Geneva Internet Platform

# Cybersecurity: What we (may not) know we (do not) know

## *An overview of the cybersecurity challenge*

By Eduardo Gelbstein

### INTRODUCTION

The Internet has become a critical component of our society and yet, it is surprising how little we know about and how little we are doing about some of its aspects, in particular cybersecurity.

This background paper is an attempt to look into what we (can and do) measure in cybersecurity and how useful that is, and then to map what we know we know about cybersecurity, what we know we don't know, and identify some elements that we may not know we do not know. These notes will be a starting point for the midday discussion at the Geneva Internet Platform on 28 October 2014: Please join us on this journey towards reducing the unknowns in cybersecurity.

Computers, data networks, and data communications have been around for a long time. All levels of society (government, business, academia, individuals) have become irreversibly dependent on them. Appendix 1 illustrates some of the key events decade by decade.

After all this time, however, we still struggle with the fundamental issues of protecting against software designed to deliberately interfere with computer systems and networks (malware) and many other activities that arose because these technologies allow them. Such malware affects the availablity of information and can also result in unauthorised disclosure and modification.

At the same time we have no appropriate legislation that defines such acts as a 'crime' or provides enforcement mechanisms. Such legislation lags behind the various threats by several years, and risks being incomplete and outdated by the time it emerges.

### WHY DOES IT MATTER?

*If you can measure that of which you speak and can express it by a number, you know something of your subject. But if you cannot measure it, your knowledge is meagre and unsatisfactory*
Lord Kelvin,
mathematical physicist and engineer
(1824-1907)

Cybersecurity is probably one piece of the Internet governance (IG) puzzle in which there are some clear trends towards measurements – such as of the volume and effects of threats,

or the scope of investments in both attacks and defence. Some of the evidences may make us raise our eyebrows and possibly become more aware of why this all matters; rarely, however, do we know how and which of these to use in the right context.

A number of companies engaged in the cybersecurity field continuously report on emerging threats. Kaspersky, a leader in anti-virus software, reported about 315 000 new malicious files detected every day during 2013 (compared to about 200 000 in 2012), and an average of over 4.5 million attacks on users every day when they were online. Other records, like those of Arbor Networks, report almost 3000 distributed denial-of-service (DDoS) attacks per day worldwide, dominantly targeting the enterprise and commerce sectors, much less so the public sector.

While not attempting to provide an exhaustive list of the impact of attacks on computer systems and networks it is worth taking note of some elements of evidence.

In 2012, General Keith Alexander, Director of the US National Security Agency stated: 'The ongoing cyber-thefts from the networks of public and private organizations, including Fortune 500 companies, represent the greatest transfer of wealth in human history.'

While the estimates of the global cost of cybercrime vary widely, *Bloomberg Business Week* in June 2014 assessed this at more than US$400 billion. The cost of data centre downtime (the time a system cannot be accessed or used) depends on the business sector served by the data centre. It is estimated that the average data centre outage costs US$50 000 an hour. This could be many times more in critical sectors, such as electricity generation or investment banking, and would bring with it business and social disruption.

The financial loss (productivity and revenue loss) arising from a potential country-scale attack on information infrastructures – similar to what happened to Estonia in 2007 – is estimated to range from over US$10 million per day for a small developing country, to over US$500 million per day for a developed economy like Switzerland. With unproven emergency response systems, the damage could last for days or weeks, raising these costs almost dramatically.

The cost of data breaches in which data are stolen consists of two components: the legal costs of having to notify the parties affected, which are in the order of US$250 per record (some attacks involve millions of records) and, in addition, the commercial value of the stolen data which may consist of intellectual property valued in hundreds of millions of US dollars.

The situation is highly unsymmetrical as the attackers only require a modest investment in technology and many attack tools are readily available free of charge or for a modest sum on an informal (and hidden) market for them. For instance, a moderate distributed denial-of-service (DDoS) attack can be ordered for below US$100, while a comprehensive system that can shut down an entire country can be composed for less than US$10 000.

On the other hand, investments in cybersecurity made by companies and institutions are rather modest. A recent report by the Gartner Group on IT security spending per employee in 2013 indicates that most industries – from insurance and utilities to banking and retail – spend less than the price of a cup of coffee (US$2.50) per employee per day!

