Interview with Dr. Maxim DOBRINOIU

Dr. Maxim DOBRINOIU is currently a Cybercrime expert with the government system and Associate Professor with the Law Faculty, Nicolae Titulescu University, and Military Technical Academy. He previously worked as Computer Project Manager with IT company Romsys and a diplomat with the Romanian Ministry of Foreign Affairs.
With a BSc in Computer Science, a BA in Law and a PhD in Law (Cybercrime), Maxim DOBRINOIU is one of the few authors focused on analyzing and intensively studying cyber-related crimes and offences in Romania. His academic work, as single author or co-author, consists of numerous books, university courses, articles published indexed reviews, international studies, and cybercrime-related training sessions designed for Romanian magistrates, often considered as significant bibliographic references for interested legal practitioners, researchers, law enforcement agents or law students. Maxim's other professional interest relates to Information Security Management Systems, Digital Evidence, Privacy and Data Protection, Electronic Surveillance, Ethical Hacking, Hacktivism and Criminal Law.

1. You are Associate Professor at "Nicolae Titulescu" University of Bucharest and you are involved in a Master Programme where you teach about Cybercrime. Can you tell us more about the importance of this discipline to your students?

Thank you very much for this opportunity to present myself and the course I deliver.

Starting 2008, I realized that the cyber-related offences were regarded as a sort of an "island" in the general picture of the Romanian penal legislation and doctrine. With relatively few books, articles and studies publicly available, Cybercrime area was somehow ignored by the authors, and even by the penal law practitioners, due to its obvious technicality related to electronic devices, computer systems, computer data and Internet.

For all that, it is worth saying that, the challenge of combating Cybercrime in Romania was successfully fulfilled in time by the prosecutors of the Directorate for Investigating Organized Crime and Terrorism (Cybercrime Division) and the policemen of the General Inspectorate of the Romanian Police (Cybercrime Branch), as they were directly involved in tackling the issue and were "forced" to upgrade their professional background through intensive training.

Taking into consideration these aspects and my passion and extensive knowledge in the area of Cybercrime, I decided to create a new form of curriculum in order to properly address the issue to the benefit of Romanian law students and even of the law practitioners.

I must confess that my academic background, with a BSc in Computer Science, a BA in Law, and a PhD in Law (Cybercrime), helped me a lot in putting in practice of this idea.

The course started as a module inserted in the specific educational programs of the Criminal Sciences Master and Financial, Banking and Insurance Law Master organized by "Nicolae Titulescu" University of Bucharest.

The module addressed (and still does) specific topics, such as: terms and definitions, relevant national and European Laws and regulations, legal and technical analysis of the cyber-related offences, criminal procedure aspects regarding Cybercrime, criminology analysis of online perpetrators, digital evidence, privacy and protection of personal data in the field of electronic communications, as well as issues related to activism on Internet, hacktivism and Cyberterrorism.

Coming back to your question, I must say that the evolving threat posed by the fast developing technologies and the sophistication of the methods and means to conduct criminal activities against computer systems and data requires the judges, prosecutors, policemen, lawyers and legal counselors to have good knowledge and certain skills in order to properly tackle such type of specific crimes. And if this could be done as early as from the university benches, I think there is an important step forward in the fight against Cybercrime.

2. How important are the legal aspects to understand the cyber-crimes?

Cybercrimes or cyber-related crimes (because there is a slight distinction between them) are just crimes. And in order to fight them properly, you must first understand them well. You need to make a deep analysis of all their conditions, primarily based on the legal provisions – which represent the perspective of the legislator, then to interpret them to the best extent on which these crimes could be then used to indict a person, while assuring him the preservation of its (constitutional) rights.

It is true that a specific legal provision offers for analysis just what the legislator envisaged as worth protecting. It is the will of the society or of the state that are endangered by the illegal cyber activities. But the Cybercrime trend is continuously evolving, so the law must follow this trend as well. Otherwise, we may witness a weak legal response of the state in this fight, with criminals free to go, or a sort of legal abuse, by wrongfully interpreting the existing and non-adapted pieces of legislation. Hope this will stay only theoretical.

