in Bonn, IUR (International User Requirements) 1.0 was presented to the Council of Ministers. It was accepted, without any objection, on 17 January 1995". While the FBI was active in the ILETS, the representatives of the law enforcement and intelligence services from the U.S., Canada and several European countries established the ENFOPOL in an FBI base in the USA. In addition, several ILETS meetings were held in the USA. Common standards for telecommunications equipment for easier surveillance of telecommunication traffic were discussed in the course of those meetings. The ENFOPOL started as an ILETS project.

Council Resolution on the lawful interception of telecommunications was published in the "Official Journal of the EU" on 4 November 1996, almost two years later. In support to the idea of establishing ENFOPOL, the draft of the Convention on the European Information System (EIS), the system that was to replace the Schengen Information System), was prepared in November 1993.[6]

In 1995, under strict confidentiality, the European Council tasked the ENFOPOL working group under the Council's K.4 Committee with making a draft of the Resolution and Law on European Police

4 Internet, 05/06/10, http://www.economypoint.org/e/echelon.html.

5 Dalibor Kekic, "Evropska obavestajna mreza (ENFOPOL)", *Evropsko zakonodavstvo,* no. 13/05, Institute for International Politics and Economics, Belgrade, 2005, p. 93.

6 *Interception capabilities 2000: The Abolition of Privacy?*, Internet, 30/05/10, http://www.fecl.org/circular/5803.htm.

Forces' Cooperation in Matters Related to Telecommunications Interception, in order to ensure the transparency of communication for the needs of national security agencies of the EU Member States. In February 1997, the EU took a secret decision in relation to the ENFOPOL, to create an international network through a clandestine network of offices in all the EU Member States. Politicians agreed that this network should be established in line with the "third pillar of the EU", and pursuant to the Maastricht Treaty. The key points of the plan were included in the Memorandum of Understanding, signed by all the representatives of EU Member States in 1995.

After several failed attempts to adopt a valid ENFOPOL document, the European parliamentarians adopted a Resolution on the ENFOPOL on 7 May 1999 (Council Resolution on Lawful Interception of Communications). The Internet providers and users were severely affected by this Resolution. In parallel with the Resolution, the Scientific and Technical Options Assessment Unit of the European Parliament (STOA) published a report on the history, scope, manner, political and technical capabilities of Communications Intelligence (Comint) with regards to communication interception capacities (the report code number *IC* 2000). The conclusion of the report was that the issue of electronic communication interception required an open debate between all representatives of user services and the users themselves.

In many EU countries, the authorities have taken steps towards successful and legitimate interception of electronic communications. In Great Britain, the courts authorize about 8,000 eavesdropping operations per year, and the NSA (the U.S. National Security Agency) intercepts communications of up to 40,000 users per year – and the British authorities are fully aware of that. The ENFOPOL does similar things with American citizens by using the system of reciprocity. At the same time, a group of police experts in the Netherlands were to draft a law under which all providers would be obliged to ensure free access to information. In Germany, legal structures and possibilities for interception of electronic communications were presented to the public on 4 May 1995. The Telecommunications Act was drafted in July 1996, and it went even further than the request presented by the ENFOPOL. This Act sought great freedom of access to user services for the intelligence services. The Act envisaged setting up the "competent management" which would have total access to all user services and thus not even the providers themselves would know the time and manner of interception.

ENFOPOL Status

Many people view the ENFOPOL as nothing more than a product of an accord between a small number of bureaucrats from Europe and America, who have agreed on a monitoring system of global and local communications networks. The problem the public has had with regards to the creation of the ENFOPOL is due to the fact that decisions and laws in the field of public communications have been adopted away from the public eye – non-transparently, behind the scenes. None of the commercial operators have voluntarily agreed that the police may search their network and intercept user data and information at will, the main reason being the violation of the EU citizens' rights to private conversation and correspondence. The providers often advocate the rights of their users in public, not because they care about the users but because of the costs that are imposed on them by the authorities. The state requires from the local providers to pay the cost of cyberspace for the operation of ENFOPOL.[7]

Thanks to the German local user service Telepolis, a secret text from 1998, agreed between the European police delegations, the EU countries' representatives meeting in Vienna and Madrid, was revealed. It is a document called ENFOPOL 98. The text was distributed over many sites on the Internet 10 days after its adoption. In the meantime, a new text titled ENFOPOL 19, on the manner of cooperation and ENFOPOL's operation, was adopted. ENFOPOL 19 was signed at a meeting of police officials in Brussels, chaired by a German representative, on 15 March 1999. The document confirmed that the police would not require special permission for tapping providers and users.[8]

Many experts such as Marc Rotenberg, Director of the Electronic Privacy Information Centre in Bonn, think that the ENFOPOL is a classic case of import of the "American legal waste", which threatens fundamental human rights and freedoms. EU politicians have varied opinions on the issue of creating a joint intelligence service. They range from the opinion that the common political and security services stems from the natural sequence of events, to those who believe that the common foreign and security policy is quite enough.

