Interview with Dr. Laurent CHRZANOVSKI

With a PhD in Roman Archaeology obtained at the University of Lausanne, a Postdoctoral Research Degree in History and Sociology at the Romanian Academy of Sciences, Cluj-Napoca Branch and an EU Habilitation to direct PhDs in History and related sciences, Laurent Chrzanovski is PhD co-director at the doctoral school of the University Lyon II Lumière and regularly holds postdoctoral courses within several major EU Universities; he is also Invited Professor at the Cluj-Napoca and Sibiu Universities as well as at the Polytechnics Universities of Bucharest and Cluj-Napoca. He is the author/editor of 18 books and of more than a hundred scientific articles.

1. In October 2014 you have organized the second edition of the congress "Cybersecurity in Romania". How did this idea come up for this project?

Well, just for the anecdote, the idea is the result of the complementarity within a couple, the willingness to work together when possible and to build together projects that can be interesting for the society we live in. My wife, a computer engineer, runs an NGO very active in the IT field, but also committed to be, as a non-profit organization, useful to the society, while I have experience of huge international congress organization. In plus, we always tried to associate our skills: since 2009, all the exhibitions I organized have a powerful IT value-added - which lead one of them to win the yearly ICOM/UNESCO price for Romania in 2011 - while I try to bring as much culture and interdisciplinary approaches as possible in the activities of the NGO led by my wife.

Analyzing the actual panorama of IT security in Romania, we both thought the best service and innovation we could bring to the Romanian society is to implement a Swiss core concept, vital for any country, meaning a non-profit, non-marketing and non-"technical" public-private dialogue platform, with an international dimension.

With the Swiss Embassy as a warrant of neutrality, we desired to create the ideal premises for private persons, entrepreneurs, IT security firms and State services to dialogue and to network.

The final impulse for this long hoped project was given during a private meeting held in June 2013 with the ITU secretary-general, Dr. Hamadoun I. Touré, who believed that such a dialogue platform in a fast-growing IT country like Romania is vital and deserves to be supported by the ITU, a decision immediately followed by the unconditional support and help given to us by the CERT-RO: that's when the adventure started.

2. Over the last years the number of conferences focused on the topic of information security has increased. What else did you contribute at the conference "Cybersecurity in Romania" with and how did you manage to attract specialists in this field to Sibiu?

All over the world, cybersecurity has become one of the top challenges our societies have to face. This means the number of events dedicated to this topic is in constant growth, both in countries with high economical and geopolitical power and in countries where IT is becoming one of the most dynamic and prosperous sectors, like Poland and Romania.

Nevertheless, in matter of congresses abundance never meant quality. For this precise field, we can observe three separate kinds of useful meetings, made by need or by profit. On the one hand, we find closed-doors congresses, compulsory for a direct dialogue between the State (Army, Security and Law Enforcement Services, National Bank, Lawmakers, Regulators) and IT security providers. On the other hand, we have "trade" meetings and fairs, mostly created to ensure business continuity and networking between IT security companies and the business sector. Last but not least, we witness the dynamism of numerous associative and professional meetings devoted to a special field (f.i. law improvement, academic/technical researches, e-banking security, digital privacy, ethical hacking etc.).

Alas, we also assist, mainly in Bucharest as far as Romania is concerned, to a lot of collateral events with very poor or hidden-branding content but with high media coverage powered by paid advertisements; this phenomenon is justified by the attractiveness of the thematic and by providing to the organizers a source of easy and immediate profit. But those meetings are only happenings, created by event-making firms among a range of other activities, which have no connection at all with security or even with IT.

We hence aimed to create a basic yet often neglected concept, as it is not a source of profit or of immediate results, even if vital for a society.

As a matter of fact, a neutral dialogue platform including all important decision makers and actors (from users to solution providers and to national authorities) can be done only if you are really sure that you will commit yourself to manage it yearly, no matter of its economic results for your NGO, and hence accepting eventual losses and a huge part of the organization made on a voluntary base, at least until you reach a "cruise altitude".

