Telos PRIMO PIANO SCALA c

MAY 2013 YEAR V NUMBER 5

Scenario number one: Beijing, Autumn 2011. The Third Department of the People's Liberation Army, responsible for cyber surveillance, attacks the Italian information network. Unit 61046 (Europe and the Middle East) violates the Italian university and research network connecting 400 sites including universities, research labs, libraries and specialised clinics. The booty: hundreds of passwords, emails, medical records, scientific studies and teacher's profiles. The FBI analyses the attack and links it to a much bigger operation called *Byzantine foothold*, which has caused serious casualties including the Massachusetts Institute of Technology and the University of California. Scenario number two: Mykolaïv, southern Ukraine, 28-31 December 2011. Using a portable device, a hacker penetrates the National Research Council in Genoa at least six times. Each time he's connected for just over half a second, but manages to send over one million emails, most of them hoaxes, using the NRC server. He succeeds by exploiting servers considered reliable in order to bypass the defences of the victims and steal their passwords, one of the most lucrative activities of the Russian mafia. The NRC network might also have been used to launder money or send confidential messages, even to fundamentalist groups in Chechnya. Scenario number three: Dubai, December 2012, venue of the World Conference on International Telecommunications, participated by the Regulatory Authorities of 193 Countries with the ambitious goal of reforming international telecom rules. The Conference is organised by a UN agency, the International Telecommunication Union (ITU). During the Conference, discussions on the management of crucial internet resources create a chasm between the US-led block, which wants to keep the internet out of the scope of the Treaty, and emerging powers such as China and Russia who want a greater say in the regulation and control of the network. To strengthen censorship, the West claims. But first and foremost, the debate raging in Dubai reflects the new geopolitical dispute: the stakes are the monopoly of the assignment of domain names, run by a public-private partnership (Icann – Internet corporation for assigned names and numbers) which answers directly to the American Department of Trade. Espionage, illicit dealings, terrorism, explicit political confrontation. Scenarios which we thought had ended with the fall of the Berlin Wall and had faded into History. But History never ends, just like the antagonism between world powers never ends, once and for all, in *perpetual peace*. Simply, the protagonists and the tools involved change. There's the feeling that the immaterial nature of information technology has multiplied the potential impact of cyber threat on critical military and civil infrastructures, in other words to our everyday lives. Are Italy and Europe ready to tackle the challenge? It's still early days.

Mariella Palazzolo @Telosaes

Telos is a member of the FIPRA network

CHIESA

THE THREAT OF THE FUTURE? INVISIBLE, BUT ALREADY PRESENT.

> “*We're already in a new era, and we already have a full-blown cyber-iron curtain. Remember what happened at the ITU World Forum in Dubai? where countries either sided with the ICANN or the ITU, de facto siding either on one side or the other of this invisible, but very real curtain. This is a constant, dangerous, and underrated threat.*”

Telos: Until recently, when we talked about a *threat to national security* we referred to kamikaze terrorists who used fanaticism as a substitute for their lack of means or crude solutions. It's devastating to learn that the biggest, current threat to critical military and civil infrastructures is a violation of computer and information security systems. What role will computer espionage play in international relations? Will it be a new, atypical *cold war* weapon between the West and emerging powers?

Raoul Chiesa: That's a very good question. Whether we like it or not we live in a world which depends, almost entirely, on *Information Technology* or sometimes called a *Digital Society*. Without computer systems and communication networks we couldn't do even the simplest of things, like booking a plane ticket or a hotel, getting money from a cash machine, having a scan, travelling on a motorway or in a train. And the situation really gets worse when it comes to power plants, waterworks, air traffic control systems, etc.
Ultimately, today true power lies in information – as I wrote on the screens of the Bank of Italy way back in 1995. Computer espionage is already the new frontier of *Information Warfare*, even if I prefer the term *Information Operations* (Info-Ops), because it gives you a better idea of what we're talking about. Attacks are launched against strategic objectives not to damage them (for example Stuxnet, the first real cyber weapon in history), but to get information about military operations or espionage. We're already in this new era, and we already have a full-blown cyber-iron curtain. Remember what happened at the ITU World Forum in Dubai? where countries either sided with the ICANN or the ITU, *de facto* siding either on one side or the other of this invisible, but very real curtain.

Military espionage, industrial espionage, attacks inspired by ideologies or religion – are these disinterested challenges or simple entertainment… Is it possible to draw a map of cyber crime and its targets? And how serious is this threat to our safety and security?

Cyber crime is the common denominator of several scenarios, motives, and goals. Military and industrial espionage uses the attack techniques and tools of cyber crime, as well as *Spear Phishing* attacks and *Social Engineering* techniques. Then there're the *hacktivists* who instead exploit any simple and publicly well-known weak point. If we're going to talk about cyber crime then we also have to talk about the underground economy which, if we're to believe official figures and the wonderful 2012 report by the Russian "Group IB", invoices something like 12 billion dollars a year; I'm talking about direct income, I mean profit, and this figure is certainly only the tip of the iceberg of a world about which we can only hazard a guess, because it's difficult to know exactly what's the real figure.