Yet the impact (not counting reputational loss) of cyber-breaches, when they happen, can amount to billions of US dollars in, for example, the banking sector. Some governments invest large sums; for example the US Department of Defence projects that its cybersecurity budget will reach US$15 billion by 2018. There is limited information on other countries' cybersecurity budgets.

Many aspects of cybersecurity are not easily measurable. While we can quantify availability by measuring downtime and can estimate the cost of downtime, it is harder to quantify the loss of confidentiality (unauthorised disclosure) or the loss of integrity (unauthorised change) of data. This raises several questions, amongst them:

- How can we use evidence emerging from investigations (forensic and law enforcement) to quantify the effectiveness of cybersecurity measures?
- Can we quantify the effectiveness of potential preventive measures (e.g. the Return on Security Investments)?
- Can we measure or predict the effects of legislation and security policies not just on cybersecurity but also on the economy and on civil liberties?
- Can we measure the extent of political awareness and readiness, intentions and trends through the text-mining of speeches and policy documents?
- Are we sufficiently conscious that there are unpredictable cybersecurity events (known as 'black swan' events)?
- Given that we can collect a huge number of metrics, what do we need to do to put them in the right context?

## WHAT ARE THE CAUSES OF OUR CONCERNS AND POSSIBLE REMEDIES??

Why do we continue to have a problem with protecting information? Let's consider the main reasons:

### *1. Imperfect technologies*

A typical device today (corporate computer or network component, personal computer, smart phone, tablet, etc.) is remarkably complex and contains components from multiple sources: the digital circuits (chips) it uses to process and store data, the operating system software, the applications software (Apps in today's jargon). None of these components can be guaranteed to be free of errors; in fact the opposite is true and vendors continually issue updates to resolve known errors.

Can we expect this to change in the foreseeable future?

**Perhaps:** Given that commercial interests are driven by competition and time to market, products are sold with questionable assurances about their quality and the vendors give, at best, a limited warranty and, at worst, accept no liability for the consequences of any malfunction.

Should the role and accountabilities or liabilities of vendors and service providers for the quality of their products and the consequences of the vulnerabilities they contain be considered?. What else would you consider or recommend?

### *2. Incomplete or imperfect information management processes*

Whether in the corporate environment, small business or at home, technologies require a certain amount of management to keep them working properly. This management takes the form of processes.

Some may be very simple and are carried out regularly, such as charging your smart phone to ensure that it can be used as and when required. Other processes are more complex and require knowledge and time. Examples of the simpler processes include backing up data to a separate and secured device and ensuring product updates are installed. Complex processes range from the classification of information into public, restricted, or confidential, ensuring any changes to systems or technology are properly tested before making them available to their users, business continuity plans, etc.

There are many sources of process descriptions including the Information Technology Infrastructure Library (ITIL), the Control Objectives for Information Technology (COBIT), several standards such as the ISO27000 family from the International Standards Organisation, the SP800 series from the USA's National Institute for Science and Technology and many more. A short list of key sources can be found in Appendix 2 – this list should be considered as a short entry point to the subject.

The challenge facing everyone is that implementing all the processes relating to computer and network planning and operations, software, data, and project management is a major task requiring an appropriate number of people who have the knowledge and experience to do so, the time required for these ac-

tivities, and the budget to acquire equipment, diagnostic tools, training, advice, independent validation (in the form of audits), certification, etc.

These are rarely forthcoming due to their incompatibility with a focus on controlling and minimising expenditures. Surprisingly, while a balance sheet will list assets such as office furniture, data and information are not treated as assets and this makes it hard to calculate a return on investment on information security expenditures.

Can we expect this to change in the foreseeable future?

**Hardly:** It would require a change in corporate culture with regard to the business value of information security and the implications of unauthorised disclosures of sensitive information and/or its modification. In addition to their direct costs, security breaches imply reputational damage, which is even harder to assess.

Even when we know what we should know about cybersecurity, implementing improvements is not easy due to reasons unrelated to technology:

- Should corporations, institutions, organisations, and individuals be accountable or liable for breaches of their systems?
- How can we reconcile the need to share information about breaches with the need to preserve reputation and maintain confidence amongst stakeholders and shareholders?
- How far should entities be required to build better security awareness and build capacity amongst their staff and service providers for improving cybersecurity?

What would you suggest be added to this list?