To be successful, any multilateral dialogue means the fulfillment of many compulsory parameters.

First, it needs to be accepted - not in words, but in facts, i.e. by massive presence at the event - by all the country's authorities in the field (CERT-RO, Intelligence Services, Police, Justice, Internal Affairs, External Affairs, Communications, Administration, Regulators etc.).

Second, the IT security companies have to be convinced to accept to come at a meeting where they will hardly gain more than a slightly enhanced network, by accepting not to deliver marketing-oriented speeches.

Third, and this is probably our own specificity and the *conditio sine qua non* to make all the above mentioned possible and perennial, to be able to ensure the more neutral and innovative platform possible. This point can be achieved only through soft

diplomacy and by bringing at the congress as many experts from abroad, may they be State representatives or independent analysts and scholars, which are not resellers of a particular company or group.

I think this point, together with the precedent ones, has been the key of our attractiveness for international experts, as several of them were hungry to come in Romania but were waiting for the most interesting occasion to make the step. Their presence, in the same time, convinced several Romanian private actors, that this congress was a quite unique opportunity to meet hardly reachable personalities and had not to be missed.

Last but not least, once such a platform is created, it needs to find its public among the business actors who are not specialists in IT. As they are not per force fully aware about the digital world trends and dangers, they are hence, often, not convinced about the utility of spending two days in such a congress.

This primordial element means *in sine*, as we mentioned, a long-term strategy and a lot of perseverance, trying to be better year after year according to the French proverb "*avant d'être reconnu, il faut être connu*" (before being recognized, you must be known).

3. This event brought for the first time in Romania a day of pre-conference training for managers with no technical background. How much do you think you could help with risks awareness in the cyber environment the companies are exposed at?

Awareness of decision-makers is the master key of a secure business world. Only if a CEO understands the enormous and immediate danger that threatens himself as a person and of course his company vital interests, he will be able to decide to build or to fund better a specific IT security department and to give to the officer in charge the latitude of choosing the best solutions for the company.

Any attempt to build a safer State without having safer companies is a full *contraditio in terminis* and can only drive a country to face severe economic losses, hence tax losses and employment losses.

The problem to be solved is not so much to convince the CEOs that they have to invest in IT security. It is to make them aware that they have to know the basics to be able to decide how to invest, without being hostages of resellers. A learned CEO can understand that some of the most expensive solutions may often be the worst choices for his company, when the most basic human rules about the technological use and its fragmentation inside the company's office and data storages can save up to eighty percent of an IT budget. If associated with hiring a good security officer, those "common sense" measures can reduce the potential attacks to the complex, tailor-suited, individually targeted ones, which fortunately are still very rare among the "constellation" of possible economic or personal digital attacks.

Our training day was a very fist attempt, with some highly appreciated trainings and some less "easy" ones, depending on how the speaker was or not acquainted with the delivery of a speech fitting to a very heterogeneous public made by businessmen and administrators with very different skills and expectations. It showed our wish to offer, in *première* to Romanian decision-makers, the core elements of the two-days training, which is already compulsory in several EU countries for the decisional staff of companies presenting high risk of attacks or generating high yearly profit.

4. The conference was organized as an event of public-private dialogue in cybersecurity. Do you think that an effective cooperation will be possible between public authorities and business environment in cybersecurity?

As in many post-socialist countries, some security institutions like the army maintained or a high rate of appreciation among the people or succeeded to regain it - for instance, in Romania, the SRI -, while other ones - we could quote the Prosecutor office - still suffer of an exaggeratedly negative reputation, mainly created by the tabloid "image" drawn in the populist media.

This climate justified why a small Romanian-Swiss NGO of 5 employees succeed to build the bases of a platform which, in many countries, is set up since years by the most neutral State actor. In Switzerland, for instance, the Federal Ministry of Finances is the warrant of MELANI, which is the Reporting and Analysis Center for Information Assurance ensuring the dialogue between the police forces, the secret services, the IT providers and the private economy representatives.