Raoul "Nobody" Chiesa was born in Turin in 1973. In the Eighties and Nineties, he was one of the first hackers in Italy. In 1997 he decided to shift to professional Information Security and founded @Mediaservice.net Srl, a vendor-neutral security advisory company with offices in Turin and Rome. Since 2003 the company – well-known all over Europe - is the Italian Training & Certification Authority for the Institute for Security and Open Methodologies, USA (ISECOM) and OPST, OPSA, OPSE, and OWSE professional certifications. Raoul is a founder member of the Italian Association for Cyber Security and is also a member, amongst others, of the Cyber World working group within the National Security Observatory of the Ministry of Defence. In November 2012 Raoul resigned as director of the company and founded, together with a large group of senior professionals, Security Brokers ScpA, a highly innovative think tank in the high-end world of Information Security Consulting, a *cooperative of cyber experts* with very different and complementary backgrounds. Since 2003 Raoul cooperates with the UN Agency UNICRI, where he works on the Hackers Profiling Project and is currently *Senior Advisor on Cybercrime Issues*. Finally, since 2010 Raoul is a member of the Permanent Stakeholders Group at the European Network & Information Security Agency (ENISA), a mandate that expires in 2015. He has written several books, including *"I sistemi di controllo globale: un'analisi approfondita dei casi Echelon ed Enfopol"* (Apogeo 2000), *"Profiling Hackers"* (Auerbach Publications 2008), and *"11 Settembre 2021"* (Franco Angeli 2012).

We all know what are the main cyber crime services, so I'll list just the main ones: Phishing, Botnet (to launch DDoS attacks), credential theft (your digital identity, like your account on Facebook or Linkedin, as well as your e-banking credentials), carding (credit or debit card theft), e-laundering (online money laundering), gambling unauthorised by Italian authorities (AAMS), again to launder dirty money. And then there're the cash-out techniques to turn the stolen digital information into real cash, the sale of exploits and 0days, electronic espionage, porno sites and paedo-pornography on the internet.

This is a constant, dangerous, and underrated threat. There's no basic culture about cyber crime in Italy. We need to teach people and make them aware, and we should start with the very young, in primary and high schools - the learning sites of native digital Italians, the digital offspring of the Gutenberg generation, as Mariapia Veladiano called them in the newspaper *La Repubblica* a few days ago. Going back to cyber crime, I've just finished editing the Italian edition of the book *Kingpin* recently published in Italy by Hoepli. It's one of the best books ever written on the subject: it reads like a novel and seems like make-believe, but… it's all too true, starting with the criminal network that steals credit cards in the USA and buys the machines to print them in the Far East. It's a book that helps people understand the complexities and global reach of this new phenomenon, and it also tells the (very real) story about the most important digital robbery of the twenty-first century.

Italy has just set up a new organisational model to fight cyber crime; it includes revamping institutional responsibilities and improving cooperation with companies that manage strategic networks. How can a public-private partnership fight this cyber threat and what stones might it find on its path?

This so-called PPP is encouraged and strongly supported by the European Commission; it is also the main focus of the European Network and Information Security Agency (ENISA) - which I belong to as one of the three members of the Permanent Stakeholders' Group (PSG). Working with the private sector is crucial: you fight cyber crime by exchanging information, if possible in real time, because nowadays cyber crime is global, it knows no frontiers and spreads very rapidly. However the decision taken by the Italian Government through the Decree of 24 January 2013 baffles me a little. On the one hand Italy has finally decided to do something, and this is a step in the right direction. On the other, this decree has already been nicknamed by some people *the seat filler*. As usual in Italy it involves creating new agencies, when all we really needed to do was perhaps make better use of what was already in place because Italy has all the experts it needs, but they work in isolation and aren't coordinated. Let's see what'll happen, I'm optimistic.

First as a hacker, and now as a consultant for UNICRI: your life revolves around information security. Can you tell us exactly what your job is about and how UNICRI is helping to develop a global response to this cyber threat?

I'm an outside consultant for UNICRI and my job is to fight cyber crime; together with Francesca Bosco I'm responsible for the Emerging Crimes Unit (ECU). I accepted so long as I could work *pro bono*, just like I do as a PSG at ENISA. When your job is to fight information crime, you have to be driven by your enthusiasm. As you quite rightly say, my whole life is information security. I began to work for UNICRI in 2003 when I was called to teach a Master Course in Law, and I started by teaching about electronic crime. In 2004, I *gifted* the Institute the open source project I was working on with the Institute for Security and Open Methodologies (ISECOM); the project is called HPP, Hacker's Profiling Project.

Although there has been no budget (!) for that project since then, it's still going strong; it's moved on to the *2.0* stage and will hopefully continue, even though there's a chronic lack of funds and sponsors. It's very sad, when you consider that profiling in the world of cyber crime is a completely new science: the whole world envies our project. The books and publications I've written with my colleagues are studied by the FBI Academy in Quantico! Let me give you an idea of what I'm talking about: when an important Department of the Italian Government recently published their assessment on cyber security (what an ugly word!) their categories of hackers, the names of the profiles and even the texts came from our HPP project and our papers: it's a shame that no one credited the UNICRI, or the wonderful work we've been doing for the last 10 years…

Right now in UNICRI we're focusing on the often hidden link between the world of organised crime, cyber crime, hacktivism, the role of Governments, and that of the armed forces and intelligence services. These are captivating, innovative, and fascinating scenarios for our colleagues; we produce results which the whole world envies and which will help to fight new forms of crime. I hope that when a company or an Institution of *good will* reads this interview, or even some visionary (like Steve Jobs), they'll understand and appreciate what we're doing and give us a hand.

Telos PRIMOPIANO SCALA c

Telos Primo Piano Scala *c* - Editor-in-chief: Maria Palazzolo. Publisher: Telos A&S srl Via del Plebiscito 107, 00186 Rome - Reg.: Court of Rome 295/209 of 18 September 2009.
Diffusion: Internet - Protocols - Isp: Eurologon srl. www.telosaes.it - telos@telosaes.it