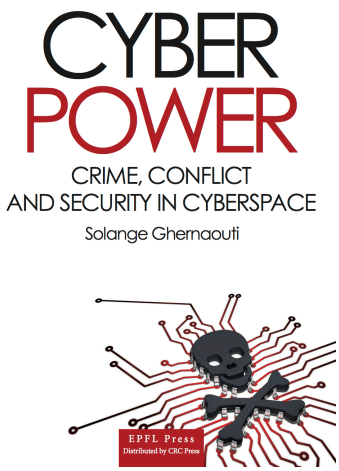
Prof. S. Ghernaouti, May 17, 2013.
ICT Discovery Museum.
First Anniversary Celebrations. ITU, Geneva.



Dear Mister General Secretary, Dear Excellences,
Dear Ladies and Gentlemen, dear friends,

It is great pleasure to be with you in this particular day, in these specific premises, to celebrate both the first anniversary of the ICT Discovery Museum and also the World Telecommunication and Information Society day.

This event is an original way of celebrating this global day of telecommunications and of the information society, a way of recognising the evolution of a society driven by information technologies, and a way of noting the changes caused by technological mutations; but above all of demonstrating our willingness to accompany these changes in the best of manners, and even, if we may dare to hope, contribute towards influencing them.

Our society has become complex, reliant on information and communication technologies.

Multiple stakes and new risks have arisen from their massive adoption in every vital domain, such as for example health, transport, energy, the economy, finance and defence.

We owe it to ourselves to prepare the women and men of today and of tomorrow to be able to grasp the complexity of the world in which we live.

We owe it to ourselves to help them to manage cyber-risks, in order to benefit the maximum possible from the outstanding opportunities that information technologies are bringing.

Information and communication technologies offer new opportunities as much for individual development as for economic development, but also, unfortunately, for the development of criminality.

The news never stops reminding us of the distortions, the abusive or criminal uses of digital technologies. It is individuals, including children, as well as institutions and states that are the victims of these, and it is thus society, at a national and international level, that bears the consequences.

As a result, we need to make available to a large public the knowledge necessary for understanding and managing the technological opportunities and the fundamental and global problems linked to cyberspace.

It is this in this spirit, and drawing on the same reasons why I am a university professor and that motivate my professional life, namely continuous learning, always understanding better, and sharing knowledge and making it fruitful, that I have written the book that is being presented today.

This book is the result of my long experience of teaching and research, and also of contributing to international dialogue on questions of cybersecurity and the struggle against cybercriminality.

It would certainly not have been the same work, had I not had the opportunity to contribute to the work of the ITU, notably the ITU projects for development, through the creation of a guide to cybersecurity for countries in development, and also the work in respect of the Global Cybersecurity Agenda and of the global strategic report.

I would therefore like to thank the whole of the ITU, and in particular Mr Touré and Mr Ntoko, to name only the first two people I met at the start of my contacts with the ITU during the preparatory phases of the World Summit on the Information Society, and who gave me their trust.

I would also like to thank The Federal Office of Communications of Switzerland (OFCOM) for its support during all these years and my editors mister Olivier Babel and mister Frederick Fenter.

This book, “Cyberpower, crime conflict and security in cyberspace”, recently published by the EPFL Press, is intended to contribute to the debate in society that has been opened by the 2003 global summit to work towards, among others objectives, the awareness and education of everybody in respect of cyber-risks and cybersecurity.

Our points of view, perspectives and approaches on crucial cyber-issues are non-political, non-partisan and non-governmental.

A lot of emphasis is put on the teaching element to propose high-level syntheses and to provide a consistent treatment of various cyber-risk-related domains, from both civil and military perspectives and from private and business perspectives.

Technology is explained in such a way that non-computer oriented people can understand the power of information and communication technologies and how cyberattacks are carried out.

Fundamental principles are explained through an interdisciplinary and transversal approach that reflects the societal, economic, political and technical issues related to the uses and misuses of information and communication technologies.

The book sets out, from a transdisciplinary perspective, the theoretical bases for understanding why the Internet and cyberspace are new economic and military battlefields and how it has changed the both ways in which crimes can be committed and wars waged and the ways in which people, organisations and states can be harassed, influenced and destabilized.

The book explores the cybercriminal ecosystem, explains how cybercriminals operate (for example, their modus operandi, their toolkits, their competences, and why cyberattacks can be effective). It analyses how cyberpower has become the newest means for people and organisations, both legitimate and criminal, to demonstrate their capabilities at national, regional or international levels.

At the same time, it presents some fundamentals of cybercrime investigation and of risk and security management and proposes a functional overview of the main cybersecurity measures to be put in place to protect digital assets and infrastructures.

It also raises questions, and proposes some approaches and key factors of success, in respect of controlling the misuse of ICT in order to be able to produce more stability and security in cyberspace and in real life.

It identifies the main challenges related to political, economical, legal and technological issues with which we are confronted today and have to face urgently.

It gives copious practical and real-life examples of instances of cybercriminality and cyber-conflicts and of the efforts being made to combat these. It also provides a number of questions at the end of each chapter to challenge the reader to consider the significance and impact of what they have read.

To conclude, during the last century, it was common to hear the admiring expression “You can’t stop progress!”

Far from trying to stop it, or to turn things back, which would be both a heresy and counter-productive, we do have today the duty and the responsibility to ask ourselves how we can influence technological progress, including cybersecurity, in a positive way, in respect of the growing and determinant impacts of the application of technology to society, on humans, on our environment, on security, and on peace.

It is impossible to address the questions of criminality, security and peace without considering the notion of justice. In this respect the statement by the former US prosecutor Benjamin B. Ferencz occurs to me: "There can be no peace without justice, no justice without law and no meaningful law without a Court to decide what is just and lawful under any given circumstances". This also applies to cyberspace and I hope that this work will help develop the knowledge and the instruments that will contribute to a little more stability and justice in cyberspace and in the physical world.

Thank you for your attention.

Professor s. Ghernaouti, University of Lausanne
Director of the Swiss Cybersecurity Advisory & Research Group
Member of the Swiss Academy of Engineering Sciences