Security in Cyberspace:
Targeting Nations, Infrastructures, Individuals

25th ISODARCO Winter Course

January 08-15, 2012
Andalo, Trento, Italy

Director of the School:
Carlo Schaerf, University of Rome “Tor Vergata”, Italy

Director of the Course:
Giampiero Giacomello, University of Bologna, Bologna, Italy

The 25th ISODARCO winter course focussed on information technologies and their relation to war and international relations; two previous ISODARCO courses on this topic were held about ten years ago, one in the summer of 1999 and one in the summer of 2002. The 2012 Course had a broad scope, addressing topics such as cyber warfare, cyber terrorism, organized crime, WikiLeaks and privacy and freedom of speech. Over the last ten years a tendency can be observed towards increasing concerns about governance and security of the cyberspace. The entire realm of cyberspace is at risk of being "securitized". A consequence could be that it would be removed from public debate and left into the sole hands of law enforcement agencies and defence and military professionals. The overall goal, as in all ISODARCO courses, was to shed some light on the issues related to the relatively new and complex phenomena of cyberspace, tackle controversial issues and provide a forum for high-level general discussion among participants and speakers alike from a broad range of disciplines.

The course has offered approximately 62 (including lecturers) participants from 12 countries and 3 different continents the opportunity to discuss openly a range of topics related to international cyber security issues.

Fifteen distinguished lecturers and panellists have accepted the invitation and challenge to share their knowledge and views on the above mentioned topics with a highly motivated, multidisciplinary and international audience. Among them were

Alexei Arbatov (Carnegie Moscow Center, Moscow, Russia), Nadezhda (Nadia) Arbatova (Institute of World Economy and International Relations, Moscow, Russia), Ralph Bendrath (Policy Advisor European Parliament, Germany), Chris Bronk (Rice University, USA), Maura Conway (School of Law and Government, Dublin City University, Ireland), Sarah Cook (Freedom House, USA), Sandro Gaycken (Free University of Berlin, Germany), Chunmei Kang (China Academy of Engineering Physics, China), Herbert Lin (US National Research Council, USA), Judith Reppy (Cornell University, USA), Gian Piero Siroli (University of Bologna, Italy), Steve Wright (Leeds University, U.K.).

After a word of welcome to the participants of the ISODARCO course by the Director of the school, the opening address was given by Giampiero Giacomello, the Director of the Course. Ten years after the first ISODARCO courses on cyber security, organised by Gary Chapman

and Diego Latella, there is renewed interest in this topic due to greater risks that developed over that period. Examples are the cyber attacks in which a large number of credit card numbers were stolen and published on the Internet, such as the embarrassing case of the Stratfor private security company in the United States that provides intelligence on security risks, and the Stuxnet Internet `worm' that targeted and physically damaged the Uranium enrichment facilities in Iran. In one of his speeches, President Obama announced cuts to military personnel and the nuclear arsenal in the United States. But he also said the United States will spend more money on intelligence operations and cyber defence, which illustrates that these issues are seen as increasingly important by the current US administration. Governments get increasingly concerned about what may happen if they do not invest in protecting themselves or their country's critical infrastructures from cyber attacks. The awareness of the public about potential risks of cyber attacks seems however not to have increased much over the last 10 years.

As a further introduction to the themes of the course, Dr. Herbert Lin gave an extensive overview of the key terminology and current issues in the area of cyber security. Cyber security is about protection of information and control systems to malicious actors that try to compromise the system by malicious software that is often capable of replicating and distributing itself while remaining undetected. It was noted that in general there is an unbalance between offensive cyber attack capabilities and defensive ones. This is intrinsically so because an offensive operation can be tried many times and needs to succeed only once. Whereas defensive capabilities should be able to capture every attack every time and deter further attacks. A further complication is that cyber attacks can be programmed in such a way that it remains undetected for quite some time and that also the perpetrator cannot be identified.
Cyber attacks usually exploit weaknesses in the software of information systems at several levels. This can be the operating system, software applications, communication protocols and even low level programmable logic circuits used to monitor sensors and actuators of control systems.

The lecture by Dr. Sandro Gaycken identified what cyber network operations are of interest and can be performed from a military point of view. The two principle options are espionage and sabotage. Cyber network operations have become interested for the military because modern society has become increasingly dependent on software-based networked systems. Examples are national critical infrastructures such as the electricity grid, telecommunications networks and transportation, banks, the stock market and so on. However, large-scale dedicated attacks probably require the expertise of many security experts, insider information on technical details of systems and thorough preparation and tests.

In a follow-up lecture, Dr. Lin addressed the ethical issues of cyber warfare. In analogy to the Just War Theory that has been established for real-world (as opposed to cyberspace) wars. The speaker posed several scenarios that raised issues such as the neutrality of countries, civilian immunity, protected entities (such as hospitals), all in the new context of cyber warfare. It became soon clear that these issues are very different and complicated to answer in this setting.