The ENFOPOL is more or less like the ECHELON system, and yet in some segments it is something completely new. The ENFOPOL is integrated into the European legal system. It is not just one system, but rather the cooperation between different systems, such as the cooperation with the Internet service providers. The ENFOPOL

7 Medoch Armin, The European Secret Service Union, Internet, 30/05/10, http://www.euronet.nl/~rembert/echelon/moech11.html.

8 Kris Millegan, CTRL The ENFOPOL 98 Affair, Internet, 11/07/10, http://www.mail-archive.com/ctrl@listserv.aol.com/msg12071.html

does not work outside the EU, and it is a unit that works within the legal framework, with the ability to operate within the entire European Union (as does the FBI in the USA). It is expected that an ENFOPOL police unit will be established in the near future. There is a possibility for the ENFOPOL to continue to cooperate closely with police structures across the EU, mostly through the ISP (Internet Service Providers).

Each piece of information is now stored in a safe place, and if a police unit or an intelligence service requires certain information, the ISP immediately forwards it to that particular service. The question is how long will the information be stored? As in America, the police must obtain a court order, before a certain piece of information is stored in a place which is under ENFOPOL's control, and everything must be documented. ENFOPOL controls the flow of information through satellites, mobile phones, credit cards, communication paths, the Internet, the new Iridium telecommunications system (based in Italy), and standardized telecommunications systems, etc.

By accepting the ENFOPOL the European Parliament has authorized the police and intelligence services to take the necessary steps towards the interception of telecommunications. In order to have total access to user data, the ENFOPOL requires the user services (service providers) to provide a "space" (the interface, a backdoor) in the network for accessing all traffic. The service is required to provide an open telephone line for the purpose of tapping and recording at the expense of the provider.

The customer service has to provide the ENFOPOL with the geographic location of potential users which would be of interest to it. Intelligence services have recently seen increasing opportunities and huge advances in telecommunications, which implies the likelihood of more effective ways and options for interception and monitoring the traffic. Every previous police attempt to eavesdrop on telecommunications traffic, before the inception of the ENFOPOL was in most cases hindered or prevented by the legislature, interest groups (especially in industry), public interest organizations, and individuals themselves – the users.

Protection of privacy is of paramount importance to the EU citizens. We can imagine what could happen if the ENFOPOL got out of control, or worse, if it were controlled by large corporations. It sounds funny now, but the ENFOPOL has to rely on the help of corporations, such as the ISP for example, to come up with relevant data. Can the ISP use some of the data for their own needs – it is clear that they can. One can only conclude that with the system such as the ENFOPOL, it is legal to spy on innocent people too.

Areas of cooperation between the European Union and the ENFOPOL in its field of action may be classified in two groups:

- cooperation in the areas of operations under the Schengen Agreement, and
- cooperation in general criminal matters.

The following is particularly covered under the Schengen Agreement:

- police cooperation for the purpose of preventing crime,
- cross-border surveillance,
- cross-border hot pursuit,
- communication and forwarding information in special cases for the purpose of combating crime and preventing offences or in the event of threat to public security or policy,
- exchange of information for effective border checks and surveillance,
- exchange of low ranking liaison officers,
- enhanced police cooperation in cross-border areas via bilateral arrangements and agreements, and
- surveillance of the EU common information system.

Mutual assistance in criminal matters:

- crime prevention,
- exchange of information on hooliganism at football stadiums and other sport events,
- genocide,
- crimes against humanity and war crimes,
- missing persons,
- police staff training,
- personal security, and
- protection of public persons.

Special manner of cooperation within the ENFOPOL includes fight against terrorism and various extremist and religious zealot organizations.

Future Expectations Regarding The ENFOPOL

If, for example, the United Kingdom, which is part of the ECHELON, accepts the ENFOPOL as its own organization, we may speak of a complete system of surveillance of communications in this country. This is contrary to many laws, but, of course, there is plenty of room to change the laws. The ENFOPOL, according to many experts, has not yet fully demonstrated its strength but that does not mean that

it shall not do so soon. The only thing the EU citizens can hope for is the protection of their own privacy.

Life in Europe is based on a high level of democracy, and it is inconceivable that the establishment and growth of an institution such the ENFOPOL would be allowed without consulting the public. In this sense, there are more and more individuals who are against this form of the invasion of privacy.

However, if we look at the history of organized crime and terrorism, it is clear that it is these organizations that most extensively use the benefits of modern communication systems. In this sense, the existence of institutions such as the ENFOPOL, is justified to some extent. Even though ordinary citizens are being tapped in over 90% of cases, it is necessary to protect their rights to privacy, and the entity that holds that information must keep it highly confidential.