Our two first attempts - I am still not speaking about our congress as a consolidated platform, for that we'll need to celebrate at least its 10th anniversary - have shown that, far from the media clichés, the Romanian Law enforcement institutions and the IT security authorities are not only extremely competent, but they are willing to communicate with the business sector and with the civil society, the single condition being that the platform guarantees them that no useless provocations will be made besides the freedom of speech within the Chatham house rule, which is granted to any participant.

Moreover, it has been the occasion for several non-IT Romanian participants to discover the excellence of their country's State actors. They saw how the CERT-RO - even if insufficiently equipped in men and means by wrong political decisions - is given as an example of good practices by the whole EU CERTs and by the ITU.

They learned that the SRI is already in permanent contact and is making a great job with all companies which are classified under the "critical infrastructure group", i.e. energy, banks, communications etc., but also companies which are sufficiently big that a successful cyber-attack provoking their failure or a foreign hostile OPA would severely hit the whole Romanian society. They realized that Romania has also one of the most capable European cybersecurity Department within the National Police, not to speak that the DIICOT prosecutor for cybercrime has the record of EU and International consecutive awards as "*best prosecutor of the year*" in her field.

The willingness of State officers to be available for questions, which faced somehow a 'cautious' silence in the meeting rooms - but not at the coffee breaks - during the first congress, was only an old souvenir this year. Entrepreneurs and companies, during the workshops, dialogued actively with the numerous State officers without complex and without trying to sell something from their side or receiving waffle answers from the other side.

Greatly helped by the presence of State officers from Switzerland, 9 EU countries plus 5 non-EU neighboring countries, the easing we saw in the 2014 discussions and during the informal dinners, concerning all the parts, showed clearly that the answer to your question is YES and that the cooperation which started at Sibiu could be extended to real regular topic-focused meetings - which will no more depend of us - but confirm that our role of facilitator starts to bring its fruits.

5. We become increasingly dependent on computing devices that are interconnected via Internet. There are many advantages of using these devices, but also many risks in cyber environment. Are you concerned about this dependence in terms of information security?

As a humanist and a researcher, I feel sometimes we are all living our lives since ten years as if it was every day the "All Fool's day". I am neither a blind nor a reactionary, and I always saluted the benefits that reasonably used technological advances can bring to humanity.

Today I feel lost, because we are no more speaking about progress. We buy immature, risky if not already fissured, devices or software. And no producer desires to work anymore on these products, as his focus is to launch new ones with even more functions, all of them poorly tested, as soon as possible not to lose his market share, without any State regulation.

This is not even technology, it is nonsense generated by pure marketing and, in a certain sense, an abuse of the client's trust associated with the creation of a constant client desire to be equipped with the latest product. It is like if car manufacturers would be allowed to sell new models without fulfilling all the prior compulsory series of performance, road stability and crash-test compliances.

My main obsession is that I cannot see any advantage but only a lot of existing troubles, and much more to come, by mixing every kind of technologies and interactivities into a single device with which we can virtually access any data we want.

For the first time ever, a - quite naive - man or woman can have all his/her life (private, public, professional, social and financial) stocked in a small little unsecured smartphone. For the rational man I am, metaphorically, this is the final accomplishment of Pandora's box, ready to be opened by anyone, more than a human desire made reality by a sort of Genius of the Lamp.

Dependence to technology existed since mankind invented the first tools, and of course we'll never come back to the typing machine, but my point remains that a phone is a phone, a laptop is a laptop, a scanner is a scanner, a printer is a printer and if I want to switch on the lights of my dining room or lower the temperature of my fridge I will always use a commuter and not my smartphone.

The most disturbing fact for me is that we have been left without options: the strategies of the multinational companies, with the complicity of all government bodies, tailored a new world where we can no more choose to live offline.

If we think that more than ninety percent of the people, paradoxically, are even not aware of the risks that this forced *digitalization of their ego* represents for their own person - not even speaking about their employer or firm - in fields like cyberstalking, spying, burglary etc. is something terrorizing.