Understanding the crimes in cyberspace requires some technical skills and knowledge as well. The virtual world has its own rules, protocols and ethics. Generally, things are actually not what they appear to be. And this is the trap most of the ordinary people (and even some of the specialists) fall into. That's why the analysis of a computer-related crime must be done also from the technical perspective, not only legal.

3. Nowadays, cyber-criminals have many powerful tools in the Dark Net. Are you concern with this kind of cybercrime evolution in Europe?

It is obvious that cybercriminals needed a "safe haven", a hidden place where they could perform almost any kind of (criminal) activities with no fear to be identified, traced, indicted or punished according to the law. And DarkNet was created. DarkNet is

a special component of the DeepWeb - the un-indexed part of the overall Internet, as we know it.

The existence of the DarkNet poses now as a large surface for attacks and threats and is considered as a great challenge for the law enforcement agencies. Even if they manage to get into this dangerous virtual environment, tracking and taking down the criminals is hardened by the anonymity of users and lack of direct incriminating evidence.

The evolution is not good in this respect. We started to witness new and sophisticated forms of virtual crimes there. And I have in mind now just a few of them: crime-as-a-service, infrastructure-as-a-service (e.g. Botnet for hire), intelligence-as-a-service, pay-per-install, money-laundering (via Bitcoin) and so forth.

With all of these, law enforcement agencies try to fight with the help of traditional legal provisions. But in the future, these may be not enough or they will not fit anymore. Then, it is the criminal doctrine that needs to come up with relevant and comprehensive proposals for legal provisions that better address the new menaces.

4. Lately, the number and the complexity of cyber-attacks have increased in Internet. How do you think these attacks will evolve in the next years in Romania?

Indeed, the IT industry highlighted an increase in both the number and the sophistication of the "predicted" 2017 cyber-attacks. And this is worldwide. In a globalized world and with no physical boundaries, the threats from cyberspace may affect now any country, irrespective of the geographical location or the (economic) development of the target state.

Romania does not differ much from any other country from the victim's perspective. We may expect new and aggressive forms of Ransomware, and even cyber-espionage campaigns targeting state institutions or financial organizations. At a low level, there will be just the "usual" cyber-related illegal activities, such as: unauthorized gathering of personal and electronic payment data through Phishing and Skimming, computer frauds, illegal operations with devices and applications, infringing the Intellectual Property laws, and, of course, illegal access to computer systems.

5. You are very active in social media in raising the awareness in the cybercrime field. How important is social media in this domain?

I experienced the web in a first stance. In order to spread my ideas, articles and studies, I created a webpage – www.e-crime.ro, where I inserted interesting materials related to Cybercrime and other relevant subjects. The page is still active, but the Internet domain I use it mostly now for running the eLearning system that I have put in place for my students. I need to keep up with the modern educational trends as well.

Since 2012 I switched the focus on social media. I am active on various online platforms (Facebook, Twitter, LinkedIn) where I keep in touch with the IT Security, law enforcement and legal online communities from where I acknowledge most of what is worth in my field of expertise.

Social media seems to be a very good vehicle for spreading the news, the knowledge and a sort of expertise. I am not the only one doing that, and I encourage my fellow colleagues to be as active as I am in order to inform and educate the users, as a

significant part of the general effort in preventing Cybercrime. By the way, my Facebook page's name is E-Crime.ro, and your readers are welcome to join it.

6. What would be the best channel in Romania to improve awareness about the cyber-risks?

I usually avoid the word "best". When you need to get to somewhere, every mean may be "the best one", as long as it drives you to your goal.

Nevertheless, Romania has a good legislation, fulfills almost all the legal requirements from the European Commission and has built a significant legal practice on Cybercrime. Romania is one of the few European countries having a national Strategy on Cybersecurity, and strong achievements in the field of protecting computer systems and critical ICT infrastructures.

But Romania still has an Achilles' heel: its citizens - ordinary users. With no proper awareness strategy on Cybersecurity designed for them, they will soon become the worst enemy of their own and society too.

The awareness may be very well conducted through various means. Education seems to be, by far, the leading one. Elements of Cybersecurity could be inserted into all-grade curriculum, as from the primary school (where pupils could be taught how to properly handle electronic devices, especially the telephones – for emergencies) and secondary school (where pupils may learn how to protect themselves while navigating on Internet or playing PCs, and how to avoid being trapped by online child molesters), to high school (where teenagers could find out how to prevent being infected with computer viruses, how to behave on social media, how to electronically interact with others, how not to cyberbully or cyberharrass colleagues or friends, or how to stay away from online criminal activities), and universities (especially, but not limited to, computer science, law, economics or public administration, defense, public order or national security academic profiles).