### 3. *Incomplete or imperfect execution of good practices*

Assuming that the conditions in the two previous sections are met, this leaves us with doing the right thing, the right way, well enough, and this is essentially a human factors issue. The Capability Maturity Model (CMM) originated in the 1990s to define the formality and optimisation of processes (originally the development of software for the US Department of Defense) and it has been adopted in several sets of good practices. The five levels of CMM are:

- *Initial:* The process is undocumented (improvised or chaotic and non-repeatable).
- *Repeatable:* The process is documented sufficiently to allow its steps to be repeated.
- *Defined:* The process is confirmed as a standard business process, and documented in detail.
- *Managed:* The process is quantitatively managed relying on agreed metrics and targets.
- *Optimised:* The process includes continuous review and improvement.

It may sound simple but it isn't – this is a major task when you consider that there are dozens of individual processes to document and track. These activities reflect the practices of the international standard ISO 9000 for Total Quality Management, intended to remove systematic (and therefore repeatable) errors from processes.

Can we expect this to change in the foreseeable future?

**Perhaps** as far as information security is concerned, subject to effective governance of these tasks.

The corporate governance challenge is one of defining what level of cybersecurity is 'good enough' for their activities and then adopting a maturity level target for their processes which, in turn, requires resources to be made available: people, knowledge, and money, and, subsequently validating that the required maturity level has been achieved and can be maintained.

What other suggestions do you have?

### 4. *Insufficient awareness of the issues and self-defence practices*

In the same way that pestilence and disease spread through populations in the past due

to lack of knowledge of how these propagate, poor personal hygiene and inadequate medicines to practice antisepsis and cure disease, malicious software and poor digital hygiene contribute to making it easier to become a victim of attacks on the information security both in the corporate and personal worlds.

More recently, attackers have concentrated on human factors by applying social engineering to get individuals to disclose confidential information or give them money.

Can we expect this to change in the foreseeable future?

**Hard to tell:** The human element is the weakest link in the security chain. For as long as people can be made to believe that they have won a major prize in a lottery they did not enter or that an unknown person is willing to give them millions to help them move funds from one country to another, there is little hope. As Albert Einstein said: 'The difference between genius and stupidity is that genius has limits.'

Education, awareness programmes, and briefings may help if they are well designed, if people are motivated to listen, and if they are supported by effective controls to monitor that the lessons are applied.

### *5. Knowledgeable attackers*

People with the knowledge of how to break into computer systems and networks have been around for as long as computers (in fact they were already able to do such things in the mid-1800s when the communications medium was the telegraph).

Their motivation covers a wide spectrum.

- *Fun:* The feeling that they learn in the process, acquire the respect of their peers and also prove how smart they are.
- *Activism* (also referred to as hacktivism): Using someone else's computer systems or networks in support of a cause, closely related to ideology.
- *Fraud:* Obtaining money to which they have no right and therefore benefitting personally from it.
- *Sabotage:* Interfering with or damaging the capabilities to operate computer systems or networks.
- *Disruption:* A form of sabotage consisting of temporarily blocking a computer system or network.
- *Espionage:* Acquiring sensitive or confidential information without permission.
- *Military:* The unconfirmed existence of cyber-armies acting on behalf of a state.
- *Terrorism:* The unconfirmed existence of people acting outside the support of a state - a considerable escalation from hacktivism.

These notes assume that such knowledgeable attackers are well organised, share information with other attackers, know where to procure malicious software, know how to hide, and are highly motivated. Moreover, becoming a knowledgeable attacker requires good mental skills and little investment in technology.

In an ideal situation, people with such skills whose motivation is not destructive should be encouraged to assist in strengthening cybersecurity. The issue is how do you tell them apart from the 'bad guys'?

Can we expect this to change in the foreseeable future?

**No, not for now.** For as long as the Internet is an unregulated environment that does not require any form of proof of identity, has no boundaries and unclear jurisdictions, finding and successfully prosecuting such attackers is not a practical proposition.

For example in May 2014, the FBI issued a notice for the intended arrest of five Chinese officials accused of conspiracy to commit fraud and other charges. It is most unlikely that anything will happen. Similarly, in October 2012, the US government failed, after a long legal battle, to secure the extradition of a British hacker, Gary McKinnon, accused of having perpetrated 'the biggest military computer hack of all time'.

Finally, these attackers seem to have an easier time dealing with administrative issues in order to procure equipment, travel, and com-

ply with internal policies and regulations than those accountable for defending the corporate world. And this will certainly not change.