The apex of the absurd is reached if we consider that EU laws, which are completely outdated by the digital era, are even not clear on the semantic (and orthographic) definition even of the worlds to use - cybercrime, cyber-attack, cyberwar, cybersecurity, not even to mention the utopic idea of 'digital privacy' - in the very time when the tsunami of NFC and Internet of things with their immense galaxy of potential risks is already overwhelming our present and immediate future...

It is the first time in history when, most of the times, a criminal knows more than a policeman who knows more than a judge, not to speak about politicians, who, in their

majority, simply do not consider this is as being an issue, while their very mission, as our representatives, is to give the input for creating laws, according budgets, elaborating strategic plans.

Politics in Europe seem to wake up only when it is too late, when major geopolitical scandals explode - like the fact that Snowden revelations proved to be true - but also have the common tendency to make sure everything comes back into a silent, sleeping phase once the public emotion is lower.

Finally, the compulsory and compulsive dependence of technologies - resulting even in smartphone addict *detoxification cures* which are more expensive than drug or alcohol cures - is a total unconscious littering of two basic principles of the citizen/human/freethinker/master of his creations and of his choices.

On the one hand, we walk with both feet on Pico della Mirandola's "*discourse on the dignity of man*", the founding text of the Renaissance after centuries of dark age, emphasizing the rights of every human in his quest of knowledge and freedom. Who even remembers this discourse existed and which was his impact on our societies, our laws and our politics until the end of the Cold War?

On the other hand, the IT&C producers, deliberately, decided not to respect anyone of Isaac Asimov's three principles also known as *Laws of Robotics*. Comparatively, it is like if doctors refused to take the oath of Hippocrates and considered their patient's body as their own property.

The 'robots', which we are using now - from smartphones and laptops to software and apps -, were never designed to serve their owner and his interests only, besides helping him to live better and never turning against him. On the contrary, most of the freeware apps, softs and networks - accepted by ignorance or by fashion by most of us - are the most striking contradiction with Asimov's laws as they are mainly used for somebody else's interests against the user's ones.

6. Lately, the number of cyber-attacks has increased in Romania. How do you think these attacks will evolve next years?

They will certainly intensify. Romania has passed the point of no return in terms of positive evolution of many hundreds of companies, which are vulnerable, as their economic growth was in general not coupled with new IT security discipline and measures. They are now together with their western EU counterparts, the targets of two major threats.

The first is merely and basically financial. As we know, Romanians are extremely skilled in IT, and, besides all the youth who have found their way in all the world's best IT companies or in smaller firms, we witness now the second generation of teenagers proving that they are among the very best hackers in the world. Some are just wishing, by their "exploits", to be noticed and directly hired at a top level in company, while others are just "competing" to see if they are smarter than the IT security architecture of a firm.

A few of them, alas, hired together with foreign hackers, enter organized criminal organizations. If until recently, for these organizations, it was more profitable, let's say, to rob the credit card numbers of rich American citizens, it has become now easier and much more interesting play "at home" and to steal the whole vital databases of a profitable local company or to blackmail his careless CEO.

The second, more dangerous, is economic and strategic spying. A lot of Romanian firms, above all in IT but also in other domains, are no more subcontractors for big international companies but started their own "success stories" with their original products, inventions, manpower and know-how.

When witnessing the boom of IT firms in Romania and Poland, which are definitely seen as the EU's future (and sake) in this geostrategic domain, we can only be scared if we compare the way the Polish government, helped by private firms, raised the security awareness of the country's companies, while a lot of companies in Romania do not know even that the CERT-RO exists or who should they alert in the very moment their security officer is unable to stop a frontal attack.

Finally, the war in Ukraine and the Islamic State progression opened Aeolus' cavern, from which the wild winds of any kind of hacktivity, malware, cybercrime are now overflowing on the globe, the enormous majority of them having absolutely nothing to see with Ukraine or with the Middle East conflicts.