Dr. Chris Bronk addressed a different issue. In the Internet there are groups that are getting more and more power due to their deep and distributed knowledge of weaknesses of software

systems on which governments, companies and citizens are dependent. Governments see this as a potential threat and would like to introduce more governance and control of the Internet. The questions raised were what kind of governance of the Internet i.e., what kind of institutions and at what level, would be suitable to guarantee on one hand free speech and access and on the other hand a minimal level of security to all who depend on the Internet.

The next lecture by Prof. Judith Reppy addressed the dual-use aspects of cyber technology by comparing these issues to examples in the realm of traditional dual-use technology such as jet engines and satellites. It was recognised that the traditional policies for dealing with dual-use technology, such as export control, do not apply to cyber technology. There is an increasingly tight entanglement between military and civilian use of the same cyber technology. It was observed that there might be an attempt by governments towards a splitting of the Internet along national borders with the aim to improve national security. On the other hand, there is a strong public support for keeping the Internet an open public space. The discussion also raised the issue of the risks of surveillance and control by police and how cyber space could (mis)used for this.

The risks of cyber terrorism were addressed by Prof. Maura Conway. Based on her analysis she presented several reasons why it is not so likely that terrorists would resort to cyber attacks. The main reasons for this are that terrorists are interested in conveying a violent, spectacular message that can be clearly attributed to them. This is not easy to perform by means of a cyber attack which needs to remain unobserved for some time, and does not easily lead to the kind of real-world violence that terrorists seek if the attack is not combined with other means. Organising such combined attacks is technologically very complex and would require high-level expertise of a considerable number of people. A final factor is that it is hard to prove who really performed the attack. Considering these difficulties, terrorists groups can probably obtain such spectacular violence easier in a traditional way rather than via cyber attacks.
The current status of the level of freedom on the Internet that citizens in different countries have was presented in the lecture by Dr. Sarah Cook. She gave an overview of a recent comparative study on 37 countries and explained the methodology used to perform the comparison. One of the observations made was that an increasing number of governments are regulating or restricting the free flow of information and that this global trend can be seen also in countries with a long democratic tradition.

The third day of lectures started with a detailed presentation of the more technical aspects of one of the most intricate cyber attacks performed recently, the so-called Stuxnet ‘worm’, that was able to create physical damage to the centrifuges of the Uranium enrichment facility in Natanz, Iran. It was shown how this piece of malicious software could spread over the Internet, find the very specialised and targeted controllers that regulate the speed of some specific centrifuges in the facility and take over their control while remaining totally unobserved until it was too late. The main problem is that society has now been built upon widespread standardised software and hardware that have an insufficient level of security. However, increasing the level of security requires an enormous effort and redesign of many systems, which is extremely costly.

The afternoon sessions covered issues concerning the establishment of norms for behaviour in cyber space from a Chinese perspective and the development of policy concerning cyber

crime and cyber security in the European parliament. The situation in China for what concerns cyber security was further discussed in a lecture on the following day. Various cases that have been covered in the Western media during 2011 have been analysed. The official position of the Chinese government is that it is firmly against cybercrimes and hacking, and that it will do everything in its power to prevent it. However, circumstantial evidence has been been found of state-originated activities of intercepting Internet communications of activists and shutting down and censorship of personal web-pages.

The case of WikiLeaks publication of a very large number of diplomatic cable messages was discussed by Prof. Judith Reppy. The case raised a number of questions about the importance of secure communication channels to successful diplomacy and the need for transparency on governmental operations. An example of the latter has been shown in a documentary on an academic analysis of the WikiLeaks messages in which a systematic search allowed for a much more accurate count of the number of civil casualties of the war in Iraq. These data confirms unofficial counts provided by other non-governmental sources. The afternoon of the fifth day was closed by Prof. Steve Wright, who introduced a remarkable documentary-movie, produced by British BBC, on the impact of social networks (such as Facebook, Twitter and others) on the so-called “Arab Spring”, followed by a general discussion on that crucial, and still open, issue.

The last day the course concluded with a roundtable discussion on what are the most important issues to be addressed concerning ``guarding the Internet'' to find the best balance between the Internet as a public good for information and communication and a sufficient level of security for its users.

The 25th winter ISODARCO closed with a brief session to evaluate the course, soliciting opinions from the participants and ideas and preferences for themes of future courses. Many participants appreciated that ISODARCO has returned to core issues of *cyberspace* and that it included a number of more technically oriented talks.

Students and lecturers attending the course enjoyed the informal atmosphere in which the lectures and discussions took place and the unique format of the course, with much time dedicated to debate and space for spontaneous activities such as PhD-sessions, presentation of films and reflections on current issues of concern.

In conclusion, this course has covered a variety of pressing topics concerning security in *cyberspace* and implications thereof, especially as far as human rights and fundamental freedoms.
As in previous years, the lively and well-informed participation of the international audience in the discussion following each lecture and in the roundtable sessions formed a invaluable contribution to the unique atmosphere in which these delicate topics could be openly discussed among students and professionals from so many different countries and disciplines.

The 2012 ISODARCO Winter course has been organized in cooperation with USPID (Unione degli Scienziati Per Il Disarmo ONLUS).

Mieke Massink