Open to discussion:

- What can be done to build effective international cooperation against cybercrime groups, such as harmonised legislation, treaties, capacity building?
- How can political will to address these issues be built (and by whom)?
- Should there be measures to encourage knowledgeable attackers not motivated by ideological or political beliefs to help to improve cybersecurity?

## CONCLUDING REMARKS

The current situation with regard to cybersecurity needs improvement because there is so much at stake. Everyone has a role to play in cybersecurity and we may be dealing with a Wicked Problem (Appendix 3).

Individuals should improve their personal digital hygiene and being prudent in their actions in cyber space and protecting their identity, their personal data, what they disclose online, and much more.

Organisations relying on information systems and networks should take good care of their data, systems, networks, external connections, supply chains, etc. This can be supported by adopting the many standards and good practices already available and ensuring that things are done as well as they should be, recognising that this may require resources beyond those already made available.

Governments should provide appropriate legislation and the means to enforce it, focus on the cyber defence of critical infrastructures, national defence and law enforcement, as well as their investigative capabilities. There may also be a role in enhancing education in cybersecurity at all levels.

At international level there is a good case for strengthening the existing mechanisms for sharing intelligence on cyber-attacks, for a framework for cyber peace, treaties, and mutual assistance, and whatever steps are appropriate to avoid a new MAD: Mutually Assured Disruption.

Recognising that some aspects of cybersecurity may not be quantifiable, many measurements used in their right context can be used as evidence to support policy-making. What we need to do now is discuss more thoroughly which measurements make sense and how to use this data.

# Appendix 1.

## Key events by decade

| | |
|---|---|
| The 1960s | Migration from analogue to digital, emergence of digital integrated circuits; IBM 360 series of mainframes; minicomputers from many vendors; SCADA is used in industrial control; proliferation of programming languages (ALGOL, COBOL, FORTRAN, BASIC and more). |
| The 1970s | Transaction processing becomes the norm; early cellular data communications and optical fibre networks; Internet e-mail and early personal computers; BASIC becomes widespread. |
| The 1980s | First 16-bit PCs; Local Area Networks enter the corporate world; packaged software for office applications becomes available from several vendors; malicious software (malware) appears. Firewall products on offer; Data Protection legislation is introduced in the UK. |
| The 1990s | Client-Server claims 'the mainframe is dead'; Graphical User Interfaces become ubiquitous; executive awareness of the critical dependence on IS/IT; Internet access makes its way into enterprises; Web 1.0 grows explosively; pioneers enter e-commerce; European Data Protection and HIPAA legislation are enacted; Y2K becomes a concern. |
| The 2000s | Technology users become proficient; malware becomes 'professional'; social networks popularity gives rise to corporate issues. Mobile technologies transformed by smartphones and tablets; Bring Your Own Device (BYOD) and mobile Apps become an enterprise issue. Risk based audits are widely adopted. |
| The 2010s | Cloud computing; Big Data; concerns about the theft of intellectual property; threats to individual privacy and the militarisation of cyber space; the Internet of Things. Standards and guidelines for good practices in information security and its governance cover many thousands of pages and are constantly updated. |
| Beyond | Who knows? Make the right guess, invest, and you could become very rich... |

# Appendix 2:

## Recent literature on cybersecurity, risk reduction, good practices and audit

### GOVERNMENT AND INTERNATIONAL ORGANISATIONS PUBLICATIONS

- Framework for improving critical infrastructure cybersecurity, 2014, National Institute for Science and Technology, USA, http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf
- ISSAI 1550 (The International Standards of Supreme Audit Institutions), The audit of disaster risk reduction (2012), http://www.intosaiksc.org/default_a.php?syn=2&e=0
- National cybersecurity framework manual, 2012, NATO, https://www.ccdcoe.org/369.html
- Senator Jean-Marie Bockel, Rapport d'Information on cyber defense, (2012). Web site: http://www.senat.fr/notice-rapport/2011/r11-681-notice.html
- US Government Accountability office: Cybersecurity guidance is available but more can be done to promote its use, GAO 12-92, (2011). Web site: http://www.gao.gov/assets/590/587529.pdf (Note that the GAO has many other related publications)
- NIST SP800 series, National Institute for Science and Technology, USA, Special Publications series 800 dedicated to information security http://csrc.nist.gov/publications/PubsSPs.html
- Protecting Critical Infrastructure in the EU, Task Force Report, by Bernhard Hammerli and Andrea Renda, Centre for European Policy Studies, Brussels, 2010, Web site http://www.ceps.eu/ceps/download/4061