Despite the criticism it has been subject to, the ENFOPOL still has a future because more and more telecommunications systems are available to people and it is necessary to bring order in the whole chaotic environment. On the other hand, the number of EU Member States is increasing and the individual police organizations and intelligence services do not have sufficient capacity to meet the current challenges, risks and threats to security, especially in the field of communications. Joint surveillance of the wealth of information flowing through various electronic systems is required.

Serbia And The ENFOPOL

When the Republic of Serbia became a sovereign state in 2006, it had to regulate its security intelligence system. Instead of that, the Republic of Serbia adopted the Law on the Basic Structure of Security Services in 2007, which essentially regulated only the National Security Council, the security services of the Republic of Serbia were only listed, and the manner of management and coordination of security intelligence, along with the ways of directing and coordinating the work of security intelligence services and mechanisms to control them, was established. Two years later, the Ministry of Defense forwarded the text of the Draft Law on the Military Security Agency and Military Intelligence Agency to a small circle of selected NGOs for discussion.[9] It is positive that the adoption of the Law on Military Security and Intelligence Agencies filled one of the gaps in the security and intelligence system of the Republic of Serbia.

9 Nacrt zakona o VBA i VOA u funkciji status quo, Internet, 24/06/10, http://institutparalaks.blogspot.com/2009/10/nacrt-yakona-o-vba-i-voa-u-funkciji.htm.

In addition to all these events, in May and June 2010 the Government of the Republic of Serbia proposed the Law on Electronic Communications, which in the opinion of numerous experts in electronic communications and security violated the Constitution of the Republic of Serbia. After a set of laws that were adopted within a year in the National Assembly of the Republic of Serbia, such as the Law on Secrecy of Data, the Law on Defense, the Law on the Army, of the Law on the Military Security Agency, the Law on the Military Intelligence Agency and the Electronic Communications Bill, the current government is, in the opinion of many, on its way not only to fully control the security and intelligence sector in Serbia, but the citizens as well. What upsets the public is that this legislation provides the national security structures with the ability to access the so-called retained data, and abruptness with which the law entered the parliamentary procedure.

In addition, a court decision is not mentioned as the basis, and such data on the communication sometime say at least as much as the very content of a phone call or an e-mail. These are the data that state who, when, how, for how long and where one interacted with someone over the Internet.[10] This is a question of retained data relating to: monitoring and identification of the source of communication; determining the destination of communication; establishing the beginning, duration and completion of communication; determining the type of communication; identification of the user's terminal equipment; and identification of the location of mobile terminal equipment.[11]

The Republic Commissioner for Information, commenting the Law, has said that "this systemic law requires a public discussion and public attention, especially within the professional community, and that some solutions of the said law are unclear, controversial and may result in violation of the Constitution and human rights guaranteed under the law. The European standards and procedures, presented in the decisions of the European Court of Human Rights favor the idea that the retained data are an integral part of communication, and that they are as important as its content. Even the Constitutional Court has deemed the provisions of Article 55 of the applicable Law on Telecommunications unconstitutional because, pursuant to the Article, the ban of activities which violate the privacy of telecommunications may be lifted, not only via a court decision, but even without it if it is envisaged under a law.

In her parliamentary exposé on the draft Law, the Minister of Telecommunications of the Republic of Serbia has stated that the

10 Ugljesa Mrdic, Prisluskivanje "Veliki brat" u skladu sa zakonom, Internet, 19/06/10, http://www.pecat.co.rs/2010/06/prisluskivanje-veliki-brat-u-skladu-sa-zakonom/.

11 Article 129, the Electronic Communications Bill, Internet 22/06/10, http://www.parlament.gov.rs/content/cir/akta/akta_detalji.asp?Id=1214&t=P#

Republic of Serbia is facing the challenges of opening the market for new operators, the transition from the analogue to the digital broadcasting of television programs, the acceleration of the process of EU accession, the sale of the state share in the company "Telekom Serbia", the harmonization of regulations with the standards of the European Union (harmonization with the EU aquis in line with the ENFOPOL requirements), and that the adoption of the Law will contribute to implementation of the above challenges. The national authorities do not agree on the adoption of this Law one hundred per cent. Representatives of the opposition parties have expressed their opinion that the Government of the Republic of Serbia is in a rush to adopt the Bill in order to "prepare the ground for the privatization of the company "Telekom Serbia".