As an historical eyewink, it can be seen a revenge of the "good old *Realpolitik*" against the "*virtual politic*". Any major geopolitical crisis always had global impacts but it will, from now on, open the doors to a worldwide wave of digital crimes. Most European States are prepared to face that. Most of European companies, not.

7. Swiss Webacademy represented the core of this conference. This Association offers training for specialists in web programming. Have you thought to train specialists in computer security? If the answer is yes, how much could this conference help you?

It is more than a thought. It is a wish that will become reality at the beginning of 2015. We realized that even if it is in conformity with academic or labor standards, the role of Swiss Webacademy's web trainings is to give young men and women a complete toolkit to enter the professional market.

For us, it seemed bizarre since the beginning, and really absurd in the times we are living in, to train web designers, web programmers and web experts without offering them at least a basic info about the IT security trends. It is like giving a driving license to people who conducted only a brand new perfectly equipped car in bright sunny days and on brand new roads, and then letting them drive an old Dacia during a foggy day on a winter country road full of holes and covered of ice and snow.

We will also start an up-to-date awareness-raising training for the general public, adapted to the local wages, and for the companies. But we will go no further, as there are training centers and institutions, which are specialized in IT security trainings, which propose excellent technical buildings. We must stay humble, recognize our limits, and see where we can be useful, as an NGO.

The conference will certainly help us to gather information for our students in programming the courses for our students, to see which are the particularities of the "e-threats" in Romania year after year, with specialists from the public and from the private sector, and also to see who among those specialists would agree to make a short presentation (real or digital) for our students. But, we will never, ever, use the conference for self-promotion. It would be a betrayal of the very principle on which we decided to create it.

8. Could you reveal some points of interest of the next edition of "Cybersecurity in Romania" Conference?

We draw precious lessons of the feedback forms we received from speakers and participants at the 2014 edition. To be short, the 2015 edition is already planned for the week 21-26 of September and will be co-organized as in 2014 with our partners, Security Brokers and Agora Group. We will focus exclusively on the quality, even if we have to make a harder selection of the speakers. We have no intention to make the conference bigger as it has been in 2014.

We planned longer slots for the speakers, zero-tolerance for marketing papers, and we hope to increase again in a significant way the audience - we doubled it between the first and the second edition -, allowing the more people possible to interact with private specialists and State experts. The pre-congress training day is confirmed, but it will be dealt only with 3 independent analyst companies with less theory and immediate basic practice, even for beginners. That means more trainers if we have many participants, but the challenge is worth to be faced.

As in 2014, it will be dealt by some of the most skilled European trainers with the best Romanian experts, making this day a unique country-specific training contrasting with the "universal solutions" - and their subsequent vendor offers - a CEO can get in specialized centers. Answering the very strong demand raised mainly from the speakers, we will organize also a *specialists-only* post-congress day, with State actors, important private security providers and analysts and IT specialists from different companies who desire to take part.

It will allow to go in-depth on some aspects unveiled during the congress, to open new discussions and to consolidate this so important Central European dialogue which could give impressive results if started in such an informal platform where speakers feel at ease.

Logistically, the Swiss Embassy will continue to patronage the event and the ITU, during our post-congress brainstorming held the 2nd of December, confirmed its commitment to give us its full support and technical assistance, allowing us to invite even more specialists from the neighboring countries.

Last but not least, the most important sign of trust and recognition of our work and the objectivity we always try to keep is that since now the SRI and the IGPR joined the CERT-RO and became partners of the event, helping us to invite their foreign counterparts, indicating us some of the hottest topics and assisting us to invite the decision-makers of very large non-IT Romanian companies.

Moreover, their willingness to be present with an increased presence of their specialists, only a few of them being speakers, shows their desire to have more men on the spot to answer any question private companies and citizens could raise, in public sessions as well as in "private coffee breaks".

This is a major step towards confidence and building solid human relation between officers and private managers, as no virtual meeting will ever replace the sincerity of a handshake and the human impressions resulting after a personal discussion.

Interview made by Ioan-Cosmin MIHAI
Vice President of RAISA