### NON-GOVERNMENTAL FRAMEWORKS AND GOOD PRACTICE GUIDELINES

- OCTAVE – Operationally Critical Threat, Asset, and Vulnerability Evaluation, methodology and tools,
- http://www.cert.org/resilience/products-services/octave/octave-method.cfm
- COBIT 5 – including publications covering information security and information risk, 2013 and 2014, Information Systems Audit and Control Association www.isaca.org

(affiliated with the Information Technology Governance Institute (www.itgi.org))

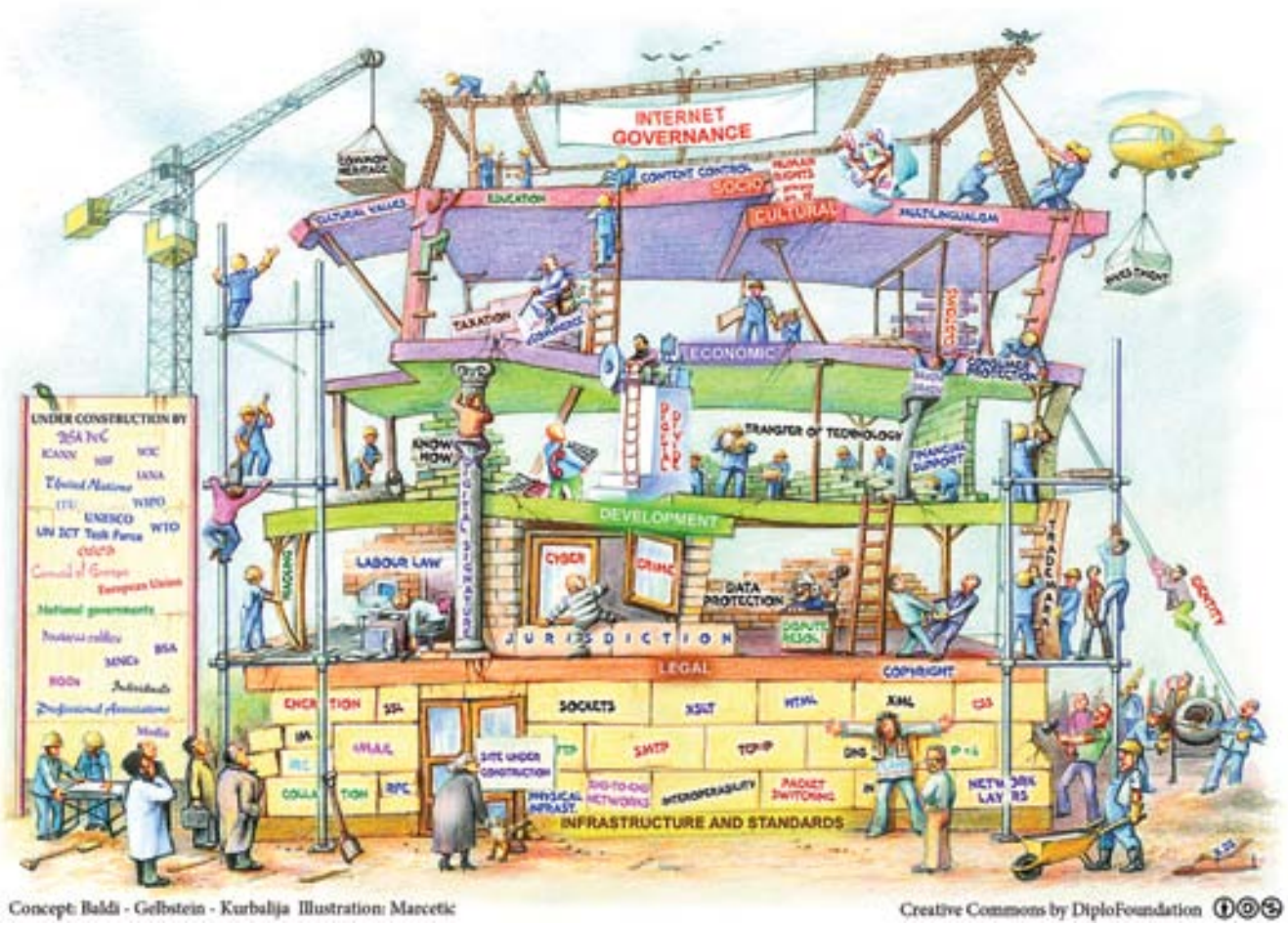
- Transforming cybersecurity using COBIT 5, 2014, www.isaca.org
- Information Technology Infrastructure Library - www.itil-officialsite.com/
- ISO 27000 family - The Management of Information Security, www.iso.org