Awareness could be done also by initial or continuous professional training, in all kinds of socio-economic domains, with the help of local IT industry.

Awareness could be performed through IT Sec, DefCamp, Ethical Hacking-type conferences, that may be organized throughout the country, chiefly in areas where there is a lot of IT hubs or IT startups.

Media has a significant role in any awareness campaign, due to its extended coverage (TV, radio, newspapers), but Internet remains the most preferred vehicle of spreading information.

Last, but not least, any contribution from individual experts, specialists, bloggers, writers or university professors may lead to an increase of the knowledge and awareness of the general or targeted public.

7. One of the latest trends is the use of cloud computing and Internet of Things technology. Are there any security risks?

Any technology comes with a certain risk. The risk could be located in HW or SW, or in the way the individuals use the technology. The technology is developed with the aim of helping people, making for them an easy life. But the reality showed us in

many occasions that every improvement in our lives brings a certain hidden cost. That cost is security or privacy.

Cloud computing makes us happy not worrying about managing large quantities of data without spending large amounts of money on servers, storage capabilities and so on. So, we transfer to others the responsibility of ensuring the confidentiality, integrity and availability of our data. But is that data really safe there? Is our privacy really out of danger? We can only find out when something bad happens. The fact that our data is in other "professional" hands doesn't mean that it cannot be attacked, compromised, leaked, illegally transferred or altered in any way. We just pass the risk for money. Cloud computing does not pose any significant problem from the criminal law point of view. Eventual legal issues are mainly privacy-concerned or civil-type ones.

IoT represents the present and the future of interconnected devices. A new way of life. And a new way of regarding Cybersecurity. The in-security of each connected electronic device contributes to the overall in-security of the system itself. On the other hand, each connected device could be breached, exploited and turned into a Botnet-part Zombie.

Other security issues refers to the possibility of a hacker to get access to one connected device, and then, to all the others, compromising running physical or logic operations or financial or personal information. But the most important one is the risk to privacy and data protection. As far as I know, the European Commission is very concerned about the rise of IoT and stressed the need for a regulation in this field or the creation of relevant standards to meet the security and privacy requirements. It is a lot to be thought about and to be done in the near future.

8. How important is the cooperation for combating the cybercrime phenomenon?

I think it is essential. Almost vital. Cybercrime is not a usual or traditional crime. It is a particular and very complex one. Imagine a Skimming operation, when data from the magnetic strip on the back of victims' credit card is read and copied by fraudulent means (RW head, micro-controller, storage device etc.) at an ATM in a certain country, then transferred by email, P2P or FTP to another country in order to be written on "blank" cards, while the extraction of money from those fake electronic payment instruments takes place in a third country. In this simple case scenario, without international co-operation, law enforcement agencies and prosecutor's offices will be blind and helpless in their effort to bring down the respective financial criminal ring.

Being about combating Cybercrime, the co-operation should bring on the following entities: the victim of the cybercrime (who provides relevant information to the authorities as prime sensor), the police unit (initiating the first measures to get electronic evidence and start investigation), the prosecutor' office (conducting and supervising the criminal procedure, ensuring international co-operation and proper indictment), the electronic communications or network service providers (freezing and making available lots of valuable information related to the attack), court of justice (assessing the case and delivering the final legal solution and the right punishment), experts (providing their valuable IT or legal input), academia (learning from the practical examples and providing IT or legal theoretical expertise), media (sharing the cybercrime-related cases and stories with the aim to raise attention of the public), and IT

Sec industry (learning from every case, assessing technological vulnerabilities, risks and attacks, while providing with new and affordable security tools).

Among all the above mentioned entities, I would personally add a special category: the hacker community. We should not be afraid of it. We should learn from its discoveries and take the good part of its tremendous work in finding and exploiting both human and machine vulnerabilities. Most of the hackers want recognition. Let's give it to them in return to their good effort to identify our weaknesses or limits. Until is not too late…

Interview made by Ioan-Cosmin MIHAI
Vice President of RAISA