Government representatives have voiced their regret over the National Assembly's rejection to expedite the adoption of the Law, since that would compromise the process of transition from the analogue to the digital television programs and prevent further implementation of the process of market liberalization and of attracting new investments in the infrastructure development, which implementation would be challenged by the absence of an adequate legal framework and the global economic crisis. The adoption of the Law on Electronic Communications should provide a modern, efficient and unified legal framework that would allow further development of electronic communications, which would directly contribute to increased competitiveness and provide a greater choice of quality services to the Serbian citizens, thus inproving the quality of everyday life. However, it seems that thanks to the Government, the opposite is happening in Serbia.

Therefore, the Security Information Agency shall, upon the adoption of the new Law on Telecommunications, have the right to tap into e-mails of the citizens of the Republic of Serbia without a court order, just upon the order of the Director of the SIA. There have been no significant expert discussions, which is the basis for the adoption of an adequate law. Another paradox is the focus of the enactment of this Law – the control over monitoring and the monitored data shall be in the hands of those who monitor them, that is, the SIA. Even though the Law was under public scrutiny in the months preceding its adoption, the MPs did not have many objections to its adoption.

All this, of course, brings to mind the preparations for the entry of the Republic of Serbia into the ENFOPOL system. In this sense, the manner of the adoption and the provisions of the future Law on Telecommunications bear an uncanny resemblance to the inception of the ENFOPOL. In this aspect, the Republic of Serbia is undisputedly making big steps towards the accession to the EU. It is clear that

it will enter the ENFOPOL system and become an integral part of the network very soon after the accession to the EU. If there were any opposition, it would not mean anything, because for such a conglomerate as the EU, an arrangement such as this one is necessary to control and combat organized crime and terrorism, whereas unauthorized monitoring of the citizens' electronic communication traffic represents a secondary side effect.

Concluding Remarks

In the modern world, power is moving away from those who are "capital rich" to those who are "information rich".[12] So, wealth eventually loses its original meaning. Moving towards this, the state still wishes to remain a reference object in the international security system which is being shaped and to keep power in its possession. The ENFOPOL is a product of that desire, even though there are outcries against this method of controlling the population. The state is able to control a three-dimensional space: territory, population, geographic area, etc. This time the state – a supranational entity of the EU – is trying to control the cyber-space, not allowing other non-state – criminal and terrorist organizations – to control it.

The ENFOPOL was modeled after a similar organization – the USA's ECHELON, and in this sense, it is not a novelty, but due to the number of people and countries that it includes, it presents a challenge in the field of police and intelligence activities. Inception of more and more similar institutions is to be expected in the future, because there are more and more new forms of communication which transcend state borders.

Thus, under the new Law on Telecommunications of the Republic of Serbia the Director of the Security and Information Agency shall be authorized to order tracking and monitoring of certain electronic traffic independently, without the approval of a court. The Republic of Serbia is expected to easily fit into the ENFOPOL system upon its accession to the European Union. Therefore, at least in this sphere the Republic of Serbia is within an inch of entering the Union.

12 Joseph J. Nye, "Soft Power", Foreign Policy, Fall. 1990, p. 152-4.

Bibliography

1. Armin Medoch, The European Secret Service Union, Internet, 30/05/10, http://www.eyronet.nl/~rembert/echelon/moech11.html.
2. Internet, 05/06/10, http://www.economypoint.org/e/echelon.html.
3. Internet, 02/06/10, http://mail.sarai.net/pipermail/reader-list/2001-Jyne/000163.html.
4. Interception capabilities 2000: The Abolition of Privacy?, Internet, 30/05/10, http://www.fecl.org/circylar/5803.htm.
5. Kekic Dalibor, "Evropska obavestajna mreza (ENFOPOL)", Evropsko zakonodavstvo, br. 13/05, Institute for International Polictics and Economics, Belgrade, 2005.
6. Keohane R. & Nye J. Jr, (1989), Power and Interdependence (2nd ed.), Little, Brown.
7. Millegan Kris, CTRL The ENFOPOL 98 Affair, Internet, 11/07/10, http://www.mail-archive.com/ctrl@listserv.aol.com/msg12071.html.
8. Mrdic Ugljesa, Prisluskivanje "Veliki brat"u skladu sa zakonom, Internet, 19/06/10, http://www.pecat.co.rs/2010/06/prisluskivanje-veliki-brat-u-skladu-sa-zakonom.
9. Nacrt zakona o VBA i VOA u funkciji status quo, Internet, 24/06/10, http://institytparalaks.blogspot.com/2009/10/nacrt-yakona-o-vba-i-voa-y-fynkciji.htm.
10. Nye J. Joseph, "Soft Power", Foreign Policy, Fall. 1990.
11. Electronic Communications Bill, Internet, 22/06/10, http://www.parlament.gov.rs/content/cir/akta/akta_detalji.asp?Id=1214&t=P#.
12. Simic R. Dragan, Nauka o bezbednosti – savremeni pristupi bezbednosti, Official Gazette of the FRY, Faculty of Political Sciences, 2002.