## BOOKS AND SELECTED ARTICLES


- Security Critical Infrastructures and Critical Control Systems, IGI Global, 2012
- James P. Farwell, Stuxnet and the future of cyber-war, *Survival Journal,* (2011) Web site http://www.tandfonline.com/doi/abs/10.1080/00396338.2011.555586
- NSA snooping was only the beginning. Meet the spy chief leading us into cyber war, *Wired* magazine, June 2013

# Appendix 3:

## Is Internet governance a Wicket Problem?




This picture, inspired by the construction of the Tower of Babel: the Book of Genesis (11.7) says: 'Let's go down and there confuse their language, so that they will not understand one another's speech.'

With so many parties involved (engineers, economists, lawyers, politicians, businesses, academia, the military, etc.) each with their own language (jargon), the potential for misunderstandings and confusion is there.

The term 'wicked problem' emerged in the early 1970s to describe problems that are difficult or impossible to solve because of incomplete, contradictory, and changing requirements that are hard to recognise. The word 'wicked' is used to mean resistance to resolution. The essence of such problems is as follows:

1. So complex that they defy a complete description
2. An optimal state cannot be defined
3. Cause and effect are not obvious – too many non-linear variables and delays
4. Attempts to find a solution are made with incomplete information
5. Every solution requires choices to be made between imperfect options
6. Every solution has unintended consequences and becomes a new problem
7. Solutions can only emerge through collaboration
8. Wicked problems are never solved, they are only transformed

# Appendix 4:
## About Eduardo Gelbstein

Appendix 4: About Eduardo Gelbstein

Ed is a Senior Fellow of the Diplo Foundation (since 2002) and his career in Information Systems and Technology spans over 50 years. He holds a doctorate from the UK, a Master's degree from the Netherlands, and an Engineering degree from Argentina.

He is a regular speaker at international conferences and the author of many articles and several books. In the last few years he has also run workshops and courses on various aspects of the governance and management of information systems for the United Nations in New York and for several organisations around the world.

His past professional activities include:

- 2002 to 2009: Advisor to the United Nations Board of Auditors and to the Cour des Comptes de France (National Audit Office of France).
- 2001 to 2004: Member of the Information and Communications Task Force set up by the UN Secretary General, Kofi Annan.
- 1993 to 2002: Director, United Nations, International Computing Centre, a service organisation providing services to most of the United Nations System organisations.
- 1991 to 1993: Information Technology Strategy Manager, British Railways (prior to privatisation).
- From 1963 to 1990: other activities, including technology transfer, consultancy and the management of major projects in the private and public sectors.

### JOURNAL ARTICLES AND BLOGS

*The Journal of the Information Systems Audit and Control Association* has published several articles written by Ed and he has been invited to write the regular column on information systems audit basics.

He contributes to the information security analogies blog at www.theanalogiesproject.org and to the British Telecom *Let's talk Security* blog at letstalk.globalservices.bt.com/en/security

### SHORT BIBLIOGRAPHY


- *Good Digital Hygiene: a Guide to Staying Secure in Cyberspace,* 2013, www.bookboon.com

- *Information Security for Non-technical Managers,* 2013, www.bookboon.com
- *Securing Critical Infrastructures and Critical Control Systems,* 2013 (author of Chapter 11), 2013, IGI Global
- *Law, Policy and Technology: Cyber-terrorism, cyber-war and digital immobilisation* (co-author and co-editor), 2012, IGI Global
- *Internet Governance* (1st edition), co-author with Jovan Kurbalija, 2005, DiploFoundation
- *Information Society Library,* DiploFoundation (a collection of booklets on Internet, security and online learning) co-authored with Jovan Kurbalija and Stefano Baldi, 2003, DiploFoundation
- *Information Insecurity,* 2002, United Nations Information and Communications Technology Task Force